DZIENNIK URZĘDOWY

Głównego Inspektoratu Transportu Drogowego

Warszawa, dnia 31 sierpnia 2023 r.

Poz. 17

Z A R Z Ą D Z E N I E N R 1 7 / 2 0 2 3

G Ł Ó W N E G O I N S P E K T O R A T R A N S P O R T U D R O G O W E G O

z dnia 30 sierpnia 2023 r.

w sprawie wprowadzenia Systemu Zarządzania Bezpieczeństwem Informacji w Głównym Inspektoracie Transportu Drogowego

Na podstawie art. 13 ust. 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2023 r. poz. 57, 1123 i 1234) w związku z § 20 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247), art. 24 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), art. 32 ust. 3 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2023 r. poz. 1206), art. 21-25 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913) oraz art. 52 ust. 1 ustawy z dnia 6 września 2001 r. o transporcie drogowym (Dz. U. z 2022 r. poz. 2201 z późn. zm.[1)]) zarządza się, co następuje:

§ 1. 1. W Głównym Inspektoracie Transportu Drogowego, zwanym dalej: GITD, ustanawia się, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali System Zarządzania

---

1) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2023 r. poz. 760, 919, 1123, 1193, 1195 i 1523.

Bezpieczeństwem Informacji, zwany dalej: SZBI, zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

2. SZBI odnosi się do ochrony informacji we wszystkich procesach, w których informacje są przetwarzane, w szczególności ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji.

3. Kierujący komórkami organizacyjnymi odpowiadają za wdrożenie i przestrzeganie SZBI w podległych sobie komórkach organizacyjnych.

4. Podstawową dokumentację SZBI stanowi załącznik do zarządzenia.

5. Załącznik do zarządzenia nr 43/2019 Głównego Inspektora Transportu Drogowego z dnia 19 września 2019 r. w sprawie wprowadzenia Systemu Zarządzania Bezpieczeństwem Informacji w Głównym Inspektoracie Transportu Drogowego (Dz. Urz. GITD z 2019 r. poz. 44, z 2020 r. poz. 1, 17 i 25 oraz z 2021 r. poz. 39) może być stosowany w odniesieniu do umów i porozumień zawartych w okresie jego obowiązywania, do czasu ich ustania.

§ 2. Traci moc zarządzenie nr 43/2019 Głównego Inspektora Transportu Drogowego z dnia 19 września 2019 r. w sprawie wprowadzenia Systemu Zarządzania Bezpieczeństwem Informacji w Głównym Inspektoracie Transportu Drogowego (Dz. Urz. GITD z 2019 r. poz. 44, z 2020 r. poz. 1, 17 i 25 oraz z 2021 r. poz. 39).

§ 3. Powołuje się Dariusza Boguckiego na Pełnomocnika do spraw bezpieczeństwa informacji, o którym mowa w Polityce Bezpieczeństwa Informacji Głównego Inspektoratu Transportu Drogowego, stanowiącej załącznik do zarządzenia.

§ 4. Powołuje się Dariusza Boguckiego na Pełnomocnika do spraw bezpieczeństwa cyberprzestrzeni w Głównym Inspektoracie Transportu Drogowego, o którym mowa w Polityce Bezpieczeństwa Informacji Głównego Inspektoratu Transportu Drogowego, stanowiącej załącznik do zarządzenia.

§ 5. Zarządzenie wchodzi w życie z dniem ogłoszenia.

Główny Inspektor Transportu Drogowego: *A. Gajadhur*

Załącznik do zarządzenia
nr 17/2023 Głównego Inspektora
Transportu Drogowego z dnia 30
sierpnia 2023 r. (poz. 17)

Polityka Bezpieczeństwa Informacji Głównego Inspektoratu Transportu Drogowego

Część I: System Zarządzania Bezpieczeństwem Informacji

Rozdział 1

[Wprowadzenie]

§ 1. 1. Polityka Bezpieczeństwa Informacji Głównego Inspektoratu Transportu Drogowego określa wymagania oraz zasady dotyczące bezpieczeństwa informacji, które mają zapewnić odpowiedni poziom tego bezpieczeństwa w Głównym Inspektoracie Transportu Drogowego, zwanym dalej „Inspektoratem”, ze szczególnym uwzględnieniem systemów informatycznych objętych zakresem stosowania polityki.

2. Polityka Bezpieczeństwa Informacji określa:

1) cel stosowania polityki;
2) zakres stosowania polityki;
3) strukturę polityki;
4) zgodność z przepisami, normami i standardami;
5) zasady dotyczące odstępstw i wyjątków od polityki;
6) kontekst systemu zarządzania bezpieczeństwem informacji;
7) interesariuszy oraz ich wymagania w zakresie bezpieczeństwa informacji;
8) zakres działania systemu zarządzania bezpieczeństwem informacji objętego polityką;
9) przywództwo, zaangażowanie i odpowiedzialność Kierownictwa za bezpieczeństwo informacji oraz ustanowienie niniejszej polityki;
10) role organizacyjne, zakresy odpowiedzialności i uprawnienia;
11) proces zarządzania ryzykiem dla bezpieczeństwa informacji;
12) cele bezpieczeństwa informacji i przypisuje je osobom oraz funkcjom;
13) metody komunikowania i aktualizowania celów bezpieczeństwa;

14) szczegółowe wytyczne do planów realizacji celów bezpieczeństwa;
15) odpowiedzialność w zakresie zapewnienia zasobów;
16) proces zapewnienia kompetencji w zakresie bezpieczeństwa informacji;
17) proces zapewnienia świadomości w zakresie bezpieczeństwa informacji;
18) proces komunikacji wewnętrznej i zewnętrznej dotyczącej bezpieczeństwa informacji;
19) proces i zasady nadzorowania informacji;
20) tryb i sposób wdrożenia i funkcjonowania polityki;
21) proces i metody monitorowania, pomiaru, analizy i oceny wyników działań na rzecz bezpieczeństwa informacji;
22) zasady prowadzenia audytów wewnętrznych w celu oceny zgodności systemu zarządzania bezpieczeństwem informacji;
23) proces prowadzenia okresowych przeglądów systemu zarządzania bezpieczeństwem informacji;
24) zasady postępowania z niezgodnościami operacyjnymi, błędami i incydentami bezpieczeństwa informacji oraz zasady realizacji działań korygujących i odpowiedzialność za ich realizację;
25) zobowiązanie do ciągłego doskonalenia przydatności, adekwatności i skuteczności systemu zarządzania bezpieczeństwem informacji.

§ 2. 1. Główny Inspektor Transportu Drogowego ustanawia niniejszą Politykę Bezpieczeństwa Informacji Głównego Inspektoratu Transportu Drogowego i zobowiązuje do jej stosowania i przestrzegania jej zapisów wszystkie strony uczestniczące w przetwarzaniu informacji, których jest właścicielem (w tym administratorem danych lub podmiotem przetwarzającym) oraz strony mające wpływ na bezpieczeństwo tych informacji.

2. Główny Inspektor Transportu Drogowego zapewnia, że planowanie, wdrożenie, utrzymywanie i ciągłe doskonalenie systemu zarządzania bezpieczeństwem informacji będzie realizowane zgodnie z wymaganiami prawnymi oraz określonymi w niniejszej polityce, normami i standardami z zakresu bezpieczeństwa informacji.

§ 3. 1. Użyte w niniejszym dokumencie pojęcia, skróty i definicje oznaczają:
1) administrator danych – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; administratorem danych przetwarzanych w Inspektoracie jest Główny Inspektor;

2) Administrator Merytoryczny Systemu (AMS) – odpowiedzialny za realizację zadań określonych w PBI oraz dokumentacji systemu;
3) Administrator Systemu Informatycznego (ASI) – odpowiedzialny za realizację zadań określonych w PBI oraz dokumentacji systemu;
4) anonimizacja – trwałe i nieodwracalne przekształcenie danych osobowych w sposób uniemożliwiający ich przyporządkowanie do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
5) BDG – Biuro Dyrektora Generalnego;
6) BDG – WDZ – Biuro Dyrektora Generalnego Wydział Doskonalenia Zawodowego;
7) BDG – WKR – Biuro Dyrektora Generalnego Wydział Kadr i Rekrutacji;
8) BT – Biuro Teleinformatyki;
9) CMDB, baza konfiguracji – (ang. Configuration Management Database) rejestr urządzeń teleinformatycznych i oprogramowania, zawierający informacje dotyczące sprzętu i oprogramowania służącego do przetwarzania informacji, obejmujący ich rodzaj i konfigurację oraz relacje między sobą i użytkownikami;
10) CSIRT – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego;
11) CSIRT GOV – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego;
12) cyberbezpieczeństwo – odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy;
13) dane osobowe – wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania bezpośrednio lub pośrednio osobie fizycznej („osobie, której dane dotyczą”), takie jak: imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
14) DG – Dyrektor Generalny;
15) dostępność – zapewnienie terminowego i niezawodnego dostępu i możliwości wykorzystania informacji (utrata dostępności oznacza zaburzenie dostępu lub możliwości wykorzystania informacji lub systemu informacyjnego);
16) Główny Inspektor – Główny Inspektor Transportu Drogowego;

17) incydent, naruszenie – zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo, bezpieczeństwo informacji, ochronę danych osobowych;
18) incydent krytyczny – incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy CSIRT;
19) incydent w podmiocie publicznym – incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny;
20) Inspektorat – Główny Inspektorat Transportu Drogowego;
21) IOD – Inspektor Ochrony Danych;
22) integralność – ochrona przed niewłaściwą modyfikacją lub zniszczeniem informacji, w tym zapewnienie niezaprzeczalności i autentyczności informacji (utrata integralności oznacza nieuprawnioną modyfikację lub zniszczenie informacji);
23) Kierownictwo – Główny Inspektor, Zastępcy Głównego Inspektora oraz Dyrektor Generalny;
24) naruszenie ochrony danych osobowych – naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
25) NSC – Narodowe Standardy Cyberbezpieczeństwa, zbiór rekomendacji standaryzujących rozwiązania zabezpieczające w sieciach i systemach informacyjnych wykorzystywanych przez podmioty chcące efektywnie zarządzać systemami bezpieczeństwa informacji, NSC realizują interwencję 2.1 celu szczegółowego 2 Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024 w zakresie opracowania i wdrożenia Narodowych Standardów Cyberbezpieczeństwa;
26) obsługa incydentu – czynności umożliwiające wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację, podejmowanie działań naprawczych i ograniczenie skutków incydentu;
27) podatność – właściwość np. systemu informacyjnego, która może być wykorzystana przez zagrożenie np. cyberbezpieczeństwa;
28) podmiot przetwarzający – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe na zlecenie administratora; w praktyce

przetwarzanie danych przez ten podmiot sprowadza się do wykonywania czynności usługowych na rzecz administratora danych;

29) poufność – zapewnienie stosowania zatwierdzonych ograniczeń w zakresie ujawniania i dostępu do informacji, w tym środków ochrony prywatności i informacji osobistych (utrata poufności oznacza nieuprawnione ujawnienie informacji);
30) ryzyko – kombinacja prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji;
31) PBFiŚ – Polityka Bezpieczeństwa Fizycznego i Środowiskowego;
32) PBI – Polityka Bezpieczeństwa Informacji;
33) PBO – Polityka Bezpieczeństwa Osobowego;
34) PBT – Polityka Bezpieczeństwa Teleinformatycznego;
35) PCD – Plan Ciągłości Działania;
36) PODO – Polityka Ochrony Danych Osobowych;
37) POIN – Plan Ochrony Informacji Niejawnych;
38) przetwarzanie – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
39) pseudonimizacja – przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
40) PZI – Polityka Zarządzania Incydentami;
41) PZK – Plan Zarządzania Kryzysowego;
42) pracownik – pracownik Inspektoratu zatrudniony na podstawie każdej dopuszczalnej formy zatrudnienia, oraz osoby realizujące m. in. staż, praktyki, wolontariat;
43) PUODO – Prezes Urzędu Ochrony Danych Osobowych;
44) RODO – rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia

dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.);

45) RPO – (ang. Recovery Point Objective) maksymalna ilość danych – mierzona czasem – która może zostać utracona po przywróceniu działania po katastrofie, awarii lub porównywalnym zdarzeniu, zanim utrata danych przekroczy poziom akceptowalny;

46) RTO – (ang. Recovery Time Objective) maksymalny akceptowalny czas na przywrócenie działania systemu i odzyskanie dostępu do danych po nieplanowanej przerwie np. katastrofie, awarii lub porównywalnym zdarzeniu;

47) system – system informacyjny, system wspierający;

48) system informacyjny – system, o którym mowa w ustawie o informatyzacji działalności podmiotów realizujących zadania publiczne wraz z przetwarzanymi w nim danymi w postaci elektronicznej; system, który wykonuje jasno określone funkcje, dla którego istnieją łatwe do zidentyfikowania względy bezpieczeństwa i potrzeby (np. elektroniczny system transferu środków, system kadrowo – finansowy – system w którym prowadzona jest ewidencja lub rejestr określone w ustawie); system może obejmować wiele pojedynczych programów i sprzętu, oprogramowania i komponentów telekomunikacyjnych, komponenty te mogą być pojedynczą aplikacją lub kombinacją sprzętu – oprogramowania ukierunkowaną na wspieranie określonej funkcji związanej z działalnością Inspektoratu. System informacyjny może również składać się z wielu pojedynczych aplikacji, jeśli wszystkie dotyczą jednej funkcji z zakresu działalności Inspektoratu (np. listy płac pracowników). Właścicielami systemów informacyjnych są kierujący komórkami organizacyjnymi, o których mowa w § 15, 18-21, oraz 23-25 zarządzenia nr 26/2020 Głównego Inspektora Transportu Drogowego z dnia 2 lipca 2020 r. w sprawie nadania regulaminu organizacyjnego Głównemu Inspektoratowi Transportu Drogowego (Dz. Urz. GITD z 2022 r. poz. 5 i 22 oraz z 2023 r. poz. 2);

49) system wspierający – połączony zestaw zasobów informacyjnych pod tym samym bezpośrednim zarządzaniem, który ma wspólną funkcjonalność; zwykle obejmuje sprzęt, oprogramowanie, informacje, dane, aplikacje, komunikację, udogodnienia i ludzi oraz zapewnia wsparcie dla różnych użytkowników lub systemów albo aplikacji; właścicielami systemów wspierających są kierujący komórkami organizacyjnymi, o których mowa w § 15 oraz § 24 zarządzenia Głównego Inspektora Transportu Drogowego z dnia 2 lipca 2020 r. w sprawie nadania regulaminu organizacyjnego Głównemu Inspektoratowi Transportu Drogowego;

50) szacowanie ryzyka – całościowy proces identyfikacji, analizy i oceny ryzyka;
51) SZBI – System Zarządzania Bezpieczeństwem Informacji odnoszący się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji, obejmujący strukturę organizacyjną, polityki, planowane działania, odpowiedzialności, zasady, procedury, procesy i aktywa. W szczególności SZBI obejmuje PBI oraz polityki stanowiące załączniki do niej, dokumentacje systemów, inne polityki, procedury, instrukcje, wytyczne, zalecenia, obowiązujące wewnętrzne akty normatywne i inne odnoszące się bezpośrednio i pośrednio do bezpieczeństwa informacji i cyberbezpieczeństwa. SZBI nie ma formy zamkniętego katalogu i podlega ciągłym zmianom, doskonaleniu i adaptowaniu do potrzeb, celów, strategii, zadań i zmieniającego się otoczenia;
52) UODO – Urząd Ochrony Danych Osobowych;
53) użytkownik – osoba lub proces indywidualny (systemowy) upoważniony do uzyskania dostępu do systemu;
54) WL BP – Wydział Legislacji Biuro Prawne;
55) właściciel informacji – Główny Inspektor posiadający uprawnienia ustawowe, zarządcze i operacyjne w zakresie informacji przetwarzanych w Inspektoracie; rolę właściciela informacji na poziomie zarządczym i operacyjnym realizują kierujący komórkami organizacyjnymi, odpowiedzialnymi za przetwarzanie informacji, w tym danych osobowych, w zakresie wynikającym z zadań określonych w regulaminie organizacyjnym Inspektoratu oraz regulaminach organizacyjnych komórek. Właściciel informacji odpowiada za czynności przetwarzania dla informacji stanowiących dane osobowe;
56) właściciel biznesowy systemu informacyjnego – kierujący komórką organizacyjną, który jest właścicielem danego systemu informacyjnego w całym cyklu jego życia, od momentu planowania, przez pozyskiwanie, eksploatację i rozwój po wycofanie z użycia;
57) właściciel systemu wspierającego – kierujący komórką organizacyjną, który jest właścicielem danego systemu wspierającego w całym cyklu jego życia, od momentu planowania, przez pozyskiwanie, eksploatację i rozwój po wycofanie z użycia;
58) właściciel – właściciel biznesowy systemu informacyjnego, właściciel systemu wspierającego;
59) zagrożenie – potencjalna przyczyna wystąpienia incydentu;

60) zarządzanie incydentem – obsługa incydentu, wyszukiwanie powiązań między incydentami, usuwanie przyczyn wystąpienia incydentu, opracowywanie wniosków wynikających z obsługi incydentu;
61) zarządzanie ryzykiem – skoordynowane działania w odniesieniu do oszacowanego ryzyka;
62) ZPOiOIN GGI – Zespół Przygotowań Obronnych i Ochrony Informacji Niejawnych Gabinet Głównego Inspektora.

§ 4. 1. PBI ma na celu zapewnienie odpowiedniego poziomu bezpieczeństwa informacji poprzez ustanowienie i wdrożenie SZBI.

2. Cele ustanowienia zasad dotyczących zapewnienia bezpieczeństwa informacji:
1) spełnienie wymagań prawnych, to jest obowiązujących przepisów prawa, norm i standardów z zakresu bezpieczeństwa informacji, cyberbezpieczeństwa i ochrony danych osobowych;
2) zapewnienie bezpieczeństwa informacji (poufności, integralności oraz dostępności z uwzględnieniem atrybutów, takich jak: autentyczność, rozliczalność, niezaprzeczalność i niezawodność);
3) zapewnienie ciągłości realizacji zadań publicznych i związanych z nimi procesów biznesowych, w których przetwarzane są informacje wymagające ochrony, w szczególności w systemach informacyjnych;
4) zapewnienie ciągłości działania zasobów niezbędnych do prawidłowego funkcjonowania Inspektoratu.

3. Podstawowe zadania służące realizacji celów określonych w ust. 2:
1) regularne przeglądanie i aktualizowanie środków ochrony ustanowionych w PBI w przypadku zidentyfikowania potrzeby, w tym w związku z wynikami szacowania ryzyka i oceny skutków dla ochrony danych;
2) inwentaryzowanie sprzętu i oprogramowania służącego do przetwarzania informacji w bazie konfiguracji i jej bieżąca aktualizacja;
3) prowadzenie, nie rzadziej niż raz na rok szacowania ryzyka dla bezpieczeństwa informacji przetwarzanych w systemach informacyjnych i podejmowanie działań minimalizujących zidentyfikowane ryzyka, oraz oceny skutków dla ochrony danych, gdy ta jest wymagana;
4) przetwarzanie przez wszystkie osoby zaangażowane w proces przetwarzania informacji, w szczególności tych podlegających ochronie prawnej, wyłącznie na podstawie

upoważnienia i przyznanych uprawnień w stopniu adekwatnym do realizowanych zadań i powierzonych obowiązków;

5) zarządzanie uprawnieniami do systemów informacyjnych oraz systemów wspierających, w tym uprzywilejowanymi, oraz niezwłoczna zmiana lub odbieranie uprawnień w sytuacjach tego wymagających;

6) organizowanie udokumentowanych szkoleń z zakresu bezpieczeństwa informacji, cyberbezpieczeństwa oraz ochrony danych osobowych organizowane dla wszystkich pracowników Inspektoratu, w tym jego Kierownictwa;

7) monitorowanie dostępu do informacji w systemach informacyjnych i systemach wspierających oraz podejmowanie czynności zmierzających do wykrycia nieautoryzowanych działań w tych systemach;

8) ustanawianie, wdrażanie i eksploatowanie, a w razie potrzeby dostosowywanie środków ochrony uniemożliwiających nieautoryzowany dostęp do informacji, w tym w systemach informacyjnych oraz systemach wspierających, w szczególności na podstawie wyników szacowania ryzyka i oceny skutków dla ochrony danych;

9) ustanawianie, wdrażanie i eksploatowanie, a w razie potrzeby dostosowywanie zasad bezpieczeństwa informacji, w tym dla pracy zdalnej;

10) stosowanie ustanowionych zasad dotyczących przetwarzania informacji w relacjach z podmiotami zewnętrznymi we wszystkich udokumentowanych relacjach, adekwatnie do zakresu powierzanych tym podmiotom zadań;

11) ustanawianie, wdrażanie i eksploatowanie, a w razie potrzeby dostosowywanie zasad postępowania z informacjami zapewniających minimalizację ryzyka wystąpienia kradzieży informacji i środków przetwarzania informacji;

12) regularne aktualizowanie oprogramowania, w szczególności implementacja poprawek bezpieczeństwa;

13) ustanawianie, wdrażanie i eksploatowanie, a w razie potrzeby dostosowywanie planów ciągłości działania i procedur postępowania w sytuacjach awaryjnych oraz ich testowanie;

14) ustanawianie, wdrażanie i eksploatowanie, a w razie potrzeby dostosowywanie zasad zarządzania podatnościami, w szczególności w systemach informacyjnych oraz systemach wspierających;

15) ustanawianie, wdrażanie i eksploatowanie, a w razie potrzeby dostosowywanie zabezpieczeń przed błędami, utratą oraz nieuprawnioną modyfikacją urządzeń, oprogramowania i informacji;

16) weryfikowanie na zgodność z ustanowionymi i wdrożonymi politykami bezpieczeństwa i wymogami prawnymi systemów informacyjnych oraz systemów wspierających w zakresie, jaki ich dotyczy;
17) niezwłoczne zgłaszanie incydentów bezpieczeństwa informacji, cyberbezpieczeństwa oraz naruszeń ochrony danych osobowych zgodnie z obowiązującymi procedurami;
18) przeprowadzanie okresowych, nie rzadziej niż raz na rok, audytów wewnętrznych w zakresie bezpieczeństwa informacji.

3. Określone w PBI zasady mają zastosowanie do wszystkich informacji przetwarzanych w Inspektoracie oraz dotyczą wszystkich form, w jakich informacje są przetwarzane, z zastrzeżeniem informacji niejawnych w rozumieniu przepisów o ochronie informacji niejawnych, których ochrona jest realizowana w oparciu o właściwe przepisy odrębne i ustanowione oraz wdrożone na ich podstawie odrębne od PBI regulacje wewnętrzne, w szczególności POIN.

4. Zasady zawarte w PBI muszą być stosowane przez wszystkie osoby, które posiadają dostęp do informacji podlegających ochronie na podstawie PBI.

5. Niniejsza PBI musi być znana wszystkim osobom uzyskującym dostęp do informacji podlegających ochronie na jej podstawie, w szczególności:

1) pracownikom;
2) personelowi podmiotów zewnętrznych realizujących usługi, dostawy lub roboty budowlane – w zakresie niezbędnym do realizacji przez te podmioty zadań;
3) wykonawcom ubiegającym się o udzielenie zamówienia publicznego w zakresie, w jakim wykonawcy potrzebują uzyskać dostęp do informacji i zasobów Inspektoratu w celu ubiegania się o udzielenie im zamówienia publicznego;
4) innym, niż wskazane w pkt 2 i 3 stronom zewnętrznym w zakresie, w jakim jest to niezbędne do wykonywania przez te strony zadań, w szczególności wynikających z zawartych umów lub porozumień.

6. PBI ma zastosowanie do wszystkich miejsc i sytuacji, w których informacje podlegające ochronie na podstawie jej zapisów są przetwarzane, w szczególności obiektów, budynków, pomieszczeń, pojazdów, miejsc wykonywania pracy w formie zdalnej oraz innych, w których realizowane są zadania obejmujące przetwarzanie informacji.

7. Wzór oświadczenia o zapoznaniu z wymaganiami i zasadami określonymi w PBI zawiera załącznik nr 1 do PBI.

§ 5. 1. Inspektorat jako podmiot realizujący zadania publiczne określone w przepisach prawa wykorzystuje systemy informacyjne wspierające realizację tych zadań i związanych z nimi procesów biznesowych.

2. Inspektorat jako podmiot publiczny jest zobowiązany do realizacji obowiązków określonych w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913), w związku z tym wymagana jest identyfikacja i utrzymywanie wykazu systemów informacyjnych wspierających realizację zadań publicznych, w przypadku których wystąpienie incydentu:

1) wpływa lub może wpłynąć na obniżenie jakości lub przerwanie ciągłości realizacji zadania publicznego (incydent w podmiocie publicznym);
2) skutkuje znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi (incydent krytyczny).

3. Systemy informacyjne Inspektoratu obejmują systemy wspierające realizację zadań publicznych określonych w przepisach prawa oraz innych zadań Inspektoratu, m.in.:

1) określonych w art. 50 pkt 2, 3, 4 i 5, art. 54 oraz 54d ust. 1 ustawy o transporcie drogowym;
2) związanych z kontrolą uiszczenia opłaty elektronicznej za przejazd po drogach krajowych, na zasadach określonych w ustawie z dnia 21 marca 1985 r. o drogach publicznych (Dz. U. z 2023 r. poz. 645,760 i 1193);
3) związanych z kontrolą przestrzegania przepisów ruchu drogowego przez kierujących pojazdami w zakresie, o którym mowa w art. 129g ust. 1 ustawy z dnia 20 czerwca 1997 r. – Prawo o ruchu drogowym (Dz. U. z 2023 r. poz. 1047 z późn zm.[2)]);
4) związanych ze sprawami kadrowo-finansowymi;
5) związanych z Elektronicznym Zarządzaniem Dokumentacją;
6) związanych z gospodarką mandatową;
7) związanych z obsługą interesantów.

4. Systemy informacyjne Inspektoratu, o których mowa w ust. 3 nie obejmują systemów zewnętrznych wykorzystywanych w Inspektoracie, za których prowadzenie odpowiedzialne są inne podmioty zewnętrzne, które mogą być jednocześnie administratorami danych przetwarzanych w tych systemach zewnętrznych.

[2)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2023 r. poz. 919, 1053, 1088, 1123, 1193, 1234 i 1394.

5. Każdy system informacyjny Inspektoratu posiada jednoznacznie przypisanego właściciela biznesowego, którego odpowiedzialność za zadanie publiczne wspierane przez system informacyjny określa regulamin organizacyjny Inspektoratu oraz regulamin organizacyjny komórki organizacyjnej.

6. Właściciele biznesowi systemów informacyjnych Inspektoratu mają obowiązek przekazać Pełnomocnikowi do spraw bezpieczeństwa cyberprzestrzeni, informacje niezbędne do realizacji przez Inspektorat obowiązków wynikających z ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, oraz zapewnić aktualność tych informacji w przypadku jakiejkolwiek ich zmiany, w tym wycofania systemu informacyjnego z eksploatacji oraz uruchamiania nowego systemu informacyjnego.

7. Informacje, o których mowa w ust. 6 Pełnomocnik do spraw bezpieczeństwa cyberprzestrzeni umieszcza w wykazie systemów, którego minimalny zakres informacyjny określa załącznik nr 1 do PBT.

§ 6. 1. Systemy wspierające obejmują sprzęt, oprogramowanie, informacje, dane, aplikacje, komunikację, udogodnienia i ludzi oraz zapewniają wsparcie i usługi dla pracowników lub systemów lub aplikacji, w tym innych systemów wspierających oraz systemów informacyjnych, o których mowa w § 5.

2. Systemy wspierające obejmują:

1) infrastrukturę teleinformatyczną administrowaną przez BT to jest systemy: usług domenowych, sieci wewnętrznej i komunikacji zewnętrznej, wirtualizacji, kopii zapasowych, monitorowania infrastruktury teleinformatycznej, monitorowania wewnętrznej i zewnętrznej komunikacji, bezpieczeństwa, zasobów plikowych, centralnego wydruku, korelacji zdarzeń, monitoringu środowiskowego serwerowni;
2) systemy i narzędzia dedykowane pracownikom to jest systemy: poczty elektronicznej i komunikacji wewnętrznej, telefonii IP, telekonferencji;
3) system wymiany plików;
4) system monitorowania urządzeń pracowników z obsługą zgłoszeń informatycznych;
5) system obsługi zgłoszeń dla systemów informacyjnych oraz systemów wspierających

– administrowane przez BT, oraz

6) służbowe urządzenia mobilne do transmisji głosowej oraz danych;
7) systemy kontroli dostępu do obszarów i pomieszczeń Inspektoratu;
8) systemy wspierające pracę serwerowni;

9) systemy monitoringu wizyjnego – w zakresie określonym w regulaminie pracy w Inspektoracie

– administrowane i zarządzane przez BDG.

3. Każdy system wspierający funkcjonujący w Inspektoracie posiada jednoznacznie przypisanego właściciela, którego odpowiedzialność za system wspierający określa regulamin organizacyjny Inspektoratu oraz regulamin organizacyjny komórki organizacyjnej.

4. Właściciele systemów wspierających zapewniających wsparcie i usługi dla systemów informacyjnych Inspektoratu, o których mowa w § 5 mają obowiązek przekazać Pełnomocnikowi do spraw bezpieczeństwa cyberprzestrzeni, informacje niezbędne do realizacji przez Inspektorat obowiązków wynikających z ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, oraz zapewnić aktualność tych informacji w przypadku jakiejkolwiek ich zmiany, w tym wycofania systemu wspierającego z eksploatacji oraz uruchamiania nowego systemu wspierającego.

5. Informacje, o których mowa w ust. 4 Pełnomocnik do spraw bezpieczeństwa cyberprzestrzeni umieszcza w wykazie systemów, którego minimalny zakres informacyjny określa załącznik nr 1 do PBT.

Rozdział 2

[Struktura i obszary PBI]

§ 7. 1. PBI składa się z części:

1) **Część I: System Zarządzania Bezpieczeństwem Informacji** – która, opisuje cel i zakres stosowania SZBI, strukturę i obszary SZBI, zakres dokumentacji SZBI oraz stosowanie odstępstw i wyjątków od wymagań określonych SZBI;
2) **Część II: Zarządzanie bezpieczeństwem informacji** – która, opisuje SZBI w zakresie organizacyjno-systemowym, w tym procesy niezbędne do sprawnego planowania, wdrażania, funkcjonowania, zabezpieczania i doskonalenia bezpieczeństwa informacji;
3) **Część III: Zapewnienie bezpieczeństwa informacji** – która opisuje wymagania i zasady ustanowione dla zapewnienia bezpieczeństwa informacji.

2. PBI obejmuje obszary:

1) bezpieczeństwo osobowe;
2) bezpieczeństwo fizyczne i środowiskowe;
3) bezpieczeństwo teleinformatyczne;
4) utrzymanie ciągłości działania;

5) zarządzanie zdarzeniami;
6) ochronę danych osobowych;
7) relacje z podmiotami zewnętrznymi.

§ 8. 1. Celem obszaru bezpieczeństwa osobowego jest zapewnienie bezpieczeństwa informacji poprzez m.in.:

1) zapewnienie, że pracownicy rozumieją swoją odpowiedzialność i posiadają odpowiednią wiedzę i umiejętności umożliwiające właściwe zabezpieczenie informacji przetwarzanych w ramach realizowanych przez nich zadań;
2) zapewnienie, że pracownicy są świadomi swoich obowiązków dotyczących bezpieczeństwa informacji i je wypełniają;
3) zabezpieczenie interesów Inspektoratu, w tym ochronę informacji na każdym etapie zatrudnienia.

2. Wymagania i zasady dotyczące obszaru bezpieczeństwa osobowego określa załącznik nr 2 do PBI.

3. Szczegółowy sposób realizacji bezpieczeństwa osobowego w systemach wskazanych w § 5 i § 6 uwzględniający odstępstwa i wyjątki jeżeli występują, określa dokumentacja tych systemów.

§ 9. 1. Celem obszaru bezpieczeństwa fizycznego i środowiskowego jest zapewnienie bezpieczeństwa informacji poprzez m.in.:

1) stosowanie zabezpieczeń fizycznych obejmujących w szczególności:
   a. wyznaczenie i rozmieszczenie granic stref bezpieczeństwa,
   b. zabezpieczenie wejść do obiektów oraz do stref bezpieczeństwa,
   c. systemy sygnalizacji włamania i napadu,
   d. systemy monitoringu wizyjnego,
   e. systemy elektronicznej kontroli dostępu,
   f. mechaniczne zabezpieczenia obiektów i pomieszczeń,
2) stosowanie zabezpieczeń środowiskowych obejmujących w szczególności:
   a. systemy przeciwpożarowe i gaśnicze,
   b. zabezpieczenia przed zalaniem,
   c. systemy klimatyzacji i wentylacji,
   d. systemy monitorowania warunków temperatury i wilgotności powietrza,
   e. środki ochrony odgromowej,

f. zabezpieczenia przeciwprzepięciowe i przeciwprzeciążeniowe,

g. systemy awaryjnego zasilania;

3) zapewnienie, że kluczowe systemy techniczne i teleinformatyczne są wyposażone w zabezpieczenia utrzymujące optymalne warunki środowiskowe i podtrzymujące zasilanie;

4) zapewnienie bezpieczeństwa okablowania teletechnicznego;

5) stosowanie zabezpieczeń organizacyjnych, w szczególności dotyczących:

a. zasad dostępu do obszarów i pomieszczeń, w tym pomieszczeń serwerowni,

b. zasad organizacji ruchu osób, materiałów i pojazdów,

c. stosowania bezpośredniej ochrony fizycznej.

2. Zakres i forma stosowanych zabezpieczeń fizycznych i środowiskowych muszą wynikać z przeprowadzonego i udokumentowanego procesu szacowania ryzyka dla danego systemu informatycznego lub czynności przetwarzania danych osobowych – wyniki analizy ryzyka są podstawą do określenia zabezpieczeń.

3. Przyjęte do stosowania, na podstawie wyników szacowania ryzyka zabezpieczenia fizyczne i środowiskowe powinny uwzględniać wymagania zewnętrzne wynikające m.in. z zasad i wymagań dotyczących korzystania przez Inspektorat z zewnętrznych rejestrów, ewidencji i systemów oraz sieci teleinformatycznych, zawartych umów i porozumień, w tym takich, w których Główny Inspektor jest podmiotem przetwarzającym dane osobowe w imieniu i na rzecz innego administratora danych.

4. Za wdrażanie zabezpieczeń fizycznych i środowiskowych odpowiedzialne jest BDG, przy współpracy i na podstawie wymagań określonych przez właściciela rozpatrywanego zagadnienia.

5. Opracowanie szczegółowych polityk, procedur i instrukcji w zakresie bezpieczeństwa fizycznego i środowiskowego, w tym elementów planów i procedur w obszarze ciągłości działania zapewniają właściciele, we współpracy z BDG oraz BT – w zakresie dotyczącym serwerowni i innych pomieszczeń, w których eksploatowana jest infrastruktura teleinformatyczna zarządzana przez BT.

6. Wymagania i zasady dotyczące bezpieczeństwa fizycznego i środowiskowego określa załącznik nr 3 do PBI. W zakresie, w jakim obiekty, pomieszczenia i obszary objęte są ochroną na podstawie przepisów o ochronie informacji niejawnych, zastosowanie mają zapisy obowiązującego POIN.

7. Szczegółowy sposób realizacji bezpieczeństwa fizycznego i środowiskowego w systemach wskazanych w § 5 i § 6 uwzględniający odstępstwa i wyjątki jeżeli występują, określa dokumentacja tych systemów.

§ 10. 1. Celem obszaru bezpieczeństwa teleinformatycznego jest zapewnienie bezpieczeństwa informacji poprzez m.in.:

1) prowadzenie i utrzymanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji;
2) zapewnienie aktualizacji oprogramowania;
3) tworzenie i testowanie kopii zapasowych;
4) zarządzanie uprawnieniami użytkowników i administratorów;
5) zapewnienie jednoznacznej identyfikacji i uwierzytelniania wszystkich użytkowników w systemach;
6) stosowanie zasad pozyskiwania, rozwoju i utrzymania systemów, w tym kontroli systemów przed ich dopuszczeniem do produkcyjnego użytkowania, m.in. w zakresie spełniania wymagań bezpieczeństwa;
7) stosowanie i doskonalenie, określonych na etapie szacowania ryzyka wdrożonych zabezpieczeń;
8) właściwe postępowanie z nośnikami informacji w całym cyklu ich życia;
9) zapewnienie konserwacji urządzeń w celu zagwarantowania ich nieprzerwanej i bezawaryjnej pracy (przeglądy i konserwacje);
10) stosowanie mechanizmów kryptograficznych w sposób adekwatny do zagrożeń i wymogów prawnych oraz wymogów wynikających z otoczenia (m.in. integracji z innymi systemami lub używania zewnętrznych rejestrów, ewidencji, systemów i sieci);
11) zapewnienie bezpieczeństwa plików systemowych;
12) zarządzanie podatnościami technicznymi systemów, w tym niezwłoczne podejmowanie działań po dostrzeżeniu podatności technicznych;
13) nadzorowania usług informatycznych dostarczanych przez podmioty zewnętrzne;
14) bieżące monitorowanie systemów i sieci oraz działań użytkowników wykonywanych w tych systemach i sieciach pod kątem wykrywania wszelkich zdarzeń mogących mających lub mogących wpływać na bezpieczeństwo informacji;
15) określenie warunków niezbędnych do zapewnienia bezpieczeństwa informacji przy wykonywaniu pracy poza obiektami, budynkami i pomieszczeniami Inspektoratu, w tym w ramach świadczenia pracy w formie zdalnej.

2. Wymagania i zasady dotyczące obszaru bezpieczeństwa teleinformatycznego określa załącznik nr 4 do PBI.

3. Szczegółowy sposób realizacji bezpieczeństwa teleinformatycznego w systemach wskazanych w § 5 i § 6 uwzględniający odstępstwa i wyjątki jeżeli występują, określa dokumentacja tych systemów.

§ 11. 1. Celem obszaru utrzymania ciągłości działania jest zapewnienie bezpieczeństwa informacji poprzez m.in.:

1) identyfikację krytycznych procesów i określenie środków niezbędnych dla ich funkcjonowania (analiza wpływu na biznes);
2) opracowanie i wdrożenie planów, procedur i instrukcji dotyczących ciągłości działania, reagowania w sytuacjach kryzysowych, oraz w zakresie działań i zasobów niezbędnych do przywrócenia działania;
3) określenie odpowiedzialności związanej z zarządzaniem ciągłością działania oraz wyznaczenie osób odpowiedzialnych za realizację zadań w ramach utrzymania ciągłości działania.

2. Wymagania i zasady dotyczące obszaru utrzymania ciągłości działania określa załącznik nr 5 do PBI.

3. Szczegółowy sposób realizacji utrzymania ciągłości działania w systemach wskazanych w § 5 i § 6 uwzględniający odstępstwa i wyjątki jeżeli występują, określa dokumentacja tych systemów.

§ 12. 1. Celem obszaru zarządzania zdarzeniami jest zapewnienie bezpieczeństwa informacji poprzez m.in.:

1) określenie zasad zgłaszania zdarzeń, które mogą stanowić incydent bezpieczeństwa informacji, incydent cyberbezpieczeństwa lub naruszenie ochrony danych osobowych;
2) określenie zasad dotyczących kategoryzacji i klasyfikacji zdarzeń;
3) określenie zasad dotyczących obsługi zdarzeń;
4) określenie zasad dokumentowania zdarzeń;
5) określenie odpowiedzialności za zgłaszanie oraz obsługę zdarzeń;
6) uwzględnienie obowiązków dotyczących współpracy z CSIRT GOV oraz PUODO, w tym odpowiedzialności i trybów zgłaszania, kategorii zdarzeń podlegających zgłoszeniu i terminów, w jakich zgłoszenia muszą być dokonane.

2. Wymagania i zasady dotyczące obszaru zarządzania zdarzeniami określa załącznik nr 6 do PBI.

3. Szczegółowy sposób zarządzania zdarzeniami w systemach wskazanych w § 5 i § 6 określa dokumentacja tych systemów.

§ 13. 1. Celem obszaru ochrony danych osobowych jest zapewnienie bezpieczeństwa informacji poprzez m.in.:

1) przetwarzanie danych osobowych wyłącznie w prawnie dopuszczalnych oraz uzasadnionych celach;
2) realizację obowiązków informacyjnych związanych z prowadzonym przetwarzaniem danych osobowych;
3) realizację praw osób, których dane osobowe są przetwarzane;
4) stosowanie zasad domyślnej ochrony danych oraz ochrony danych w fazie projektowania;
5) realizację innych obowiązków związanych z przetwarzaniem danych osobowych, do których realizacji administrator danych jest zobowiązany;
6) realizację obowiązków związanych z przetwarzaniem danych osobowych jako podmiot przetwarzający dane osobowe w imieniu innego administratora danych.

2. Wymagania i zasady dotyczące ochrony danych osobowych określa załącznik nr 7 do PBI.

3. Szczegółowy sposób realizacji ochrony danych osobowych w systemach wskazanych w § 5 i § 6 uwzględniający odstępstwa i wyjątki jeżeli występują, określa dokumentacja tych systemów.

§ 14. 1. Celem obszaru relacji z podmiotami zewnętrznymi jest zapewnienie bezpieczeństwa informacji poprzez m.in.:

1) określenie zasad bezpieczeństwa informacji w relacjach ze stronami trzecimi;
2) określenie odpowiedzialności za stosowanie zasad bezpieczeństwa informacji w relacjach ze stronami trzecimi.

2. Wymagania i zasady dotyczące obszaru relacji z podmiotami zewnętrznymi określa załącznik nr 8 do PBI.

3. Szczegółowy sposób realizacji bezpieczeństwa w relacjach z podmiotami zewnętrznymi, w tym będącymi uprawnionymi użytkownikami w systemach wskazanych w § 5 i § 6 uwzględniający odstępstwa i wyjątki jeżeli występują, określa dokumentacja tych systemów.

Rozdział 3

[Zgodność z przepisami, normami i standardami]

§ 15. PBI została opracowana na podstawie przepisów prawa krajowego i międzynarodowego, w oparciu o normy i standardy w obszarze bezpieczeństwa informacji i cyberbezpieczeństwa oraz wewnętrzne regulacje, w szczególności:

1) ustawę z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne;
2) ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;
3) rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (RODO);
4) ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1789);
5) ustawę z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, zwaną dalej „ustawą”;
6) rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych;
7) PN-ISO/IEC 27001 – Technika informatyczna -- Techniki bezpieczeństwa -- Systemy zarządzania bezpieczeństwem informacji -- Wymagania;
8) PN-ISO/IEC 27002 – Technika informatyczna -- Techniki bezpieczeństwa -- Praktyczne zasady zabezpieczania informacji;
9) PN-ISO/IEC 27005 – Technika informatyczna -- Techniki bezpieczeństwa -- Zarządzanie ryzykiem w bezpieczeństwie informacji;
10) PN-EN ISO 22301 – Bezpieczeństwo powszechne -- Systemy zarządzania ciągłością działania -- Wymagania;
11) PN-EN ISO 22313 – Bezpieczeństwo i odporność -- Systemy zarządzania ciągłością działania -- Wytyczne dotyczące stosowania ISO 22301;
12) Narodowe Standardy Cyberbezpieczeństwa[3)];

[3)] https://www.gov.pl/web/baza-wiedzy/narodowe-standardy-cyber

13) Zarządzenie Nr 92 Prezesa Rady Ministrów z dnia 26 października 2012 r. w sprawie nadania statutu Głównemu Inspektoratowi Transportu;
14) Zarządzenie nr 26/2020 Głównego Inspektora Transportu Drogowego z dnia 2 lipca 2020 r. w sprawie nadania regulaminu organizacyjnego Głównemu Inspektoratowi Transportu Drogowego;
15) obowiązujące zarządzenia Dyrektora Generalnego Głównego Inspektoratu Transportu Drogowego w sprawie nadania komórkom organizacyjnym ich regulaminów;
16) obowiązujące zarządzenie Dyrektora Generalnego Głównego Inspektoratu Transportu Drogowego w sprawie wprowadzenia Regulaminu pracy w Głównym Inspektoracie Transportu Drogowego wraz z porozumieniami dotyczącymi zasad wykonywania pracy w Inspektoracie, które zostały zawarte z organizacjami związkowymi;
17) obowiązujący Plan Zarządzania Kryzysowego Głównego Inspektoratu Transportu Drogowego;
18) obowiązujący Plan Ochrony Informacji Niejawnych w Głównym Inspektoracie Transportu Drogowego.

Rozdział 4

[Odstępstwa i wyjątki]

§ 16. 1. PBI stanowi zbiór zdefiniowanych zasad, których celem jest zapewnienie bezpieczeństwa informacji. W szczególnie uzasadnionych przypadkach dopuszczalne jest zastosowanie odstępstw i wyjątków od tych zasad na zasadach określonych w PBI.

2. Odstępstwa i wyjątki od zasad określonych w PBI w systemach wskazanych w § 5 i § 6 jeżeli występują, określa szczegółowo dokumentacja tych systemów.

§ 17. 1. Nadzorowanie odstępstw służy zapewnieniu bezpieczeństwa informacji poprzez formalne uregulowanie czasowych odstąpień od realizacji zdefiniowanych w PBI zasad bezpieczeństwa informacji.

2. Odstępstwo należy rozumieć jako czasowe odstąpienie od ustanowionych i wdrożonych PBI zasad bezpieczeństwa informacji, które możliwie w najkrótszym terminie powinno być wycofane.

3. Odstępstwo podlega obowiązkowemu szacowaniu ryzyka, jak również musi zostać ostatecznie zaakceptowane przez Głównego Inspektora.

4. Odstępstwo może być dopuszczone tylko w wyjątkowych i uzasadnionych sytuacjach.

5. Każde odstępstwo podlega ścisłemu nadzorowi, udokumentowaniu, uprzednim szacowaniu ryzyka, jak również późniejszej ocenie skutków jego dopuszczenia.

6. Pełnomocnik do spraw bezpieczeństwa informacji nadzoruje proces zarządzania odstępstwami, m.in. weryfikuje kompletność wymaganej dokumentacji, przedstawia Głównemu Inspektorowi rekomendacje dotyczące zgłoszonych odstępstw i ocenia skutki ich zastosowania.

7. Wnioskujący o odstępstwo odpowiadają za:

1) opracowanie dokumentacji opisującej m.in. cel i uzasadnienie, zakres, oczekiwany termin i czas trwania odstępstwa, o które wnioskują;
2) przeprowadzenie udokumentowanego szacowania ryzyka w związku z wnioskowanym odstępstwem oceniającego m.in., jakie ryzyka związane z zastosowaniem odstępstwa mogą wystąpić oraz określającego środki ochrony, które mają wystąpieniu tych ryzyk przeciwdziałać.

§ 18. 1. Nadzorowanie wyjątków służy zapewnieniu bezpieczeństwa informacji poprzez formalne uregulowanie jednorazowych wyjątków od stosowania zdefiniowanych zasad bezpieczeństwa informacji.

2. Wyjątek należy rozumieć jako jednorazowe, szczególne odstąpienie od stosowania ustanowionych i wdrożonych PBI zasad bezpieczeństwa informacji.

3. Wyjątek podlega obowiązkowemu szacowaniu ryzyka, jak również musi zostać ostatecznie zaakceptowany przez Głównego Inspektora.

4. Wyjątek może być dopuszczony tylko incydentalnie (sytuacje awaryjne), w sposób przemyślany, ograniczony i uzasadniony.

5. Każdy wyjątek podlega ścisłemu nadzorowi, udokumentowaniu, uprzednim szacowaniu ryzyka, jak również późniejszej ocenie skutków jego dopuszczenia.

6. Pełnomocnik do spraw bezpieczeństwa informacji nadzoruje proces zarządzania wyjątkami, m.in. weryfikuje kompletność wymaganej dokumentacji, przedstawia Głównemu Inspektorowi rekomendacje dotyczące zgłoszonych wyjątków i ocenia skutki ich zastosowania.

7. Wnioskujący o wyjątek odpowiadają za:

1) opracowanie dokumentacji opisującej m.in. cel i uzasadnienie, zakres, oczekiwany termin zastosowania wyjątku, o który wnioskują;
2) przeprowadzenie udokumentowanego szacowania ryzyka w związku z wnioskowanym wyjątkiem oceniającego m.in., jakie ryzyka związane z zastosowaniem wyjątku mogą

wystąpić oraz określającego środki ochrony, które mają wystąpieniu tych ryzyk przeciwdziałać.

Rozdział 5

[Dokumentacja SZBI]

§ 19. 1. PBI wraz z załącznikami jest podstawowym dokumentem SZBI w Inspektoracie, dokumentem najwyższego poziomu w zakresie zasad bezpieczeństwa informacji, który należy uwzględniać przy opracowywaniu dokumentacji, o której mowa w ust. 2.

2. Na dokumentację SZBI w Inspektoracie składają się również dokumenty niższego poziomu, m.in.:

1) polityki, procedury, instrukcje i plany dla systemów wskazanych w § 5 i § 6;
2) dokumentacja ochrony danych osobowych dla czynności przetwarzania, w tym w systemach wskazanych w § 5 i § 6;
3) szczegółowa dokumentacja zabezpieczeń, m.in. dokumentacja powykonawcza dotycząca stosowanych zabezpieczeń fizycznych, technicznych, osobowych i organizacyjnych, w tym dotyczących systemów wskazanych w § 5 i § 6 oraz dokumentacja ochrony danych osobowych;
4) dokumentacja z przeprowadzania szacowania ryzyka oraz ocen skutków dla ochrony danych;
5) regulacje wewnętrzne dotyczące zasad prowadzenia audytów i kontroli w zakresie bezpieczeństwa informacji;
6) dokumentacja przeglądów SZBI;
7) dokumentacja incydentów bezpieczeństwa informacji oraz naruszeń ochrony danych osobowych;
8) dokumentacja szkoleń z zakresu bezpieczeństwa informacji oraz szkoleń z zakresu ochrony danych osobowych;
9) dokumentacja dotycząca upoważnień do przetwarzania określonych grup informacji, związane z nimi oświadczenia, rejestry i ewidencje;
10) wszelkie inne dokumenty, które obejmują swoim zakresem wybrane aspekty bezpieczeństwa informacji, m.in. odrębne wewnętrzne regulacje obowiązujące w Inspektoracie.

3. Dokumentacja systemów, o której mowa w ust. 2 pkt 1-4 powinna obejmować m.in.:

1) sposób i zasady prowadzenia i utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji (CMDB) obejmującej ich rodzaj i konfigurację oraz odpowiedzialność w tym zakresie;
2) raport z przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;
3) sposób i zasady zarządzania uprawnieniami użytkowników w zakresie przydzielania, odbierania i zmiany uprawnień oraz odpowiedzialność w tym zakresie;
4) sposób i zasady zarządzania uprawnieniami uprzywilejowanymi w zakresie przydzielania, odbierania i zmiany uprawnień uprzywilejowanych oraz odpowiedzialność w tym zakresie;
5) środki zapewniające bezpieczeństwo informacji w systemie, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich oraz zasady ich stosowania i odpowiedzialność za ich stosowanie;
6) sposób i zasady monitorowania dostępu do systemu/informacji przetwarzanych w systemie oraz odpowiedzialność w tym zakresie;
7) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji oraz odpowiedzialność za ich wykonywanie;
8) zabezpieczenia uniemożliwiające nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;
9) podstawowe zasady gwarantujące bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość oraz odpowiedzialność za ich stosowanie;
10) zabezpieczenia informacji uniemożliwiające nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie;
11) zasady postępowania z informacjami, zapewniające minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;
12) sposób i zasady aktualizacji oprogramowania oraz odpowiedzialność w tym zakresie;
13) sposób i zasady minimalizowania ryzyka utraty informacji w wyniku zdarzeń niepożądanych oraz odpowiedzialność w tym zakresie;
14) stosowane mechanizmy kryptograficzne oraz odpowiedzialność w tym zakresie;
15) sposób i zasady zapewnienia bezpieczeństwa plików systemowych oraz odpowiedzialność w tym zakresie;

16) sposób i zasady zarządzania podatnościami technicznymi systemów oraz odpowiedzialność w tym zakresie;
17) sposób i zasady kontroli zgodności systemu z odpowiednimi normami i politykami bezpieczeństwa oraz odpowiedzialność w tym zakresie;
18) sposób i zasady zgłaszania incydentów oraz podejmowania działań naprawczych i korygujących, jak również odpowiedzialność w tym zakresie;
19) zasady aktualizacji dokumentacji określonej w pkt 1-18 oraz odpowiedzialność w tym zakresie.

4. Zakres dokumentacji, o której mowa w ust. 3 należy każdorazowo dostosować do warunków i wymagań rozpatrywanego systemu, którego ta dokumentacja ma dotyczyć, w szczególności uwzględniając kategorię przetwarzanych w tym systemie informacji i wymagania prawne z tego wynikające oraz techniczne aspekty jego działania i zastosowane zabezpieczenia.

5. Dokumentacja, o której mowa w ust. 3 powinna być opracowana na etapach planowania, budowy i wdrażania systemu z zastrzeżeniem dokumentacji, której prowadzenie jest możliwe dopiero po jego uruchomieniu, w szczególności dokumentacji wykonywania procedur.

6. Dokumentacja, o której mowa w ust. 3 oraz dobór zabezpieczeń powinny być wykonane z uwzględnieniem wytycznych i zaleceń określonych w PBI oraz przede wszystkim w:

1) PN-ISO/IEC 27001, PN-ISO/IEC 27002, PN-ISO/IEC 27005, PN-EN ISO 22301, PN-EN ISO 22313 i/lub
2) NSC 199, NSC 200, NSC 800–18, NSC 800–30, NSC 800–34, NSC 800–37, NSC 800–39, NSC 800–46, NSC 800–53, NSC 800–53A, NSC 800–53B, NSC 800–53 MAP, NSC 800–60 cz. 1, NSC 800–60 cz. 2, NSC 800–61, NSC 800–82, NSC 800–114, NSC 800–144, NSC 800–207, NSC 800–210, NSC 500–325, NSC 7298.

7. W przypadku stosowania innych lub dodatkowych – ponad określone w PBI – środków ochrony danych osobowych, w szczególności dotyczących sposobów zabezpieczenia tych danych oraz sposobu realizacji wymagań określonych w art. 32 RODO oraz art. 31-32 Ustawy wymagane jest opracowanie dokumentacji opisującej te środki lub sposób realizacji wymagań określonych w art. 32 RODO oraz art. 31-32 ustawy.

§ 20. 1. PBI wraz z załącznikami zatwierdza Główny Inspektor zgodnie z trybem zatwierdzania zarządzeń.

2. PBI jest udostępniona w całości w Dzienniku Urzędowym Inspektoratu i dostępna bez ograniczeń dla wszystkich stron zaangażowanych w przetwarzanie informacji i ich ochronę oraz mających na tą ochronę wpływ.

3. Dokumentacja, o której mowa w § 19 ust. 2 pkt 1-4 oraz 6 – w zakresie przeglądów zarządzania na poziomie operacyjnym jest zatwierdzana przez właścicieli.

4. Udostępnianie dokumentacji, o której mowa w § 19 ust. 2, w szczególności wskazanej w § 19 ust. 2 pkt 1-4 oraz 6 zawierającej opisy stosowanych zabezpieczeń oraz konfiguracje, podlega ograniczeniu dostępu do niej. Dokumentacja taka powinna podlegać ochronie przed nieuprawnionym dostępem do niej, nieuprawnioną i niekontrolowana zmianą lub zniszczeniem lub utratą i nie powinna być udostępniana publicznie. W przypadku konieczności jej udostępnienia szerszemu gronu odbiorców zapisy kluczowe z punktu widzenia zapewnienia bezpieczeństwa informacji należy skutecznie usunąć przed takim udostępnieniem.

5. Dokumentacja, o której mowa w § 19 ust. 2, może być udostępniona w całości lub w części pracownikom lub podmiotom zewnętrznym, w tym realizującym na rzecz Inspektoratu określone zadania i usługi na podstawie zwartych umów lub porozumień lub we współpracy z Inspektoratem, wyłącznie w zakresie koniecznym oraz przy zapewnieniu zachowania jej treści w poufności.

6. Dokumentację należy udostępniać w wersji aktualnej, obowiązującej.

§ 21. 1. Właścicielem PBI jest Pełnomocnik do spraw bezpieczeństwa informacji, który odpowiada za:

1) opracowanie dokumentu;
2) przeglądy i aktualizacje dokumentu, w tym na podstawie analizy potrzeb zmian zgłaszanych przez Kierownictwo, komórki organizacyjne, właścicieli oraz na podstawie zaleceń z kontroli i audytów.

2. Właścicielami dokumentacji, o której mowa w § 19 ust. 2 pkt 1-4 i 6 są właściciele.

3. Właściciele, o których mowa w ust. 2 odpowiadają za:

1) zapewnienie opracowania dokumentacji, o której mowa w § 19 ust. 2;
2) zapewnienie przeglądów i aktualizacji oraz utrzymywania dokumentacji w aktualności;
3) zapewnienie ochrony dokumentacji zawierającej dane i informacje kluczowe z punktu widzenia zapewnienia bezpieczeństwa informacji;
4) zapewnienie określenia szczegółowych zasad zarządzania dokumentacją, w tym wprowadzania do niej zmian;
5) formalne zatwierdzenie dokumentacji i jej aktualizacji.

§ 22. 1. Zgłoszenia uzasadnionych potrzeb dokonania zmian w PBI należy kierować do Pełnomocnika do spraw bezpieczeństwa informacji z wykorzystaniem elektronicznego systemu obiegu dokumentów. Zgłoszenie musi zawierać propozycję nowych zapisów PBI oraz uzasadnienie proponowanej zmiany, a jeżeli zmiana dotyczy eksploatowanych zabezpieczeń, również obowiązkowe szacowanie ryzyka dla tej zmiany wykonane przez zgłaszającego.

2. Pełnomocnik do spraw bezpieczeństwa informacji analizuje zasadność zmiany. W przypadku:

1) uznania zmiany za zasadną Pełnomocnik do spraw bezpieczeństwa informacji opracowuje aktualizację PBI i przekazuje do WL BP celem jej procedowania zgodnie z zasadami dotyczącymi ustanawiania wewnętrznych aktów normatywnych;
2) uznania zmiany za niezasadną Pełnomocnik do spraw bezpieczeństwa informacji informuje o tym zgłaszającego zmianę wraz z uzasadnieniem.

§ 23. Zasady dokonywania zmian w dokumentacji, o której mowa w § 19 ust. 2 dotyczącej systemów informacyjnych oraz systemów wspierających powinny określać zapisy tej dokumentacji.

Część II: Zarządzanie bezpieczeństwem informacji

Rozdział 6

[Role i odpowiedzialność]

§ 24. Zarządzanie bezpieczeństwem informacji jest realizowane m.in. poprzez:

1) polityki i procedury bezpieczeństwa informacji w konkretnych obszarach, określające zasady postępowania i mechanizmy kontroli;
2) szacowania ryzyka, analizy wpływu na biznes, audyty i kontrole;
3) szkolenia z zakresu bezpieczeństwa informacji;
4) przeglądy zarządzania oraz przeglądy PBI;
5) zarządzanie zdarzeniami;
6) podejmowanie przez Kierownictwo oraz kierujących komórkami organizacyjnymi decyzji w zakresie bezpieczeństwa informacji zgodnie ze swoimi kompetencjami;
7) stosowanie standardów bezpieczeństwa oraz rozwiązywanie problemów wynikających z naruszenia tych standardów;
8) nadzór nad realizacją zadań określonych w politykach i procedurach;
9) nadzór nad realizacją działań korekcyjnych i zapobiegawczych, działań określonych w planach postępowania z ryzykiem oraz zaleceniach pokontrolnych i poaudytowych;
10) monitorowanie stopnia realizacji zadań oraz skuteczności podejmowanych działań i wdrażanych rozwiązań.

2. Organizacja struktur zarządzania bezpieczeństwem informacji w Inspektoracie uwzględnia następujące zasady:

1) rozdzielenie funkcji zarządzających i kontrolnych od funkcji wykonawczych;
2) rozdzielenie, w ramach procesów związanych z bezpieczeństwem informacji, obowiązków i odpowiedzialności pozostających w konflikcie ze sobą, w celu ograniczenia nadużyć i błędów;
3) obiektywizm i bezstronność kontroli i audytów.

§ 25. 1. Główny Inspektor:

1) decyduje o celach i środkach przetwarzania informacji, w tym danych osobowych jako ich administrator;
2) ustanawia SZBI poprzez zatwierdzenie niniejszej PBI;

3) wyznacza IOD oraz osobę zastępującą IOD w czasie nieobecności, Pełnomocnika do spraw bezpieczeństwa informacji oraz Pełnomocnika do spraw bezpieczeństwa cyberprzestrzeni;
4) akceptuje wyniki przeglądów SZBI.

2. Główny Inspektor, Zastępcy Głównego Inspektora oraz Dyrektor Generalny oświadczają, że dbają o zapewnienie adekwatnego do zidentyfikowanych zagrożeń, prawdopodobieństwa ich wystąpienia oraz skutków jakie mogą wywołać, poziomu bezpieczeństwa informacji przetwarzanych w Inspektoracie w oparciu o obowiązujące przepisy prawa, normy i standardy z zakresu bezpieczeństwa informacji, ochrony danych osobowych, jak również cyberbezpieczeństwa. Świadomi negatywnego wpływu zagrożeń na bezpieczeństwo informacji przetwarzanych w Inspektoracie, kompleksowo wspierają procesy dotyczące bezpieczeństwa informacji poprzez:

1) wyznaczenie osób odpowiedzialnych za realizację zadań związanych z bezpieczeństwem informacji oraz cyberbezpieczeństwem;
2) wyznaczenie właścicieli biznesowych systemów informacyjnych oraz właścicieli informacji, którzy zobowiązani są do zapewnienia odpowiednich i bezpiecznych warunków przetwarzania informacji w ramach swoich regulaminowych zadań i odpowiedzialności za ich realizację;
3) przyjęcie do stosowania polityk, procedur i zasad bezpieczeństwa informacji przez wszystkich pracowników oraz podmioty zewnętrzne zaangażowanych w procesy biznesowe realizowane w Inspektoracie, w których dochodzi do przetwarzania informacji;
4) ciągłe doskonalenie systemu zarządzania bezpieczeństwem informacji funkcjonującego w Inspektoracie, w tym uwzględnianie zaleceń pokontrolnych i poaudytowych oraz nowych i zmieniających się norm i standardów z zakresu bezpieczeństwa informacji oraz cyberbezpieczeństwa;
5) wsparcie w realizacji celów bezpieczeństwa informacji, w tym związanych z ciągłym doskonaleniem stosowanych środków ochrony, jak również kształceniem i rozwojem kadry Inspektoratu, w szczególności realizującej zadania związane z zarządzaniem i zapewnieniem bezpieczeństwa informacji, ochroną danych osobowych, cyberbezpieczeństwem, kontrolą i audytem;
6) pomoc i gotowość do stałej współpracy w zakresie realizacji zapisów dokumentacji SZBI.

§ 26. 1. Pełnomocnik do spraw bezpieczeństwa informacji odpowiada za koordynację zarządzania bezpieczeństwem informacji w Inspektoracie poprzez realizację zadań określonych w PBI.

2. Pełnomocnik do spraw bezpieczeństwa informacji jest uprawniony do:

1) wydawania zaleceń w zakresie stosowania PBI;
2) uzyskania wyjaśnień od pracowników w przypadku wystąpienia incydentów bezpieczeństwa informacji oraz nieprawidłowości w zakresie funkcjonowania i stosowania PBI;
3) podejmowania działań w kwestiach bezpieczeństwa informacji w zakresie niezastrzeżonym do kompetencji innych osób;
4) rekomendowania rozwiązań organizacyjno-technicznych zwiększających skuteczność zarządzania w obszarze bezpieczeństwa informacji.

§ 27. 1. Pełnomocnik do spraw bezpieczeństwa cyberprzestrzeni odpowiada za koordynację zarządzania bezpieczeństwem cyberprzestrzeni w Inspektoracie, w szczególności:

1) koordynuje utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa;
2) koordynuje zarządzanie incydentem w podmiocie publicznym, w tym jego zgłoszenie do CSIRT GOV;
3) przekazuje do CSIRT GOV dane innych osób wyznaczonych do utrzymywania kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa wyznaczonych na zasadach określonych w PBI;
4) zapewnia w imieniu Głównego Inspektora osobom, na rzecz których zadanie publiczne jest realizowane, dostęp do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami, w szczególności przez publikowanie informacji w tym zakresie na stronie internetowej Inspektoratu we współpracy z właścicielem biznesowym tego systemu;
5) prowadzi wykaz systemów informacyjnych i wspierających.

2. W celu realizacji zadań, o których mowa w ust. 1, Pełnomocnik do spraw bezpieczeństwa cyberprzestrzeni może wydawać zalecenia, występować z wnioskami oraz żądać udzielenia informacji i opinii od komórek organizacyjnych, pracowników, właścicieli biznesowych systemów informacyjnych, właścicieli systemów wspierających.

3. Pełnomocnik do spraw bezpieczeństwa cyberprzestrzeni musi być informowany przez inne osoby wyznaczone do utrzymywania kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa na zasadach określonych w niniejszej PBI, o podejmowanych przez te osoby działaniach i otrzymywanych informacjach z zakresu cyberbezpieczeństwa.

§ 28. IOD realizuje zadania określone w przepisach prawa krajowego i międzynarodowego, Regulaminie organizacyjnym Inspektoratu oraz regulaminie organizacyjnym komórki, w której funkcjonuje, w szczególności nadzoruje i monitoruje zgodność przetwarzania danych osobowych z przepisami prawa i politykami oraz doradza administratorowi danych w realizacji jego obowiązków.

§ 29. Komórka audytu wewnętrznego zapewnia prowadzenie kontroli i audytów funkcjonowania bezpieczeństwa informacji w Inspektoracie zgodnie z właściwymi przepisami prawa oraz wewnętrznymi regulacjami obowiązującymi w Inspektoracie, w tym Księgą Procedur Audytu.

§ 30. 1. Kierujący komórką organizacyjną odpowiada za zapewnienie stosowania i przestrzegania wymagań i zasad bezpieczeństwa określonych w PBI przez pracowników kierowanej przez niego komórki organizacyjnej.

2. Kierujący komórką organizacyjną odpowiada za zapewnienie stosowania i przestrzegania wymagań i zasad bezpieczeństwa określonych w dokumentacji systemów informacyjnych oraz systemów wspierających używanych przez pracowników kierowanej przez niego komórki organizacyjnej.

3. Kierujący komórką organizacyjną będący właścicielem informacji odpowiada za zapewnienie realizacji zadań określonych w PBI, w tym włączanie IOD we wszelkie sprawy związane z ochroną danych osobowych. Do obowiązków właściciela informacji należy:

1) realizacja zadań określonych szczegółowo w PODO, w szczególności współpraca z IOD przy prowadzeniu rejestrów czynności przetwarzania oraz kategorii czynności przetwarzania;
2) opracowanie dokumentacji, o której mowa w § 19 ust. 7 w zakresie, w jakim jest to wymagane w danym przypadku.

4. Kierujący komórką organizacyjną będący właścicielem biznesowym systemu informacyjnego odpowiada za zapewnienie bezpieczeństwa informacji w systemie informacyjnym, w szczególności:

1) zapewnia opracowanie planu bezpieczeństwa systemu informacyjnego oraz planów awaryjnych/planów ciągłości działania przy wsparciu właścicieli informacji, właścicieli systemów wspierających, AMS, ASI oraz użytkowników;
2) zapewnia utrzymanie planu bezpieczeństwa systemu informacyjnego oraz planów awaryjnych/planów ciągłości działania;
3) zapewnia, że system informacyjny jest wdrażany i obsługiwany zgodnie z uzgodnionymi i zatwierdzonymi wymogami bezpieczeństwa;
4) zapewnia, że użytkownicy systemu informacyjnego, AMS oraz ASI zostaną odpowiednio przeszkoleni/zapoznani z zasadami dotyczącymi bezpieczeństwa systemu informacyjnego;
5) zapewnia aktualizację planu bezpieczeństwa systemu informacyjnego oraz planów awaryjnych/planów ciągłości działania za każdym razem, gdy nastąpi znacząca zmiana;
6) pomaga w identyfikacji, wdrażaniu i ocenie zabezpieczeń systemu informacyjnego w oparciu o udokumentowane szacowanie ryzyka;
7) zapewnia opracowanie wymaganej przepisami prawa dokumentacji systemu informacyjnego określonej w § 19 ust. 3;
8) podejmuje niezwłoczne i adekwatne działania w przypadku wystąpienia incydentów w systemie informacyjnym oraz współpracuje celem ich wyjaśnienia i obsługi;
9) we współpracy z innymi komórkami organizacyjnymi oraz podmiotami zewnętrznymi zapewnia określenie zasad użytkowania systemu informacyjnego;
10) wyznacza AMS systemu informacyjnego;
11) zapewnia pozyskiwanie wymagań funkcjonalnych i niefunkcjonalnych dotyczących procesów biznesowych wspieranych przez system informacyjny;
12) zapewnia opracowanie, utrzymywanie i aktualizowanie dokumentacji biznesowej systemu informacyjnego za każdym razem, gdy nastąpi znacząca zmiana;
13) zapewnia realizację obowiązku określonego w § 5 ust. 6;
14) zapewnia realizację innych zadań określonych w dokumentacji systemu informacyjnego przypisanych właścicielowi biznesowemu systemu informacyjnego.

5. Właściciel biznesowy systemu informacyjnego może delegować realizację zadań na podległych pracowników.

6. Kierujący komórką organizacyjną będący właścicielem systemu wspierającego odpowiada za zapewnienie bezpieczeństwa informacji w systemie informacyjnym, w szczególności:

1) zapewnia opracowanie planu bezpieczeństwa systemu wspierającego oraz planów awaryjnych/planów ciągłości działania przy wsparciu właścicieli informacji, właścicieli biznesowych systemów informacyjnych, AMS, ASI oraz użytkowników;
2) zapewnia utrzymanie planu bezpieczeństwa systemu wspierający oraz planów awaryjnych/planów ciągłości działania;
3) zapewnia, że system wspierający jest wdrażany i obsługiwany zgodnie z uzgodnionymi i zatwierdzonymi wymogami bezpieczeństwa;
4) zapewnia, że użytkownicy systemu wspierającego oraz ASI zostaną odpowiednio przeszkoleni/zapoznani z zasadami dotyczącymi bezpieczeństwa systemu wspierającego;
5) zapewnia aktualizację planu bezpieczeństwa systemu wspierającego oraz planów awaryjnych/planów ciągłości działania za każdym razem, gdy nastąpi znacząca zmiana;
6) pomaga w identyfikacji, wdrażaniu i ocenie zabezpieczeń systemu wspierającego w oparciu o udokumentowane szacowanie ryzyka;
7) zapewnia opracowanie wymaganej przepisami prawa dokumentacji systemu wspierającego określonej w § 19 ust. 3;
8) podejmuje niezwłoczne i adekwatne działania w przypadku wystąpienia incydentów w systemie wspierającym oraz współpracuje celem ich wyjaśnienia i obsługi;
9) we współpracy z innymi komórkami organizacyjnymi zapewnia określenie zasad użytkowania systemu wspierającego;
10) wyznacza ASI/AMS systemu wspierającego;
11) zapewnia identyfikację i wprowadzanie zmian w systemie wspierającym w oparciu o zgłoszone uzasadnione potrzeby komórek organizacyjnych Inspektoratu i pracowników;
12) zapewnia opracowanie, utrzymywanie i aktualizowanie dokumentacji eksploatacyjnej systemu wspierającego za każdym razem, gdy nastąpi znacząca zmiana;
13) zapewnia realizację obowiązku określonego w § 6 ust. 4;
14) zapewnia realizację innych zadań określonych w dokumentacji systemu wspierającego przypisanych właścicielowi systemu wspierającego.

7. Właściciel systemu wspierającego może delegować realizację zadań na podległych pracowników.

§ 31. 1. Pracownicy odpowiadają za bezpieczeństwo informacji w zakresie wynikającym z realizowanych przez nich obowiązków służbowych i związanej z tym odpowiedzialności i uprawnień, zgodnie z postanowieniami m.in. przepisów prawa pracy, przepisów o służbie cywilnej, Regulaminu pracy w Inspektoracie, PBI, dokumentacji systemów informacyjnych

i systemów wspierających oraz innych regulacji wewnętrznych obowiązujących w Inspektoracie.

2. Pracownicy mają obowiązek w szczególności:

1) przestrzegania zasad ochrony informacji określonych w przepisach prawa oraz PBI;
2) przetwarzania informacji wyłącznie w ramach posiadanych upoważnień i przyznanych uprawnień, w tym w systemach informacyjnych oraz systemach wspierających, także tych, których właścicielem są podmioty zewnętrzne;
3) przestrzegania zasad prawidłowej i bezpiecznej eksploatacji systemów informacyjnych oraz systemów wspierających określonych w dokumentacji tych systemów, w tym korzystania z nich wyłącznie zgodnie z ich przeznaczeniem i w zakresie wynikającym z zakresu realizowanych zadań i przyznanych uprawnień;
4) ochrony zasobów Inspektoratu oraz zasobów podmiotów zewnętrznych, w tym w trakcie transportu i korzystania z nich poza obiektami, budynkami i pomieszczeniami Inspektoratu;
5) należytego zabezpieczania stanowiska pracy, w tym stanowiska pracy zdalnej, użytkowanych urządzeń komputerowych, oprogramowania i nośników informacji niezależnie od ich formy, z uwzględnieniem przepisów i wymagań dotyczących ochrony tajemnic prawnie chronionych;
6) informowania przełożonego o wszelkich zauważonych nieprawidłowościach i zdarzeniach skutkujących lub mogących skutkować naruszeniem bezpieczeństwa informacji;
7) niezwłocznego zgłaszania zdarzeń stanowiących lub mogących stanowić incydent bezpieczeństwa informacji, cyberbezpieczeństwa lub naruszenie ochrony danych osobowych i aktywnego uczestniczenia w czynnościach wyjaśniających;
8) zapewnienia bezpieczeństwa przetwarzanych informacji oraz poufności sposobów ich zabezpieczenia, w trakcie wykonywania powierzonych zadań i po ich zakończeniu, w tym zabezpieczenia informacji przed nieuprawnionym ujawnieniem, nieuzasadnioną modyfikacją, utratą lub zniszczeniem;
9) uczestniczenia w szkoleniach z zakresu bezpieczeństwa informacji i cyberbezpieczeństwa oraz ochrony danych osobowych organizowanych w Inspektoracie.

§ 32. 1. Istotne dla bezpieczeństwa informacji zadania realizują również:

1) pracownicy BDG realizujący zadania z zakresu zapewnienia ochrony i monitoringu nieruchomości będących w trwałym zarządzie Inspektoratu, w tym współpracy z zewnętrznymi podmiotami świadczącymi usługi na rzecz Inspektoratu;
2) pracownicy ZPOiOIN GGI, w tym Pełnomocnik do spraw ochrony informacji niejawnych, realizujący zadania z zakresu zarządzania kryzysowego i ochrony informacji niejawnych szczegółowo określone w regulaminie organizacyjnym tej komórki oraz odrębnych przepisach i wewnętrznych regulacjach;
3) pracownicy BDG realizujący zadania z zakresu spraw dotyczących rozwoju zawodowego pracowników, analizy potrzeb szkoleniowych pracowników Inspektoratu, opracowywania planów szkoleń pracowników Inspektoratu oraz organizacji szkoleń, kursów, seminariów i innych form kształcenia i doskonalenia zawodowego;
4) pracownicy BDG realizujący zadania z zakresu spraw wynikających z procesów rekrutacji i selekcji, spraw wynikających z nawiązania, trwania i ustania stosunku pracy pracowników Inspektoratu, organizacji praktyk i staży zawodowych;
5) pracownicy BDG realizujący zadania z zakresu administrowania pomieszczeniami Inspektoratu, w tym przygotowywania umów lub porozumień dotyczących użytkowania nieruchomości, oraz zapewniania właściwego funkcjonowania obiektów i instalacji technicznych;
6) pracownicy BDG realizujący zadania z zakresu administrowania służbowymi telefonami komórkowymi.

§ 33. 1. Jeżeli jest to celowe i uzasadnione względami, m. in. bezpieczeństwa czy organizacyjnymi, właściciele biznesowi systemów informacyjnych oraz właściciele systemów wspierających mogą wyznaczyć osoby do utrzymywania kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. W szczególności mogą to być ASI lub AMS.

2. Dyrektor BT wyznacza dodatkową osobę do utrzymywania kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.

3. Zgłoszenia i odwoływania osób, o których mowa w ust. 1 i 2 do CSIRT GOV dokonuje Pełnomocnik do spraw bezpieczeństwa cyberprzestrzeni, na podstawie informacji od właścicieli, o których mowa w ust. 1.

§ 34. 1. AMS sprawuje nadzór merytoryczny nad systemem informacyjnym, w szczególności do jego obowiązków należy:

1) zarządzanie uprawnieniami użytkowników systemu informacyjnego, w tym prowadzenie kontroli uprawnień użytkowników nie rzadziej niż raz na rok;
2) opracowanie procedur dotyczących zarządzania uprawnieniami, o których mowa w ust. 1, obejmujących przyznawanie, zmianę i odbieranie uprawnień użytkownikom, oraz prowadzenie okresowej kontroli uprawnień użytkowników;
3) współudział w opracowywaniu dokumentacji określonej w § 19 ust. 3 pkt 1-3, 5, 7, 9-11, 13-14, oraz 18-19 i wymagań funkcjonalnych oraz niefunkcjonalnych dotyczących m.in. mechanizmów kontroli dostępu do systemu informacyjnego;
4) informowanie ASI systemu informacyjnego o pracownikach Inspektoratu posiadających uprawnienia do pracy w systemie informacyjnym, oraz ich zmianie i odebraniu w celu zapewnienia poprawności i aktualności CMDB;
5) podejmowanie niezwłocznych i odpowiednich działań w przypadku wystąpienia incydentów oraz współpraca celem ich wyjaśniania i obsługi, w tym zgłaszanie incydentów zgodnie z obowiązującymi procedurami;
6) wykonywanie innych zadań przypisanych AMS w dokumentacji systemu informacyjnego określonej w § 19 ust. 3 oraz zadań delegowanych przez właściciela biznesowego systemu informacyjnego, jeżeli takie zostały określone w dokumentacji lub delegowane;
7) dokumentowanie realizacji zadań AMS zgodnie z właściwymi procedurami określonymi w dokumentacji systemu, o której mowa w § 19 ust. 3.

2. W przypadku delegowania zadań AMS na innych pracowników lub podmioty zewnętrzne, AMS sprawuje nadzór nad ich realizacją i powinien zapewnić rozliczalność realizacji tych zadań.

3. W celu zapewnienia ciągłości realizacji zadań przez AMS właściciel biznesowy danego systemu powinien rozważyć wyznaczenie więcej, niż 1 osoby do roli AMS. Wyznaczenie może obejmować całość zadań przypisanych do roli lub określone obszary (w tym wymagania funkcjonalne, nadawanie uprawnień).

4. Właściciel systemu wspierającego może powierzyć ASI realizację zadań AMS, w takim przypadku AMS może nie być wyznaczony.

5. Wyznaczenie do roli AMS powinno być udokumentowane. Przykładowy wzór udokumentowanego wyznaczenia osoby do roli AMS, który może być wykorzystany i dowolnie dostosowany wg potrzeb zawiera załącznik nr 9 do PBI.

6. Wyznaczenie AMS powinno nastąpić już na etapie planowania systemu informacyjnego/wspierającego, aby zapewnić realizację zadań w całym cyklu życia danego

systemu informacyjnego/wspierającego poczynając od jego planowania, przez budowę, eksploatację, rozwój po wycofanie z użycia. W szczególności AMS powinien uczestniczyć w definiowaniu wymagań funkcjonalnych i niefunkcjonalnych dotyczących zarządzania uprawnieniami w systemie informacyjnym/wspierającym oraz w doborze zabezpieczeń.

§ 35. 1. ASI sprawuje nadzór techniczny nad systemem informacyjnym lub systemem wspierającym, w szczególności do jego obowiązków należy:

1) zarządzanie uprawnieniami użytkowników uprzywilejowanych systemu informacyjnego, w tym prowadzenie kontroli uprawnień użytkowników uprzywilejowanych nie rzadziej niż raz na pół roku;
2) zarządzanie uprawnieniami użytkowników systemu wspierającego, w tym prowadzenie kontroli uprawnień użytkowników nie rzadziej niż raz na rok;
3) opracowanie procedur dotyczących zarządzania uprawnieniami, o których mowa w ust. 1 i 2 obejmujących przyznawanie, zmianę i odbieranie uprawnień, oraz prowadzenie okresowej kontroli uprawnień;
4) współudział w opracowywaniu dokumentacji określonej w § 19 ust. 3 pkt 1-19 i wymagań technicznych, oraz funkcjonalnych i niefunkcjonalnych dotyczących technicznego administrowania systemem informacyjnym/wspierającym;
5) współpraca z AMS systemu informacyjnego w zakresie wymiany informacji o pracownikach Inspektoratu posiadających uprawnienia do pracy w systemie informacyjnym, oraz ich zmianie i odebraniu w celu zapewnienia poprawności i aktualności CMDB;
6) wykonywanie innych zadań przypisanych ASI w dokumentacji systemu informacyjnego/wspierającego określonej w § 19 ust. 3 oraz zadań delegowanych przez właściciela systemu wspierającego, jeżeli takie zostały określone w dokumentacji lub delegowane;
7) wykonywanie zadań przypisanych AMS w przypadku, gdy nie został wyznaczony dla systemu wspierającego;
8) dokumentowanie realizacji zadań ASI zgodnie z właściwymi procedurami określonymi w dokumentacji systemu, o której mowa w § 19 ust. 3.

2. W przypadku delegowania zadań na innych pracowników lub podmioty zewnętrzne ASI sprawuje nadzór nad ich realizacją i powinien zapewnić rozliczalność realizacji tych zadań.

3. W celu zapewnienia ciągłości realizacji zadań określonych w ust. 1 właściciel systemu wspierającego powinien rozważyć wyznaczenie więcej, niż 1 osoby do roli ASI. Wyznaczenie

może obejmować całość zadań przypisanych do roli lub określone obszary (w tym administrowanie serwerami, bazami danych, siecią, nadawanie uprawnień uprzywilejowanego dostępu, raportowanie, monitorowanie).

4. Wyznaczenie do roli ASI powinno być udokumentowane. Wzór udokumentowanego wyznaczenia osoby do roli ASI, zawiera załącznik nr 9 do PBI.

5. ASI dla systemów informacyjnych, które są posadowione na infrastrukturze teleinformatycznej administrowanej przez BT wyznacza dyrektor BT.

6. ASI dla systemów informacyjnych innych, niż wskazane w ust. 5 może wyznaczyć właściciel biznesowy takiego systemu, jeżeli jest to uzasadnione a realizacja zadań przez ASI możliwa.

7. Wyznaczenie ASI powinno nastąpić już na etapie planowania systemu informacyjnego/wspierającego, aby zapewnić realizację zadań w całym cyklu życia danego systemu informacyjnego/wspierającego poczynając od jego planowania, przez budowę, eksploatację, rozwój po wycofanie z użycia. W szczególności ASI powinien uczestniczyć w definiowaniu wymagań funkcjonalnych i niefunkcjonalnych dotyczących technicznego administrowania systemem informacyjnym/wspierającym oraz w doborze zabezpieczeń.

§ 36. W sytuacji, gdy zadania określone w § 34 lub § 35 zostaną powierzone do realizacji podmiotom zewnętrznym, AMS/ASI mają obowiązek prowadzić udokumentowany nadzór i rozliczalność zadań, które zostały powierzone podmiotom zewnętrznym.

Rozdział 7

[Zarządzanie ryzykiem]

§ 37. 1. Zarządzanie ryzykiem wspiera i wpływa na większą efektywność zarządzania bezpieczeństwem informacji, przez:

1) identyfikację potencjalnych zagrożeń i podatności oraz określenie ich wpływu na realizację celów bezpieczeństwa informacji;
2) zapobieganie wystąpieniu niepożądanych skutków lub ich zredukowanie przez zastosowanie zabezpieczeń obniżających ryzyko do poziomu akceptowalnego.

2. Zarządzanie ryzykiem jest procesem ciągłym obejmującym następujące działania:

1) przygotowanie do szacowania ryzyka;
2) szacowanie ryzyka obejmujące:
   a. identyfikację źródeł zagrożeń,
   b. identyfikację podatności i warunków predyspozycji,

c. ustalenie prawdopodobieństwa wystąpienia zdarzeń,

d. określenie wielkości oddziaływania,

e. ustalenie ryzyka;

3) przekazywanie wyników szacowania ryzyka;

4) utrzymywanie wyników szacowania ryzyka.

3. Działania podejmowane w ramach zarządzania ryzykiem należy dokumentować.

4. Wyniki szacowania ryzyka należy poddawać systematycznej cyklicznej ocenie.

5. Planowanie i wdrażanie procesów biznesowych związanych i z nimi rozwiązań teleinformatycznych oraz czynności przetwarzania danych osobowych należy realizować z uwzględnieniem zasad wynikających z PBI, wymagań prawnych i uzasadnionych potrzeb biznesowych.

6. Identyfikacja i analiza oraz postępowanie z ryzykiem powinny być stosowane przy podejmowaniu wszystkich ważniejszych decyzji, w tym dotyczących wdrażania nowych lub zmiany istniejących procesów biznesowych i związanych z nimi rozwiązań teleinformatycznych i czynności przetwarzania danych osobowych.

§ 38. 1. Szacowanie ryzyka jest obligatoryjne i przeprowadza się je cyklicznie, nie rzadziej niż raz na rok, dla wszystkich systemów informacyjnych oraz systemów wspierających.

2. Szacowanie ryzyka należy również przeprowadzać zgodnie z identyfikowanymi potrzebami, w szczególności przed wprowadzeniem istotnych zmian w systemach informacyjnych oraz systemach wspierających, które mogą mieć wpływ na bezpieczeństwo przetwarzanych informacji.

3. Za zapewnienie przeprowadzenia szacowania ryzyka dla systemów informacyjnych oraz systemów wspierających odpowiedzialni są ich właściciele.

4. W przypadku, gdy właściciel biznesowy systemu informacyjnego / właściciel systemu wspierającego nie jest jednocześnie właścicielem informacji, właściciel ten prowadzi szacowanie ryzyka przy udziale właściciela informacji.

§ 39. 1. Wyniki szacowania ryzyka i plan postępowania z ryzykiem są zatwierdzane przez właściciela biznesowego systemu informacyjnego/właściciela systemu wspierającego, oraz w przypadku określonym w § 38 ust. 4 również przez właściciela informacji.

2. Właściciele biznesowi systemów informacyjnych/właściciele systemów wspierających są właścicielami ryzyk zidentyfikowanych podczas szacowania ryzyka dla tych systemów i przetwarzanych w nich informacji.

3. Właściciele informacji są właścicielami ryzyk zidentyfikowanych podczas prowadzenia oceny skutków dla ochrony danych w odniesieniu do danych osobowych.

4. Kierujący komórkami organizacyjnymi są właścicielami ryzyk w zakresie odpowiedzialności tych komórek organizacyjnych wynikającej z regulaminu organizacyjnego Inspektoratu oraz regulaminów organizacyjnych tych komórek.

§ 40. 1. Szacowanie ryzyka przeprowadza się w oparciu o NSC 800–30 „*Przewodnik dotyczący postępowania w zakresie szacowania ryzyka w podmiotach realizujących zadania publiczne*” z uwzględnieniem wytycznych opisanych w NSC 800–39 „*Zarządzanie ryzykiem bezpieczeństwa informacji*” oraz:

1) NSC 200 „*Minimalne wymagania bezpieczeństwa informacji i systemów informacyjnych podmiotów publicznych*”;
2) NSC 800–53 „*Zabezpieczenia i ochrona prywatności systemów informacyjnych oraz organizacji*”;
3) NSC 800–53B „*Zabezpieczenia bazowe systemów informacyjnych oraz organizacji*”.

Aktualna wersja dokumentów stanowiących NSC znajduje się na portalu GOV.PL[4)].

2. Dopuszczalne jest stosowanie innego, niż wskazane w ust. 1 podejścia do szacowania ryzyka, w szczególności podejścia opisanego w PN-ISO/IEC 27005.

3. W przypadku stosowania innego, niż określone w ust. 1 i 2 podejścia do szacowania ryzykiem, w raporcie z szacowania ryzyka należy obowiązkowo opisać zastosowaną metodę szacowania ryzyka.

4. Ocena skutków dla ochrony danych osobowych jest prowadzona zgodnie z zasadami określonymi w PODO.

Rozdział 8

[Zarządzanie urządzeniami teleinformatycznymi i oprogramowaniem]

§ 41. 1. W Inspektoracie zarządza się urządzeniami teleinformatycznymi i oprogramowaniem w celu zapewnienia im bezpieczeństwa, w zakresie obejmującym:

1) urządzenia teleinformatyczne i oprogramowanie wykorzystywane do przetwarzania informacji, w szczególności obejmujące:
   a. sprzęt – m.in. urządzenia komputerowe stacjonarne i przenośne oraz mobilne, serwery, urządzenia peryferyjne (w tym drukarki, skanery), nośniki danych,

[4)] https://www.gov.pl/web/baza-wiedzy/narodowe-standardy-cyber

b. oprogramowanie, w tym aplikacje i systemy operacyjne oraz oprogramowanie dedykowane,

c. sieć, w tym urządzenia telekomunikacyjne;

2) osoby odpowiedzialne za urządzenia teleinformatyczne i oprogramowanie;

3) pomieszczenia, w których eksploatowane są urządzenia teleinformatyczne i oprogramowanie;

4) strukturę organizacyjną – komórki organizacyjne oraz podmioty zewnętrzne korzystające z urządzeń teleinformatycznych i oprogramowania;

5) usługi i umowy dotyczące serwisu i napraw, utrzymania i rozwoju urządzeń teleinformatycznych i oprogramowania.

2. Urządzenia teleinformatyczne i oprogramowanie, o których mowa w ust. 1 podlegają ochronie ze względu na:

1) wymagania wynikające z przepisów prawa;

2) warunki licencji;

3) wymagania wynikające z postanowień umów lub porozumień zawartych między Inspektoratem a podmiotami zewnętrznymi;

4) wartość biznesową tych zasobów odpowiadającą ich wadze dla prowadzonej działalności, w szczególności w związku z realizacją zadań ustawowych;

5) inne regulacje wewnętrzne, z których wynika potrzeba ochrony tych zasobów.

3. Zarządzanie urządzeniami teleinformatycznymi i oprogramowaniem jest realizowane zgodnie z następującymi zasadami:

1) wszystkie urządzenia teleinformatyczne i oprogramowanie muszą być zidentyfikowane;

2) należy utworzyć i utrzymywać rejestr urządzeń teleinformatycznych i oprogramowania (CMDB) obejmujący ich wzajemne powiązania między sobą;

3) dla wszystkich urządzeń teleinformatycznych i oprogramowania należy określić ich właścicieli oraz określić i przydzielić tym właścicielom odpowiedzialność w zakresie zarządzania tymi zasobami, w tym:

a. sporządzenie i utrzymywanie CMDB,

b. zapewnienie właściwej klasyfikacji urządzeń teleinformatycznych i oprogramowania na podstawie kategorii przetwarzanych informacji,

c. wdrożenie, utrzymanie i doskonalenie zabezpieczeń,

d. monitorowanie stanu zabezpieczeń,

e. zapewnienie usuwania i niszczenia zasobów w sposób skuteczny zgodnie z przyjętymi zasadami,

f. przeglądy w zakresie praw dostępu;

4) należy określić i stosować zasady dopuszczalnego wykorzystania urządzeń teleinformatycznych i oprogramowania przez pracowników, jak również przez podmioty zewnętrzne uzyskujące dostęp do nich na podstawie umów lub porozumień, w tym obowiązek ich zwrotu w związku z zakończeniem zatrudnienia, umowy lub porozumienia lub zmianą zakresu zadań;

5) należy określić i stosować zasady klasyfikacji informacji, zasady postępowania z informacją, jej przetwarzania, przechowywania i przekazywania oraz oznaczania zgodnie z przyjętymi zasadami, a także ochrony informacji zgodnie z wymaganiami określonymi w odniesieniu do danej grupy informacji;

6) należy określić i stosować zasady zarządzania nośnikami informacji oraz zasady ich ochrony, w tym poza obiektami, budynkami i pomieszczeniami Inspektoratu, m.in. w trakcie transportu, a także zasady wycofywania nośników informacji z użycia i ich niszczenia.

5. Wymagania i zasady dotyczące prowadzenia CMDB określa załącznik nr 4 do PBI.

6. Wymagania i zasady dotyczące dopuszczalnego wykorzystania urządzeń teleinformatycznych i oprogramowania oraz informacji określają załączniki nr 4 oraz nr 10 do PBI.

7. Wymagania i zasady dotyczące klasyfikacji i postępowania z informacjami określa załącznik nr 10 do PBI.

8. Wymagania i zasady dotyczące zarządzania nośnikami informacji określają załączniki nr 4 oraz nr 10 do PBI.

Rozdział 9

[Zarządzanie zasobami, wiedzą i kompetencjami]

§ 42. 1. Kierownictwo zapewnia zasoby niezbędne dla ustanowienia, wdrożenia, utrzymywania i ciągłego doskonalenia SZBI w Inspektoracie.

2. Kierownictwo zapewnia odpowiednie dla swojego zakresu oddziaływania, odpowiedzialności i uprawnień, kompetencje w zakresie bezpieczeństwa informacji, ochrony danych osobowych i cyberbezpieczeństwa oraz ról reprezentujących i zaangażowanych w realizację funkcji związanych z ustanowieniem, wdrożeniem, utrzymywaniem i ciągłym

doskonaleniem zasad bezpieczeństwa informacji ustanowionych niniejszą PBI, w celu zapewnienia odpowiedniego i adekwatnego do zidentyfikowanych zagrożeń poziomu bezpieczeństwa informacji w Inspektoracie.

3. Zarządzanie wiedzą z zakresu bezpieczeństwa informacji jest procesem ciągłym i dotyczy każdego z uczestników przetwarzania informacji w Inspektoracie, w tym pracowników, współpracowników, zleceniobiorców, wykonawców.

4. Zarządzanie wiedzą obejmuje:

1) podnoszenie świadomości na temat zagrożeń bezpieczeństwa informacji;
2) zrozumienie możliwych skutków naruszenia zasad bezpieczeństwa informacji, w tym możliwej odpowiedzialności prawnej;
3) stosowanie środków zapewniających bezpieczeństwo informacji i ograniczających ryzyko materializacji zagrożeń lub wysokość skutków ich wystąpienia.

5. Zasady zarządzania zasobami, wiedzą i kompetencjami określa PBO.

§ 43. 1. Podmioty zewnętrzne zobowiązane do stosowania postanowień dokumentacji SZBI w Inspektoracie mają obowiązek zapewnić zasoby niezbędne do ochrony informacji w zakresie adekwatnym do obszaru oddziaływania i udziału każdego z tych podmiotów w procesach biznesowych i związanych z nimi systemów informacyjnych oraz systemów wspierających, zgodnie z wymogami określonymi w przepisach prawa, normach i standardach z zakresu bezpieczeństwa informacji, cyberbezpieczeństwa oraz PBI.

2. Podmioty zewnętrzne zobowiązane do stosowania postanowień dokumentacji SZBI w Inspektoracie mają obowiązek zapewnić odpowiednie dla swojego zakresu oddziaływania, odpowiedzialności i uprawnień, kompetencje w zakresie bezpieczeństwa informacji, ochrony danych osobowych i cyberbezpieczeństwa oraz ról reprezentujących i zaangażowanych w realizację funkcji związanych bezpieczeństwem informacji oraz cyberbezpieczeństwem, zgodnie z wymogami określonymi w przepisach prawa, normach i standardach z zakresu bezpieczeństwa informacji oraz cyberbezpieczeństwa oraz niniejszej PBI, w celu zapewnienia odpowiedniego i adekwatnego do zidentyfikowanych zagrożeń poziomu bezpieczeństwa informacji w Inspektoracie.

3. Podmioty zewnętrzne zobowiązane do stosowania postanowień dokumentacji SZBI w Inspektoracie mają obowiązek zapewnić zarządzanie wiedzą z zakresu bezpieczeństwa informacji odpowiednie dla swojego zakresu oddziaływania, odpowiedzialności i uprawnień, kompetencje w zakresie bezpieczeństwa informacji, ochrony danych osobowych i cyberbezpieczeństwa oraz ról reprezentujących i zaangażowanych w realizację funkcji

związanych bezpieczeństwem informacji oraz cyberbezpieczeństwem, zgodnie z wymogami określonymi w przepisach prawa, normach i standardach z zakresu bezpieczeństwa informacji oraz cyberbezpieczeństwa oraz niniejszej PBI, w celu zapewnienia odpowiedniego i adekwatnego do zidentyfikowanych zagrożeń poziomu bezpieczeństwa informacji w Inspektoracie.

Rozdział 10

[Zarządzanie komunikacją w ramach SZBI]

§ 44. 1. Zarządzanie komunikacją obejmuje informowanie o:

1) zasadach określonych w PBI;
2) innych zagadnieniach uznanych za ważne dla zapewnienia bezpieczeństwa informacji.

2. Zasady określone w PBI są komunikowane pracownikom poprzez wiadomości elektroniczne oraz szkolenia z zakresu bezpieczeństwa informacji.

3. Inne zagadnienia uznawane za ważne dla zapewnienia bezpieczeństwa informacji są komunikowane pracownikom poprzez wiadomości elektroniczne oraz szkolenia z zakresu bezpieczeństwa informacji.

Rozdział 11

[Monitorowanie, pomiary, analiza i ocena]

§ 45. 1. Ocena skuteczności wdrożonej PBI jest kluczowym elementem SZBI. Ocena na poziomie zarządczym dokonywana jest cyklicznie w ramach przeglądów zarządzania, gdzie analizowane są takie elementy jak:

1) wyniki kontroli i audytów obejmujące ocenę skuteczności wdrożonych zabezpieczeń opisanych w PBI i zidentyfikowane w tym zakresie niezgodności;
2) zgodność PBI z przepisami prawa;
3) działania podejmowane w celu podnoszenia kompetencji i świadomości w obszarze bezpieczeństwa informacji;
4) cele bezpieczeństwa informacji i ich realizacja;
5) celowość ustanowionych w PBI zabezpieczeń;
6) zarządzanie incydentami bezpieczeństwa;
7) odstępstwa i wyjątki od zasad ustanowionych w PBI.

2. Monitorowanie, pomiar, analiza i ocena na poziomie zarządczym realizowane są cyklicznie w ramach przeglądu zarządzania.

§ 46. 1. Monitorowanie, pomiary, analizy i oceny na poziomie operacyjnym obejmującym systemy informacyjne ich właściciele powinni realizować w trybie ciągłym w celu zapewnienia aktualnych informacji niezbędnych do właściwej oceny sytuacji, podejmowania właściwych decyzji i działań odnośnie funkcjonowania i bezpieczeństwa tych systemów i czynności przetwarzania.

2. Działania, o których mowa w ust. 1 to między innymi analiza i ocena skuteczności obsługi incydentów, niezgodności i podejmowanych działań korygujących oraz analiza odstępstw i wyjątków, w odniesieniu do systemów.

3. Wyniki monitorowania, pomiaru, analizy i oceny na poziomie operacyjnym powinny być dokumentowane.

Rozdział 12

[Audyt wewnętrzny]

§ 47. 1. Audyt wewnętrzny jest mechanizmem niezależnej, bezstronnej i obiektywnej oceny, która służy potwierdzeniu zgodności PBI z wymaganiami dotyczącymi bezpieczeństwa informacji wynikającymi z przepisów prawa i wewnętrznych regulacji.

2. Wyniki audytu wewnętrznego bezpieczeństwa informacji w zakresie, jaki dotyczy niniejszej PBI powinny być udostępniane Pełnomocnikowi do spraw bezpieczeństwa informacji, w celu zaplanowania i wdrożenia działań korygujących i doskonalących dotyczących PBI.

3. Audyt wewnętrzny w zakresie bezpieczeństwa informacji jest procesem systematycznym – cyklicznie powtarzalnym, który należy przeprowadzać co najmniej raz w roku.

4. Audyt wewnętrzny jest realizowany zgodnie z obowiązującymi przepisami prawa i wewnętrznymi regulacjami, m.in. Księgą Procedur Audytu.

Rozdział 13

[Przeglądy zarządzania]

§ 48. 1. Przeglądy zarządzania mają na celu zapewnienie stałej przydatności, adekwatności i skuteczności PBI w zakresie zapewnienia adekwatnego do zagrożeń poziomu bezpieczeństwa informacji w Inspektoracie.

2. Przeglądy zarządzania to działanie zarządcze, cykliczne, polegające na zebraniu danych dotyczących stanu i poziomu bezpieczeństwa informacji oraz skuteczności ustanowionych

i wdrożonych rozwiązań, ocenie zidentyfikowanych niezgodności i potrzeb doskonalenia oraz podjęciu decyzji, co do realizacji niezbędnych działań korygujących.

3. Przeglądy zarządzania odbywają się cyklicznie, co najmniej raz do roku.

4. W przeglądach zarządzania uczestniczą:

1) Główny Inspektor;
2) Zastępcy Głównego Inspektora;
3) DG;
4) kierujący komórkami organizacyjnymi w zakresie zadań realizowanych przez te komórki dotyczących zarządzania bezpieczeństwem informacji;
5) IOD;
6) Pełnomocnik do spraw bezpieczeństwa cyberprzestrzeni;
7) Pełnomocnik do spraw bezpieczeństwa informacji.

5. W przeglądach zarządzania mogą uczestniczyć również audytorzy wewnętrzni, w szczególności w zakresie niezgodności zidentyfikowanych w ramach kontroli i audytów wewnętrznych oraz podjętych w ich następstwie działań korygujących.

6. Przegląd zarządzania przeprowadza się w trybie obiegowym. Przegląd zarządzania może być również zorganizowany w trybie stacjonarnym lub zdalnym. Decyzję o zmianie trybu organizacji danego przeglądu zarządzania podejmuje Kierownictwo.

7. Przegląd zarządzania bezpieczeństwem informacji powinien uwzględniać oraz poddać analizie i ocenie, co najmniej następujące informacje:

1) status działań podjętych w następstwie wcześniejszych przeglądów zarządzania;
2) cel, zakres i kontekst funkcjonowania systemu zarządzania bezpieczeństwem informacji oraz zmiany jego otoczenia (w tym zmiany wymagań prawnych, norm i standardów);
3) zasoby niezbędne do funkcjonowania systemu zarządzania bezpieczeństwem informacji;
4) stopień osiągnięcia celów bezpieczeństwa;
5) skuteczność funkcjonowania procesów określonych niniejsza polityką;
6) występowanie, skalę, zakres oddziaływania i skutki niezgodności;
7) wyniki szacowania ryzyka i stan realizacji zadań określonych w planie postępowania z ryzykiem;
8) wyniki audytów wewnętrznych i stopień realizacji zaleceń poaudytowych;
9) informacje z obszaru zarządzania incydentami bezpieczeństwa informacji;
10) informacje dotyczące zarejestrowanych odstępstw i wyjątków;

11) inne informacje istotne dla funkcjonowania systemu zarządzania bezpieczeństwem informacji.

8. Wynikiem przeglądu zarządzania bezpieczeństwem informacji są zalecenia oraz decyzje dotyczące:

1) realizacji działań korygujących w odniesieniu do ustanowionych środków ochrony: organizacyjnych, technicznych, osobowych lub fizycznych w zakresie polityki bezpieczeństwa informacji;
2) doskonalenia skuteczności systemu zarządzania bezpieczeństwem informacji ustanowionego niniejszą polityką.

9. Wyniki przeglądu zarządzania bezpieczeństwem informacji są dokumentowane.

10. Zalecenia oraz wszelkie decyzje podjęte podczas przeglądu zarządzania powinny być bez zbędnej zwłoki wdrożone w obszarze, którego dotyczą.

§ 49. 1. Przeglądy zarządzania na poziomie operacyjnym (systemów informacyjnych oraz systemów wspierających) ich właściciele organizują zgodnie z zasadami określonymi w dokumentacji tych systemów z uwzględnieniem wytycznych określonych w ust. 2 i 3.

2. Uczestnikami przeglądów zarządzania na poziomie operacyjnym powinni być co najmniej właściciel biznesowy systemu informacyjnego/właściciel systemu wspierającego, ASI, AMS oraz IOD – jeżeli w danym systemie przetwarzane są dane osobowe. Zakres uczestników należy dostosować do danej sytuacji.

3. Uczestnikami przeglądów zarządzania na poziomie operacyjnym powinni być również przedstawiciele podmiotów zewnętrznych, które są odpowiedzialne za utrzymanie, rozwój oraz bezpieczeństwo systemów, o których mowa w ust. 1. Zakres uczestników należy dostosować do sytuacji.

Rozdział 14

[Niezgodności i działania korygujące]

§ 50. 1. Niezgodność jest działaniem lub rozwiązaniem niezgodnym z postanowieniami PBI i wdrożonymi zabezpieczeniami, które zostało wykonane lub wdrożone bez uzyskania wymaganej zgody (odstępstwo lub wyjątek). Niezgodności mogą zwiększać podatność na zagrożenia bezpieczeństwa informacji, jak również same mogą stanowić takie zagrożenie, dlatego wymagają objęcia specjalnym nadzorem.

2. Nadzorowanie niezgodności zapewnia bezpieczeństwo informacji poprzez:

1) identyfikację niezgodności, ich charakteru, zakresu, sposobu i zasięgu oddziaływania, oraz ewentualnych wywoływanych skutków wystąpienia;
2) podejmowanie działań zapobiegających działaniu w niewłaściwy, niezgodny z PBI sposób lub wykorzystywaniu, stosowaniu niewłaściwych, niezgodnych z nią rozwiązań;
3) modyfikację stanu niezgodnego ze stanem właściwym określonym w PBI, skorygowanie niezgodnego zabezpieczenia lub podejmowanego działania;
4) zapobieganie wykonywaniu nieuzasadnionych zmian;
5) monitorowanie i zarządzanie skutkami niezgodności.

3. Działania korygujące to działania mające na celu niedopuszczenie do powtórnego wystąpienia zaistniałych niezgodności. Działania korygujące zwiększają odporność i zmniejszają podatności na zagrożenia bezpieczeństwa informacji, stanowią nadto działania przeciwdziałające tym zagrożeniom.

4. Realizacja działań korygujących obejmuje m.in:

1) analizę niezgodności;
2) identyfikację przyczyn wystąpienia niezgodności;
3) wdrożenie działań eliminujących przyczyny powstania niezgodności;
4) monitorowanie skuteczności działań korygujących.

5. Nadzorowanie niezgodności i realizację działań korygujących należy dokumentować.

6. Proces nadzorowania niezgodności podlega dokumentowaniu.

7. Niezgodności i działania korygujące podlegają weryfikacji w ramach audytów wewnętrznych.

8. Działania korygujące realizują właściciele obszarów (m.in. kierujący komórkami organizacyjnymi, właściciele biznesowi systemów informacyjnych, właściciele systemów wspierających, ASI, AMS, Pełnomocnik do spraw bezpieczeństwa informacji), w których niezgodności zostały zidentyfikowane.

Rozdział 15

[Zarządzanie incydentami bezpieczeństwa informacji]

§ 51. 1. Zarządzanie incydentami bezpieczeństwa informacji obejmuje obsługę zgłoszonych lub zidentyfikowanych zdarzeń i działań niezgodnych z postanowieniami niniejszej PBI, oraz innych zdarzeń, które powodują lub mogą powodować negatywne skutki dla bezpieczeństwa informacji przetwarzanych w Inspektoracie.

2. Zarządzanie incydentami bezpieczeństwa informacji, w tym obsługa zgłoszeń kierowanych na adres: incydent@gitd.gov.pl, jest realizowana zgodnie z zasadami opisanymi w załączniku nr 6 do PBI.

3. Właściciele biznesowi systemów informacyjnych oraz właściciele systemów wspierających mają obowiązek zapewnić, odpowiednio w procedurach dotyczących systemów oraz umowach z podmiotami zewnętrznymi obowiązek zgłaszania incydentów bezpieczeństwa informacji zgodnie z zasadami opisanymi w załączniku nr 6 do PBI, w tym w szczególności incydentów w podmiocie publicznym oraz naruszeń ochrony danych osobowych.

Rozdział 16

[Ciągłe doskonalenie]

§ 52. 1. PBI podlega ciągłemu doskonaleniu w odniesieniu do jego przydatności, adekwatności i skuteczności w zapewnieniu wymaganego poziomu bezpieczeństwa informacji przetwarzanych w Inspektoracie.

2. Ciągłe doskonalenie jest realizowane w odniesieniu do ustanowionych celów bezpieczeństwa informacji, poprzez zarządzanie ryzykiem, wdrażanie zabezpieczeń adekwatnych do zidentyfikowanych zagrożeń, monitorowanie, pomiary, analizy i oceny, kontrole i audyty wewnętrzne, przeglądy zarządzania i działania korygujące i doskonalące.

3. Wszelkie inicjatywy doskonalące rozwiązania przyjęte w niniejszej PBI należy realizować zgodnie z zasadami opisanymi w rozdziale 5 PBI.

Część III – Zapewnienie bezpieczeństwa informacji

Rozdział 17

[Polityki bezpieczeństwa informacji]

§ 53. 1. PBI, polityki niższego poziomu oraz wymagane plany, procedury i instrukcje dotyczące bezpieczeństwa informacji w systemach informacyjnych / wspierających stanowiące razem dokumentację SZBI w Inspektoracie, a także ich aktualizacje zatwierdzają osoby określone w PBI.

2. Po zatwierdzeniu, dokumenty o których mowa w ust. 1 należy udostępnić w całości lub części uprawnionym pracownikom, a także, gdy jest to wymagane np. do prawidłowego świadczenia usług na rzecz Inspektoratu – podmiotom zewnętrznym.

3. Dokumenty o których mowa w ust. 1 są poddawane regularnym przeglądom, nie rzadziej niż raz do roku oraz zawsze, gdy wystąpią istotne zmiany w obszarach na nie oddziałujących.

4. Za zapewnienie regularnych przeglądów odpowiadają:

1) Pełnomocnik do spraw bezpieczeństwa informacji – w odniesieniu do PBI;
2) właściciele biznesowi systemów informacyjnych/właściciele systemów wspierających – w odniesieniu do dokumentacji tych systemów.

5. Szczegółowy sposób realizacji zabezpieczeń opisanych w części II PBI w systemach informacyjnych oraz systemach wspierających uwzględniający odstępstwa i wyjątki, jeżeli występują określa dokumentacja tych systemów.

Rozdział 18

[Organizacja bezpieczeństwa informacji]

§ 54. Celem stosowania zabezpieczenia jest ustanowienie struktury zarządzania bezpieczeństwem informacji w celu zainicjowania oraz nadzorowania wdrażania i eksploatacji procesów bezpieczeństwa informacji w Inspektoracie.

§ 55. 1. Za bezpieczeństwo informacji, ochronę poszczególnych informacji i środków ich przetwarzania oraz realizację procesów bezpieczeństwa informacji odpowiadają wszyscy pracownicy, w tym wyznaczone do pełnienia ról związanych z realizacją określonych zadań.

2. Osoby wyznaczone do pełnienia ról związanych z bezpieczeństwem informacji mogą delegować swoje zadania na innych pracowników lub podmioty zewnętrzne, jednak pozostają za nie odpowiedzialne i mają obowiązek nadzorować realizację delegowanych zadań.

3. Obowiązki i odpowiedzialności osób odpowiedzialnych za bezpieczeństwo informacji pozostające w konflikcie są ze sobą rozdzielane w celu zredukowania ryzyka niewłaściwego umyślnego lub nieumyślnego użycia informacji.

4. W celu ochrony przed wystąpieniem ryzyka niewłaściwego umyślnego lub nieumyślnego użycia informacji zapewniana jest rozliczalność działań związanych z dostępem do tych informacji. Redukcji ryzyka niewłaściwego użycia informacji służą również dodatkowe zabezpieczenia m.in. monitorowanie aktywności, analizy dzienników zdarzeń oraz nadzór nad przetwarzaniem informacji.

5. W zakresie bezpieczeństwa informacji utrzymywane są kontakty z właściwymi podmiotami zewnętrznymi, w tym podmiotami krajowego systemu cyberbezpieczeństwa.

6. AMS i ASI oraz inne osoby odpowiedzialne za prawidłowe i bezpieczne użytkowanie systemów informacyjnych oraz systemów wspierających utrzymują kontakty ze specjalistami, jak również specjalistycznymi forami oraz stowarzyszeniami zawodowymi w celu bieżącego uzupełniania wiedzy, wymiany informacji o nowych technologiach, produktach, zagrożeniach i podatnościach.

7. Bezpieczeństwo informacji jest uwzględniane w ramach zarządzania wszystkimi projektami w Inspektoracie obejmującymi swoim zakresem systemy informacyjne oraz systemy wspierające, w szczególności:

1) cele bezpieczeństwa informacji są włączane do celów projektów, a samo bezpieczeństwo informacji jest elementem wszystkich etapów wykorzystywanej metodyki projektu;
2) dobór zabezpieczeń opiera się o wyniki szacowania ryzyka realizowanego we wstępnym etapie projektu i powtarzanego, gdy zachodzi taka potrzeba.

8. Szczegółowy sposób organizacji bezpieczeństwa w projektach, systemach informacyjnych oraz systemach wspierających określa dokumentacja tych projektów i systemów.

Rozdział 19

[Urządzenia mobilne i praca na odległość]

§ 56. 1. Celem stosowania zabezpieczenia jest zapewnienie bezpieczeństwa informacji urządzeń mobilnych oraz przy pracy na odległość, w tym pracy zdalnej.

2. Wymagania i zasady dotyczące użytkowania urządzeń mobilnych określa załącznik nr 4 do PBI.

3. Wymagania i zasady dotyczące bezpieczeństwa informacji pracy na odległość, w tym pracy zdalnej określa załącznik nr 4 do PBI.

4. Szczegółowe zabezpieczenia urządzeń mobilnych w systemach informacyjnych oraz systemach wspierających określa dokumentacja tych systemów.

Rozdział 20

[Bezpieczeństwo osobowe]

§ 57. 1. Celem stosowania zabezpieczenia jest uświadomienie odpowiedzialności, zapewnienie wymaganej weryfikacji osób zatrudnianych, uświadomienie obowiązków dotyczących bezpieczeństwa informacji, zabezpieczenie interesów Inspektoratu w trakcie zmiany lub zakończenia zatrudnienia.

2. Wymagania i zasady dotyczące bezpieczeństwa osobowego określa załącznik nr 2 do PBI.

3. Szczegółowe zabezpieczenia osobowe w systemach informacyjnych oraz systemach wspierających określa dokumentacja tych systemów.

Rozdział 21

[Zarządzanie urządzeniami teleinformatycznymi i oprogramowaniem]

§ 58. Celem stosowania zabezpieczenia jest identyfikacja środków wykorzystywanych do przetwarzania informacji, przypisanie odpowiedzialności w zakresie ich ochrony, określenie poziomu ochrony informacji, zapobieganie nieuprawnionemu przetwarzaniu informacji zapisanych na nośnikach.

§ 59. 1. Urządzenia teleinformatyczne i oprogramowanie są zidentyfikowane i posiadają jednoznacznie przypisanego właściciela.

2. Prowadzony i utrzymywany w aktualności jest rejestr urządzeń teleinformatycznych i oprogramowania (CMDB).

3. Za zapewnienie prowadzenia CMDB odpowiadają:

1) właściciele systemów wspierających – w zakresie urządzeń i oprogramowania przez nich zarządzanego, w tym komputerów pracowników;
2) właściciele biznesowi systemów informacyjnych – w pozostałym zakresie nieujętym w pkt 1.

4. Urządzenia teleinformatyczne i oprogramowanie posiadają ustanowione zasady ich akceptowalnego użycia.

5. Każda osoba używająca urządzeń teleinformatycznych i oprogramowania Inspektoratu, w szczególności pracownik, ponosi odpowiedzialność za prawidłowe z nich korzystanie, tj. wyłącznie w celu i zakresie, w jakim zostały tej osobie udostępnione do użycia.

6. Pracownicy w momencie zakończenia zatrudnienia mają obowiązek zwrócić wszystkie posiadane i udostępnione im m.in. służbowe urządzenia teleinformatyczne i oprogramowanie, nośniki, oraz zawarte na nich informacje.

7. Podmioty zewnętrzne realizujące zadania na rzecz Inspektoratu w momencie zakończenia okresu obowiązywania umowy lub zobowiązań z niej wynikających (np. gwarancja) mają obowiązek zwrócić wszystkie posiadane i udostępnione im do używania urządzenia teleinformatyczne i oprogramowanie, nośniki, oraz zawarte na nich informacje. Wymagane w tym zakresie zapisy należy zawrzeć w umowach z podmiotami zewnętrznymi.

8. Wymagania i zasady dotyczące zarządzania urządzeniami teleinformatycznymi i oprogramowaniem określają załączniki nr 4 oraz nr 10 do PBI.

§ 60. 1. Informacje klasyfikowane są przez ich właścicieli z uwzględnieniem wymagań prawnych i biznesowych.

2. Wymagania i zasady dotyczące klasyfikacji i oznaczania informacji określa załącznik nr 10 do PBI.

§ 61. 1. Nośniki informacji są chronione przed nieuprawnionym dostępem, zniszczeniem, utratą lub naruszeniem integralności zapisanych na nich informacji.

2. Nośniki informacji są nadzorowane, a nośniki wycofywane z użycia są skutecznie pozbawiane zapisanych na nich informacji lub poddawane niszczeniu w sposób uniemożliwiający odtworzenie zapisanych na tych nośnikach informacji.

3. Wymagania i zasady dotyczące postępowania z nośnikami informacji określają załączniki nr 4 oraz nr 10 do PBI.

Rozdział 22

[Kontrola dostępu]

§ 62. Celem stosowania zabezpieczenia jest ograniczenie dostępu do informacji i środków ich przetwarzania do uprawnionych użytkowników, zapobieganie nieuprawnionemu dostępowi do systemów i usług, zapewnienie rozliczalności działań, zapobieganie nieuprawnionemu dostępowi do systemów.

§ 63. 1. Kontrola dostępu jest zgodna z wymaganiami biznesowymi, prawnymi oraz wymaganiami bezpieczeństwa informacji przyjętymi dla systemu informacyjnego / systemu wspierającego.

2. Użytkownicy posiadają dostęp wyłącznie do tych sieci i usług, systemów, aplikacji oraz innych zasobów, do których zostały im nadane uprawnienia.

§ 64. 1. Wdrożony jest formalny proces zarządzania uprawnieniami, w tym uprawnieniami uprzywilejowanymi.

2. Przydzielanie praw uprzywilejowanego dostępu jest ograniczone wyłącznie do tych użytkowników i administratorów, którym jest to niezbędne do realizacji zadań służbowych i wynika to z zakresu ich zadań.

3. AMS i ASI regularnie przeglądają uprawnienia użytkowników i administratorów.

4. Uprawnienia są odbierane niezwłocznie po ustaniu zatrudnienia pracownika oraz zmieniane niezwłocznie, gdy zajdzie taka potrzeba.

5. Uprawnienia podmiotów zewnętrznych świadczących usługi na rzecz Inspektoratu są odbierane niezwłocznie po zakończeniu obowiązywania umowy, oraz przydzielane i dostosowywane w oparciu o udokumentowany zakres wykonywanych zadań.

6. Wymagania i zasady dotyczące zarządzania dostępem użytkowników określa załącznik nr 4 do PBI.

§ 65. 1. Użytkownicy mają określoną odpowiedzialność dotyczącą obowiązku przestrzegania przyjętych w danym systemie informacyjnym/wspierającym zasad stosowania informacji uwierzytelniających z uwzględnieniem wymagań określonych w niniejszej PBI.

2. Wymagania i zasady dotyczące informacji uwierzytelniających określa załącznik nr 4 do PBI.

§ 66. 1. Dostęp do informacji oraz funkcji systemu informacyjnego / wspierającego jest ograniczany do zakresu, który jest niezbędny do realizacji zadań służbowych i wynika z zakresu zadań pracownika / podmiotu zewnętrznego / innego użytkownika.

2. Każdy użytkownik ma obowiązek przestrzegania przyjętych w danym systemie teleinformatycznym zasad bezpiecznego logowania z uwzględnieniem wymagań określonych w niniejszej PBI.

3. Systemy informacyjne/wspierające zapewniają stosowanie haseł wysokiej jakości z uwzględnieniem wymagań określonych w PBI.

4. Specjalistyczne programy narzędziowe, w szczególności mogące posłużyć do nieuprawnionego testowania zabezpieczeń, podlegają w zakresie ich instalacji i eksploatacji odpowiedniemu nadzorowi z uwzględnieniem wymagań określonych w niniejszej PBI.

5. Dostęp do kodu źródłowego oprogramowania jest ograniczany do pracowników i podmiotów zewnętrznych, którym jest to niezbędne do wykonywania zadań służbowych lub realizacji zadań na rzecz Inspektoratu.

6. Wymagania i zasady dotyczące kontroli dostępu do systemów określa załącznik nr 4 do PBI.

Rozdział 23

[Kryptografia]

§ 67. Celem stosowania zabezpieczenia jest zapewnienie poufności, autentyczności i integralności informacji.

§ 68. 1. Stosowanie zabezpieczeń kryptograficznych w systemach informacyjnych/ wspierających wymaga udokumentowania zasad i warunków stosowania tych zabezpieczeń, z uwzględnieniem kwestii związanych z procesem zarządzania kluczami kryptograficznymi i certyfikatami.

2. Wymagania i zasady dotyczące stosowania zabezpieczeń kryptograficznych określa załącznik nr 4 do PBI.

§ 69. 1. Jeżeli z charakteru informacji wynika potrzeba ochrony ich poufności, autentyczności i integralności (informacje wrażliwe, informacje prawnie chronione m.in. dane osobowe), informacje takie podlegają ochronie przed nieuprawnionym dostępem do nich stosując dostępne mechanizmy szyfrowania.

2. Wymagania i zasady dotyczące szyfrowania informacji określa załącznik nr 4 do PBI.

Rozdział 24

[Bezpieczeństwo fizyczne i środowiskowe]

§ 70. Celem stosowania zabezpieczenia jest zapobieganie nieuprawnionemu fizycznemu dostępowi do informacji, zapobieganie ich utracie lub naruszeniu integralności.

§ 71. 1. Obszary, w których przetwarzane są informacje oraz umieszczone środki ich przetwarzania są określone.

2. Dostęp do obszarów przetwarzania informacji podlega ochronie przed nieuprawnionym dostępem poprzez stosowanie m.in. środków ochrony budowlano-mechanicznych, elektronicznych oraz organizacyjnych.

3. Obiekty i pomieszczenia są objęte fizycznymi zabezpieczeniami uwzględniającymi m.in. ograniczenie publicznego dostępu do nich, ograniczenie do minimum informacji dotyczących przeznaczenia obiektów, pomieszczeń i przetwarzanych w nich informacji, a także zastosowanie zabezpieczeń przed podglądem i podsłuchem informacji.

4. Praca w obszarach chronionych może być wykonywana przez uprawnionych do tego pracowników oraz personel podmiotów zewnętrznych, którym takie uprawnienia przyznano. Przez uprawnienie należy rozumieć prawa dostępu do obszarów chronionych określone uprawnieniami w systemie elektronicznej kontroli dostępu lub zdefiniowane w wewnętrznych regulacjach dla danego obiektu.

5. Przebywanie osób nieuprawnionych w pomieszczeniach chronionych podlega ograniczeniu i nadzorowaniu.

6. Dobór zabezpieczeń fizycznych jest realizowany w oparciu o udokumentowane szacowanie ryzyka, zidentyfikowane potrzeby biznesowe oraz wymagania prawne związane z ochroną poszczególnych kategorii informacji. Dobór zabezpieczeń powinien również uwzględniać wymagania i ograniczenia wynikające z otoczenia.

7. Wymagania i zasady dotyczące bezpieczeństwa fizycznego określa załącznik nr 3 do PBI.

§ 72. 1. Rozmieszczenie urządzeń teleinformatycznych jest planowane w taki sposób, aby możliwa była jego ochrona przed nieuprawnionym dostępem oraz wpływem zagrożeń środowiskowych.

2. Urządzenia teleinformatyczne są chronione przed skutkami awarii systemów technicznych (np.: zasilania w energię, klimatyzacji, kontroli warunków środowiskowych, kontroli dostępu).

3. Okablowanie zasilające oraz teleinformatyczne przenoszące dane są planowane i instalowane tak, aby możliwe było zapewnienie im ochrony przed uszkodzeniem lub zniszczeniem oraz nieuprawnionym podłączaniem urządzeń do sieci.

4. Urządzenia teleinformatyczne podlegają serwisowi i przeglądom konserwacyjnym zgodnie z zaleceniami ich producentów.

5. Urządzenia teleinformatyczne mogą być wynoszone poza siedzibę tylko po spełnieniu wymagań w zakresie bezpieczeństwa informacji i uzyskaniu zgody przełożonego lub osoby

odpowiedzialnej za dane urządzenie, zgodnie z właściwymi regulacjami wewnętrznymi, m.in. obowiązującym Regulaminem pracy w Inspektoracie.

6. Urządzenia teleinformatyczne wynoszone poza siedzibę są zabezpieczone przed wystąpieniem zagrożeń fizycznych i środowiskowych m.in. poprzez stosowanie plecaków, futerałów itp. przeznaczonych do transportowania.

7. Przed zbyciem lub przekazaniem urządzeń teleinformatycznych do ponownego użycia nośniki danych są sprawdzane pod kątem prawidłowego usunięcia lub nadpisania zapisanych na nich informacji lub nośniki te muszą pozostać w Inspektoracie bez możliwości ich zbycia.

8. Użytkownicy urządzeń teleinformatycznych mają obowiązek zapewnienia właściwej ochrony tych urządzeń zgodnie z wymaganiami i zasadami określonymi w niniejszej PBI oraz innych regulacjach wewnętrznych obowiązujących w Inspektoracie.

9. Wymagania i zasady dotyczące ochrony fizycznej i środowiskowej urządzeń teleinformatycznych określają załączniki nr 3 i nr 4 do PBI.

Rozdział 25

[Bezpieczna eksploatacja]

§ 73. Celem stosowania zabezpieczenia jest zapewnienie bezpiecznej eksploatacji środków przetwarzania informacji, ochrona przed szkodliwym oprogramowaniem, ochrona przed utratą danych, rejestrowanie i gromadzenie materiałów dowodowych, zapobieganie wykorzystaniu technicznych podatności oraz minimalizacja wpływu audytu na funkcjonowanie systemów informacyjnych / wspierających.

§ 74. 1. Działania eksploatacyjne podlegają udokumentowaniu m.in. w planach, procedurach i instrukcjach, które są dostępne tylko uprawnionym użytkownikom i administratorom. Wykonywanie procedur jest dokumentowane.

2. Zmiany w procesach biznesowych, środkach przetwarzania informacji i systemach informacyjnych / wspierających, w szczególności mające wpływ na bezpieczeństwo informacji podlegają nadzorowi w formalnym i udokumentowanym procesie zarządzania zmianą.

3. Wykorzystanie systemów informacyjnych / wspierających jest monitorowane, również w zakresie ich wydajności i pojemności, wraz z dbałością o odpowiednie zasoby sprzętowe (np. pojemość pamięci masowej, przepustowość sieci, wydajność infrastruktury serwerowej).

4. Środowiska rozwojowe, testowe i produkcyjne są rozdzielane w celu redukcji ryzyka związanego z nieuprawnionym dostępem lub zmianami w środowisku produkcyjnym.

5. Wymagania i zasady dotyczące dokumentacji systemów określa § 19 oraz załącznik nr 4 do PBI.

§ 75. 1. W celu ochrony przed działaniem szkodliwego oprogramowania obowiązkowo stosowane są zabezpieczenia techniczne i organizacyjne, których zadaniem jest wykrywanie i zapobieganie wystąpieniu i negatywnym skutkom działania szkodliwego oprogramowania.

2. Wymagania i zasady dotyczące ochrony przed złośliwym oprogramowaniem określa załącznik nr 4 do PBI.

§ 76. 1. Zapasowe kopie informacji, oprogramowania, systemów operacyjnych i konfiguracji są regularnie wykonywane i testowane pod względem możliwości ich wykorzystania i poprawnego odtworzenia.

2. Zakres i parametry kopii zapasowych m.in. RTO, RPO, retencja danych, ilość przechowywanych kopii zapasowych, okresy objęte kopiami zapasowymi ustalane są na podstawie istotności systemu informacyjnego / wspierającego, potrzeb biznesowych oraz przede wszystkim wymagań prawnych.

3. W przypadku, gdy system informacyjny / wspierający jest zintegrowany z innymi systemami, w tym systemami podmiotów zewnętrznych (jest klientem), uwzględniane są wymagania określone w dokumentacji dotyczącej integracji z tymi systemami.

4. Wymagania i zasady dotyczące kopii zapasowych określa załącznik nr 4 do PBI.

§ 77. 1. Dzienniki zdarzeń rejestrujące działania użytkowników i administratorów, usterki i awarie oraz zdarzenia związane z bezpieczeństwem informacji są tworzone, bezpiecznie przechowywane i systematycznie przeglądane.

2. Dzienniki zdarzeń są przechowywane przez okres wymagany przepisami prawa dotyczącymi danego zadania lub procesu biznesowego, lub okres wynikający z wymagań systemów zewnętrznych, a w przypadku braku takich wymagań przez okres co najmniej 2 lat od daty zarejestrowania zdarzenia.

3. W przypadku, gdy system informacyjny lub wspierający jest zintegrowany z innymi systemami, w tym systemami podmiotów zewnętrznych (jest klientem) uwzględniane są wymagania określone w dokumentacji dotyczącej integracji z tymi systemami.

4. Dzienniki zdarzeń i zawarte w nich informacje podlegają ochronie przed nieuprawnionym dostępem, modyfikacją lub usunięciem. Dostęp do dzienników zdarzeń jest rejestrowany i ograniczony wyłącznie do pracowników oraz personelu podmiotów

zewnętrznych, których zadania dotyczą administrowania systemem informacyjnym/ wspierającym.

5. Zegary urządzeń i systemów operacyjnych są synchronizowane z wzorcowym źródłem czasu.

6. Wymagania i zasady dotyczące rejestrowania zdarzeń oraz monitorowania określa załącznik nr 4 do PBI.

§ 78. 1. Sprawowany jest nadzór nad wykorzystywanym oprogramowaniem.

2. Uprawnienia do instalacji i modyfikacji, zmian jego konfiguracji oraz odinstalowywania oprogramowania posiadają wyłącznie użytkownicy uprzywilejowani realizujący zadania w tym zakresie wynikające z zakresu ich obowiązków. Standardowy użytkownik ma odebraną możliwość samodzielnego dokonywania zmian w jakimkolwiek oprogramowaniu, w szczególności obejmującym zabezpieczenia i ich konfigurację.

3. Wymagania i zasady dotyczące nadzoru nad oprogramowaniem określa załącznik nr 4 do PBI.

§ 79. 1. Informacje o podatnościach technicznych eksploatowanych urządzeń i oprogramowania są monitorowane i analizowane pod względem możliwości wykorzystania ujawnionych podatności do naruszenia bezpieczeństwa informacji.

2. Dla podatności, których ryzyko wykorzystania lub potencjalne skutki wykorzystania są wysokie niezwłocznie podejmowane są działania zapobiegawcze.

3. Nieujawnione wcześniej podatności są zgłaszane, oraz podejmowane są działania zapobiegawcze rekomendowane w celu ograniczenia ryzyka ich wykorzystania.

4. Wymagania i zasady dotyczące zarządzania podatnościami technicznymi określa załącznik nr 4 do PBI.

§ 80. 1. Wymagania audytu oraz działania obejmujące weryfikację systemów są starannie planowane i uzgadniane w celu zminimalizowania ryzyka wystąpienia zakłóceń w działaniu systemów informacyjnych / wspierających lub ryzyka naruszenia bezpieczeństwa informacji przetwarzanych w tych systemach.

2. Audyt wewnętrzny w systemach informacyjnych / wspierających jest przeprowadzany nie rzadziej niż raz do roku na podstawie planów audytu wewnętrznego na dany rok.

3. Audyt wewnętrzny jest prowadzony w oparciu o przepisy prawa oraz obowiązujące w Inspektoracie regulacje wewnętrzne, m.in. Księgę Procedur Audytu.

Rozdział 26

[Bezpieczeństwo komunikacji]

§ 81. Celem stosowania zabezpieczenia jest zapewnienie ochrony informacji przesyłanych w sieciach i innych środkach przetwarzania informacji w komunikacji wewnątrz Inspektoratu, jak i na zewnątrz.

§ 82. 1. W celu ochrony informacji, sieci teleinformatyczne są zarządzane, nadzorowane a ich wykorzystanie jest monitorowane.

2. W umowach dotyczących sieci teleinformatycznych zawierane są zidentyfikowane zabezpieczenia, parametry dotyczące świadczenia usług i wymagania dotyczące zarządzania, nadzoru i monitorowania.

3. Wdrożona jest separacja sieci, systemów, usług i użytkowników.

4. Stosowane są zabezpieczenia fizyczne w celu zapewnienia ochrony urządzeniom sieciowym i okablowaniu.

5. Wymagania i zasady dotyczące bezpieczeństwa sieci teleinformatycznych określa załącznik nr 4 do PBI.

§ 83. 1. Określono obowiązek stosowania zapisów polityk, procedur i zasad przesyłania i zabezpieczania informacji w celu ochrony informacji przesyłanych przy użyciu wszystkich rodzajów środków łączności.

2. Bezpieczne przesyłanie informacji w relacjach z podmiotami zewnętrznymi jest uwzględniane we właściwych umowach i porozumieniach.

3. Informacje kluczowe z punktu widzenia ich bezpieczeństwa są przekazywane w zabezpieczonej formie (np. zaszyfrowana wiadomość, wiadomość zawierająca zaszyfrowany załącznik).

4. Wymagania odnoszące się do umów o zachowaniu poufności są regularnie przeglądane w sposób odzwierciedlający potrzeby Inspektoratu w zakresie ochrony informacji, w tym wynikające z obowiązujących przepisów prawa.

5. Wymagania i zasady dotyczące bezpieczeństwa przesyłania informacji określa załącznik nr 4 do PBI.

Rozdział 27

[Pozyskiwanie, rozwój i utrzymanie systemów]

§ 84. Celem stosowania zabezpieczenia jest zapewnienie, że bezpieczeństwo informacji będzie uwzględniane w całym cyklu życia systemów.

§ 85. 1. Wymagania dotyczące bezpieczeństwa informacji są włączane do wymagań stawianych nowym i rozbudowywanym systemom informacyjnym/wspierającym, w tym poprzez zapewnienie odpowiedniego procesu wytwórczego oraz zarządzania zmianami.

2. Informacje przesyłane w sieciach publicznych są zabezpieczane przed ich nieuprawnionym podglądem lub modyfikacją.

3. Informacje przetwarzane w systemach informacyjnych/wspierających są chronione m.in. poprzez stosowanie odpowiednich zabezpieczeń zarówno na poziomie serwerów, baz danych jak i logiki biznesowej.

4. Wymagania i zasady dotyczące projektowania bezpiecznych systemów określają załączniki nr 4 i nr 7 do PBI.

§ 86. 1. Wymagania i zasady bezpieczeństwa dotyczące rozwoju systemów są stosowane z uwzględnieniem potrzeb biznesowych i przeznaczenia budowanych lub rozwijanych komponentów oprogramowania.

2. Zmiany w systemach są nadzorowane podczas całego cyklu ich życia, przy użyciu procedur kontroli zmian oraz w oparciu o wdrożone środki techniczne.

3. Zmiany w systemach są testowane, w tym pod kątem funkcjonalności i bezpieczeństwa, przed ich wprowadzeniem na środowiska produkcyjne.

4. Modyfikacje oprogramowania są ograniczane do zmian uzasadnionych i niezbędnych, a wszystkie zmiany ściśle nadzorowane w ramach procesu zarządzania zmianą.

5. Systemy informacyjne/wspierające posiadają odpowiednio skonfigurowane i chronione środowiska przeznaczone do rozwoju oraz integracji.

6. Prace rozwojowe zlecane podmiotom zewnętrznym są nadzorowane i monitorowane.

7. Plany testów obejmujące przeprowadzanie, w zależności od zidentyfikowanych potrzeb m.in. testów akceptacyjnych, wydajnościowych, regresji czy bezpieczeństwa są ustalane.

8. Wymagania i zasady dotyczące projektowania bezpiecznych systemów określają załączniki nr 4 i nr 7 do PBI.

§ 87. 1. Dane testowe są starannie przygotowywane, aby były poprawne merytorycznie.

2. W przypadku wykorzystywania danych rzeczywistych, tym danym zapewnia się bezpieczeństwo np. poprzez ich anonimizację lub pseudonimizację, przy czym unika się wykorzystywania danych rzeczywistych do testowania, jeżeli nie jest to uzasadnione i konieczne.

3. W przypadku wykorzystywania danych rzeczywistych do testowania, opracowuje się udokumentowaną procedurę anonimizacji lub pseudonimizacji, określającą szczegółowo m.in. odpowiedzialność za jej wykonanie, sposób w jaki proces będzie realizowany i w jaki sposób zostanie zapewnione bezpieczeństwo danych rzeczywistych.

4. Wymagania i zasady dotyczące danych testowych określa załącznik nr 4 do PBI.

Rozdział 28

[Relacje z podmiotami zewnętrznymi]

§ 88. Celem stosowania zabezpieczenia jest zapewnienie bezpieczeństwa informacji w relacjach z dostawcami, utrzymanie uzgodnionego poziomu bezpieczeństwa informacji oraz jakości usług objętych umowami.

§ 89. 1. Wymagania w zakresie bezpieczeństwa informacji w relacjach z podmiotami zewnętrznymi są określane i dokumentowane w umowach. Wymagania te obejmują m.in.:

1) zasady dostępu do informacji;
2) zasady dostępu do systemów;
3) ograniczenia w takim dostępie;
4) dodatkowe zabezpieczenia w tym zakresie, jeżeli są wymagane.

2. Wymagania bezpieczeństwa informacji są określane indywidualnie w umowach z podmiotami zewnętrznymi, którzy mają uzyskać dostęp do informacji i środków ich przetwarzania.

3. W przypadku przetwarzania danych osobowych uwzględniane są odpowiednie wymagania z tym związane, w szczególności w umowach powierzenia przetwarzania danych osobowych.

4. W umowach z podmiotami zewnętrznymi są uwzględniane wymagania odnoszące się do ryzyka w bezpieczeństwie informacji związanego z usługami technologii informacyjnych i telekomunikacyjnych oraz łańcuchem dostaw produktów.

5. W umowach z dostawcami są uwzględniane parametry dotyczące świadczenia usług m.in. czasy reakcji, czasy naprawy, parametry dotyczące ciągłości działania, parametry jakościowe usług.

6. W umowach z dostawcami są uwzględniane wymagania związane z obsługą incydentów bezpieczeństwa informacji, incydentów cyberbezpieczeństwa oraz naruszeń ochrony danych osobowych wynikające z przepisów prawa w taki sposób, aby po stronie Inspektoratu możliwe było spełnienie wymagań prawnych w tym zakresie.

7. Wymagania i zasady dotyczące bezpieczeństwa informacji w relacjach z podmiotami zewnętrznymi określa załącznik nr 8 do PBI.

§ 90. 1. Usługi świadczone przez podmioty zewnętrzne są monitorowane oraz weryfikowane pod kątem spełnienia warunków określonych w umowach z tymi podmiotami.

2. Wymagania i zasady dotyczące zarządzaniem usługami świadczonymi przez podmioty zewnętrzne określa załącznik nr 8 do PBI.

Rozdział 29

[Zarządzanie incydentami]

§ 91. 1. Celem stosowania zabezpieczenia jest zapewnienie skutecznego reagowania na incydenty oraz informowanie o zdarzeniach i słabościach.

2. PBI określa odpowiedzialność oraz procedury zapewniające szybką, skuteczną i zorganizowaną reakcję na zdarzenia związane z bezpieczeństwem informacji.

3. Zgłaszanie zdarzeń dotyczących bezpieczeństwa informacji jest realizowane przez dedykowane do tego celu kanały komunikacyjne, zapewniające szybkie i skuteczne przekazanie informacji.

4. Pracownicy oraz osoby lub podmioty zewnętrzne realizujące zadania na rzecz Inspektoratu są zobowiązani do zgłaszania wszelkich zdarzeń mających lub mogących wpływać na bezpieczeństwo informacji, jak również zaobserwowanych lub podejrzewanych słabości związanych z bezpieczeństwem informacji, w tym podatności w systemach.

5. Zdarzenia związane z bezpieczeństwem informacji są analizowane i w uzasadnionych przypadkach kwalifikowane, jako incydenty związane z bezpieczeństwem informacji, incydenty cyberbezpieczeństwa lub naruszenia ochrony danych osobowych oraz w odpowiedni sposób obsługiwane.

6. Analizy incydentów są wykorzystywane do zminimalizowania prawdopodobieństwa wystąpienia przyszłych incydentów bezpieczeństwa informacji i ograniczenia ich skutków.

7. Wymagania i zasady dotyczące zarządzania incydentami określa załącznik nr 6 do PBI.

Rozdział 30

[Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania]

§ 92. Celem stosowania zabezpieczenia jest zapewnienie ciągłości działania Inspektoratu, realizowanych zadań publicznych, procesów biznesowych, systemów informacyjnych/ wspierających, oraz zapewnienie ciągłości dostępu do informacji.

§ 93. 1. Wymagania dotyczące bezpieczeństwa informacji i ciągłości zarządzania bezpieczeństwem w sytuacjach kryzysowych lub podczas katastrof i wrogich ataków opracowywane są dla każdego systemu informacyjnego/wspierającego. Wymagania te określają:

1) dopuszczalny czas nieplanowanej niedostępności;
2) zasady powiadamiania o sytuacjach nadzwyczajnych, w tym czas od wystąpienia zdarzenia do powiadomienia;
3) maksymalny dopuszczalny czas przywrócenia działania lub dostępu do informacji;
4) czas potrzebny na odtworzenie z kopii zapasowych, w przypadku wystąpienia takiej konieczności.

2. Dla systemów opracowywane są plany, procedury i wdrażane zabezpieczenia, wymagane dla zapewnienia ciągłości bezpieczeństwa informacji w sytuacjach kryzysowych, w tym w zakresie środowiskowym i fizycznym, ze szczególnym uwzględnieniem obszaru kopii zapasowych, przełączenia między ośrodkami (jeżeli dotyczy), procedur odtworzeniowych.

3. Wdrożone zabezpieczenia dla ciągłości bezpieczeństwa informacji są regularnie weryfikowane podczas audytów wewnętrznych i testów.

4. Wymagania i zasady dotyczące utrzymania ciągłości działania określa załącznik nr 5 do PBI.

§ 94. 1. W celu spełnienia wymagań w zakresie dostępności, środki przetwarzania informacji są wdrażane z uwzględnieniem wymogu nadmiarowości.

2. Wymagania i zasady dotyczące projektowania bezpiecznych systemów określa załącznik nr 4 i nr 7 do PBI.

Rozdział 31

[Zgodność]

§ 95. Celem stosowania zabezpieczenia jest unikanie naruszania przepisów prawa i innych regulacji dotyczących bezpieczeństwa informacji oraz zapewnienie wdrożenia i stosowania zasad bezpieczeństwa informacji.

§ 96. 1. W dokumentacjach systemów informacyjnych / wspierających zawarte i aktualizowane są wszystkie istotne wymagania prawne i umowne oraz weryfikowane jest na bieżąco podejście do ich przestrzegania. Dotyczy to zarówno przepisów obowiązującego prawa, jak również wytycznych wynikających z innych dokumentów, takich jak normy i standardy z zakresu bezpieczeństwa informacji.

2. W zakresie praw własności intelektualnej i użytkowania prawnie zastrzeżonego oprogramowania dozwolone jest przetwarzanie tylko w zgodzie z poszanowaniem tych praw oraz przepisów obowiązującego prawa.

3. Informacje istotne dla zapewnienia bezpieczeństwa informacji podlegają ochronione przed nieuprawnionym dostępem i zmianą, utratą lub zniszczeniem.

4. Zapewnia się prywatność i ochronę danych identyfikujących osoby fizyczne, ze szczególnym uwzględnieniem przepisów prawa dotyczących ochrony danych osobowych.

§ 97. 1. Podejście do zarządzania bezpieczeństwem informacji oraz jego wdrożenie są poddawane przeglądowi w zaplanowanych odstępach czasu lub wtedy, gdy następują istotne zmiany. Przeglądy dokonywane są nie rzadziej, niż raz w roku.

2. Przeglądy zarządzania bezpieczeństwem informacji są realizowane na zasadach określonych w części I PBI.

3. Właściciele biznesowi systemów informacyjnych/właściciele systemów wspierających regularnie dokonują przeglądów zgodności tych systemów z ich politykami bezpieczeństwa, standardami i wymaganiami prawnymi dotyczącymi bezpieczeństwa informacji. W tym celu mogą wykorzystać:

1) metodyki i ankiety dotyczące kontroli i audytu systemów;
2) formularz oceny spełniania obowiązków wynikających z RODO oraz ustawy o ochronie danych osobowych dostępne na portalu GOV.PL.

Rozdział 32

[Załączniki do PBI]

§ 98. Załączniki do PBI stanowią jej integralną część.

Załącznik nr 1 do Polityki Bezpieczeństwa Informacji
Głównego Inspektoratu Transportu Drogowego

Oświadczenie o zapoznaniu i zobowiązanie do przestrzegania zasad ochrony informacji określonych Polityką Bezpieczeństwa Informacji Głównego Inspektoratu Transportu Drogowego

Niniejszym oświadczam, że *zapoznałam / zapoznałem** się z wymaganiami i zasadami opisanymi w Polityce Bezpieczeństwa Informacji Głównego Inspektoratu Transportu Drogowego dotyczącymi ochrony informacji, w tym danych osobowych i zobowiązuję się do ich przestrzegania.

Zobowiązuję się do ochrony informacji, w szczególności informacji prawnie chronionych, w tym danych osobowych przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz ich przypadkową utratą, zniszczeniem lub uszkodzeniem, a także do nieujawniania sposobów zabezpieczenia tych informacji, w tym danych osobowych zarówno w trakcie wykonywania zadań służbowych, jak i po ich zakończeniu.

Oświadczam, że bez upoważnienia nie będę *wykorzystywała / wykorzystywał** informacji, w tym danych osobowych przetwarzanych w zbiorach danych osobowych prowadzonych przez Głównego Inspektora Transportu Drogowego, powierzonych do przetwarzania Głównemu Inspektorowi Transportu Drogowego przez inne podmioty oraz zbiorach danych osobowych innych podmiotów, do których będę *miała / miał** dostęp w związku z wykonywaniem przeze mnie obowiązków służbowych.

Mam świadomość, że celem Polityki Bezpieczeństwa Informacji jest zapewnienie odpowiedniego poziomu bezpieczeństwa informacji, w tym danych osobowych, przetwarzanych w Głównym Inspektoracie Transportu Drogowego, a naruszenia zasad ochrony informacji mogą skutkować odpowiedzialnością na zasadach i w trybie przewidzianym w przepisach prawa, w tym w ustawie z dnia 21 listopada 2008 r. o służbie cywilnej (Dz. U. z 2022 r. poz. 1691, z późn. zm.), ustawie z dnia 26 czerwca 1974 r. – Kodeks pracy (Dz. U. z 2022 r. poz. 1510, z późn. zm.), Rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781) oraz ustawie z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125, z późn. zm.).

…….. ……..
/miejsce i data złożenia oświadczenia/ /czytelny podpis pracownika/

* niepotrzebne skreślić

Załącznik nr 2 do Polityki Bezpieczeństwa Informacji
Głównego Inspektoratu Transportu Drogowego

Polityka Bezpieczeństwa Osobowego

§ 1. Przed zatrudnieniem

1. W procesie rekrutacji pracowników powinno się weryfikować:

1) tożsamość kandydata oraz poprawność podanych przez niego danych oraz zgody udzielone na ich przetwarzanie;
2) wykształcenie i kwalifikacje zawodowe, gdy jest to niezbędne do wykonywania pracy określonego rodzaju lub na określonym stanowisku, na podstawie złożonych dokumentów oraz np. rozmowy kwalifikacyjnej, testu weryfikującego wiedzę i kompetencje na określone stanowisko;
3) przebieg dotychczasowego zatrudnienia, gdy jest to niezbędne do wykonywania pracy określonego rodzaju lub na określonym stanowisku;
4) korzystanie z pełni praw publicznych oraz karalność za umyślne przestępstwo lub umyślne przestępstwo skarbowe, na podstawie złożonego oświadczenia;
5) gotowość do poddania się procedurze weryfikacji, zgodnie z zasadami określonymi w ustawie z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2023 r. poz. 756, z późn. zm.) w przypadku, gdy jest to niezbędne do wykonywania pracy określonego rodzaju lub na określonym stanowisku, na podstawie złożonego oświadczenia;
6) przebieg dotychczasowego zatrudnienia w Inspektoracie w przypadku zmiany zakresu obowiązków lub zmiany stanowiska/komórki organizacyjnej;
7) inne uzasadnione zakresem obowiązków i zadań na danym stanowisku informacje o kandydacie, w granicach i na podstawie obowiązującego prawa.

2. Dokumentacja z procesu rekrutacji winna być przechowywana i chroniona zgodnie z obowiązującymi przepisami prawa pracy oraz ochrony danych osobowych. Za właściwe przechowywanie dokumentacji odpowiadają pracownicy BDG – WKR.

3. Za właściwe i zgodne z przepisami prawa postępowanie z informacjami w ramach procesu rekrutacji odpowiadają wszyscy uczestnicy tego procesu, w szczególności członkowie komisji rekrutacyjnej.

§ 2. W trakcie zatrudnienia

1. Pracownik zobowiązany jest do przestrzegania postanowień m.in.:

1) przepisów prawa pracy, przepisów o służbie cywilnej, przepisów dotyczących bezpieczeństwa i higieny pracy, jak również przepisów dotyczących ochrony informacji oraz ochrony danych osobowych;
2) obowiązującego Regulaminu pracy w Inspektoracie oraz innych dokumentów regulujących zasady pracy (m.in. porozumienia ze związkami zawodowymi);
3) obowiązujących w Inspektoracie wymagań i zasad ochrony informacji, w tym danych osobowych określonych w PBI;
4) obowiązujących w Inspektoracie innych, niż wskazane w pkt 1 i 2 wewnętrznych regulacji, w tym polityk, planów, procedur, instrukcji oraz innych dokumentów odnoszących się do bezpieczeństwa informacji, w tym ochrony danych osobowych;
5) obowiązujących dokumentacji SZBI systemów, których jest użytkownikiem.

2. Pracownik może uzyskać dostęp do informacji i środków ich przetwarzania (m.in. dokumentów, nośników informacji, systemów, obiektów, stref dostępu, pomieszczeń, urządzeń teleinformatycznych itp.) po złożeniu oświadczenia potwierdzającego zapoznanie z obowiązującymi w Inspektoracie zasadami ochrony informacji, w tym danych osobowych.

3. Pracownik może uzyskać dostęp do danych osobowych wyłącznie po uzyskaniu upoważnienia do ich przetwarzania.

4. Pracownik może uzyskać dostęp do informacji, w tym danych osobowych wyłącznie w zakresie niezbędnym do realizacji zadań służbowych na danym stanowisku. Nieprawidłowe jest przyznawanie dostępu w zakresie nieadekwatnym do realizowanych zadań służbowych, w szczególności nadmiernych praw dostępu.

5. Bezpośredni przełożony pracownika ma obowiązek:

1) określić wymagania w zakresie dostępu do informacji oraz związaną z tym potrzebę uprawnień w systemach, niezbędne do wykonania zadań służbowych na danym stanowisku oraz złożyć wymagane w tym zakresie wnioski o przyznanie uprawnień, zgodnie z obowiązującymi procedurami;
2) określić wymagania w zakresie dostępu do obiektów, stref, pomieszczeń itp. i złożyć wymagane w tym zakresie wnioski o przyznanie uprawnień w systemach kontroli fizycznej do BDG lub innej komórki organizacyjnej właściwej dla danego obiektu, strefy, pomieszczenia itp.;
3) wprowadzić pracownika w obowiązki i odpowiedzialność związane z bezpieczeństwem informacji na danym stanowisku, w tym wynikające z pracy w systemach;

4) udzielać pracownikowi wytycznych i porad w zakresie bezpieczeństwa informacji związanych z wykonywaniem obowiązków służbowych na danym stanowisku pracy;
5) nadzorować i monitorować stosowanie przez pracownika zasad ochrony informacji, w tym danych osobowych w ramach wykonywanych przez tego pracownika zadań służbowych na danym stanowisku;
6) umożliwiać pracownikowi udział w szkoleniach, w szczególności z zakresu bezpieczeństwa informacji, cyberbezpieczeństwa oraz ochrony danych osobowych.

6. Właściciel biznesowy systemu informacyjnego / systemu wspierającego ma obowiązek:

1) wprowadzić pracownika w obowiązki i odpowiedzialność w zakresie zasad bezpiecznej eksploatacji systemu;
2) udzielić pracownikowi wytycznych w zakresie realizacji wymagań bezpieczeństwa systemu;
3) monitorować działania w systemie w odniesieniu do poufności, integralności i dostępności informacji z zapewnieniem atrybutów takich, jak rozliczalność, niezaprzeczalność, autentyczność i niezawodność.

7. IOD ma obowiązek zapewnić pracownikowi:

1) informację o obowiązkach spoczywających na pracowniku w związku z przetwarzaniem przez niego danych osobowych;
2) doradztwo w sprawach związanych ze stosowaniem zasad ochrony danych osobowych i realizacji obowiązków w tym zakresie;
3) działania zwiększające świadomość w zakresie ochrony danych osobowych;
4) szkolenia z zakresu ochrony danych osobowych;
5) wykonywanie wobec pracownika roli punktu kontaktowego we wszystkich sprawach związanych z przetwarzaniem jego danych osobowych oraz z wykonywaniem przysługujących mu z mocy przepisów prawa uprawnień.

8. Pełnomocnik do spraw bezpieczeństwa informacji ma obowiązek zapewnić pracownikowi:

1) szkolenia z zakresu bezpieczeństwa informacji;
2) działania zwiększające świadomość w zakresie bezpieczeństwa informacji.

§ 3. Zmiana zatrudnienia

1. W przypadku zmiany stanowiska w obrębie tej samej lub przeniesieniem do innej komórki organizacyjnej, dotychczasowy bezpośredni przełożony pracownika ma obowiązek:

1) zapewnić przejęcie akt spraw prowadzonych przez pracownika zmieniającego stanowisko, jeżeli zmiana wiąże się z zaprzestaniem realizacji dotychczas wykonywanych zadań służbowych;
2) złożyć wnioski o odebranie praw dostępu w systemach, jeżeli zmiana stanowiska wiąże się z zaprzestaniem realizacji dotychczas wykonywanych zadań służbowych w tej komórce organizacyjnej lub złożyć wnioski o zmianę praw dostępu w systemach, jeżeli zmiana stanowiska wiąże się ze zmianą zakresu dotychczas wykonywanych zadań służbowych w tej komórce organizacyjnej;
3) złożyć wnioski o odebranie praw dostępu do obiektów, stref, pomieszczeń itp. w zakresie, który był niezbędny do wykonywania zadań służbowych w tej komórce organizacyjnej lub na danym stanowisku, a nowy zakres zadań służbowych pracownika nie wymusza, aby pracownik takie prawa dostępu posiadał (nadmiarowe prawa dostępu należy odebrać).

2. W przypadku przeniesienia do innej komórki organizacyjnej nowy bezpośredni przełożony pracownika ma obowiązek:

1) złożyć wnioski o przyznanie praw dostępu w systemach, do których dostęp jest niezbędny do wykonywania zadań służbowych na danym stanowisku;
2) złożyć wnioski o przyznanie praw dostępu do innych, niż domyślne, obiektów, stref, pomieszczeń itp. do których dostęp jest niezbędny do wykonywania zadań służbowych na danym stanowisku.

3. W przypadku zmiany komórki organizacyjnej (w tym wydziału, zespołu itp.) prawa dostępu w systemach powinny zostać odebrane na podstawie wniosku dotychczasowego przełożonego pracownika, a następnie na nowo przydzielone na podstawie wniosku nowego przełożonego pracownika. Dopuszcza się zmianę praw dostępu z wyprzedzeniem, o ile systemy, których to dotyczy, umożliwiają konfigurację początku i końca obowiązywania poszczególnych praw dostępu dla wskazanej daty; w przeciwnym razie prawa dostępu powinny być konfigurowane na podstawie złożonych wniosków lub informacji z BDG – WKR w przypadkach, w których taka informacja jest przekazywana.

§ 4. Nieobecność pracownika

1. W sytuacji dłuższej nieobecności pracownika wynikającej z sytuacji planowanych lub nieplanowanych kierujący komórką organizacyjną, w której pracownik jest zatrudniony może zdecydować o czasowym zawieszeniu praw dostępu pracownika do systemów, obiektów, stref lub pomieszczeń. Zawieszenie uprawnień jest realizowane na podstawie wniosku kierowanego

przez tego kierującego komórką organizacyjną zgodnie z procedurą właściwą dla danego systemu lub obiektu.

2. Jeżeli nieobecność pracownika wynosi 30 i więcej dni, w przypadku systemów administrowanych przez BT, ASI mogą dokonać czasowego zablokowania dostępu do tych systemów na podstawie informacji przekazanej przez BDG – WKR.

§ 5. Zakończenie zatrudnienia

1. W przypadku zakończenia zatrudnienia przez pracownika, bezpośredni przełożony ma obowiązek zapewnić:

1) złożenie wniosków o odebranie uprawnień w systemach, do których pracownik posiadał dostęp;
2) złożenie wniosków o odebranie uprawnień dostępu do obiektów, stref, pomieszczeń, w szczególności nadanych w elektronicznych systemach kontroli dostępu;
3) rozliczenie pracownika z udostępnionego wyposażenia związanego z przetwarzaniem informacji (komputerów, telefonów, nośników danych itp.);
4) przejęcie akt spraw oraz innych dokumentów i nośników informacji będących w posiadaniu pracownika związanych z wykonywaniem zadań służbowych.

2. Uprawnienia w systemach oraz elektronicznych systemach kontroli dostępu należy odbierać niezwłocznie z chwilą ustania zatrudnienia, z zastrzeżeniem sytuacji, gdy pracownik kończący zatrudnienie nie świadczy pracy przed jego ustaniem. W takim przypadku należy rozważyć odebranie uprawnień, w szczególności w systemach już z chwilą ustania obowiązku świadczenia pracy (w tym również w przypadku rozpoczęcia urlopu (np. wykorzystanie zaległego urlopu)).

3. W przypadku zwolnienia pracownika z obowiązku świadczenia pracy (wypowiedzenie umowy o pracę z jednoczesnym zwolnieniem pracownika z obowiązku świadczenia pracy lub porozumienie pomiędzy pracodawcą i pracownikiem zwalniające czasowo tego drugiego z obowiązku świadczenia pracy), takiemu pracownikowi należy odebrać prawa dostępu do systemów (wypowiedzenie umowy o pracę) lub czasowo zawiesić (odebrać na określony czas, jeżeli system nie umożliwia ich czasowego zawieszenia) (porozumienie w sprawie czasowego zwolnienia z obowiązku świadczenia pracy) na okres określony pomiędzy pracodawcą i pracownikiem. Odebranie lub zawieszenie praw dostępu jest realizowane na podstawie wniosku kierowanego przez kierującego komórką organizacyjną zgodnie z procedurami właściwymi dla danego systemu.

4. Potwierdzenie zwrotu wyposażenia udostępnionego pracownikowi kończącemu zatrudnienie, w tym kart dostępu w elektronicznych systemach kontroli dostępu, kart mikroprocesorowych umożliwiających dostęp do systemów, telefonów oraz modemów i kart sim odbywa się zgodnie z wewnętrznymi procedurami obowiązującymi w Inspektoracie.

§ 6. Naruszenie zasad bezpieczeństwa i odpowiedzialność pracownika

1. Postępowanie wyjaśniające wobec pracownika naruszającego zasady bezpieczeństwa informacji, w tym ochrony danych osobowych jest prowadzone na podstawie obowiązujących przepisów prawa i regulacji obowiązujących w Inspektoracie w zakresie odpowiedzialności służbowej i dyscyplinarnej.

2. Postępowanie wyjaśniające powinno być prowadzone po skutecznej weryfikacji i potwierdzeniu, że faktycznie nastąpiło naruszenie bezpieczeństwa informacji, na podstawie zgromadzonego i zabezpieczonego materiału dowodowego.

3. W sytuacji wystąpienia incydentu bezpieczeństwa związanego z kontami pracownika w systemach lub elektronicznych systemach kontroli dostępu, może być wprowadzone zawieszenie lub odebranie praw dostępu jeżeli zachodzi podejrzenie, że dane konto zostało wykorzystane lub jest wykorzystywane do wykonywania działań niezgodnych z obowiązującymi przepisami prawa, w szczególności określonymi w art. 267 – 269b ustawy z dnia 6 czerwca 1997 r. – Kodeks karny.

4. Decyzję o zawieszeniu lub odebraniu praw dostępu podejmuje właściciel biznesowy systemu informacyjnego / właściciel systemu wspierającego, ewentualnie Dyrektor Generalny, Główny Inspektor lub jego Zastępcy, w tym na podstawie rekomendacji i wniosków z analizy incydentu m.in. dyrektora BT w odniesieniu do systemów, dyrektora BDG w odniesieniu do ochrony fizycznej, IOD, Pełnomocnika do spraw bezpieczeństwa informacji lub Pełnomocnika do spraw bezpieczeństwa cyberprzestrzeni.

5. Zawieszenie lub odebranie praw dostępu pracownikowi może być również wynikiem realizacji polecenia wydanego przez właściwe organy śledcze uprawnione do wydania takiej dyspozycji m.in. w związku z prowadzonymi czynnościami śledczymi.

§ 7. Uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji

1. Pełnomocnik do spraw bezpieczeństwa informacji przy wsparciu BDG – WDZ organizuje szkolenia wstępne i okresowe z zakresu bezpieczeństwa informacji dla wszystkich pracowników.

2. Szkolenia są prowadzone w formule e-learning z wykorzystaniem funkcjonującej w Inspektoracie wewnętrznej platformy szkoleniowej do szkoleń e-learning. Szkolenia kończą się testem, którego zaliczenie pozwala uzyskać certyfikat potwierdzający ukończenie szkolenia. Każdy pracownik jest zobowiązany do odbycia szkolenia wstępnego w ciągu miesiąca od rozpoczęcia pracy w Inspektoracie.

3. Każdy pracownik ma obowiązek odbycia szkolenia wstępnego i okresowego.

4. Szkolenia okresowe są organizowane co najmniej raz na 2 lata, w formule e-learning. Szkolenia kończą się testem, którego zaliczenie pozwala uzyskać certyfikat potwierdzający ukończenie szkolenia.

5. Dopuszcza się organizowanie szkoleń stacjonarnych, o ile warunki epidemiczne, lokalowe lub techniczne pozwalają na taką formę szkolenia.

6. Szkolenia, o których mowa w ust. 1 obejmują co najmniej:

1) zagrożenia bezpieczeństwa informacji;
2) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawną;
3) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzeń i oprogramowania minimalizującego ryzyko błędów ludzkich.

7. Dopuszcza się zastępowanie szkoleń okresowych organizowanych na wewnętrznej platformie szkoleniowej innymi szkoleniami, o ile obejmują one swoim zakresem co najmniej zagadnienia wskazane w ust. 6, mają udokumentowany zakres oraz udział w nich jest udokumentowany np. certyfikatem uczestnictwa. W szczególności dotyczy to szkoleń organizowanych przez inne organy administracji publicznej dla pracowników podmiotów krajowego systemu cyberbezpieczeństwa. Pełnomocnik do spraw bezpieczeństwa informacji we współpracy z BDG – WDZ określa szkolenia, które mogą być dopuszczone jako zaliczające szkolenia okresowe.

8. Szkolenia, o których mowa powyżej są dokumentowane.

§ 8. Uświadamianie, kształcenie i szkolenia z zakresu ochrony danych osobowych

1. IOD zapoznaje pracowników z przepisami prawa i zasadami ochrony danych osobowych obowiązującymi w Inspektoracie, przed uzyskaniem przez te osoby upoważnienia do przetwarzania danych osobowych. Zapoznanie to jest warunkiem niezbędnym do udzielenia pracownikowi upoważnienia do przetwarzania danych osobowych.

2. IOD przy wsparciu BDG – WDZ organizuje szkolenia z zakresu przepisów prawa i zasad ochrony danych osobowych dla wszystkich pracowników. Formułę szkolenia IOD ustala w porozumieniu z BDG – WDZ.

3. Szkolenia prowadzone w formule e-learning kończą się testem.

4. Każdy pracownik upoważniony do przetwarzania danych osobowych ma obowiązek odbycia szkolenia wstępnego w ciągu miesiąca od rozpoczęcia zatrudnienia. Szkolenie to jest uzupełnieniem zapoznania, o którym mowa w ust. 1.

5. Każdy pracownik upoważniony do przetwarzania danych osobowych ma obowiązek odbycia szkolenia okresowego.

6. Szkolenia okresowe są organizowane co najmniej raz na 2 lata – domyślnie w formule e-learning z wykorzystaniem wewnętrznej platformy szkoleniowej.

7. Dopuszcza się organizowanie szkoleń stacjonarnych lub online (wideokonferencja), o ile warunki epidemiczne, lokalowe lub techniczne pozwalają na taką formę szkolenia.

8. Szkolenia, o których mowa powyżej są dokumentowane.

Załącznik nr 3 do Polityki Bezpieczeństwa Informacji
Głównego Inspektoratu Transportu Drogowego

Polityka Bezpieczeństwa Fizycznego i Środowiskowego

§ 1. Organizacja bezpieczeństwa fizycznego i środowiskowego

1. Działaniami w zakresie bezpieczeństwa fizycznego i środowiskowego kierują:

1) komórka organizacyjna właściwa do spraw ochrony fizycznej;
2) podmiot właściwy do administrowania danym obiektem.

2. Komórka organizacyjna właściwa do spraw ochrony fizycznej powinna sprawować nadzór nad działaniami realizowanymi przez podmioty zewnętrzne realizujące usługi ochrony fizycznej obiektów.

3. W działaniach w zakresie bezpieczeństwa fizycznego i środowiskowego uczestniczą:

1) kierujący komórkami organizacyjnymi i bezpośredni przełożeni w zakresie nadzoru nad przestrzeganiem przez podległych pracowników zasad ochrony;
2) właściciele biznesowi systemów informacyjnych, właściciele systemów wspierających oraz właściciele informacji w zakresie określania potrzeb dotyczących ochrony systemów informacyjnych, systemów wspierających oraz informacji, w szczególności podlegających ochronie prawnej;
3) wszyscy pracownicy w zakresie przestrzegania i stosowania zasad ochrony;
4) podmioty zewnętrzne, jeżeli zakres ich zadań wymaga stosowania się do zasad ochrony fizycznej i środowiskowej lub ma wpływ na tą ochronę.

§ 2. Podstawowe środki i zasady bezpieczeństwa fizycznego i środowiskowego

1. Środki bezpieczeństwa fizycznego dotyczą:

1) rozmieszczenia i granic stref bezpieczeństwa;
2) konstrukcji budowlanych wyznaczających granice stref bezpieczeństwa;
3) sposobu zabezpieczenia wejścia do obiektu oraz do stref bezpieczeństwa;
4) stosowania bezpośredniej ochrony fizycznej;
5) stosowania systemu sygnalizacji napadu i włamania;
6) stosowania systemu monitoringu wizyjnego;
7) stosowania mechanicznych zabezpieczeń technicznych;
8) dostępu do obszarów bezpiecznych oraz wykonywanie prac w obszarach bezpiecznych.

2. Bezpieczeństwo środowiskowe obejmuje:

1) stosowanie urządzeń ochrony przeciwpożarowej;
2) zabezpieczenie przed zalaniem wodą;
3) zapewnienie właściwych warunków pracy w zakresie temperatury i wilgotności powietrza;
4) stosowanie środków ochrony odgromowej na liniach telekomunikacyjnych;
5) stosowanie zabezpieczeń przeciwprzepięciowych.

3. Stosowane środki bezpieczeństwa fizycznego i środowiskowego powinny wynikać z przeprowadzonego i udokumentowanego szacowania ryzyka/oceny skutków dla ochrony danych.

4. Szacowanie ryzyka i określanie wymagań bezpieczeństwa fizycznego i środowiskowego należy prowadzić z uwzględnieniem:

1) charakterystyki obiektu i pełnionych przez niego funkcji, w szczególności rodzaju umieszczonych w nim zasobów podlegających ochronie;
2) zidentyfikowanych kategorii potencjalnych zagrożeń;
3) opisu topografii, konstrukcji obiektu i architektury, najbliższego otoczenia (m.in. zabezpieczenia budowlane i mechaniczne, ogrodzenie, bramy, furty, oświetlenie, miejsca do parkowania, drogi komunikacyjne i ewakuacyjne, inne budowle i elementy towarzyszące);
4) dotychczas zaobserwowanych incydentów;
5) aktualnego stanu ochrony fizycznej i środowiskowej obiektu;
6) opisu i oceny funkcjonalności i poprawności zainstalowanych technicznych systemów bezpieczeństwa fizycznego i środowiskowego, ich poprawności eksploatacji oraz aktualnego stanu technicznego (m.in. poziom technologiczny, sprawność, dokumentacja, serwisowanie);
7) opisu stosowanych procedur i rozwiązań organizacyjnych;
8) wniosków dotyczących adekwatności, kompletności i poprawności zastosowanych zabezpieczeń określonych w wynikach kontroli i audytów;
9) propozycji doskonalenia systemów ochrony fizycznej i środowiskowej oraz procedur ochrony obiektu.

§ 3. Zapewnianie bezpieczeństwa fizycznego i środowiskowego

1. Kierownictwo oraz kierujący komórkami organizacyjnymi powinni określić podział powierzchni zajmowanych przez komórki organizacyjne na:

1) strefy ogólne, do których prawa dostępu mogą posiadać wszyscy pracownicy;
2) strefy ograniczonego dostępu / strefy szczególnie chronione, do których dostęp powinien być ograniczony do określonych pracowników / grup pracowników i/lub posiadać wyższy poziom zastosowanych zabezpieczeń;
3) strefy ogólnodostępne, do których dostęp mogą posiadać np. interesanci.

2. Ochrona stref ogólnych i stref szczególnie chronionych powinna być realizowana na zasadach określonych z uwzględnieniem:

1) przepisów o ochronie osób i mienia;
2) planów ochrony obiektów (jeżeli zostały opracowane);
3) innych planów ochrony, w szczególności obowiązującego POIN;
4) przepisów szczególnych np. ustawy o dokumentach publicznych.

3. Na granicy strefy ogólnej powinna odbywać się kontrola ruchu osobowego i materiałowego. Wejścia gości do strefy ogólnej należy rejestrować.

4. Strefa szczególnie chroniona powinna być ustalona w miarę istniejących możliwości na obszarze wydzielonym solidnymi konstrukcjami budowlanymi. Za solidne konstrukcje budowlane uznaje się takie, których ściany zewnętrzne i stropy budynków, w których zlokalizowane są strefy szczególnie chronione, posiadają klasę odporności włamaniowej równoważnej murowi o grubości 25 cm wykonanemu z pełnej cegły. Natomiast pomieszczenia w strefie szczególnie chronionej w miarę istniejących możliwości powinny mieć ściany o odporności włamaniowej równoważnej murowi o grubości 12,5 cm. Zasady organizacji bezpieczeństwa fizycznego Kancelarii Tajnej oraz innych stref i pomieszczeń objętych ochroną informacji niejawnych określają odrębne regulacje wewnętrzne i właściwe przepisy prawa.

5. Wszystkie osoby przebywające w strefie ogólnej powinny posiadać identyfikatory, które powinny być noszone w widocznym miejscu. Pracownicy posiadają identyfikatory zgodne z obowiązującymi w regulacjami wewnętrznymi dotyczącymi identyfikatorów pracowniczych. Wszystkim gościom powinny być wydawane identyfikatory z napisem „GOŚĆ”. Innym osobom, np. personelowi podmiotów zewnętrznych realizujących zadania w siedzibie Inspektoratu przez dłuższy okres mogą być wydane identyfikatory, które powinny zapewnić ich identyfikację co najmniej w zakresie nazwy podmiotu i imienia oraz nazwiska (ewentualne umieszczenie zdjęcia wymaga udzielenia dobrowolnej zgody).

6. Goście powinni móc poruszać się w obrębie strefy ogólnej wyłącznie w asyście pracownika odpowiedzialnego za ich przyjęcie. Pracownik ten przed wprowadzeniem gości do strefy ogólnej winien dopilnować pobrania przez nich w strefie ogólnodostępnej lub na stanowisku recepcyjnym identyfikatorów „GOŚĆ". Odstępstwa w tym zakresie dotyczą wyłącznie gości Kierownictwa i są szczegółowo opisane w POIN. Inne odstępstwa mogą być stosowane (np. w przypadku wydarzeń z dużą liczbą gości), o ile zapewni się kontrolę ruchu osobowego (np. na podstawie list gości).

7. W obiektach, w których odbywa się obsługa interesantów dopuszcza się wydzielenie z części strefy ogólnej strefy ogólnodostępnej, w której goście – interesanci mogą przebywać bez identyfikatorów. Strefa ogólnodostępna musi być oddzielona od pozostałych części strefy ogólnej przejściami zapewniającymi kontrolę ruchu osobowego (w sposób automatyczny lub manualny (organizacyjny).

8. W przypadku stosowania systemu kontroli dostępu dla obiektów i pomieszczeń, w których przetwarzane są informacje o średniej lub wysokiej wartości (wartość powinna być określona np. w analizie wpływu na biznes), powinien być to system zapewniający adekwatny do zidentyfikowanych zagrożeń poziom ochrony, np. 3 stopień wg PN–EN 60839–11–1 z zastrzeżeniem, że:

1) docelowe zabezpieczenia fizyczne oraz ich poziom / stopień powinny być określane indywidualnie dla każdego kontrolowanego przejścia biorąc pod uwagę jego otoczenie oraz już istniejące zabezpieczenia, jak również wymagania dotyczące m.in. konieczności kontroli i rejestrowania wejść i wyjść;
2) mogą występować odrębne wymagania w zakresie stosowania zabezpieczeń fizycznych wynikające w szczególności z przepisów prawa np. dotyczące ochrony dokumentów publicznych lub wymagań dostępu do rejestrów i ewidencji prowadzonych przez inne podmioty publiczne.

9. Wszystkie drzwi z kontrolą dostępu powinny być zaopatrzone w mechanizmy samozamykające.

10. Kontrolę ruchu osobowego i materiałowego na granicy strefy ogólnej może sprawować pracownik ze strefy ogólnodostępnej lub pracownik stanowiska recepcyjnego, który wydaje identyfikatory gościom, w tym pracownik zarządcy danego obiektu lub pracownik agencji ochrony. Wybór rozwiązania powinien uwzględniać warunki danego obiektu.

11. Pomieszczenia biurowe powinny posiadać zamki oraz drzwi o klasie odporności adekwatnej do miejsca ich użytkowania oraz zidentyfikowanych na etapie szacowania ryzyka zagrożeń (np. wg PN-EN 12209 dla zamków oraz PN-EN 14351-1+A2 lub PN-EN 1627:2021 dla drzwi), z uwzględnieniem dodatkowych wymagań wskazanych w ust. 8 pkt 2, jeżeli takie występują.

12. Wejścia oraz wyjścia ze stref szczególnie chronionych powinny być rejestrowane (kontrola obustronna realizowana w sposób automatyczny lub manualny (organizacyjny)). Ponadto rejestracji powinna podlegać tożsamość osób spoza Inspektoratu, ich cel pobytu oraz czas ich wejścia i wyjścia (np. pracownicy serwisu zewnętrznego, personel sprzątający).

§ 4. Zarządzanie kluczami

1. Klucze do pomieszczeń powinny być przechowywane:

1) na recepcji lub ochronie obiektu;
2) w dedykowanych do tego celu depozytorach;
3) w zamykanych szafach zapewniających ich odpowiednią ochronę;

przy czym powinna być zapewniona rozliczalność ich pobierania i zdawania w sposób automatyczny lub manualny (organizacyjny).

2. Fakt wydania kluczy i przyjęcia ich na przechowanie powinien być odnotowany w sposób automatyczny lub manualny (organizacyjny). Wykaz osób uprawnionych do pobierania kluczy powinien być prowadzony w formie papierowej lub w formie elektronicznej i okresowo weryfikowany np. co 6 lub 12 miesięcy. Rejestry, w tym elektroniczne dotyczące pobierania i zdawania kluczy powinny być weryfikowane w celu identyfikacji ewentualnych działań nieuprawnionych.

3. Za przyznanie i odebranie uprawnień do pobierania kluczy do konkretnego pomieszczenia odpowiedzialni są m.in.:

1) pracownicy komórki organizacyjnej właściwej do spraw ochrony fizycznej lub
2) pracownicy komórki organizacyjnej odpowiedzialnej za dane pomieszczenie lub obiekt lub
3) administratorzy obiektów na podstawie informacji przekazywanych przez pracowników komórki organizacyjnej właściwej do spraw ochrony fizycznej.

4. Klucze do szaf i mebli biurowych, w których przechowywane są dokumenty i nośniki zawierające informacje wrażliwe lub prawnie chronione, w tym dane osobowe, nie mogą

po zakończeniu pracy pozostawać w zamkach. Za bezpieczne przechowywanie kluczy do takich szaf i mebli biurowych odpowiadają pracownicy je użytkujący.

5. Zasady organizacji przechowywania kluczy do szaf, sejfów i mebli biurowych, w których przechowuje się informacje niejawne określają odrębne regulacje.

§ 5. Zarządzanie uprawnieniami w systemach kontroli dostępu

1. W przypadku zastosowania systemu kontroli dostępu uprawnienia powinny być jednoznacznie powiązane z kartami aktywującymi przejście, które mogą również pełnić role identyfikatorów.

2. Wstęp do poszczególnych obiektów, stref i pomieszczeń powinien być ograniczony tylko do tych osób, które mają uzasadnioną i wynikającą z realizowanych zadań służbowych potrzebę w nich przebywania, na podstawie stosownych praw dostępu.

3. Prawa dostępu do obiektów, stref i pomieszczeń powinny być przyznawane zgodne z zakresem odpowiedzialności i uprawnień na danym stanowisku. Prawa dostępu powinny być nadawane wyłącznie w zakresie wynikającym z zajmowanego stanowiska i potrzebą wykonywania zadań służbowych na danym stanowisku pracy. Bezpodstawne nadawanie uprawnień do obiektów, stref i pomieszczeń jest kwalifikowane jako incydent związany z naruszeniem bezpieczeństwa informacji.

4. Za przyznawanie, zmianę oraz odbieranie uprawnień dostępu w systemach kontroli dostępu odpowiedzialni są m.in.:

1) pracownicy komórki organizacyjnej właściwej do spraw ochrony fizycznej lub
2) pracownicy komórki organizacyjnej odpowiedzialnej za dane pomieszczenie lub obiekt lub
3) administratorzy obiektów na podstawie informacji przekazywanych przez pracowników komórki organizacyjnej właściwej do spraw ochrony fizycznej.

6. Prawa dostępu należy bezzwłocznie zablokować w przypadku zgłoszenia przez pracownika lub jego bezpośredniego przełożonego utraty lub podejrzenia utraty karty – dla tej karty. Przywrócenie praw dostępu powinno nastąpić dopiero po weryfikacji, że nie będzie to stanowiło zagrożenia dla bezpieczeństwa informacji.

7. Prawa dostępu należy okresowo przeglądać na zasadach określonych w PBI.

§ 6. Pomieszczenia i zasoby chronione

1. Wnoszenie i wynoszenie do i ze stref szczególnie chronionych komputerowych nośników danych powinno mieć miejsce tylko w przypadkach wynikających z procedur

eksploatacji zainstalowanego tam sprzętu teleinformatycznego lub z wykonywanych zadań służbowych (np. nośnik w aktach sprawy).

2. Dla stref lub pomieszczeń szczególnie chronionych należy rozważyć stosowanie systemów sygnalizacji włamania i napadu.

3. W uzasadnionych przypadkach, zarówno strefy ogólnodostępne, strefy ogólne jak i strefy szczególnie chronione powinny być poddane monitoringowi wizyjnemu.

4. Strefy szczególnie chronione nie powinny posiadać oznakowania wewnątrz lub na zewnątrz, które wskazywałyby na to, że znajdują się w nich szczególnie chronione zasoby. Nie dotyczy to oznaczenia stref określonych w POIN.

5. W strefach szczególnie chronionych przebywanie osób bez uprawnień dostępu do tych stref powinno odbywać się tylko w wyjątkowych przypadkach uzasadnionych np. koniecznością wykonania określonych prac i obowiązkowo pod nadzorem pracownika uprawnionego do przebywania.

6. Pobyt osoby, która nie posiada uprawnień do przebywania w strefie szczególnie chronionej podlega zarejestrowaniu zgodnie z rozwiązaniem przyjętym w danej strefie. Za odnotowanie odpowiedzialne są osoby uprawnione do przebywania w danej strefie wprowadzające osobę nieuprawnioną.

7. Należy w ramach szacowania ryzyka rozważyć umieszczenie infrastruktury systemów informacyjnych lub wspierających obejmującej m.in. serwery, urządzenia sieci teleinformatycznych, centrale telefoniczne, systemy kopii zapasowych, systemy przechowywania danych w strefach szczególnie chronionych lub strefach ogólnych o podwyższonym standardzie zabezpieczeń określonym na podstawie wyników tego szacowania.

8. Urządzenia teleinformatyczne należy zabezpieczać przed pożarem i zalaniem, przy uwzględnieniu istniejących warunków środowiskowych i związanych z nimi zagrożeń.

9. Rozmieszczenie infrastruktury systemów informacyjnych / wspierających powinno być poprzedzone udokumentowanym szacowaniem ryzyka uwzględniającego istniejące zabezpieczenia lub wymóg stosowania zabezpieczeń technicznych oraz systemów wspomagających (m.in. wentylacyjno-klimatyzacyjnych, awaryjnego zasilania i podtrzymania zasilania) oraz istniejące instalacje m.in. wodno-kanalizacyjne, grzewcze.

§ 7. Bezpieczeństwo środowiskowe

1. Przy planowaniu zabezpieczeń technicznych i organizacyjnych, ich rodzaju i siły, należy brać pod uwagę ryzyka związane z występującymi lokalnie zagrożeniami, takimi jak pożar, zalanie, trzęsienie ziemi, wybuch, wyładowania atmosferyczne, niepokoje społeczne i inne formy naturalnych lub spowodowanych przez działania umyślne bądź błędy człowieka katastrof. Ponadto analizie należy poddawać wpływ otoczenia, m.in. innych obiektów lub lokalnych instalacji i dróg (np. pożar w sąsiednim budynku, woda przeciekająca przez dach, powódź, bliska katastrofa komunikacyjna, eksplozja, zamieszki uliczne).

2. Pomieszczenia, w których zlokalizowane są systemy informacyjne/wspierające dla ciągłości realizacji zadań publicznych oraz innych zadań Inspektoratu należy wyposażać w:

1) system sygnalizujący wystąpienie zagrożenia pożarowego;
2) system sygnalizacji warunków środowiskowych m.in. wilgotności;
3) system klimatyzacji o całkowitej mocy chłodzącej zapewniającej bezpieczną i zgodną ze wskazaniami producentów pracę wszystkich urządzeń teleinformatycznych pracujących w serwerowniach.

3. Należy unikać prowadzenia instalacji wodnych przez pomieszczenia, w których zlokalizowane są zasoby kluczowe do przetwarzania informacji (np. serwerownie) oraz unikać budowania serwerowni w takich pomieszczeniach lub innych, które ze względu na położenie instalacji wodnych w bezpośrednim lub pośrednim otoczeniu są narażone na ich zalanie.

4. Urządzenia zapewniające ochronę środowiskową należy poddawać okresowej kontroli zgodnie z obowiązującymi przepisami prawa, normami oraz zaleceniami producentów.

5. Na wypadek zagrożenia pożarem należy opracować instrukcje przeciwpożarowe, ciągi komunikacyjne powinny być zaopatrzone w tabliczki informujące o kierunku ewakuacji i w miarę potrzeby wyposażone w oświetlenie awaryjne. Obowiązują w tym zakresie przepisy prawa właściwe w sprawach przeciwpożarowych, bezpieczeństwa i higieny pracy oraz zarządzania kryzysowego, jak również zapisy PZK.

6. W przypadku, jeśli któreś z wymagań w zakresie bezpieczeństwa środowiskowego nie może być z przyczyn obiektywnych spełnione, zastosowanie może mieć odstępstwo od zasad, przy czym powinno ono zawierać co najmniej udokumentowane informacje, jak: rodzaj odstępstwa, ryzyko wynikające z odstępstwa, zastosowane środki ochrony doraźnej lub zamiennej, plan dojścia do rozwiązania docelowego.

7. Parametry środowiskowe serwerowni, w których pracuje kluczowa infrastruktura teleinformatyczna, m.in. temperatura i wilgotność, należy monitorować w celu natychmiastowego wykrycia odchyleń, które mogłyby mieć negatywne skutki.

8. Samoczynnie załączające się oświetlenie powinno być stosowane w pomieszczeniach, w których nawet krótkotrwałe wyłączenie oświetlenia podstawowego może spowodować zagrożenie zdrowia i życia podczas ewakuacji. Obowiązują w tym zakresie przepisy prawa właściwe w sprawach przeciwpożarowych, bezpieczeństwa i higieny pracy.

§ 8. Wymagania dla systemów wspomagających

1. Jeżeli jest to możliwe, należy projektować nadmiarową klimatyzację tak, aby w przypadku awarii lub przeglądu serwisowego jednego elementu pozostałe były w stanie zapewnić wymagane parametry środowiskowe, w szczególności środowiska eksploatacyjnego w serwerowniach.

2. Rozmieszczenie kanałów oraz czerpni należy zaprojektować uwzględniając ryzyko takich zdarzeń, jak przedostanie się przez nie do pomieszczeń chronionych wody, środków niebezpiecznych czy też zwierząt – w zależności od warunków występujących dla danego obiektu.

3. W przypadku prowadzenia instalacji wodno-kanalizacyjnych i grzewczych w sąsiedztwie (również bezpośrednio nad lub pod pomieszczeniem) serwerowni i pomieszczeń, w których usytuowano infrastrukturę teleinformatyczną, lub usytuowania obiektów na obszarach narażonych na zalanie lub podtopienia, należy wdrożyć systemy zapewniające wykrycie i alarmowanie w przypadku zalania pomieszczenia lub wystąpienia nadmiernego poziomu wilgoci oraz zainstalować rozwiązania umożliwiające szybkie usunięcie wody.

4. Przy ocenie sprawności instalacji wodno-kanalizacyjnej i grzewczej należy uwzględnić jej współdziałanie z innymi systemami wspomagającymi, takimi jak system klimatyzacyjno-wentylacyjny oraz w szczególności system przeciwpożarowy.

§ 9. Systemy zabezpieczeń technicznych oraz systemy wspomagające

1. Rozważając wdrożenie systemów zabezpieczeń technicznych należy rozważyć m.in. następujące funkcje tych systemów:

1) zabezpieczenia powinny zagwarantować uniemożliwienie dostępu osobom niepowołanym do chronionych pomieszczeń i urządzeń oraz zabezpieczać osoby i mienie przed potencjalnymi zagrożeniami;
2) system sygnalizacji napadu i włamania powinien zapewniać skuteczne przekazanie sygnału o realnym zagrożeniu do określonych osób, miejsc i urządzeń;
3) system monitorowania w przypadku wystąpienia alarmu powinien zapewniać podjęcie odpowiednich działań stosownych do zaistniałego zdarzenia;

4) system monitoringu wizyjnego powinien zapewniać, poprzez rozmieszczone kamery, rozpoznanie rodzaju zagrożenia i śledzenie rozwoju sytuacji, prowadzenie obserwacji obrazu z kilku kamer oraz automatyczną jednoczesną rejestrację tych obrazów;
5) system kontroli dostępu powinien zabezpieczać chronione pomieszczenie lub wydzieloną strefę przed dostępem do nich osób nieuprawnionych.

2. Wszystkie systemy zabezpieczeń należy poddawać okresowym przeglądom przez osoby posiadające odpowiednie uprawnienia.

1) Przegląd polega na sprawdzeniu poprawności działania danego systemu zgodnie z jego dokumentacją techniczno-eksploatacyjną. Przeglądy każdego systemu zabezpieczeń powinny być zaplanowane w harmonogramie z uwzględnieniem zaleceń producentów tych systemów dotyczących okresów wykonywania przeglądów i konserwacji.
2) Prace konserwacyjne polegają na wykonaniu niezbędnych czynności mających na celu utrzymanie systemu w sprawności techniczno-użytkowej zgodnie z jego dokumentacją techniczno-eksploatacyjną. Prace konserwacyjne powinny być wykonywane zgodnie z zaleceniami producentów systemów lub w przypadku wystąpienia takiej potrzeby (np. wymiana filtrów klimatyzacji).

3. Zalecane jest, aby przeglądy obejmowały sprawdzenie stanu technicznego kart systemu kontroli dostępu, które są przez długi okres czasu nieużywane oraz kart przeznaczonych dla gości oraz, jeśli mają zastosowanie.

4. Przeglądy systemów zabezpieczeń poza ustalonym harmonogramem powinny być przeprowadzane każdorazowo w przypadku wystąpienia incydentów zagrażających lub mogących powodować zagrożenie dla bezpieczeństwa osób i mienia (np. katastrofa budowlana w sąsiedztwie obiektu, tąpnięcie, kolizja drogowa powodująca szczególne zagrożenie w pobliżu budynku, pożar, roboty budowlane w sąsiednich budynkach, ewakuacja osób i mienia z budynku, interwencja służb ratunkowych mająca wpływ na stan techniczny obiektu, wystąpienie anomalii pogodowych, itp.).

5. Przeprowadzenie przeglądów należy dokumentować. Dokumentacja przeglądów powinna obejmować:

1) datę i czas przeglądu;
2) dane personalne wykonującego przegląd;
3) wynik przeglądu;
4) dane personalne osoby nadzorującej lub kontrolującej;
5) uwagi z przeglądu.

6. Jeżeli przeglądy są wykonywane przez personel podmiotów zewnętrznych, powinien być prowadzony nadzór nad takimi pracami przez pracownika komórki organizacyjnej właściwej do spraw ochrony fizycznej.

7. Dla każdego systemu zabezpieczeń powinien być założony dziennik zawierający:

1) rejestr wyposażenia;
2) rejestr zdarzeń;
3) rejestr prac konserwacyjnych;
4) rejestr prac serwisowych.

§ 10. Zabezpieczenia mechaniczne

1. Do zabezpieczeń mechanicznych zalicza się m.in. kraty, żaluzje, okiennice, folie antywłamaniowe, zamki w drzwiach (w szczególności te, do których bezpośredni dostęp mają osoby postronne), inne zabezpieczenia otworów okiennych, włazów, kanałów wentylacyjnych, m.in. rygle, kłódki, zamki, zasuwy z blokadą mechaniczną.

2. Zabezpieczenia mechaniczne, które tego wymagają, powinny być montowane przez uprawniony podmiot zgodnie z warunkami technicznymi wynikającymi z certyfikatu lub aprobaty technicznej.

3. Zabezpieczenia mechaniczne, które są dostępne dla osób postronnych (np. zamki w zewnętrznych drzwiach wejściowych) i nie ma możliwości nadzoru nad nimi przez inne systemy zabezpieczeń, należy poddawać okresowym przeglądom.

4. Ustalając zakres przeglądów należy rozważyć wykonanie czynności:

1) w przypadku krat, żaluzji, okiennic i innych zabezpieczeń otworów okiennych, włazów, kanałów wentylacyjnych:
   a. sprawdzenie mocowań do murów (np. poprzez poruszenie elementów zabezpieczenia w pionie i poziomie i obserwacji reakcji elementów mocujących),
   b. sprawdzenie istnienia odkształceń mechanicznych na poszczególnych elementach, przy zastosowaniu metody porównawczej z opisem w dokumentacji technicznej,
   c. sprawdzenie występowania śladów po próbach penetracji lub usunięcia zabezpieczenia np. w postaci opiłków, śladów tynku, rysach na elementach zabezpieczeń, itp.,
   d. sprawdzić stan powłok lakierniczych i zabezpieczeń antykorozyjnych elementów narażonych na bezpośrednie działanie czynników atmosferycznych lub innych

szkodliwych czynników dla mechanizmów kłódek, zamków, rygli (szczególnie kurz, pył);

2) w przypadku kłódek i zamków – sprawdzenie działania kluczy zapasowych oraz mechanizmu ryglującego przez otwarcie i zamknięcie kłódek i zamków, przegród mechanicznych i budowlanych;

3) w przypadku rygli i zasuw z blokadą mechaniczną – porównanie położenia elementów ruchomych z opisem w dokumentacji technicznej.

5. Przynajmniej dwa razy do roku powinno się dokonać oceny stanu powłoki lakierniczej, śladów korozji elementów zabezpieczeń narażonych na bezpośrednie działanie czynników atmosferycznych lub innych szkodliwych czynników dla mechanizmów.

6. Wycofane z użycia elementy zabezpieczeń mechanicznych zawierające informacje o kodzie zamków (klucze, wkładki, karty elektroniczne) należy niszczyć mechanicznie.

7. Wycofanie elementu zabezpieczenia mechanicznego powinno być realizowane po uzyskaniu informacji od dystrybutora/producenta wyrobu o konieczności jego wymiany lub po uzyskaniu informacji o pojawieniu się metod/narzędzi powodujących przełamanie zabezpieczenia lub obniżenie jego właściwości.

8. Z zastrzeżeniem ust. 6, koniec okresu ważności certyfikatu lub świadectwa kwalifikacyjnego nie stanowi przyczyny demontażu elementu zabezpieczenia, jeżeli to zachowuje swoje funkcje i właściwości związane z zapewnianiem bezpieczeństwa.

§ 11. Zabezpieczenia techniczno-budowlane

1. Do zabezpieczeń techniczno-budowlanych zalicza się m.in. drzwi, śluzy, ściany, stropy, ogrodzenia (wykonane z różnych materiałów), furtki, bramy, zapory, szlabany, kołowroty (w szczególności te, do których bezpośrednio dostęp mają osoby postronne).

2. Zabezpieczenia techniczno-budowlane, które są dostępne dla osób postronnych (np. zamki w zewnętrznych drzwiach wejściowych) i nie ma możliwości nadzoru nad nimi przez inne systemy zabezpieczeń, należy poddawać okresowym przeglądom.

3. Ustalając zakres przeglądów należy rozważyć wykonanie czynności:

1) sprawdzenie mocowań elementów ruchomych i elementów umocowanych na stałe do podłoża (np. poprzez poruszenie elementów konstrukcji zabezpieczenia i obserwacji reakcji elementów mocujących);

2) sprawdzenie istnienia odkształceń mechanicznych na poszczególnych elementach, przy zastosowaniu metody porównawczej z opisem w dokumentacji technicznej;

3) sprawdzenie występowania śladów po próbach penetracji lub usunięcia zabezpieczenia np. w postaci opiłków, śladów tynku, rysach na elementach zabezpieczeń, rdzy;
4) sprawdzenie mechanizmów ryglowych (w tym. zamków, rygli);
5) porównanie położenia elementów ruchomych z opisem w dokumentacji technicznej.

4. Przynajmniej dwa razy do roku powinno się dokonać oceny stanu powłoki lakierniczej, śladów korozji elementów zabezpieczeń narażonych na bezpośrednie działanie czynników atmosferycznych lub innych szkodliwych czynników środowiskowych.

5. Wymiana lub naprawa zabezpieczeń powinna być realizowana pod nadzorem pracownika komórki organizacyjnej właściwej do spraw ochrony fizycznej.

§ 12. Okablowanie zasilające i teleinformatyczne w zakresie konstrukcyjno-mechanicznym

1. Do systemów okablowania w zakresie konstrukcyjno-mechanicznym zalicza się m.in. trakty kablowe (listwy PCV, szyny, rury, przepusty), osłony włazów i studzienek, szafy dystrybucyjne, tablice, krosownice.

2. Systemy okablowania znajdujące się w obszarze dostępnym publicznie powinno się poddawać okresowym przeglądom. Za realizację przeglądów odpowiadają pracownicy komórki organizacyjnej właściwej do spraw ochrony fizycznej oraz ASI.

3. Przeglądy polegają na sprawdzeniu stanu technicznego (konstrukcyjno-mechanicznego) elementów okablowania i weryfikacji z dokumentacją techniczną pod kątem identyfikacji nieuprawnionych podłączeń.

4. Przeglądy zabezpieczeń elektronicznych systemów okablowania polegają na sprawdzeniu poprawności funkcjonowania np. systemów sygnalizacji włamania zastosowanych do zabezpieczenia szaf dystrybucyjnych, krosownic lub innych zabezpieczeń. znajdujące się w obszarze dostępnym publicznie należy poddawać okresowym przeglądom. Za realizację przeglądów odpowiadają pracownicy komórki organizacyjnej właściwej do spraw ochrony fizycznej.

5. Ustalając zakres przeglądów należy rozważyć wykonanie sprawdzenia:
1) ciągłości struktury (mocowanie listew) traktów kablowych w miejscach ogólnie dostępnych – np. narażonych na uszkodzenia mechaniczne spowodowane przez przenoszenie przedmiotów o dużych gabarytach, ruch osobowy, celowe działania;

2) stanu powłoki lakierniczej, śladów korozji elementów narażonych na bezpośrednie działanie czynników atmosferycznych lub innych szkodliwych czynników dla obudów, osłon lub innych zabezpieczeń systemów okablowania;
3) występowania śladów prób penetracji lub usunięcia zabezpieczenia, np. w postaci opiłków, śladów tynku, rys na elementach zabezpieczeń, itp.
4) przestrzegania zasad ochrony okablowania oraz punktów połączeń okablowania (inspekcja pod kątem podłączonych nieautoryzowanych urządzeń lub połączeń);
5) zamknięcia szaf, tablic, osłon włazów i studzienek;
6) zgodności stanu faktycznego z dokumentacją techniczną okablowania;
7) stanu technicznego instalacji poprzez wykonanie pomiarów okablowania.

§ 13. Elektroniczne systemy zabezpieczeń

1. Do elektronicznych systemów zabezpieczeń zalicza się m.in. systemy sygnalizacji włamania i napadu, systemy kontroli dostępu, systemy telewizji dozorowej (monitoringu wizyjnego) oraz inne systemy współdziałające z elektronicznymi systemami zabezpieczeniowymi, np. system oświetlenia podczerwienią dla systemu telewizji dozorowej.

2. Elektroniczne systemy zabezpieczeń i systemy współdziałające należy poddawać okresowym przeglądom zgodnie ze wskazaniami ich producentów. Za realizację przeglądów odpowiadają pracownicy komórki organizacyjnej właściwej do spraw ochrony fizycznej.

3. Ustalając zakres przeglądów systemów sygnalizacji włamania i napadu należy rozważyć sprawdzenie:

1) trybu pracy urządzeń wg wskazań paneli sterujących poprzez porównanie z dokumentacją techniczno-eksploatacyjną systemu;
2) działania przycisków sygnalizacji napadu/przycisków wezwania pomocy;
3) działania poszczególnych klawiatur poprzez załączanie i rozłączanie systemu wprowadzając odpowiedni kod,
4) ilości i rozmieszczenia klawiatur strefowych z dokumentacją i identyfikowanymi potrzebami;
5) prawidłowości funkcjonowania systemu w zakresie określonym w dokumentacji technicznej;
6) ciągłości działania zasilania podstawowego i sprawności zasilania awaryjnego (wymiana akumulatorów powinna być wykonywana zgodnie z harmonogramem określonym w dokumentacji technicznej systemu);

7) poprawności działania akustycznych lub optycznych sygnalizatorów alarmowych;
8) czujników systemu;
9) mocowania czujek do podłoża (uchwytów, ścian), w szczególności zamontowanych w strefach ogólnych i ogólnodostępnych oraz znajdujących się poza pomieszczeniami Inspektoratu (płaszczyzna ścian, ogrodzenia), jeżeli takie występują.

5. Ustalając zakres przeglądów systemów kontroli dostępu należy rozważyć sprawdzenie:

1) trybu pracy urządzeń wg wskazań paneli sterujących bądź aplikacji zarządzającej, poprzez porównanie z dokumentacją systemu;
2) działania przycisków otwierających wyjścia z czytnikami działającymi jednostronnie, w tym działania przycisków ewakuacyjnych w przypadku, gdy system nie współpracuje z systemem ochrony przeciwpożarowej;
3) działania czytników systemu z odpowiednią kartą dostępu;
4) mocowania czytników, samozamykaczy, zamków elektromagnetycznych drzwi i przejść, w tym istnienia śladów prób penetracji (rysy, wgniecenia, próby podważania, demontażu);
5) ilości i rozmieszczenia czytników zgodnie z danymi w dokumentacji systemu;
6) limitu użytkowników systemu.

6. Czynności konserwacyjne powinny obejmować te wskazane w dokumentacji producenta systemu, przy czym zaleca się rozważenie sprawdzenia:

1) prawidłowości funkcjonowania systemu w zakresie określonym w dokumentacji technicznej;
2) ciągłości działania zasilania podstawowego i sprawności zasilania awaryjnego, w tym wymiana akumulatorów zgodnie z harmonogramem określonym w dokumentacji technicznej systemu;
3) działania części elektromechanicznych m.in. elektrozaczepów, trzymaczy elektromagnetycznych, śluz, tripodów.

7. Ustalając zakres przeglądów systemów monitoringu wizyjnego należy rozważyć sprawdzenie:

1) trybu pracy urządzeń rejestrujących poprzez porównanie z dokumentacją techniczno-eksploatacyjną na podstawie wskazań paneli sterujących informujących o trybie pracy urządzeń;
2) jakości obrazu i pola obserwacji na monitorach poprzez porównanie z opisem oraz zdjęciem obrazu wykonanym w trybie dziennym i nocnym;

3) wymiany nośników w urządzeniu rejestrującym zgodnie z dokumentacją techniczną systemu;
4) poprawności pracy urządzeń rejestrujących poprzez nagranie i odtworzenie przebiegu zdarzeń w trybie czasu rzeczywistego oraz losowo wybranego zdarzenia w czasie przeszłym;
5) sprawdzenie ciągłości działania zasilania podstawowego i sprawności zasilania awaryjnego;
6) wyłączenie monitora i sprawdzenie „poświaty” (efekt „wypalania się” kineskopu objawiający się „pozostawaniem” obrazu na ekranie po odłączeniu źródła sygnału);
7) sprawdzenie jakości zarejestrowanego obrazu z kamer rejestrujących punkty newralgiczne (szczególnie z kamer zewnętrznych, rejestracja wykonana w godzinach nocnych);
8) sprawdzenie zapisu z wewnętrznych pamięci kamer (jeśli kamery posiadają taką pamięć);
9) sprawdzenie mocowania kamer zewnętrznych, jeśli są narażone na działania czynników atmosferycznych i innych np. konary drzew;
10) sprawdzenie działania wycieraczek, obwodów, grzałek (elementy przeciwśnieżne, jeśli zostały zainstalowane);
11) sprawdzenie działania głowic obrotowych i funkcji „zoom” (optyczny i elektroniczny);
12) sprawdzenie mocowania reflektorów podczerwieni i oświetlenia sztucznego związanego z systemem monitoringu wizyjnego m.in. halogenów włączane automatycznie z czasowym wyłącznikiem.

§ 14. Systemy wspomagające oświetlenie

1. Przeglądy systemów wspomagających oświetlenie należy prowadzić zgodnie z ustalonym harmonogramem. Przeglądy te powinny obejmować sprawdzenie systemów sterujących (włączających i wyłączających oświetlenie).

2. Ustalając zakres czynności konserwacyjnych prowadzonych zgodnie z zaleceniami producenta należy rozważyć:

1) sprawdzenie zasilania podstawowego i awaryjnego;
2) sprawdzenie innych elementów, zgodnie z dokumentacją systemu.

§ 15. Systemy transmisji sygnałów alarmowych do centrów monitoringu

1. Przeglądy systemu transmisji sygnałów alarmowych do centrów monitoringu należy prowadzić zgodnie z ustalonym harmonogramem. Przeglądy te powinny obejmować

sprawdzenie trybu pracy urządzenia wg wskazań paneli sterujących poprzez porównanie z dokumentacją systemu.

2. Ustalając zakres czynności konserwacyjnych prowadzonych zgodnie z zaleceniami producenta należy rozważyć:

1) sprawdzenie ciągłości działania zasilania podstawowego i sprawności zasilania awaryjnego (wymiana akumulatorów zgodnie z harmonogramem określonym w dokumentacji technicznej systemu);
2) sprawdzenie systemu anten, masztów, stanu uziemienia;
3) sprawdzenie/potwierdzenie prawidłowego działania systemu/systemów w centrum monitoringu.

§ 16. Rejestrowanie i przechowywanie informacji w elektronicznych systemach zabezpieczeń

1. Zdarzenia rejestrowane w elektronicznych systemach zabezpieczeniowych podlegają regularnym przeglądom przez pracownika komórki organizacyjnej właściwej do spraw ochrony fizycznej.

2. Częstotliwość przeglądu zapisów powinna być wyznaczona na podstawie pojemności pamięci zdarzeń danego systemu:

1) przed czynnością włączenia/wyłączenia dla systemów, których pamięć zdarzeń jest kasowana podczas włączania/wyłączania, lub
2) przed zapełnieniem pamięci systemu powodującej nadpisywanie danych (według danych w dokumentacji techniczno-eksploatacyjnej systemu), nie rzadziej jednak niż raz na kwartał.

3. Zapisy w systemach monitoringu wizyjnego, kontroli dostępu, sygnalizacji włamania i napadu oraz w dziennikach/rejestrach wejścia/wyjścia należy wyrywkowo kontrolować pod kątem korelacji rejestrowanych zdarzeń. Pracownik komórki organizacyjnej właściwej do spraw ochrony fizycznej odpowiada za prowadzenie kontroli wyrywkowych we współpracy z użytkownikami pomieszczeń i stref, którzy są zobowiązani do prowadzenia dzienników/rejestrów wejścia wyjścia.

4. W przypadku wystąpienia incydentu naruszenia bezpieczeństwa lub podejrzenia jego wystąpienia, co do którego okoliczności mogą być wyjaśnione dzięki zapisom z rejestrów elektronicznych systemów zabezpieczeń, pracownik komórki organizacyjnej właściwej

do spraw ochrony fizycznej zapewnia utrwalenie zapisów z tych rejestrów elektronicznych systemów zabezpieczeń na potrzeby dowodowe.

§ 17. Prowadzenie dokumentacji związanej z systemami zabezpieczeń

1. Pracownik komórki organizacyjnej właściwej do spraw ochrony fizycznej jest odpowiedzialny za prowadzenie dokumentacji systemów zabezpieczeń, wszelkich ewidencji, wykazów uprawnień i rejestrów, w tym rejestrów zdarzeń.

2. Wszelka dokumentacja wskazana w ust. 1 jest klasyfikowana jako informacja wrażliwa.

3. Pracownik komórki organizacyjnej właściwej do spraw ochrony fizycznej jest odpowiedzialny za aktualność i kompletność dokumentacji systemów zabezpieczeń (tzn. dokumentacji powykonawczej, zmian w tej dokumentacji, aktualnych plików konfiguracyjnych systemów i urządzeń).

§ 18. Zarządzanie zapisami pochodzącymi z elektronicznych systemów zabezpieczeń

1. Pracownik komórki organizacyjnej właściwej do spraw ochrony fizycznej jest odpowiedzialny za utrzymanie rejestrów elektronicznych nadzorowanych systemów zabezpieczeń.

2. Okres przechowywania zapisów pochodzących z elektronicznych systemów zabezpieczeń powinien wynosić co najmniej 30 dni z zastrzeżeniem zapisów monitoringu wizyjnego, dla którego należy uwzględnić okres przechowywania określony w Regulaminie pracy w Inspektoracie.

3. W przypadku powierzenia utrzymania systemów zabezpieczeń podmiotowi zewnętrznemu, umowa z tym podmiotem powinna zapewniać skuteczną kontrolę nad tymi systemami poprzez określenie m.in.:

1) warunków świadczenia usług;
2) wymagań bezpieczeństwa w odniesieniu do systemów zabezpieczeń;
3) zasad dostępu personelu podmiotu zewnętrznego do systemu, w tym przechowywanych zapisów oraz uzyskania kopii stanowiących materiał dowodowy, jeśli zachodzi taka potrzeba;
4) sposobów komunikowania się z usługodawcą;
5) zakresu odpowiedzialności usługodawcy;
6) zasad i warunków powierzenia przetwarzania danych osobowych oraz wsparcia w realizacji praw osób, których dane dotyczą.

4. W przypadku stwierdzenia incydentu naruszenia bezpieczeństwa informacji pracownik komórki organizacyjnej właściwej do spraw ochrony fizycznej powinien wykonać kopie rejestrów elektronicznych systemów zabezpieczeń dla celów dowodowych.

Załącznik nr 4 do Polityki Bezpieczeństwa Informacji
Głównego Inspektoratu Transportu Drogowego

Polityka Bezpieczeństwa Teleinformatycznego

Wymagania i zasady dotyczące prowadzenia CMDB

§ 1. 1. Należy opracować i wdrożyć procedury opisujące sposób zarządzania sprzętem informatycznym i oprogramowaniem (w tym licencjami na oprogramowanie) oraz funkcjonowania CMDB obejmujące:

1) formę prowadzenia rejestru;
2) procedury prowadzenia rejestru, w tym określające sposób i częstotliwość aktualizacji rejestru;
3) odpowiedzialność za przeprowadzanie rejestru;
4) procedury przydzielania, zwrotu sprzętu i oprogramowania.

2. Rejestr powinien zawierać informacje o wszystkich zidentyfikowanych urządzeniach i oprogramowaniu, m.in. szczegółowe dane o urządzeniach, oprogramowaniu i środkach komunikacji, ich rodzaju, parametrach, aktualnej konfiguracji i relacjach między elementami konfiguracji oraz użytkowniku.

3. Dla urządzeń należy rozważać elementy informacyjne rejestru, takie jak:

1) rodzaj urządzenia;
2) numer seryjny oraz numer inwentarzowy urządzenia;
3) nazwa urządzenia, w tym nazwa w sieci;
4) adres (lub adresy) IP oraz adres (lub adresy) MAC;
5) komórka organizacyjna użytkującą urządzenie;
6) użytkownik korzystający z urządzenia;
7) cel, w jakim urządzenie jest eksploatowane;
8) parametry konfiguracyjne;
9) zainstalowane oprogramowanie, poprzez powiązane z listą inwentarzową;
10) fizyczna lokalizacja urządzenia;
11) data wdrożenia urządzenia;
12) data wycofania urządzenia;
13) informacje o wsparciu serwisowym;
14) informacje o klasyfikacji urządzenia w związku z informacjami przetwarzanymi przy jego użyciu.

4. Dla oprogramowania należy rozważać elementy informacyjne rejestru, takie jak:

1) nazwa oprogramowania;
2) miejsce instalacji;
3) użytkownik oprogramowania;
4) warunki licencjonowania;
5) dowody licencyjne;
6) ilość licencji/dopuszczalna ilość użytkowników.

Wymagania i zasady dotyczące zarządzania nośnikami elektronicznymi

§ 2. 1. Korzystanie z innych niż służbowe i udostępniane przez Inspektorat nośników danych, w szczególności korzystanie z prywatnych nośników danych (dyskietka, dysk zewnętrzny, pendrive, karta pamięci, nośniki optyczne, itp.) jest zabronione, z zastrzeżeniem ust. 2.

2. Dopuszcza się odstępstwa od zakazu określonego w ust. 1 dla:

1) nośników, które są przekazywane do Inspektoratu w korespondencji związanej z realizowanymi zadaniami;
2) nośników, które pracownik otrzymał na konferencji, wydarzeniu promocyjnym itp. pod warunkiem zgłoszenia takiego nośnika do BT w celu zaewidencjonowania oraz sprawdzenia pod względem występowania szkodliwego oprogramowania lub innych zagrożeń; ostateczną decyzję o dopuszczeniu takiego nośnika do użytkowania wydaje dyrektor BT lub jego zastępca.

3. Nośniki danych udostępniane pracownikom, które nie posiadają wbudowanej funkcjonalności szyfrowania zawartości pracownik, wykorzystując te nośniki do przechowywania (w tym wysłania na zewnętrz) informacji wymagających ochrony, w szczególności danych osobowych, ma obowiązek zabezpieczenia stosując wymagania i zasady określone w PBT, w szczególności wymagania i zasady dotyczące stosowania zabezpieczeń kryptograficznych.

4. Niezależnie od obowiązków określonych w ust. 3 pracownik ma obowiązek zapewnić odpowiednią ochronę fizyczną samego nośnika w transporcie przed uszkodzeniami fizycznymi (np. stosując bezpieczne koperty, opakowania, walizki lub futerały), oraz jego utratą m.in. nieprzechowywanie nośnika w kieszeniach odzieży wierzchniej, niepozostawianie nośnika bez stałego nadzoru nad nim przez okres transportu.

5. Nośniki danych, w szczególności wykorzystywane przez pracowników nośniki wymienne (m.in. pendrive, CD, DVD, dyski przenośne USB), gdy nie są wykorzystywane muszą być przechowywane w sposób zapewniający ochronę przed dostępem do nich osób nieuprawnionych, np. w zamykanych szufladach mebli biurowych, w zamykanych szafach lub sejfach. Dotyczy do w szczególności pomieszczeń, do których dostęp mają osoby obce, m.in. w strefach ogólnodostępnych gdzie odbywa się obsługa interesantów oraz miejsc wykonywania pracy zdalnej.

6. Wymóg bezpiecznego przechowywania nośników elektronicznych dotyczy również dysków stałych wymontowanych z urządzeń, do czasu usunięcia z tych nośników zapisanych na nich danych lub ich skutecznej utylizacji / zniszczenia.

7. Sprzęt informatyczny przeznaczony do naprawy należy przekazywać bez nośników.

8. Nośniki z wycofywanego z eksploatacji lub zwracanego (np. sprzęt wymieniany na inny lub oddawany z uwagi na zakończenie zatrudnienia) sprzętu należy wymontować, a następnie zutylizować lub sprzęt z tymi nośnikami przekazać do ponownego użycia po zapewnieniu usunięcia zapisanych na nich informacji. Za usunięcie informacji z nośników odpowiada BT.

9. Informacje z nośników, które nie podlegają ponownemu wykorzystaniu należy usuwać w sposób uniemożliwiający ich odczytanie, np. poprzez:

1) wielokrotne nadpisanie zawartości nośnika przy użyciu odpowiedniego oprogramowania;
2) fizyczne zniszczenie nośnika danych.

10. Likwidację uszkodzonych lub niepotrzebnych nośników należy realizować poprzez fizyczne zniszczenie takiego nośnika (np.: złamanie, pocięcie, przedziurawienie) lub przekazanie na podstawie umowy do specjalistycznej firmy dokonującej likwidacji nośników dającej gwarancję zachowania poufności.

11. Wszelkie nośniki danych przeznaczone do powtórnego wykorzystania muszą zostać pozbawione zapisanych na nich danych i informacji w sposób uniemożliwiający ich odczytanie np. poprzez wielokrotne nadpisanie danych przy użyciu odpowiedniego oprogramowania.

12. Pracownik w przypadku wymiany urządzenia na inne ma obowiązek zabezpieczyć informacje przechowywane w jego pamięci, np. poprzez czasowe przeniesienie ich na nośnik zewnętrzny lub do zasobów sieciowych.

13. Pracownik zdający urządzenie w związku z zakończeniem zatrudnienia ma obowiązek przekazać wszystkie informacje służbowe zapisane w pamięci urządzenia pracownikowi, który przejmuje jego zadania lub bezpośredniemu przełożonemu. Obowiązkiem bezpośredniego przełożonego jest dopilnowanie, że wszystkie informacje służbowe niezbędne do zachowania

ciągłości realizacji zadań zapisane w pamięci takiego urządzenia zostaną przekazane jemu lub pracownikowi przejmującemu zadania.

Wymagania i zasady dotyczące użytkowania urządzeń mobilnych

§ 3. 1. Powierzone pracownikom urządzenia mobilne mogą być wykorzystywane wyłącznie w celu wykonywania obowiązków służbowych, w tym poza pomieszczeniami Inspektoratu, w szczególności w miejscach wykonywania pracy zdalnej. Wyniesienie urządzenia poza siedzibę Inspektoratu wymaga zgody bezpośredniego przełożonego, zgodnie z Regulaminem pracy w Inspektoracie.

2. Korzystanie z urządzenia mobilnego powinno być ekonomicznie uzasadnione, jak również nie powinno narażać Inspektoratu na niepotrzebne dodatkowe koszty. W związku z tym pracownik powinien powstrzymać się od korzystania z urządzenia mobilnego, jeżeli:

1) urządzenie mobilne ma być wykorzystane do rozmowy telefonicznej, a rozmowę tę można wykonać przy użyciu telefonu stacjonarnego w biurze;
2) urządzenie mobilne ma być wykorzystane do wymiany danych i komunikacji elektronicznej, a to samo zadanie może być wykonane przy użyciu infrastruktury teleinformatycznej w siedzibie Inspektoratu.

3. Pracownicy odpowiadają za bezpieczeństwo powierzonych im urządzeń mobilnych, w szczególności mają obowiązek ochrony urządzeń mobilnych przed utratą, uszkodzeniem lub zniszczeniem.

4. Zabronione jest pozostawianie urządzeń mobilnych bez nadzoru w sposób powodujący wysokie ryzyko kradzieży lub uszkodzenia, w tym podczas pracy zdalnej lub transportu, m.in. w bagażu bez zapewnienia stałego nadzoru nad nimi.

5. Zabronione jest udostępnianie powierzonych pracownikowi służbowych urządzeń mobilnych jakimkolwiek osobom trzecim, w tym osobom z najbliższego otoczenia pracownika.

6. Rozmawiając w szczególności w miejscu publicznym lub miejscu wykonywania pracy zdalnej o sprawach służbowych należy zwracać uwagę na ryzyko podsłuchania rozmowy przez osoby przebywające w pobliżu. Pracownik powinien powstrzymać się od rozmowy w takim miejscu, jeżeli jej podsłuchanie może spowodować ujawnienie informacji, które powinny pozostać znane tylko określonym osobom, w konsekwencji powodować negatywne skutki dla Inspektoratu, w szczególności konsekwencje natury prawnej i karnej.

7. Pracownik zobowiązany jest do ochrony wyświetlanych na urządzeniu mobilnym treści przed ich podejrzeniem przez osoby znajdujące się w pobliżu, dotyczy to również ryzyka zarejestrowania wyświetlanych treści przez systemy monitoringu wizyjnego.

8. Praca na urządzeniach mobilnych w środkach komunikacji publicznej, która skutkuje wyświetlaniem treści na ekranie urządzenia jest zabroniona z uwagi na wysokie ryzyko podejrzenia, w konsekwencji utraty poufności informacji, które mogą obejmować informacje prawnie chronione.

9. Pracownik nie powinien nagrywać na automatycznej sekretarce wiadomości zawierających informacje, których ujawnienie może spowodować negatywne skutki związane z ujawnieniem informacji, w szczególności wywoływać konsekwencje natury prawnej.

10. Urządzenia mobilne należy tak konfigurować, aby oprócz obowiązkowego kodu PIN karty SIM do odblokowania urządzenia wymagane było użycie zabezpieczenia przed nieuprawnionym dostępem, np. kodu, hasła, symbolu, biometrii; dostępność zabezpieczeń jest uzależniona od funkcjonalności danego urządzenia mobilnego, którym dysponuje pracownik. Pracownik odpowiada za włączenie i wybór zabezpieczenia oraz jego ustawienie, które będzie znane tylko jemu (kod, hasło, symbol) lub które tylko on posiada (biometria).

11. Hasła, o których mowa w ust. 10 powinny spełniać wymagania dotyczące ustanawiania silnych haseł określone w PBT.

12. Zabronione jest wyłączanie zabezpieczeń, o których mowa w ust. 10.

13. Pracownik użytkujący urządzenie mobilne ma obowiązek unikać podłączania tego urządzenia do nieznanych i obcych sieci przewodowych i bezprzewodowych, w szczególności do otwartych sieci bezprzewodowych dostępnych m. in. w miejscach publicznych, hotelach. Podłączenie urządzenia mobilnego do obcej sieci tj. innej niż udostępniana przez Inspektorat lub pracownika jest dopuszczalne jedynie w przypadku, gdy jest to absolutnie niezbędne do wykonania obowiązków służbowych oraz gdy nie istnieją wątpliwości co do tożsamości takiej sieci i możliwości jej użycia (np. sieć dla gości w podmiocie publicznym).

14. Zabrania się dokonywania samodzielnie przez pracowników użytkujących urządzenia mobilne, z zastrzeżeniem wyjątków określonych w PBT, jakichkolwiek zmian w konfiguracji urządzeń i zainstalowanego na nich oprogramowania, w szczególności w odniesieniu do konfiguracji zabezpieczeń. Takich zmian mogą dokonywać wyłącznie pracownicy komórki organizacyjnej właściwej do spraw administrowania telefonami służbowymi.

15. Oprogramowanie użytkowe urządzeń mobilnych powinno być instalowane wyłącznie z zaufanych źródeł i wyłącznie takie, które jest niezbędne do wykonywania przez pracownika zadań służbowych.

16. Urządzenia mobilne, które są wycofywane z użycia, przekazywane do serwisu lub zdawane i przekazywane do ponownego użycia (w tym odsprzedawane), należy pozbawiać zapisanych w nich informacji. W tym celu należy postępować zgodnie z instrukcjami tych urządzeń i zaleceniami ich producentów określającymi skuteczną metodę czyszczenia pamięci urządzenia.

17. Za wyczyszczenie pamięci służbowego urządzenia mobilnego odpowiada komórka organizacyjna właściwa do spraw administrowania tymi urządzeniami. Pracownikom zaleca się czyszczenie pamięci swoich prywatnych urządzeń mobilnych zgodnie z ust. 16 w celu zapewnienia bezpieczeństwa m.in. ich prywatnych kont poczty elektronicznej, mediów społecznościowych, bankowości elektronicznej, czy poufności prywatnych informacji.

18. Materiały, które mogą być pomocne w szczególności dla pracowników o których mowa w ust. 17, dotyczące bezpieczeństwa urządzeń mobilnych zawiera szkolenie wewnętrzne z bezpieczeństwa informacji (e-learning) na wewnętrznej platformie szkoleniowej.

Wymagania i zasady dotyczące użytkowania urządzeń przenośnych

§ 4. 1. Powierzone pracownikom do używania urządzenia przenośne mogą być wykorzystywane wyłącznie w celu wykonywania obowiązków służbowych, w tym poza pomieszczeniami Inspektoratu, w szczególności w miejscach wykonywania pracy zdalnej. Wyniesienie urządzenia poza siedzibę Inspektoratu wymaga zgody bezpośredniego przełożonego, zgodnie z Regulaminem pracy w Inspektoracie.

2. Pracownicy odpowiadają za bezpieczeństwo powierzonych im urządzeń przenośnych, w szczególności mają obowiązek ochrony urządzeń przenośnych przed utratą, uszkodzeniem lub zniszczeniem.

3. Zabronione jest pozostawianie urządzeń przenośnych bez nadzoru w sposób powodujący wysokie ryzyko kradzieży lub uszkodzenia, w tym podczas pracy zdalnej lub transportu, m.in. w bagażu bez zapewnienia stałego nadzoru nad nimi.

4. Zabronione jest udostępnianie powierzonych pracownikowi służbowych urządzeń przenośnych jakimkolwiek osobom trzecim, w tym osobom z najbliższego otoczenia pracownika z wyłączeniem sytuacji, gdy urządzenie jest współużytkowane przez więcej niż 1 pracownika.

5. Urządzenia przenośne należy transportować w przeznaczonych do tego torbach, plecakach itp. zapewniających podstawową ochronę przed uszkodzeniami mechanicznymi i skutkami działania czynników atmosferycznych.

6. Praca na urządzeniach przenośnych w środkach komunikacji publicznej jest zabroniona z uwagi na wysokie ryzyko podejrzenia, w konsekwencji utraty poufności informacji, które mogą obejmować informacje prawnie chronione.

7. Zabronione jest wyłączanie oprogramowania pełniącego funkcję ochrony przed zagrożeniami, samodzielnej zmiany konfiguracji tych zabezpieczeń oraz innej konfiguracji urządzenia, jak również pozostawianie niezabezpieczonego systemu operacyjnego. Pracownik oddalając się od urządzenia na krótki czas ma obowiązek każdorazowego blokowania systemu operacyjnego, a w przypadku dłuższej nieobecności przy stanowisku pracy lub zakończenia pracy w danym dniu pracownik ma obowiązek wylogować się z systemu operacyjnego i wszystkich innych systemów, z których podczas pracy korzystał, jak również wyłączenia urządzenia. Ponadto pracownik wykonujący zadania na pracy zdalnej po zakończonej pracy ma obowiązek zabezpieczyć urządzenia służbowe przed dostępem do nich osób trzecich, w tym pozostałych osób przebywających w miejscu wykonywania pracy zdalnej (obejmuje to w szczególności pozostałe osoby zamieszkujące z pracownikiem w miejscu wykonywania przez niego pracy zdalnej).

8. Pracownik użytkujący urządzenie przenośne ma obowiązek unikać podłączania tego urządzenia do nieznanych i obcych sieci przewodowych i bezprzewodowych, w szczególności do otwartych sieci bezprzewodowych dostępnych w miejscach publicznych, hotelach, itp. Podłączenie urządzenia mobilnego do obcej sieci tj. innej niż udostępniana przez Inspektorat lub pracownika jest dopuszczalne jedynie w przypadku, gdy jest to absolutnie niezbędne do wykonania obowiązków służbowych oraz gdy nie istnieją wątpliwości co do tożsamości takiej sieci i możliwości jej użycia (np. sieć dla gości w podmiocie publicznym).

9. Pracownik ponosi osobistą odpowiedzialność za wszelkie incydenty bezpieczeństwa, które były wynikiem niedopełnienia przez niego obowiązków związanych z ochroną urządzeń przenośnych, w szczególności w czasie gdy jego konta pozostawały w tym czasie zalogowane w systemach.

Wymagania i zasady dotyczące bezpieczeństwa informacji przy pracy na odległość, w tym pracy zdalnej

§ 5. 1. Przetwarzanie informacji wymagających ochrony, w szczególności danych osobowych oraz innych informacji prawnie chronionych w związku z wykonywaniem przez pracowników zadań służbowych w formie pracy zdalnej lub innej wykonywanej poza siedzibą Inspektoratu lub miejscem wykonywania pracy zdalnej, może następować wyłącznie na służbowych urządzeniach udostępnionych pracownikom przez Inspektorat, z zastosowaniem połączeń VPN, które umożliwiają dostęp zdalny do wewnętrznej sieci oraz oprogramowania zainstalowanego na tych urządzeniach służbowych. Powyższe dotyczy również kont poczty elektronicznej – zabronione jest korzystanie z jakichkolwiek innych, niż służbowe kont poczty elektronicznej, w tym przekierowywania służbowej poczty elektronicznej na zewnętrzne i nieudostępnione przez Inspektorat konta poczty elektronicznej.

2. Pracownicy, o których mowa w ust. 1 mają obowiązek wskazać numer telefonu, pod którym ASI, AMS, pracownicy BT, bezpośredni przełożony lub kierujący komórką organizacyjną będą mogli uzyskać bieżące informacje dotyczące zadań służbowych, w szczególności realizowanych z wykorzystaniem zdalnego dostępu do sieci wewnętrznej oraz systemów funkcjonujących w Inspektoracie. W miarę możliwości powinien to być numer służbowy przydzielony pracownikowi na zasadach określonych w odrębnych regulacjach wewnętrznych. Udostępnienie prywatnego numeru telefonu jest wyłączną decyzją pracownika (dobrowolną zgodą w rozumieniu RODO), którą należy udokumentować i którą pracownik może w dowolnym momencie zmienić. Jednakże w przypadku niepodania przez pracownika numeru telefonu umożlwiającego szybki kontakt z nim powinno się rozważyć odmową wyrażenia zgody na wykonywanie zadań służbowych z wykorzystaniem zdalnego dostępu.

3. Zdalny dostęp do sieci wewnętrznej wymaga stosowania przez pracownika uwierzytelniania dwuskładnikowego (token fizyczny lub programowy), jakiekolwiek odstępstwo w tym zakresie nie występuje.

4. Pracownik ma obowiązek wydzielić odpowiednią przestrzeń w miejscu wykonywania pracy zdalnej, tak aby inne osoby przebywające w tym miejscu nie miały dostępu do urządzeń, nośników oraz dokumentów i informacji służbowych. Należy stosować się do obowiązujących zasad dotyczących bezpieczeństwa i higieny pracy dla stanowisk związanych z pracą zdalną.

5. Wszelkie działania pracowników posiadających zdalny dostęp do sieci wewnętrznej są monitorowane zgodnie z Regulaminem pracy w Inspektoracie. Urządzenia i konta pracownika, u którego zostaną zidentyfikowane podejrzane działania na urządzeniu, w sieci

wewnętrznej lub systemach z wykorzystaniem jego kont mogą zostać zablokowane przez ASI, w tym bez ostrzeżenia, jeżeli tego będzie wymagała reakcja na incydent bezpieczeństwa.

6. Pracownik ma obowiązek stosować się do zasad bezpieczeństwa określonych w PBI oraz dokumentacji systemów, tak aby w wyniku jego działań nie doszło do nieuprawnionych operacji, w szczególności skutkujących naruszeniem bezpieczeństwa informacji.

7. Pracownikom nie wolno wykorzystywać uzyskanych praw zdalnego dostępu do celów innych, niż określone we wniosku o nadanie uprawnień i związanych z wykonywaniem zadań służbowych.

8. Pracownik ma bezwzględny zakaz udostępniania zdalnego połączenia do sieci wewnętrznej innym urządzeniom, systemom, osobom. Dotyczy to również udostępniania jakichkolwiek usług i zasobów lokalnych urządzenia służbowego.

9. Pracownik ma obowiązek niezwłocznego zgłoszenia, bezpośrednio lub za pośrednictwem bezpośredniego przełożonego, wszelkich zdarzeń, które mogą spowodować lub powodują zagrożenie dla bezpieczeństwa informacji. Powyższe dotyczy w szczególności zaobserwowanych prób ataków, utraty, zniszczenia lub uszkodzenia urządzeń, ujawnienia informacji uwierzytelniających, utraty nośników informacji w tym dokumentów.

10. Problemy techniczne inne niż zdarzenia wskazane w ust. 9 pracownik zobowiązany jest zgłaszać bezpośrednio lub za pośrednictwem bezpośredniego przełożonego, w wewnętrznym systemie zgłoszeń.

11. W sytuacji ujawnienia przypadków korzystania ze zdalnego dostępu w sposób niezgodny z zasadami bezpieczeństwa czy przyznanym zakresem uprawnień ASI ma prawo m.in. do cofnięcia lub czasowego zawieszenia dostępu do kont, sieci wewnętrznej i systemów co najmniej do czasu wyjaśnienia zdarzenia.

12. W sytuacji wystąpienia zdarzenia, o którym mowa w ust. 11, które zostanie zaklasyfikowane jako incydent bezpieczeństwa, dyrektor BT może wystąpić do bezpośredniego przełożonego pracownika lub kierującego komórką organizacyjną pracownika o zastosowanie wobec pracownika przewidzianej właściwymi przepisami kary porządkowej w związku z incydentem bezpieczeństwa i niestosowaniem zasad bezpieczeństwa, postanowień Regulaminu pracy w Inspektoracie, przepisów kodeksu pracy czy przepisów dotyczących służby cywilnej.

Polityka korzystania z urządzeń prywatnych (BYOD)

§ 6. 1. Dopuszcza się wykorzystanie przez pracownika następujących urządzeń prywatnych:

1) urządzeń mobilnych do wykonywania połączeń głosowych i udostępniania transmisji danych dla przenośnego urządzenia służbowego;
2) domowych urządzeń sieciowych w zakresie bezprzewodowego podłączenia do nich użytkowanych urządzeń służbowych w celu transmisji danych;
2) urządzeń, których wykorzystanie jest niezbędne do zapewnienia zgodności stanowiska pracy zdalnej z przepisami prawa; dotyczy to wyłącznie monitora, klawiatury oraz urządzenia wskazującego (mysz);
3) słuchawek, mikrofonu lub słuchawek z wbudowanym mikrofonem.

2. Korzystanie z jakichkolwiek innych, niż wskazane w ust. 1 urządzeń prywatnych, w tym komputerów stacjonarnych, laptopów, notebooków, netbooków, tabletów, oraz wymiennych nośników informacji (m.in. dyski zewnętrzne, karty pamięci, pendrive) jest zabronione i wykrycie tego typu działań będzie traktowane jako incydent bezpieczeństwa.

Wymagania i zasady dotyczące informacji uwierzytelniających

§ 7. 1. System:

1) powinien wykorzystywać bezpieczny algorytm funkcji skrótu do przechowywania haseł;
2) nie powinien wymuszać okresowej zmiany haseł;
3) nie powinien pozwalać na ustawienie hasła znajdującego się na liście słabych/często używanych haseł;
4) nie powinien pozwalać na ustawienie hasła zawierającego przewidywalne człony (np. nazwa firmy, usługi);
5) powinien ustalać minimalną długość hasła na co najmniej 12 znaków, a dla haseł kont administracyjnych na co najmniej 14 znaków;
6) powinien pozwalać na ustawienie hasła o długości co najmniej do 64 znaków;
7) nie powinien wymagać dodatkowych kryteriów złożoności, np. znaków specjalnych, cyfr czy dużych liter;
8) powinien wymuszać zmianę hasła jeśli potwierdzono, bądź zachodzi podejrzenie, że aktualne hasło zostało przejęte lub upublicznione;
9) powinien podawać dokładny powód w przypadku odrzucenia nowego hasła;
10) nie powinien blokować wykorzystania funkcji „wklej” na polu hasła;

11) powinien podpowiadać użytkownikowi, jaka jest siła wprowadzonego hasła.

2. Zaleca się, aby system wspierał uwierzytelnianie dwuskładnikowe.

3. Pracownicy oraz użytkownicy, w tym administratorzy systemów mają obowiązek stosowania silnych haseł w tych systemach, z których korzystają. Szczegółowe wymagania dla haseł określa dokumentacja danego systemu.

4. Silne hasła[5), 6)]:

1) W celu stworzenia silnego hasła, które będziemy w stanie zapamiętać, można używać zasady pełnych zdań. Należy unikać znanych cytatów czy powiedzeń, ale po modyfikacji mogą nam one posłużyć jako inspiracja. Tak stworzone hasło powinno składać się z przynajmniej pięciu słów. Przykładowo: WlazlKostekNaMostekIStuka – jest przykładem silnego hasła, które można łatwo zapamiętać.
2) Inną wartą polecenia metodą jest budowanie hasła z opisu wyimaginowanej sceny, której obraz jest łatwy do zapamiętania i jednoznacznego opisania: zielonyParkingDla3malychSamolotow – jest przykładem takiego hasła. Przy czym należy zwrócić uwagę, że scena, którą opisuje nasze hasło, powinna zawierać jakiś element nierealistyczny albo abstrakcyjny. Wynika to z tego, że ludzie mają tendencję do używania obiektów, z którymi mieli ostatnio styczność, widzą je, albo są w ich pobliżu, jako składowe wymyślonego hasła. Pozwala to na użycie mniejszego słownika przy próbie łamania haseł, poprzez dostosowanie go pod konkretną osobę lub grupę osób.
3) Kolejnym pomysłem na generowanie silnego hasła jest użycie słów z kilku języków. Przykładem takiego hasła może być: DwaBialeLatajaceSophisticatedKroliki. Jego siła bierze się z tego, że próby łamania haseł opartych o całe zdanie muszą zostać wykonane metodą słownikową, a takie słowniki najczęściej zawierają słowa/zwroty z jednego języka.

5. Dopuszcza się stosowanie menedżerów haseł. Dostęp do bazy haseł powinien być zabezpieczony silnym hasłem o długości co najmniej 14 znaków, a jeżeli wykorzystywane rozwiązanie umożliwia stosowanie uwierzytelnienia dwuskładnikowego, również tego uwierzytelnienia. Zalecane jest stosowanie rozwiązań wykorzystujących do ochrony haseł wieloiteracyjnych funkcji skrótu z użyciem soli oraz dodatkowo pieprzu[7)].

[5)] Źródło: https://cert.pl/posts/2022/01/kompleksowo-o-haslach/

[6)] Haseł podanych w przykładach nie należy stosować z uwagi na ich ujawnienie do publicznej wiadomości.

[7)] Solenie hasła jest używane w połączeniu z mieszaniem. Kiedy solisz hasło, dodajesz losowe liczby całkowite i łańcuchy do każdego hasła, zanim je zaszyfrujesz. Sól to losowa, dość duża wartość generowana podczas korzystania z bezpiecznego generatora liczb losowych lub generatora losowych bitów. Sole są przechowywane z każdą wartością skrótu hasła na serwerze, tworząc w ten sposób unikalne wartości skrótu dla haseł. Pieprzenie hasła to technika ochrony haseł polegająca na dodaniu tajnego i losowego ciągu znaków do hasła, zanim zostanie ono

6. Hasła domyślne należy obowiązkowo zmieniać na hasła silne. Jeżeli domyślne konta w systemach nie są używane, powinny zostać wyłączone, a uprawnienia przypisane do tych kont odebrane.

7. W przypadku wykorzystywania do uwierzytelnienia kodów PIN m.in. w urządzeniach mobilnych lub korzystając z kart kryptograficznych z certyfikatami:

1) PIN powinien być co najmniej 4-znakowy, zalecane jest stosowanie 8-znakowego; dla różnych systemów mogą być określone różne wymagania długości kodu PIN; należy unikać oczywistych informacji m.in. dat urodzenia lub numerów związanych z osobą lub jej otoczeniem;
2) blokowanie urządzenia mobilnego lub karty powinno następować po maksymalnie 3 kolejnych nieudanych próbach uwierzytelnienia z użyciem kodu PIN.

Wymagania i zasady dotyczące kontroli dostępu

§ 8. 1. Każdy system musi posiadać formalny i prowadzony w sposób udokumentowany, proces rejestrowania i wyrejestrowywania użytkowników oraz przydzielania i odbierania praw dostępu do wszystkich usług wszystkim kategoriom użytkowników.

2. Użytkownicy mogą korzystać wyłącznie z tych zasobów i funkcjonalności, do których zostały im nadane prawa dostępu. Zakazane są próby uzyskania dostępu do zasobów i funkcjonalności, do których użytkownikowi nie nadano uprawnień, a także samodzielne próby potwierdzania lub wykorzystywania podatności. Wykrycie takich prób będzie traktowane jako incydent bezpieczeństwa i może skutkować dla użytkownika odpowiedzialnością dyscyplinarną oraz karną.

3. Rozpoczynając pracę użytkownik musi podać wszystkie wymagane własne informacje uwierzytelniające w sposób uniemożliwiający ich ujawnienie innym osobom.

4. Użytkownik zobowiązany jest uwierzytelniać się z wykorzystaniem wyłącznie własnych informacji uwierzytelniających. Uwierzytelnienie lub próby uwierzytelniania z wykorzystaniem informacji innego użytkownika będzie traktowane jako świadome naruszenie zasad bezpieczeństwa.

5. Prawa uprzywilejowanego dostępu mogą posiadać wyłącznie osoby, które w ramach wykonywanych zadań służbowych realizują zadania związane z administrowaniem, utrzymaniem, bezpieczeństwem i ciągłością działania danego systemu. Zakres przyznanych

zasolone i zaszyfrowane, aby uczynić je bezpieczniejszym. Ciąg znaków dodawany do hasła nazywa się pieprzem. Pieprz całkowicie zmienia hash hasła i czyni je odpornym na ataki siłowe i łamanie haseł przy użyciu tabel słowników i tęczowych tabel.

uprawnień musi być ograniczony do tych umożliwiających realizację zadań służbowych i nie powinien obejmować dostępu do danych w systemie, jeżeli istnieje taka możliwość.

6. Prawa dostępu, w tym uprzywilejowanego dostępu do systemu mogą posiadać pracownicy podmiotów zewnętrznych na podstawie zawartych umów, wyłącznie w zakresie i celu niezbędnym do realizacji powierzonych umowami zadań. Okres dostępu pracowników podmiotów zewnętrznych powinien być ograniczony i nie może wykraczać poza okres obowiązywania umowy. Za określenie okresu przyznania uprawnień odpowiada kierujący komórką organizacyjną (właściciel umowy) lub pracownik wskazany w umowie odpowiedzialny za jej realizację. Dostępy dla pracowników podmiotów zewnętrznych mogą być przyznane wyłącznie do określonych usług, portów, podsieci lub poszczególnych adresów IP, wyłącznie w zakresie i celu niezbędnym do wykonania zadań wynikających z zawartej umowy.

7. Przeglądy praw dostępu obejmują pełny przegląd uprawnień użytkowników, który powinien być realizowany przez AMS i ASI nie rzadziej niż raz na rok (pół roku dla uprawnień uprzywilejowanych). Celem przeglądu jest weryfikacja kont w systemie oraz prawidłowości przydzielonych praw dostępu.

8. Należy zapewnić kontrolę dostępu do kodów źródłowych oprogramowania. Za bezpieczne przechowywanie kodu źródłowego odpowiada właściciel danego systemu, który powinien formalnie wyznaczyć pracowników uprawnionych do dostępu do tego kodu. Kody źródłowe oprogramowania należy przechowywać w sposób zapewniający poufność, integralność, dostępność, autentyczność i rozliczalność.

Wymagania i zasady dotyczące stosowania zabezpieczeń kryptograficznych

§ 9. 1. Tam, gdzie jest to uzasadnione wynikami szacowania ryzyka, oraz w szczególności w komunikacji z wykorzystaniem sieci publicznej Internet lub gdy przesyłane są informacje wymagające ochrony z uwagi na ich klasyfikację, uwzględniając m.in. cel, koszty adekwatność należy stosować zabezpieczenia kryptograficzne do ochrony informacji.

2. W przypadku stosowania zabezpieczeń kryptograficznych należy opracować politykę określającą m.in. zasady korzystania z ochrony kryptograficznej, sposób zapewnienia ochrony, odpowiedzialność, okresy ważności kluczy kryptograficznych.

3. Przesyłanie lub przechowywanie informacji wymagających ochrony z uwagi na ich klasyfikację wymaga ich zaszyfrowania. W tym celu pracownicy mają obowiązek stosowania zabezpieczeń m.in.:

1) w komunikacji wewnętrznej – szyfrowanie wiadomości zawierających informacje wymagające ochrony z wykorzystaniem mechanizmów poczty elektronicznej;
2) w komunikacji zewnętrznej:
   a. szyfrowanie wiadomości z wykorzystaniem mechanizmów poczty elektronicznej pod warunkiem posiadania dedykowanego do tego celu certyfikatu i kluczy kryptograficznych,
   b. szyfrowanie załączników do wiadomości z wykorzystaniem np. PGP[8)] lub funkcjonalności szyfrowania oprogramowania do archiwizacji;
3) przy przechowywaniu plików na dysku lokalnym komputera lub w zasobach sieciowych – ograniczenie dostępu do folderów z wykorzystaniem mechanizmu uprawnień, a najlepiej zaszyfrowanie przechowywanych informacji z wykorzystaniem np. PGP lub funkcjonalności szyfrowania oprogramowania do archiwizacji;
4) przy przesyłaniu do zewnętrznych odbiorców nośników zawierających informacje wymagające ochrony, w szczególności dane osobowe – zaszyfrowanie informacji zapisywanych na nośniku z wykorzystaniem np. PGP lub funkcjonalności szyfrowania oprogramowania do archiwizacji lub korzystanie z nośników posiadających wbudowaną funkcjonalność szyfrowania zawartości.

4. W przypadku konieczności wymiany informacji wymagających ochrony, w szczególności danych osobowych z podmiotami zewnętrznymi, m.in. wykonawcami realizującymi usługi na rzecz Inspektoratu, należy w umowach z tymi wykonawcami lub niezwłocznie po zawarciu takich umów ustalić sposób bezpiecznej wymiany informacji wymagających ochrony, w tym uwzględnić możliwość wykorzystania jednej z metod wskazanych w ust. 3.

5. Pamięć stała (dyski zainstalowane w urządzeniu) wszystkich komputerów używanych przez pracowników, w szczególności używanych do wykonywania zadań służbowych w formie pracy zdalnej lub innej pracy na odległość / w terenie musi być zaszyfrowana bez możliwości odszyfrowania inicjowanego przez pracownika lub bez konieczności podania hasła / klucza odszyfrowania.

Wymagania i zasady dotyczące dokumentacji systemów

§ 10. 1. Zapewniając prowadzenie dokumentacji systemów właściciel systemu powinien zapewnić właściwy sposób zaadresowania zagadnień:

[8)] W przypadku chęci skorzystania z PGP należy zawnioskować o instalację oprogramowania do obsługi PGP w systemie zgłoszeń informatycznych.

1) dokumentacja systemu powinna być oznaczona w sposób identyfikujący właściciela (Główny Inspektorat Transportu Drogowego) oraz system, którego dotyczy;
2) dokumentacja systemu powinna zawierać informację o kategorii, jaką dany dokument stanowi np. informacje wrażliwe, dokument wewnętrzny;
3) dokumentacja systemu, która zawiera opis stosowanych zabezpieczeń oraz szczegółowe konfiguracje, jest uznawana za dokumentację zawierającą informacje wrażliwe i wymaga zapewnienia odpowiedniej ochrony poufności, integralności i dostępności;
4) dokumentacja systemu powinna być objęta formalnym procesem jej zatwierdzania i wprowadzania zmian, w tym zarządzeniem wersjami;
5) dokumentacja systemu w szczególności w zakresie jej elementów dotyczących bezpieczeństwa powinna być poddawana okresowym przeglądom, które należy przeprowadzać nie rzadziej niż raz na rok, oraz w razie zmiany otoczenia systemu czy identyfikacji potrzeby aktualizacji, czego efektem powinno być opracowanie zaktualizowanej dokumentacji i jej formalne zatwierdzenie;
6) dokumentacja systemu powinna być poddawana przeglądom i aktualizacji każdorazowo w związku z wdrażanymi zmianami w systemie;
7) dla użytkowników, administratorów itp. zawsze powinna być dostępna dokumentacja systemu w aktualnej wersji, w zakresie jaki jest im niezbędny do wykonywania zadań służbowych np. podręcznik użytkownika, dokumentacja administratora;
8) użytkownicy mogą być adresatami tylko części dokumentacji, nie powinni mieć dostępu do szerszego zakresu dokumentacji niż jest im niezbędny do pracy;
9) dystrybucja dokumentacji systemu powinna być prowadzona na podstawie ustalonych zasad jej dystrybucji, czyli określenia właściwego dla danego interesariusza zakresu dokumentacji i przekazania ustalonym kanałem komunikacji, z zachowaniem zasad bezpiecznej komunikacji;
10) dokumentacja systemu powinna być przechowywana uwzględniając jej formę, w miejscach i w sposób gwarantujący zapewnienie poufności, integralności i dostępności.

2. Właściciel danego systemu ma zapewnić, aby ASI oraz AMS dokumentowali działania wykonywane w systemie co najmniej obejmujących:

1) zarządzanie uprawnieniami w systemie;
2) serwis sprzętu i oprogramowania systemu;
3) zarządzanie incydentami w systemie;
4) kopie zapasowe oraz ich testowanie;

5) zarządzanie zmianami w systemie;
6) stosowanie poszczególnych zabezpieczeń i ich obsługę w systemie;
7) monitorowanie działania systemu i jego bezpieczeństwa, w tym przeglądy i weryfikacje dzienników zdarzeń;
8) zarządzanie podatnościami;
9) aktualizacje oprogramowania

– w zakresie szczegółowym wynikającym z obowiązujących przepisów prawa, na podstawie polityk i procedur ustanowionych i wdrożonych dla systemu.

3. Do opracowania dokumentacji bezpieczeństwa systemu zaleca się wykorzystać zalecenia i wytyczne określone w dokumencie NSC 800–18 „*Przewodnik do opracowywania planów bezpieczeństwa systemów informacyjnych w podmiotach publicznych*”.

Wymagania i zasady dotyczące kopii zapasowych

§ 11. 1. ASI mają obowiązek ustalić zakres i sposób wykonywania kopii zapasowych (polityka kopii zapasowych wraz z procedurami szczegółowymi) w systemie z uwzględnieniem wymogów prawnych, potrzeb biznesowych właściciela oraz możliwości technicznych, uwzględniając w dokumentacji:

1) zakres systemu i danych podlegających zabezpieczeniu;
2) częstotliwość wykonywania kopii zapasowych (harmonogram szczegółowy);
3) czas i miejsce wykonywania kopii zapasowych;
4) nośniki wykorzystywane do przechowywania kopii zapasowych, jeżeli kopie te są przechowywane na takich nośnikach oraz miejsce ich przechowywania;
5) odpowiedzialnych za wykonywanie i weryfikację poprawności wykonania kopii zapasowych oraz za nośniki wykorzystywane w procesie i ich transport do lokalizacji zapasowej, jeżeli dotyczy;
6) częstotliwość, zakres i odpowiedzialnych za testowanie kopii zapasowych;
7) sposób wykonywania kopii zapasowych (procedury szczegółowe) uwzględniający obowiązek dokumentowania wykonywanych działań i błędów w wykonaniu kopii zapasowych oraz ich obsługi przez ASI, jak również sporządzania raportów z weryfikacji kopii zapasowych.

2. Wykonanie kopii zapasowych, błędy wykonania kopii zapasowych oraz awaryjne i okresowe testowe odtworzenia należy dokumentować zgodnie z procedurami. Czynności mogą być odnotowywane automatycznie przez oprogramowanie wykorzystywane

do zarządzania kopiami zapasowymi, o ile posiada ono taką funkcjonalność. Czynności, których odnotowanie nie jest możliwe w sposób automatyczny, są dokumentowane przez ASI zgodnie z procedurami.

3. Za wykonywanie kopii zapasowych odpowiada ASI.

4. Zalecane jest przechowywanie jednego zestawu kopii zapasowych poza fizyczną lokalizacją, w której znajduje się ten system lub jego podstawowa kopia zapasowa.

5. Przed dokonywaniem istotnych zmian konfiguracyjnych mogących skutkować niestabilnym działaniem systemu (np. wgranie nowej wersji oprogramowania), należy wykonać dodatkową kopię zapasową, z wyłączeniem elementów systemu, dla których uprzednio wykonana kopia pozostaje aktualna na dzień wykonywania zmiany.

6. Informacje zapisywane lokalnie na urządzeniach pracownik ma obowiązek zabezpieczyć, m.in. poprzez umieszczenie ich w wewnętrznych zasobach sieciowych, dla których wykonywane są kopie zapasowe.

7. Kopie zapasowe ustawień urządzeń sieciowych wykonywane są każdorazowo po zmianie konfiguracji urządzeń. Wymagane jest przechowywanie, co najmniej bieżącej i poprzedniej konfiguracji urządzenia sieciowego, jeżeli dokumentacja danego systemu nie stanowi inaczej.

8. Odtwarzanie kopii zapasowych co do zasady może nastąpić w wyniku:

1) działań związanych z obsługą awarii lub zmianą konfiguracji;
2) okresowego sprawdzania możliwości odtworzenia kopii zapasowej;
3) na podstawie decyzji właściciela danego systemu;
4) na wniosek użytkownika, jeżeli dotyczy to zasobów zgromadzonych na jego udziale sieciowym lub udziale wspólnym;
5) innych nieokreślonych powyżej przyczyn i powodów, w tym na podstawie oceny danej sytuacji czy planów ciągłości działania.

9. Odtworzenie z kopii zapasowej jest realizowane i dokumentowane przez ASI.

10. Jeżeli odtwarzanie z kopii zapasowych może negatywnie wpłynąć na dostępność systemu lub ciągłość procesu biznesowego, odtwarzanie należy wykonać po godzinach pracy Inspektoratu, w przewidzianym oknie serwisowym systemu lub w innym czasie, w którym niedostępność będzie dla użytkowników lub procesów biznesowych najmniej problematyczna. Powyższe nie dotyczy sytuacji wyjątkowych, m.in. awarii i incydentów bezpieczeństwa.

11. Weryfikację technicznej możliwości odtworzenia danej kopii zapasowej (przydatności do wykorzystania) powinno się wykonywać nie rzadziej, niż raz na pół roku. Okres ten może

być wydłużony maksymalnie do 1 roku. Weryfikacja powinna w miarę możliwości być realizowana automatycznie przez system do zarządzania kopiami zapasowymi.

12. Za weryfikację kopii zapasowych oraz wykonywanie testów odtworzeniowych odpowiedzialni są ASI. Testy odtworzenia kopii zapasowych należy wykonywać na wydzielonym środowisku. Weryfikacja i testy odtworzenia kopii zapasowych podlegają udokumentowaniu.

Wymagania i zasady dotyczące rejestrowania zdarzeń oraz monitorowania

§ 12. 1. Monitorowanie należy realizować w sposób ciągły co najmniej poprzez bieżący oraz okresowy przegląd dzienników zdarzeń. Za monitorowanie odpowiedzialni są ASI.

2. Zakres i sposób realizacji czynności związanych z monitorowaniem należy określić w procedurach. Za opracowanie procedur odpowiedzialni są ASI.

3. Zalecane jest wdrożenie rozwiązań technicznych umożliwiających korelację i analizę zdarzeń pochodzących z różnych źródeł.

4. Każdy system musi rejestrować zdarzenia, których obowiązek rejestrowania wynika z przepisów prawa. Realizując ten obowiązek system musi zapewnić autentyczność, rozliczalność i niezaprzeczalność informacji.

5. Systemy powinny zapewnić rozliczalność parametrów SLA, w miarę możliwości w sposób automatyczny, na podstawie gromadzonych informacji o działaniu systemu i jego poszczególnych usług (m.in. czas uruchomienia i zakończenia działania usługi).

6. W systemach należy stosować rozwiązania techniczne pozwalające na rejestrowanie działań wykonywanych przez ASI, w szczególności pomijające standardowe mechanizmy rejestracji zdarzeń w danym systemie.

7. Zaleca się wdrożenie niezależnych mechanizmów i rozwiązań pozwalających na zbieranie, przeglądanie, analizę i monitorowanie zdarzeń w odniesieniu do czynności administracyjnych.

8. W odniesieniu do wykonywania procedur ASI oraz AMS są zobowiązani do prowadzenia ewidencji wykonywanych czynności np.: dzienników administratora, kart kontroli czynności codziennych lub okresowych itp. w celu zapewnienia pełnej rozliczalności i nadzoru nad realizacją swoich działań, jak również w celu kontroli wykonywania swoich obowiązków. Ewidencja wykonywanych czynności może być prowadzona elektronicznie, z wykorzystaniem rozwiązań teleinformatycznych w tym rejestrujących czynności

automatycznie pod warunkiem, że zapewnia rozliczalność tych czynności oraz ochronę zawartych tam wpisów.

9. System musi posiadać mechanizmy zabezpieczające przed nieuprawnionym dostępem, utratą i zmianami zapisów w dziennikach zdarzeń (poufność, dostępność i integralność tych zapisów) poprzez stosowanie m.in. mechanizmów kontroli dostępu, mechanizmów znakowania zapisów w dziennikach zdarzeń (np. znacznik czasu, podpis certyfikatem).

10. Dzienniki zdarzeń muszą być zabezpieczone (w sposób automatyczny lub organizacyjno-techniczny) przed ich przepełnieniem, mając na uwadze konieczność przechowywania zapisów w tych dziennikach przez okresy wynikające z przepisów prawa właściwe dla danego systemu.

Wymagania i zasady dotyczące nadzoru nad sprzętem i oprogramowaniem

§ 13. 1. Instalacja sprzętu i oprogramowania musi podlegać nadzorowi i być realizowana w sposób zapewniający bezpieczeństwo przetwarzanych informacji.

2. Sprzęt oraz oprogramowanie mogą być dopuszczone do eksploatacji jedynie po uzyskaniu akceptacji właściciela danego systemu, a w przypadku systemów, których infrastrukturą teleinformatyczną administruje BT, również akceptacji dyrektora BT. Powyższe dotyczy również wszelkiego nowego oprogramowania, które ma być instalowane na sprzęcie pracowników.

3. Należy zdecydowanie unikać wdrażania oprogramowania, które powiela funkcjonalność oprogramowania już eksploatowanego.

4. Dopuszczone do eksploatacji sprzęt i oprogramowanie podlegają zaewidencjonowaniu w CMDB.

5. W przypadku wykrycia korzystania przez pracowników lub personel podmiotów zewnętrznych z nieautoryzowanego sprzętu lub oprogramowania, w szczególności pozwalającego na omijanie zabezpieczeń lub naruszającego warunki jego licencji, o zdarzeniu informowany jest przełożony pracownika, kierujący komórką organizacyjną oraz Dyrektor Generalny. Zdarzenie opisane w zdaniu poprzednim stanowi incydent bezpieczeństwa.

6. Incydent bezpieczeństwa, opisany w ust. 5 nie dotyczy sprzętu i oprogramowania wykorzystywanego przez personel podmiotów zewnętrznych, gdy ten sprzęt i oprogramowanie stanowią własność tych podmiotów, pod warunkiem, że zostały formalnie uzgodnione zasady korzystania przez personel podmiotu zewnętrznego z własnego sprzętu i oprogramowania oraz

sposób jego wykorzystania uwzględniające wymogi ochrony informacji Inspektoratu. W przeciwnym razie zdarzenie stanowi incydent bezpieczeństwa.

Przeglądy, konserwacje i naprawy sprzętu

§ 14. 1. Okresowe przeglądy i konserwacje mające na celu weryfikację prawidłowości działania urządzeń należy realizować z uwzględnieniem zaleceń producentów tych urządzeń.

2. Przeglądy, konserwacje i naprawy powinny być realizowane przez ASI lub podmioty zewnętrzne pod nadzorem ASI.

3. W przypadku, gdy prace wykonuje personel podmiotu zewnętrznego, w miarę możliwości powinny być one prowadzone bez dostępu do informacji.

4. W wypadku konieczności dostępu personelu podmiotu zewnętrznego do informacji należy zapewnić realizację wymagań związanych z ochroną informacji, w szczególności danych osobowych. W przypadku dostępu do danych osobowych może być wymagane powierzenie przetwarzania tych danych zgodnie z wymogami prawnymi.

Użytkowanie oprogramowania

§ 15. 1. Oprogramowanie powinno być użytkowane zgodnie z jego warunkami licencyjnymi.

2. Do użytkowania może być dopuszczone m.in. oprogramowanie:

1) komercyjne, w zakresie wykupionej licencji i warunków w niej określonych;
2) open source, freeware i podobne, jeżeli licencja dopuszcza jego użytkowanie do celów komercyjnych lub przez podmiot publiczny;
3) shareware, trial oraz inne podobne w ramach licencji testowej tylko na czas ważności tej licencji i tylko w takim zakresie, w jakim licencja ta pozwala na eksploatację oprogramowania;
4) dedykowane/dziedzinowe, tj. wytworzone na zamówienie Inspektoratu;
5) inne niewymienione w pkt 1-4, jeżeli warunki użytkowania tego oprogramowania na to pozwalają.

2. Co najmniej raz w roku należy przeprowadzić przegląd licencji oprogramowania mający na celu m.in.:

1) weryfikację zgodności ilości użytkowanego oprogramowania z liczbą posiadanych licencji;
2) weryfikację zgodności sposobu użytkowania oprogramowania z postanowieniami warunków licencyjnych;

3) weryfikację, czy nie upływa okres posiadanego wsparcia, jeżeli było wykupione;
4) weryfikację, czy nie upływa okres ważności licencji dla licencji terminowych;
5) weryfikację, czy oprogramowanie nie wchodzi w okres końca wsparcia (ang. End Of Support) lub końca życia (ang. End Of Life);
6) potwierdzenie przydatności oprogramowania.

3. Przegląd licencji powinien przeprowadzać ASI, w tym z wykorzystaniem CMDB.

4. Dopuszczenie oprogramowania do eksploatacji powinno być poprzedzone jego dogłębną weryfikacją. Uwzględniając m. in. zakres, cel, kontekst, potrzeby, weryfikacja oprogramowania powinna obejmować:

1) funkcjonalność; czy realizuje potrzeby biznesowe;
2) wymagania sprzętowe i programowe niezbędne do jego bezproblemowego działania;
3) wymagania w zakresie uprawnień użytkownika uruchamiającego oprogramowanie m.in. czy nie wymaga ono nadmiarowych, w tym administracyjnych praw dostępu do normalnego działania;
4) formaty plików wykorzystywanych przez oprogramowanie, m.in. kompatybilność z innym oprogramowaniem eksploatowanym w Inspektoracie oraz z wymaganiami prawnymi, jeżeli ma być w tym zakresie wykorzystywane;
5) komunikację oprogramowania z innymi elementami infrastruktury informatycznej, w szczególności wewnątrz i poza sieć wewnętrzną, w tym czy występuje komunikacja z obcymi serwerami i co ta komunikacja obejmuje;
6) zachowanie się oprogramowania w przypadku błędów, jeżeli występują i nie zostały usunięte przez producenta;
7) bezpieczeństwo tego oprogramowania, w tym możliwość jego automatycznej aktualizacji;
8) wsparcie i jego zakres realizowane przez dostawcę lub producenta;
9) warunki licencyjne;
10) koszty związane z wdrożeniem i eksploatacją, w tym usuwaniem błędów i aktualizacjami.

5. Weryfikacja oprogramowania może zostać przeprowadzona na podstawie analizy dokumentacji oprogramowania, informacji z rynku oraz testów oprogramowania przeprowadzanych w środowisku nieprodukcyjnym, przy czym nie dopuszcza się weryfikacji oprogramowania wyłącznie na podstawie jego dokumentacji.

6. Wynik weryfikacji oprogramowania powinien być udokumentowany co najmniej w formie elektronicznej.

Wycofywanie oprogramowania z eksploatacji

§ 16. 1. Oprogramowanie powinno być wycofane z eksploatacji m.in. w przypadku, gdy:

1) funkcjonalność oprogramowania nie jest dłużej wykorzystywana;
2) oprogramowanie zostało zastąpione przez inne, przy czym możliwe jest odczytywanie danych przez nowe oprogramowanie lub migracja danych;
3) w innym uzasadnionym przypadku.

2. Wycofanie oprogramowania powinno być odnotowane w CMDB.

Instalowanie oprogramowania

§ 17. 1. Oprogramowanie powinno być instalowane wyłącznie przez ASI lub innych uprawnionych do tego pracowników w ramach realizowanych przez nich zadań służbowych, w tym personel podmiotów zewnętrznych, jeżeli powierzono im takie zadania do realizacji.

2. Zwykły użytkownik nie powinien posiadać uprawnień do samodzielnej instalacji oprogramowania. Użytkownik taki powinien posiadać wyłącznie uprawnienia, które są mu niezbędne do wykonywania zadań służbowych na danym stanowisku.

3. Jeżeli nie jest to niezbędne do realizacji zadań służbowych, użytkownicy i administratorzy systemów nie powinni posiadać dostępu do narzędzi umożliwiających m.in.:

1) wykonanie operacji uprzywilejowanych, w tym zmieniających parametry konfiguracyjne oprogramowania w sposób wpływający na jego bezpieczeństwo;
2) weryfikację poziomu bezpieczeństwa zasobu, w tym wykrywanie podatności;
3) przeprowadzanie prób ataków;
4) omijanie stosowanych zabezpieczeń.

4. Wykrycie nieautoryzowanych narzędzi, o których mowa w ust. 3 jest traktowane jako incydent bezpieczeństwa.

5. Instalacja oprogramowania powinna odbywać się na podstawie zasadnego wniosku złożonego przez pracownika lub jego bezpośredniego przełożonego.

6. ASI powinien zweryfikować, czy:

1) wniosek jest zasadny m.in. z bezpośrednim przełożonym, jeżeli wniosek został złożony przez pracownika;
2) oprogramowanie, którego wniosek dotyczy zostało dopuszczone do użytku;
3) Inspektorat posiada licencję umożliwiającą instalację i użytkowanie tego oprogramowania.

7. Pozytywna weryfikacja powinna skutkować:

1) instalacją i konfiguracją oprogramowania;
2) weryfikacją poprawności działania oprogramowania po instalacji;
3) aktualizacją CMDB.

8. W przypadku oprogramowania, które nie zostało dopuszczone do użytku lub z innych powodów nie jest możliwa jego instalacja, należy o tym poinformować wnioskodawcę.

Repozytoria nośników instalacyjnych i pakietów instalacyjnych oprogramowania

§ 18. 1. Repozytoria nośników instalacyjnych i pakietów instalacyjnych oprogramowania powinni prowadzić ASI.

2. Nośniki instalacyjne oprogramowania oraz pakiety instalacyjne oprogramowania, w szczególności objęte licencjami i prawami autorskimi nie powinny być wynoszone poza pomieszczenia Inspektoratu. W przypadku konieczności ich wyniesienia poza pomieszczenia Inspektoratu takim nośnikom powinna być zapewniona odpowiednia ochrona przed ich zniszczeniem lub utratą.

3. Repozytoria oprogramowania powinny być zabezpieczone przed nieuprawnionym dostępem, podmianą lub inną ingerencją w integralność tego oprogramowania oraz przed zniszczeniem lub utratą.

4. Repozytoria oprogramowania powinny być prowadzone w taki sposób, aby zapewnić kontrolę wersji oprogramowania, jak również ograniczyć ryzyko wykorzystania niewłaściwej jego wersji.

Aktualizowanie oprogramowania

§ 19. 1. Odpowiedzialność za aktualizację oprogramowania ponoszą ASI, którzy tym oprogramowaniem zarządzają.

2. Informacje o aktualizacjach oprogramowania ASI powinien pozyskiwać z ogólnodostępnych źródeł, w szczególności publikacji producentów.

3. Dla każdej aktualizacji oprogramowania ASI powinien dokonać oceny zasadności jej implementacji. Aktualizacje usuwające błędy i podatności związane z bezpieczeństwem powinny być uznawane za wymagające dalszego procesowania w celu ich implementacji bez zbędnej zwłoki, jeżeli ich implementacja nie spowoduje negatywnych skutków. W przypadku identyfikacji negatywnych skutków powinny być zastosowane rozwiązania alternatywne do czasu, gdy możliwa będzie instalacja aktualizacji związanych z bezpieczeństwem nie powodująca negatywnych skutków.

4. Aktualizacje przeznaczone do implementacji należy poddawać, w miarę posiadanych możliwości technicznych testom w środowisku nieprodukcyjnym. Za wykonanie testów odpowiedzialny jest ASI.

5. Aktualizacje wykonywane w infrastrukturze serwerowej i sieciowej w środowiskach produkcyjnych powinny być instalowane przy zapewnieniu, że ASI posiada odpowiednią kopię zapasową umożliwiającą, w przypadku niepowodzenia implementacji, przywrócenie stanu danego systemu do stanu sprzed aktualizacji bez utraty danych. Z tego powodu aktualizacje w infrastrukturze serwerowej i sieciowej w środowiskach produkcyjnych powinny być wykonywane w miarę możliwości po godzinach pracy, oraz przy minimalnym obciążeniu operacjami lub po odłączeniu komunikacji, ograniczając ryzyko utraty danych.

6. Aktualizacje oprogramowania, w tym jego konfiguracji powinny być odnotowane w CMDB.

Bezpieczne użytkowanie sprzętu i oprogramowania

§ 20. 1. Każdy pracownik ma obowiązek użytkować powierzony mu sprzęt i oprogramowanie zgodnie z przeznaczeniem oraz w miarę posiadanych możliwości chronić przed zagrożeniami ze strony otoczenia (m in. ogień, zalanie, kurz, wyładowania elektryczne i elektrostatyczne) oraz osób trzecich. Należy unikać działań mogących stać się przyczyną utraty, uszkodzenia lub zniszczenia sprzętu.

2. W przypadku utraty sprzętu (w tym urządzeń mobilnych) niezależnie od jej formy (np. kradzież, zgubienie) pracownik ma obowiązek niezwłocznie zgłosić ten fakt jako incydent bezpieczeństwa, bezpośrednio lub za pośrednictwem bezpośredniego przełożonego. Ponadto pracownik jest zobowiązany do zgłoszenia utraty powierzonego mu wyposażenia służbowego do pracodawcy zgodnie z obowiązującymi w Inspektoracie regulacjami wewnętrznymi.

3. Zabronione jest samodzielne, przez pracowników instalowanie oraz zmiany konfiguracji oprogramowania i sprzętu bez uzyskania zgody dyrektora BT, chyba że działanie takie wynika bezpośrednio z zakresu obowiązków pracownika i realizowanych przez niego zadań służbowych.

4. Pracownik, któremu powierzono do użytkowania sprzęt i oprogramowanie odpowiada za ich bezpieczeństwo, w szczególności ponosi odpowiedzialność za umożliwienie wykorzystania powierzonego mu sprzętu i oprogramowania oraz dostęp za ich pośrednictwem do informacji i danych przez nieuprawnioną do tego osobę, w tym domowników i inne osoby z jej najbliższego otoczenia.

5. Zabronione jest ujawnianie informacji o konfiguracji urządzeń, oprogramowania czy systemów, w szczególności dotyczących stosowanych zabezpieczeń, jeżeli nie wynika to z umowy lub uprawnień, które wpływają na możliwość uzyskania takich informacji przez osobę lub podmiot zewnętrzny np. właściwe służby.

6. Przed przystąpieniem do pracy z wykorzystaniem urządzeń teleinformatycznych pracownik powinien sprawdzić ich stan ze zwróceniem szczególnej uwagi, czy nie zaszły okoliczności wskazujące na incydent bezpieczeństwa, w tym czy nie występują uszkodzenia, które mogą powodować zagrożenie dla zdrowia lub życia pracownika. Należy stosować się do obowiązujących zasad dotyczących bezpieczeństwa i higieny pracy.

Ochrona przed szkodliwym oprogramowaniem

§ 21. 1. Oprogramowanie służące do ochrony przed szkodliwym oprogramowaniem powinno być zainstalowane na wszystkich urządzeniach, na których jest to uzasadnione względami bezpieczeństwa, w szczególności na:

1) urządzeniach komputerowych powierzonych pracownikom;
2) urządzeniach mobilnych powierzonych pracownikom, jeżeli te urządzenia są wykorzystywane np. do dostępu do poczty elektronicznej;
2) serwerach.

2. Oprogramowanie służące do ochrony przed szkodliwym oprogramowaniem nie powinno zakłócać poprawnej pracy urządzenia, w tym jego wydajności. Parametr ten powinien być uwzględniony np. przy zakupie oprogramowania służącego do ochrony przed szkodliwym oprogramowaniem.

3. Za instalację i konfigurację oprogramowania służącego do ochrony przed szkodliwym oprogramowaniem odpowiada ASI. Konfiguracja powinna zapewniać:

1) automatyczne pełne skanowanie wszystkich podłączonych nośników w zdefiniowanych odstępach czasu;
2) automatyczne skanowanie wybranych obszarów urządzenia podczas uruchamiania;
3) możliwość skanowania na żądanie plików i folderów przez użytkownika;
4) uniemożliwienie wyłączenia ochrony lub zmian w jego konfiguracji np. bez podania hasła administracyjnego;
5) automatyczne aktualizacje baz sygnatur i definicji oraz samego oprogramowania, co najmniej raz dziennie;

6) automatyczne leczenie zainfekowanych plików, a w przypadku niemożliwości wykonania tej funkcji usuwanie tych plików lub umieszczanie ich w kwarantannie bez możliwości ich uwolnienia przez użytkownika.

4. Działanie oprogramowania służącego do ochrony przed szkodliwym oprogramowaniem powinno podlegać monitorowaniu i rejestrowaniu zdarzeń z wykorzystaniem centralnej konsoli zarządzania, zaś alerty o wykryciu szkodliwego oprogramowania powinny być niezwłocznie sygnalizowane w tej konsoli lub za pomocą powiadomień (np. na e-mail).

5. Oprogramowanie służące do ochrony przed szkodliwym oprogramowaniem powinno dostarczać funkcjonalność:

1) ochrony poczty elektronicznej;
2) ochrony przeglądarek internetowych;
3) skanowania podłączanych do urządzenia nośników lub aktywnego skanowania uruchamianych plików;
4) ochrony plików systemowych.

6. Zabronione jest wykonywanie jakichkolwiek samodzielnych zmian w konfiguracji oprogramowania służącego do ochrony przed szkodliwym oprogramowaniem, w tym jego czasowe lub permanentne wyłączanie.

7. Wszystkie pochodzące z zewnątrz nośniki informacji pracownik ma obowiązek sprawdzić przy pomocy zainstalowanego oprogramowania służącego do ochrony przed szkodliwym oprogramowaniem przed uruchomieniem jakiegokolwiek pliku z takiego nośnika.

8. Jeżeli pracownik zaobserwuje, że oprogramowanie służące do ochrony przed szkodliwym oprogramowaniem nie pracuje poprawnie na użytkowanym przez niego urządzeniu, ma obowiązek niezwłocznie zgłosić ten fakt w systemie zgłoszeń informatycznych lub bezpośrednio do właściwych pracowników BT.

9. Zalecanym do wdrożenia przez ASI zabezpieczeniem uzupełniającym zapobiegającym automatycznemu uruchamianiu się szkodliwego oprogramowani z podłączanych nośników powinno być wyłączenie możliwości automatycznego uruchamiania podłączanych nośników w systemie operacyjnym.

Wymagania i zasady dotyczące zarządzania podatnościami technicznymi

§ 22. 1. Dla każdego systemu wymagane jest zarządzanie podatnościami wykorzystywanego w danym systemie sprzętu i oprogramowania.

2. ASI oraz wszyscy użytkownicy są odpowiedzialni za zgłaszanie zauważonych podatności systemów, które użytkują.

3. Każdy użytkownik, który pozyskał informację o podatności, jest zobowiązany do niezwłocznego poinformowania o tym fakcie ASI.

4. Informacje na temat podatności w eksploatowanym oprogramowaniu ASI powinni pozyskiwać na podstawie:

1) zgłoszeń dotyczących problemów z poprawnym działaniem systemu;
2) informacji pochodzących z monitorowania systemu;
3) informacji pozyskiwanych z zewnątrz m.in. od producentów sprzętu i oprogramowania, repozytoriów CVE;
4) informacji od innych podmiotów i grup zainteresowania, w tym organów administracji publicznej, m.in.: różnych CSIRT, Rządowego Centrum Bezpieczeństwa, Pełnomocnika Rządu do spraw Cyberbezpieczeństwa.

5. Podatności mogą być usuwane m.in. poprzez:

1) aktualizację oprogramowania;
2) modyfikację konfiguracji;
3) wymianę na inną wersję lub inny produkt.

6. Podatności należy usuwać bez zbędnej zwłoki, jeżeli jest to możliwe w danym środowisku informatycznym.

7. W przypadku podatności, które nie mogą być usunięte niezwłocznie lub nie mogą być usunięte z powodu braku rozwiązań technicznych w tym zakresie, należy przedsięwziąć środki minimalizujące ryzyko wykorzystania tych podatności.

Wymagania i zasady dotyczące bezpieczeństwa sieci teleinformatycznych

§ 23. 1. Zdalny dostęp do sieci wewnętrznej jest możliwy jedynie z wykorzystaniem protokołów zapewniających poufność przesyłanych informacji oraz uwierzytelnianie połączeń i użytkowników.

2. Wymagane jest stosowanie mechanizmów filtrowania ruchu sieciowego pozwalającego na skuteczne ograniczenie dostępu jedynie do zdefiniowanych zasobów sieciowych niezbędnych do realizacji zadań wykonywanych w sposób zdalny.

3. Dostęp do zasobów innych sieci, w tym sieci publicznej zaleca się ograniczyć wyłącznie do usług i protokołów, które są niezbędne do wykonywania przez pracowników ich zadań. Należy przyjmować, że użytkownicy mogą mieć dostęp wyłącznie do zasobów udostępnianych

za pośrednictwem protokołów HTTP (zalecane jest w ogóle nie używać komunikacji niezabezpieczonej), HTTPS. Jako usługi udostępniane za pośrednictwem wymienionych protokołów należy rozumieć dostęp wyłącznie do serwerów WWW z wykluczeniem innych usług (np.: komunikatory, serwery proxy lub inne usługi mogące być wykorzystane do tworzenia ukrytych kanałów wymiany/przesyłu informacji).

4. Użytkownicy sieci wewnętrznej muszą poprawnie przejść proces uwierzytelnienia wymuszany przez elementy infrastruktury informatycznej.

5. Wszystkie pliki pobierane z sieci należy poddawać kontroli i sprawdzeniu, czy nie zawierają szkodliwego oprogramowania.

Wymagania i zasady dotyczące projektowania bezpiecznych systemów

§ 24. 1. Realizując prace rozwojowe systemu należy m.in. zapewnić:

1) zdefiniowanie wymagań dla systemu, w tym odnoszących się do bezpieczeństwa tego systemu oraz danych i informacji w nim przetwarzanych, zapewniających poufność, integralność i dostępność systemu oraz tych danych i informacji, z uwzględnieniem atrybutów bezpieczeństwa takich jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność;
2) bezpieczeństwo m. in. środowisk deweloperskich, rozwojowych;
3) bezpieczeństwo oprogramowania i danych na każdym etapie prac;
4) kontrolę realizacji wszystkich zdefiniowanych wymagań na każdym etapie prac;
5) bezpieczeństwo wykorzystywanych repozytoriów (m.in. rozliczalność i dostępność, oraz jeżeli tego wymaga specyfika przechowywanych w repozytoriach informacji, również poufność);
6) kontrolę wersji oprogramowania i dokumentacji;
7) realizację prac przez osoby i podmioty posiadające odpowiednią wiedzę i umiejętności;
8) zarządzenie i kontrolę zmian zakresu (zarządzanie zmianami);
9) testy systemu, m.in. testy funkcjonalne, bezpieczeństwa, wydajnościowe, regresji, odtworzenia, potwierdzające spełnianie przez system wszystkich zdefiniowanych wymagań. Zakres i rodzaje wykonywanych testów każdorazowo należy dostosować do danego przypadku (np. dla małej zmiany wykonywanie wszystkich testów może nie być uzasadnione merytorycznie).

2. Testy mają na celu potwierdzenie, że system spełnia wszystkie zdefiniowane wymagania (lub wymagania dla zmiany). Testy należy prowadzić na podstawie

zaakceptowanych planów testów i scenariuszy testowych. Zakres testów należy dostosować do specyfikacji wymagań, z zastrzeżeniem, że testy nie powinny ograniczać się wyłącznie do wymagań określonych w specyfikacji i powinny uwzględniać testy wynikające z dobrych praktyk, standardów, norm, zaleceń i wytycznych podmiotów uprawnionych do ich wydawania (np.: CSIRT, Pełnomocnik Rządu do spraw bezpieczeństwa cyberprzestrzeni).

3. Testy należy wykonywać przy bezpośrednim udziale przedstawicieli właściciela systemu, pracowników innych komórek organizacyjnych użytkujących, mających użytkować lub odpowiadać za działanie systemu, oraz opcjonalnie innych zewnętrznych interesariuszy, którzy są lub będą jego użytkownikami (np. uczestniczyli w definiowaniu wymagań).

4. Testy należy powtarzać, jeżeli ich wyniki nie są pozytywne, po wdrożeniu odpowiednich działań korygujących lub naprawczych.

5. Testy należy prowadzić w środowiskach nieprodukcyjnych.

6. Przebieg i wyniki testów należy dokumentować.

7. Opracowując specyfikację wymagań dla systemu należy wziąć pod uwagę ryzyka związane z implementacją wymagań, m.in. funkcjonalnych oraz niefunkcjonalnych, bezpieczeństwa, architektonicznych oraz technologicznych.

8. Specyfikacja wymagań funkcjonalnych powinna zapewnić realizację procesów biznesowych, uwzględniając wymogi prawne związane z tymi procesami.

9. W miarę możliwości do specyfikowania wymagań należy stosować notację UML lub BPMN, alternatywnie opisy procesów i wymagań z nimi związanych powinny umożliwić ich zamodelowanie w jednej ze wskazanych notacji.

10. Wymagania bezpieczeństwa i zabezpieczenia systemów powinny być określone na podstawie wyników szacowania ryzyka; w tym zakresie zaleca się wykorzystanie zaleceń i wytycznych oraz zabezpieczeń określonych w normie PN-ISO/IEC 27002 lub dokumentach:

1) NSC 200 „*Minimalne wymagania bezpieczeństwa informacji i systemów informacyjnych podmiotów publicznych*”;
2) NSC 800–53 „*Zabezpieczenia i ochrona prywatności systemów informacyjnych oraz organizacji*”;
3) NSC 800–53B „*Zabezpieczenia bazowe systemów informacyjnych oraz organizacji*”.

Dopuszczenie systemu do eksploatacji

§ 25. 1. Podstawą do wdrożenia systemu (lub danej zmiany) na środowiska produkcyjne powinien być pozytywny wynik testów. Odstępstwa w tym zakresie muszą być zatwierdzone

przez właściciela danego systemu w sposób udokumentowany, ze wskazaniem powodów odstępstwa i działań naprawczych lub korygujących, które zostaną podjęte. Niedopuszczalne jest wdrożenie na środowiska produkcyjne systemu (lub jego zmian), w sytuacji negatywnego wyniku testów, braku udokumentowanej zgody na odstępstwo i bez określenia działań korygujących i naprawczych, które zostaną podjęte w odniesieniu do testów zakończonych wynikiem negatywnym.

2. O dopuszczeniu systemu do użytkowania w środowisku produkcyjnym decyduje jego właściciel.

3. System (lub jego zmiana) może zostać dopuszczony do użytkowania w środowisku produkcyjnym, jeżeli:

1) posiada dokumentację umożliwiającą bieżącą eksploatację systemu;
2) posiada dokumentację obejmującą m.in.:
   a. procedury konfiguracji w zakresie pozwalającym na instalację i konfigurację systemu od podstaw (w tym elementy dokumentacji powykonawczej systemu),
   b. procedury zarządzania uprawnieniami użytkowników,
   c. procedury tworzenia kopii zapasowych,
   d. procedury ponownego uruchomiania systemu,
   e. procedury odtwarzania systemu w przypadku awarii,
   f. procedury zarządzania systemowymi dziennikami zdarzeń,
   g. procedury obsługi błędów i awarii,
   h. procedury wdrażania zmian,
   i. procedury testowania systemu po zmianach, w tym aktualizacjach,
   j. procedury monitorowania systemu,
   k. pozostałą dokumentację wynikająca wprost z przepisów prawa.

Prace związane z budową lub rozwojem systemów zlecane podmiotom zewnętrznym

§ 26. 1. Umowy dotyczące powierzania prac związanych z budową lub rozwojem systemów podmiotom zewnętrznym powinny uwzględniać:

1) opis wymagań systemu (lub jego zmiany), m.in. wymagań bezpieczeństwa, w tym w odniesieniu do wymogów wynikających z obowiązujących przepisów prawa;
2) opis wymagań dotyczących jakości świadczonych usług (SLA) zarówno w zakresie usług systemu, jak i usług realizowanych przez podmiot zewnętrzny (np.: czasy reakcji na zgłoszenia, czasy rozwiązywania zgłoszeń, błędów, awarii, problemów, napraw

gwarancyjnych, poszczególnych czynności eksploatacyjnych, utrzymaniowych czy administracyjnych);

3) obowiązek zapewnienia nadzoru nad dostępem do kodu źródłowego tworzonego oprogramowania oraz środowiska, w którym oprogramowanie jest rozwijane; dostęp do powyższych powinni posiadać tylko upoważnieni pracownicy, adekwatnie do zakresu zadań i wykonywanych czynności;
4) obowiązek przekazania kodu źródłowego oprogramowania wraz z prawami autorskimi oraz dokumentacją i – jeżeli ma zastosowanie – innym oprogramowaniem, m. in. bibliotekami, (wraz z odpowiednią licencją lub prawami autorskimi) umożliwiającymi samodzielną kompilację tego kodu, jego użytkowanie, udostępnianie, powierzanie, modyfikowanie itp. bez ograniczeń czasowych i terytorialnych;
5) obowiązek zabezpieczenia środowisk rozwojowych, deweloperskich itp. po stronie podmiotu zewnętrznego oraz jego podwykonawców, przed zagrożeniami, m.in. nieuprawnionym dostępem i modyfikacją informacji;
6) obowiązek zapewnienia i organizowania testów;
7) obowiązek wsparcia w zakresie przeprowadzenia analizy ryzyka dla systemu;
8) obowiązek dostarczenia pełnej dokumentacji systemu, określonej szczegółowo w wymaganiach;
9) obowiązek naprawy błędów i usuwania awarii;
10) opcjonalnie obowiązek naprawy błędów i usuwania awarii w przypadku wykonania przez Inspektorat audytu systemu we własnym zakresie na podstawie raportu z takiego audytu;
11) możliwość nadzoru i kontroli oraz audytu zadań powierzonych podmiotowi zewnętrznemu do realizacji, w tym przez upoważniony przez Inspektorat inny podmiot.

2. Jeżeli system ma być wykorzystywany do przetwarzania danych osobowych, należy zapewnić powierzenie przetwarzania danych osobowych podmiotowi zewnętrznemu w zakresie, jaki jest niezbędny do realizacji przez ten podmiot zadań.

3. Każda umowa, której realizacja wiąże się z możliwością dostępu personelu podmiotu zewnętrznego do informacji przetwarzanych w Inspektoracie, musi zawierać postanowienia zobowiązujące do zachowania poufności informacji, m.in. w odniesieniu do stosowanych w Inspektoracie zabezpieczeń oraz informacji podlegających prawnej ochronie, oraz do zwrotu m. in. przekazywanych informacji, dokumentów, nośników lub ich skutecznego usunięcia z własnych zasobów po zakończeniu umowy.

Wymagania i zasady dotyczące danych testowych i środowisk

§ 27. 1. Należy zapewnić separację środowisk nieprodukcyjnych od produkcyjnych, jak również:

1) testowanie zmian przed ich wdrożeniem na środowiska produkcyjne;
2) wysoką jakość i poprawność merytoryczną danych testowych;
3) wykorzystywanie danych produkcyjnych do celów testowych wyłącznie po wykonaniu pseudonimizacji lub anonimizacji tych danych;
4) rozliczalność dostępu do środowisk nieprodukcyjnych.

2. Zabronione jest korzystanie z danych rzeczywistych (pochodzących ze środowisk produkcyjnych) zawierających dane osobowe lub inne informacje wrażliwe lub prawnie chronione, do celów testowych, bez poddania tych danych pseudonimizacji lub anonimizacji oraz zapewnieniu rozliczalności dostępu do tych danych. Jeżeli takie dane są niezbędne do wykonania testów np. migracji danych, środowisko na którym są wykonywane podlega wszystkim rygorom i zabezpieczeniom, jak środowisko produkcyjne.

3. W przypadku wykorzystania danych produkcyjnych do celów testowych należy określić w procedurze lub innym dokumencie sposób pseudonimizacji lub anonimizacji danych produkcyjnych.

4. Należy zapewnić rozdzielność uprawnień w systemach produkcyjnych i nieprodukcyjnych, tj. każde środowisko musi posiadać odrębny mechanizm uprawnień dla niego dedykowany.

5. Środowiska nieprodukcyjne można wykorzystywać do testowania kopii zapasowych, o ile środowisko nieprodukcyjne na czas takie operacji podlega wyłączeniu z eksploatacji, tj. żaden inny użytkownik niż ASI wykonujący test odtworzenia nie może mieć dostępu do środowiska i danych w nim odtwarzanych, a po całej operacji, przed udostępnieniem środowiska nieprodukcyjnego użytkownikom, odtworzone dane są ze środowiska usuwane i zastępowane danymi właściwymi dla danego środowiska.

Zarządzanie zmianami w systemach

§ 28. 1. Zmiany w systemach należy skutecznie nadzorować oraz zarządzać procesem wprowadzania tych zmian, m.in. poprzez:

1) identyfikowanie i rejestrowanie zmian;
2) planowanie zmian;
3) testowanie zmian;

4) określanie wpływu zmian na cały system i nie ograniczanie się wyłącznie do zakresu danej zmiany;
5) szacowanie wpływu zmian na bezpieczeństwo (analiza ryzyka);
6) realizowanie zmian w sposób zorganizowany, zgodnie z przyjętymi procedurami zarządzania zmianami w danym systemie;
7) weryfikowanie na każdym etapie realizacji zmiany, czy spełnione są określone dla danej zmiany wymagania, m.in. wymagania bezpieczeństwa;
8) ustanowienia procedur technicznych opisujących sposób realizacji zmian w systemach uwzględniających odpowiedzialnych za wdrażanie i wycofywanie zmian, w tym odtwarzanie systemu lub jego elementów w przypadku takiej konieczności, oraz czynności niezbędne to realizacji poszczególnych zadań;
9) ustanowienie zasad wprowadzania zmian awaryjnych (w tym obejmujących skrócenie ścieżek decyzyjnych).

2. Należy dążyć do ujednolicenia, co najmniej w obrębie danego systemu, procedur dotyczących zarządzania zmianami, zarówno wynikającymi z eksploatacji oraz utrzymania, jak i rozwoju systemu.

3. Zalecane jest stosowanie jednolitych zasad zarządzania zmianami w więcej niż 1 systemie, w miarę możliwości we wszystkich systemach.

4. Za zapewnienie procesu zarządzania zmianami w systemie, aby proces ten przebiegał w sposób zorganizowany i udokumentowany odpowiada właściciel danego systemu.

Wymagania i zasady dotyczące zarządzania ciągłością działania

§ 29. 1. ASI są zobowiązani do:
1) monitorowania wykorzystania pojemności systemów;
2) monitorowania wydajności systemów;
3) planowania pojemności systemów wynikającej z bieżących potrzeb;
4) planowania wydajności systemów wynikającej z bieżących potrzeb;
5) monitorowania dostępności systemów.

2. ASI powinni być włączani w proces budowy i rozwoju w zakresie wymagań związanych z pojemnością i wydajnością systemów.

3. W celu zachowania możliwie optymalnej wydajności i pojemności systemów zalecane jest:

1) usuwanie lub archiwizowanie na zewnętrzne zasoby lub nośniki nieaktualnych danych, jeżeli jest to możliwe pod względem prawnym, w tym uwzględnienie okresów retencji danych;
2) usuwanie lub archiwizowanie na zewnętrzne zasoby lub nośniki aplikacji, systemów, baz danych, środowisk, jeżeli nie są używane;
3) optymalizowanie procesów wsadowych, środowisk, baz danych, systemów;
4) optymalizowanie logiki systemów, zapytań do baz danych;
5) odpowiednie zarządzanie usługami systemów wymagającymi wielu, czasem współdzielonych zasobów.

4. Wydajność systemu i jego usług powinna być jednym ze zdefiniowanych parametrów jakości usług raportowanych i podlegających rozliczeniu.

5. Dostępność systemów należy zapewnić poprzez wdrożenie właściwych zabezpieczeń określonych na etapie szacowania ryzyka.

6. Dla systemów, w których konsekwencje naruszenia dostępności informacji mogą powodować skutki natury prawnej, należy zdefiniować w planach ciągłości działania podejście do przywrócenia dostępności systemu, jego usług oraz informacji, w tym odtworzenie sprzętu i oprogramowania oraz zasobów ludzkich, jeżeli zajdzie taka konieczność.

7. ASI mają obowiązek opracować procedurę definiującą działania niezbędne do przywrócenia dostępności, obejmującą m.in. włączanie i wyłączanie całego systemu lub poszczególnych jego usług oraz zasoby niezbędne do realizacji procedury (np.: personel, hasła, kopie zapasowe).

8. Architektura infrastruktury informatycznej dla nowych systemów powinna być tak określana, aby zapewniała redundantność kluczowych jej elementów oraz możliwość szybkiego zastąpienia lub przejęcia działania w przypadku awarii jednego z tych elementów.

9. Dostępność systemu i jego usług powinna być jednym ze zdefiniowanych parametrów jakości usług raportowanych i podlegających rozliczeniu.

Wymagania i zasady dotyczące zarządzania ciągłością realizacji zadań

§ 30. 1. Kierujący komórkami organizacyjnymi, w szczególności właściciele systemów oraz bezpośredni przełożeni pracowników są odpowiedzialni za organizację pracy pracowników tych komórek w taki sposób, aby zminimalizować ryzyko niemożliwości zapewnienia ciągłości realizacji zadań. W tym celu są zobowiązani m.in. do:

1) zarządzania wiedzą i kompetencjami podległych sobie pracowników w taki sposób, aby co najmniej dwaj pracownicy byli w stanie wykonać dane zadanie;
2) zarządzania dostępem do informacji w taki, sposób, aby zastępujący się nawzajem pracownicy mieli możliwość dostępu do informacji niezbędnych im do wykonywania obowiązków służbowych, z zachowaniem rozliczalności wykonywanych czynności;
3) zarządzania urlopami i delegacjami pracowników w taki sposób, aby dostępny był przynajmniej jeden pracownik posiadający kompetencje niezbędne do wykonania danego zadania;
4) w przypadku planowanego odejścia pracownika podjąć działania w celu zapewnienia ciągłości realizacji zadań, które odchodzący pracownik realizował.

2. Kierujący komórkami organizacyjnymi mają obowiązek zapewnić opracowanie przez bezpośrednich przełożonych schematów zastępstw pracowniczych w podległych komórkach organizacyjnych.

3. Korzystanie przez Inspektorat z usług świadczonych przez podmioty zewnętrzne nie może prowadzić do uzależnienia działalności Inspektoratu od tych podmiotów i zagrażać ciągłości realizacji zadań publicznych.

Synchronizacja zegarów z wzorcowym źródłem czasu

§ 31. 1. Wszystkie zegary w systemach należy synchronizować z jednym wzorcowym źródłem czasu. Poprawne ustawienie zegarów jest istotne dla zapewnienia rozliczalności działań w systemie.

2. Za prawidłowe ustawienie synchronizacji zegarów w systemach odpowiadają ASI.

Bezpieczeństwo okablowania

§ 32. 1. Okablowanie sieci powinno być prowadzone w listwach lub innych przeznaczonych do tego miejscach poprowadzenia okablowania, w sposób minimalizujący ryzyko uszkodzeń fizycznych, nieautoryzowanego dostępu oraz zmniejszający ryzyko podsłuchu przesyłanych informacji.

2. Tam, gdzie istnieje potrzeba prowadzenia okablowania przez obszary nienależące do Inspektoratu należy stosować zabezpieczenia kryptograficzne przesyłanych informacji lub odpowiednie zabezpieczenia fizyczne.

3. Pomieszczenia, w których są zlokalizowane szafy krosownicze powinny zapewniać ochronę urządzeń i okablowania przed nieuprawnionym dostępem, uszkodzeniem, zniszczeniem, kradzieżą itp. zagrożeniami ze strony czynnika ludzkiego.

4. Niewykorzystywane gniazdka sieci należy wyłączać.

5. Gniazdka i kable powinny być oznaczone w sposób umożliwiający ich identyfikację przez ASI.

6. Zalecane jest umożliwienie łączenia się z siecią lokalną wyłącznie urządzeń autoryzowanych i wykorzystywanie w tym celu odpowiednich zabezpieczeń np. filtrowanie MAC, certyfikaty dla urządzeń.

Bezpieczeństwo wideokonferencji

§ 33. 1. Przed rozpoczęciem wideokonferencji należy:

1) zapoznać się z ogólnymi warunkami użytkowania lub polityką prywatności programu, w którym ma być organizowana wideokonferencja oraz regulaminem udziału w wideokonferencji, jeżeli jest dostępny;
2) sprawdzić, czy rozmowy będą nagrywane i przechowywane oraz jaki będzie zakres ich przetwarzania (przetwarzanie polegające na utrwalaniu, powielaniu, wprowadzaniu do pamięci komputera oraz do sieci komputerowej lub multimedialnej, zwielokrotnianiu jakąkolwiek techniką);
3) zweryfikować, do jakich celów wykorzystywane będą dane osobowe; należy pamiętać, że polityka prywatności dostawcy usługi wideokonferencji to nie wszystko i jeżeli do osiągnięcia danego celu musi być dokonany zapis przebiegu wideokonferencji lub nawet samego głosu, muszą być spełnione obowiązki informacyjne z art. 13 i 14 RODO, w tym zebrane stosowne zgody na nagrywanie, przechowywanie i dalsze przetwarzanie wizerunku i głosu oraz wykorzystanie wypowiedzi każdego z uczestników;
4) sprawdzić, o przyznanie jakich uprawnień program monituje – lista kontaktów, lokalizacja, dostęp do plików lokalnych itp. uprawnienia nie powinny być przyznawane;
5) korzystać z aplikacji przeglądarkowych, nie desktopowych;
6) jeżeli wymagane jest użycie aplikacji desktopowej, do zainstalowania aplikacji na komputerze używać oficjalnej strony programu (potrzebę instalacji należy zgłosić w systemie zgłoszeń informatycznych); w przypadku urządzeń mobilnych należy wybierać programy z oficjalnych sklepów – Google Play lub App Store;
7) przeskanować program do telekonferencji systemem antywirusowym lub antymalware przed jego instalacją;
8) upewnić się, że osoby postronne nie mają dostępu do ekranu monitora / wyświetlacza;

9) sprawdzić, czy aplikacja dysponuje niezbędnymi środkami bezpieczeństwa, takimi jak szyfrowanie połączenia;
10) w przypadku korzystania z udostępnianego przez siebie połączenia Wi-Fi, zabezpieczyć dostęp do niej silnym hasłem;
11) przed udostępnieniem ekranu podczas rozmowy zamknąć wszystkie niepotrzebne okna programów, tak aby inni uczestnicy konferencji ich nie zobaczyli;
12) przy podłączeniu się do telekonferencji korzystać z haseł dostępu lub kodów PIN, jeżeli je udostępniono.

2. W trakcie korzystania z wideokonferencji należy:

1) ograniczyć ilość podawanych danych osobowych – w narzędziu konfigurować wyłącznie podstawowe dane, jak imię i nazwisko oraz służbowy adres e-mail;
2) używać innego hasła, niż wykorzystywane w innych usługach;
3) nie udostępniać linków do konferencji, w szczególności na portalach i w mediach społecznościowych;
4) włączyć (jeśli to możliwe i jesteś organizatorem spotkania) domyślną ochronę hasłem;
5) zarządzać opcjami udostępniania ekranu tj. nie udostępniać swojego ekranu, gdy nie jest to konieczne;
6) w miarę możliwości wykorzystywać dostęp do sieci za pomocą szyfrowanego połączenia VPN;
7) nie udostępniać dokumentów służbowych, za pomocą czatu, który może być publiczny;
8) jeżeli to możliwe, korzystać z opcji zamazywania tła (tak, żeby rozmówcy nie widzieli otoczenia uczestnika);
9) jeżeli jesteś organizatorem, korzystać z opcji „poczekalnia” tak, aby można kontrolować osoby uczestniczące w telekonferencji, unikając przypadkowych lub niechcianych osób;
10) logując się do telekonferencji, wyłączyć mikrofon i kamerę i włączać je wtedy, gdy będzie to potrzebne.

3. Po zakończeniu wideokonferencji należy:

1) wyłączyć mikrofon i kamerę;
2) upewnić się, że zakończono wideokonferencję i zamknięto aplikację lub stronę z wideokonferencją w przeglądarce;
3) sprawdzić, czy program do telekonferencji nie pozostał działający w tle (w przypadku klientów desktopowych) i jeżeli działa – wyłączyć.

4. Uruchamiając własną usługę wideokonferencji należy:

1) zapoznać uczestników z ogólnymi warunkami użytkowania lub polityką prywatności programu, który będzie wykorzystywany do przeprowadzenia wideokonferencji;
2) ustalić, czy rozmowy mają być nagrywane i przechowywane oraz w jakim celu, jak również określić jaki będzie zakres ich dalszego przetwarzania (przetwarzanie polegające na utrwalaniu, powielaniu, wprowadzaniu do pamięci komputera oraz do sieci komputerowej lub multimedialnej; zwielokrotnianiu jakąkolwiek techniką). Należy określić, do jakich celów będą wykorzystywane dane osobowe w postaci wizerunku lub głosu. Należy pamiętać, że polityka prywatności dostawcy usługi wideokonferencji to nie wszystko i jeżeli do osiągnięcia danego celu musi być dokonany zapis przebiegu wideokonferencji lub nawet samego głosu, muszą być spełnione obowiązki informacyjne z art. 13 i 14 RODO, w tym zebrane stosowne zgody na nagrywanie, przechowywanie i dalsze przetwarzanie wizerunku i głosu oraz wykorzystanie wypowiedzi;
3) zapisy wizerunku lub głosu stanowią informację prawnie chronioną i jej udostępnienie np. na stronie internetowej musi być poprzedzone stosowną zgodą uczestników, możliwą i łatwą do wycofania w każdym momencie;
4) wymagać minimalnych uprawnień do zasobów uczestników wideokonferencji – dostęp narzędzia do mikrofonu, ewentualnie kamery będzie wystarczający. Nie należy wymagać udostępniania lokalizacji, kontaktów ani innych informacji, które nie są niezbędne do uzyskania połączenia i udziału w wideokonferencji;
5) jeżeli to możliwe, nie wymagać od uczestników instalowania narzędzia na swoich komputerach, ale stosować wersję przeglądarkową narzędzia. Jeżeli konieczne jest udostępnienie klienta narzędzia instalowanego lokalnie, należy odpowiednio wcześniej uprzedzić o tym uczestników (mogą być wymagane uprawnienia podwyższone, których użytkownik nie posiada), wskazać oficjalną stronę narzędzia; w przypadku urządzeń mobilnych należy wskazać narzędzie w oficjalnym sklepie – Google Play lub App Store;
6) zapewnić, że narzędzie dysponuje i posiada skonfigurowane niezbędne środki bezpieczeństwa, takie jak szyfrowanie połączenia;
7) zapewnić dostęp do wideokonferencji z wykorzystaniem haseł dostępu lub kodów PIN;
8) w miarę możliwości zapewnić dostęp do usług wideokonferencji za pomocą szyfrowanego połączenia VPN;
9) przed instalacją narzędzia lub jakiejkolwiek jego aktualizacji przeskanować to narzędzie programem antywirusowym.

Wykaz systemów informatycznych i wspierających

§ 34. 1. Wykaz systemów informacyjnych oraz systemów wspierających prowadzone przez Pełnomocnika do spraw bezpieczeństwa cyberprzestrzeni powinny zawierać informacje niezbędne do realizacji działań określonych w ustawie o krajowym systemie cyberbezpieczeństwa oraz sprawnego zarządzania incydentami cyberbezpieczeństwa.

2. Szablony wykazów systemów informacyjnych oraz systemów wspierających określa załącznik nr 1 do PBT.

3. Wykazy, o których mowa w ust. 1 określone w Części A załącznika nr 1 do PBT podlegają zatwierdzeniu przez Głównego Inspektora.

4. Pełnomocnik do spraw bezpieczeństwa cyberprzestrzeni przedstawia do zatwierdzenia przez Głównego Inspektora wykaz, o którym mowa w ust. 3 w terminie 30 dni od jego pierwszego utworzenia oraz w terminie 14 dni od otrzymania informacji od właściciela danego systemu w przypadku dodawania/usuwania systemów lub zmian kategorii informacji, kategorii bezpieczeństwa informacji, kategorii bezpieczeństwa systemu.

5. Wykazy, o których mowa w ust. 1 określone w Części B załącznika nr 1 do PBT są prowadzone przez Pełnomocnika do spraw bezpieczeństwa cyberprzestrzeni na podstawie informacji od właścicieli systemów.

6. Właściciele systemów przekażą Pełnomocnikowi do spraw bezpieczeństwa cyberprzestrzeni informacje określone w Części B załącznika nr 1 do PBT w terminie 60 dni od otrzymania od Pełnomocnika do spraw bezpieczeństwa cyberprzestrzeni tych wykazów, wstępnie przygotowanych na podstawie wykazów zatwierdzonych przez Głównego Inspektora określonych w Części A załącznika nr 1 do PBT.

Załącznik nr 1 do PBT

Część A

WYKAZ SYSTEMÓW INFORMACYJNYCH WSKAZANYCH W § 5 PBI		
Lp.	**Nazwa systemu informacyjnego**	**Właściciel biznesowy systemu informacyjnego**
	1	**2**
1		
2		

WYKAZ SYSTEMÓW WSPIERAJĄCYCH WSKAZANYCH W § 6 PBI		
Lp.	**System**	**Właściciel systemu wspierającego**
	1	**2**
1		
2		

Nazwa systemu informacyjnego / System – nazwa systemu zgodna z jego dokumentacją lub przyjętą nomenklaturą

Właściciel biznesowy systemu informacyjnego / właściciel systemu wspierającego – właściciele, o których mowa w § 3 pkt 56 i 57 PBI

Część B

INFORMACJE DOTYCZĄCE SYSTEMÓW ZAWARTYCH W WYKAZIE SYSTEMÓW INFORMACYJNYCH WSKAZANYCH W § 5 PBI														
Lp.	**Nazwa systemu**	**Czy rejestr publiczny? (nie, tak – podstawa prawna)**	**Cel stosowania / zadania publiczne**	**Właściciel biznesowy**	**AMS**	**ASI**	**Kategorie informacji przetwarzane w systemie informacyjnym (kategoria informacji, kategoria bezpieczeństwa informacji)**	**Kategoria bezpieczeństwa systemu informacyjnego**	**Skala systemu**	**Powiązania z innymi systemami**	**Warstwa techniczna**	**Producent**	**Czy są umowy serwisowe / dotyczące administrowania**	**Inne**
1														

INFORMACJE DOTYCZĄCE SYSTEMÓW ZAWARTYCH W WYKAZIE SYSTEMÓW INFORMACYJNYCH WSKAZANYCH W § 6 PBI													
Lp.	**System**	**Cel stosowania**	**Właściciel systemu wspierającego**	**AMS**	**ASI**	**Kategorie informacji przetwarzane w systemie wspierającym (kategoria informacji, kategoria bezpieczeństwa informacji)**	**Kategoria bezpieczeństwa systemu wspierającego**	**Skala systemu**	**Powiązania z innymi systemami**	**Warstwa techniczna**	**Producent**	**Czy są umowy serwisowe / dotyczące administrowania**	**Inne**
1													

Nazwa systemu informacyjnego / System – nazwa systemu zgodna z jego dokumentacją lub przyjętą nomenklaturą

Czy rejestr publiczny? – czy system jest rejestrem publicznym? Jeżeli tak, wskazanie podstawy prawnej prowadzenia rejestru publicznego.

Cel stosowania / zadania publiczne – cel stosowania systemu / wskazanie zadań publicznych, które system wspiera (wraz z odniesieniem do podstawy prawnej wskazującej obowiązek ich realizacji).

Właściciel biznesowy systemu informacyjnego / właściciel systemu wspierającego – właściciele, o których mowa w § 3 pkt 56 i 57 PBI

AMS – wskazanie danych kontaktowych AMS.

ASI – wskazanie danych kontaktowych ASI.

Kategoria bezpieczeństwa systemu informacyjnego – jak ważny jest system dla urzędu, jak ważne są dane i informacje w nim przetwarzane i gromadzone, jak istotne jest funkcjonowanie systemu dla użytkowników wewnętrznych, zewnętrznych, jakie skutki mogą wystąpić w przypadku naruszenia poufności, integralności lub dostępności systemu informacyjnego. Kategoryzacja systemu informacyjnego zgodnie z NSC 199 (NISKA, UMIARKOWANA, WYSOKA).

Kategorie informacji przetwarzane w systemie informacyjnym – klasyfikacja informacji przetwarzanych w systemie informacyjnym na podstawie załącznika nr 10 do PBI (najwyższa grupa informacji z zakresu: informacje jawne, informacje wrażliwe, informacje prawnie chronione) wraz ze wskazaniem kategorii bezpieczeństwa informacji zgodnie z NSC 199 (NISKA, UMIARKOWANA, WYSOKA).

Skala systemu – jaki jest zasięg terytorialny systemu (lokalny, krajowy, międzynarodowy).

Powiązania z innymi systemami – z którymi systemami dany system jest zintegrowany w celu wymiany informacji, wskazanie kierunku integracji.

Warstwa techniczna – rodzaj architektury, platforma sprzętowa, technologia bazodanowa, rodzaj zabezpieczeń informatycznych, wykorzystywane media telekomunikacyjne, itp.

Producent – kto jest producentem/dostawcą systemu.

Czy są umowy serwisowe / dotyczące administrowania – czy system jest objęty umową/umowami serwisowymi, z jaką firmą jest podpisana umowa serwisowa. Czy serwis dotyczy wyłącznie utrzymania czy także rozwoju systemu.

Inne – dodatkowe informacje podane przez właściciela systemu inne niż wskazane w pozostałych kolumnach.

Załącznik nr 5 do Polityki Bezpieczeństwa Informacji
Głównego Inspektoratu Transportu Drogowego

Polityka Utrzymania Ciągłości Działania

§ 1. 1. Mając na uwadze potrzebę zapewnienia ciągłości działania Inspektoratu, w sytuacji kryzysowej zwoływana jest narada Kierownictwa lub posiedzenie Zespołu Zarządzania Kryzysowego w sprawie określenia kierunków działania w sytuacji kryzysowej, w tym w szczególności:

1) potwierdzenie najważniejszych celów i zadań realizowanych z wykorzystaniem systemów;
2) potwierdzenie priorytetów realizacji celów i zadań Inspektoratu;
3) potwierdzenie osób odpowiedzialnych za realizację poszczególnych działań w celu zapewnienia ciągłości działania komórek organizacyjnych;
4) potwierdzenie maksymalnego dopuszczalnego czasu wstrzymania zadań, bez istotnych konsekwencji dla właściwego zapewnienia usług świadczonych przez poszczególne komórki organizacyjne (uwzględniając funkcjonowanie systemów);
5) wyodrębnienie pracowników i zasobów (materialnych/finansowych) niezbędnych do zapewnienia ciągłości działań w wymaganym przedziale czasowym;
6) ustalenie sekwencji działań i osób odpowiedzialnych za ich realizację;
7) ustalenie metod i zasad komunikacji pomiędzy tymi osobami.

2. Odprawa DG z kierującymi komórkami organizacyjnymi ma na celu przegląd i ocenę, aktualności planów zapewnienia ciągłości działania poszczególnych komórek organizacyjnych w odniesieniu do aktualnej sytuacji, pod kątem podjęcia niezbędnych działań dla zapewnienia bezpieczeństwa pracownikom oraz utrzymania ciągłości działania Inspektoratu, dokonanie ewentualnych korekt w szczegółowych planach ciągłości działania, w tym w szczególności:

1) dokonanie oceny potencjalnych skutków wystąpienia sytuacji kryzysowej;
2) podjęcie decyzji o opracowaniu lub aktualizacji procedur awaryjnych, jeżeli zaistnieje taka potrzeba;
3) określenie sposobów postępowania w sytuacji niedostępności podstawowego personelu odpowiedzialnego za utrzymanie systemów;
4) określenie zasad organizacji pracy zapewniających:
   a. możliwość pracy zdalnej (w szczególności zdalnego zarządzania systemami),
   b. priorytetyzację usług oraz przygotowanie harmonogramów ich realizacji,

c. możliwość przenoszenia pracowników i infrastruktury realizujących zadania o niższym priorytecie do realizacji zadań o priorytecie wyższym,

d. odpowiednie środki komunikacji z personelem oraz dostęp do informacji przy jednoczesnym uwzględnieniu wymagań dotyczących poufności,

e. aktualizację wykazów osób, których obecność jest obowiązkowa do zachowania ciągłości działania,

f. aktualizację wykazów osób, które mają możliwość świadczenia pracy zdalnie.

3. Zasady i tryb pracy zdalnej oraz podróży służbowych w Inspektoracie w sytuacji kryzysowej:

1) szczegółowe zasady udzielania i organizacji pracy zdalnej określa Regulamin pracy w Inspektoracie oraz stosowne porozumienia z organizacjami związkowymi;
2) możliwe jest wprowadzenie ograniczeń w podróżach służbowych w celu zapewnienia większej dostępności personelu do ewentualnego zastępstwa w realizacji zadań, w tym utrzymania systemów.

§ 2. 1. Odpowiedzialność za zapewnienie opracowania Planów Awaryjnych lub PCD dla zadań komórki organizacyjnej spoczywa na kierującym komórką organizacyjną. Odpowiedzialność za zapewnienie opracowania Planów Awaryjnych lub PCD dla systemu spoczywa na właścicielu.

2. Szczegółowe Plany Awaryjne lub PCD obejmują m.in.:

1) identyfikację najważniejszych usług, w tym realizowanych z wykorzystaniem systemów ze wskazaniem ich administratorów oraz personelu technicznego – podstawowego i alternatywnego;
2) wykazy pracowników mogących pełnić funkcję koordynatora działań podejmowanych w ramach realizacji planu (inicjowanie uruchomienia planu);
3) wykaz niezbędnych działań, które muszą być podejmowane w ramach realizacji planu;
4) wykaz osób, które będą brały udział w realizacji zaplanowanych działań;
5) określenie zasobów, których udostępniane jest niezbędne w celu realizacji planu;
6) określanie maksymalnych dopuszczalnych czasów przerwania realizacji poszczególnych procesów.

3. Do utworzenia szczegółowych Planów Awaryjnych lub PCD, w szczególności dla systemów zaleca się wykorzystanie wytycznych i zaleceń określonych w normach z zakresu ciągłości działania lub dokumencie NSC 800–34 „*Poradnik Planowania Awaryjnego*” oraz zapisów PZK, z którym PCD powinien być zgodny.

Załącznik nr 6 do Polityki Bezpieczeństwa Informacji
Głównego Inspektoratu Transportu Drogowego

Polityka Zarządzania Incydentami

Zarządzanie zdarzeniami związanymi z bezpieczeństwem informacji

§ 1. 1. Zarządzanie zdarzeniami związanymi z bezpieczeństwem informacji nadzorują i koordynują:

1) w przypadku naruszeń ochrony danych osobowych – IOD;
2) w przypadku incydentów w podmiocie publicznym oraz incydentów krytycznych – Pełnomocnik do spraw bezpieczeństwa cyberprzestrzeni;
3) w przypadku innych, niż określone w pkt 1 i 2 incydentów bezpieczeństwa informacji – Pełnomocnik do spraw bezpieczeństwa informacji.

2. Rejestry zdarzeń związanych z bezpieczeństwem informacji prowadzą:

1) IOD – rejestr naruszeń ochrony danych osobowych;
2) Pełnomocnik do spraw bezpieczeństwa informacji – rejestr incydentów bezpieczeństwa informacji uwzględniający incydenty cyberbezpieczeństwa określne w ust 1 pkt 2.

3. Osoby, o których mowa w ust. 2 zapewniają kompletność tych rejestrów, ich poufność, integralność oraz dostępność z zachowaniem zasad określonych w PBI.

4. Rejestr, o którym mowa w ust. 2 pkt 2 obejmuje:

1) opis incydentu;
2) datę i godzinę zgłoszenia incydentu;
3) dane identyfikujące osobę zgłaszającą;
4) dane osoby przekazującej informację o incydencie;
5) datę zarejestrowania incydentu;
6) informację o zgromadzonych materiałach dowodowych;
7) informacje dotyczące sposobu postępowania z incydentem.

5. Informacje o zakresie informacyjnym rejestru naruszeń, o którym mowa w ust. 2 pkt 1 określa PODO.

Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji

§ 2. 1. Wszyscy pracownicy oraz pracownicy reprezentujący podmiot zewnętrzny, którzy mają dostęp do systemów Inspektoratu i zobowiązali się do przestrzegania jej regulacji wewnętrznych związanych z bezpieczeństwem informacji, mają obowiązek zgłaszania

wszelkich zdarzeń, które naruszają lub mogą naruszyć przepisy prawa oraz polityki, regulaminy i procedury dotyczące bezpieczeństwa informacji oraz polityki bezpieczeństwa tych systemów.

2. ASI ma obowiązek zareagować na alarmy i alerty generowane przez moduły automatycznego powiadamiania w systemach zabezpieczeń.

1) W przypadku zidentyfikowania zagrożenia naruszenia ochrony danych osobowych ASI niezwłocznie informuje IOD.
2) W przypadku zidentyfikowania zagrożenia dla obniżenia jakości lub przerwania realizacji zadania publicznego realizowanego z wykorzystaniem systemu, ASI niezwłocznie informuje Pełnomocnika do spraw bezpieczeństwa cyberprzestrzeni.
3) W przypadku zidentyfikowania zagrożenia dla bezpieczeństwa informacji innego, niż określone w pkt 1 i 2, ASI niezwłocznie informuje Pełnomocnika do spraw bezpieczeństwa informacji.

3. Poinformowanie osób, o których mowa w ust. 2 powinno nastąpić w sposób zapewniający, że informacja zostanie odebrana w możliwie najkrótszym czasie od jej przekazania.

4. W przypadku powierzenia obowiązków zarządzania systemami informacyjnymi podmiotom zewnętrznym, poinformowanie ASI oraz osób, o których mowa w ust. 2 o zdarzeniu odbywa się na zasadach określonych w umowie z tym podmiotem oraz procedurach obowiązujących dla danego systemu.

5. W przypadku powierzenia obowiązków zarządzania systemami podmiotom zewnętrznym właściciel danego systemu ma obowiązek zapewnić w umowie z takim podmiotem realizację obowiązków dotyczących zgłaszania zdarzeń zgodnie z PZI, w szczególności naruszeń ochrony danych osobowych oraz incydentów w podmiocie publicznym.

6. Incydenty krytyczne są przekazywane przez CSIRT zgodnie z przepisami ustawy o krajowym systemie cyberbezpieczeństwa.

Postępowanie z incydentami

§ 3. 1. Osoby, o których mowa w § 1 ust. 1 dokonują wstępnej identyfikacji zdarzenia i na podstawie dostępnych informacji oraz analizy okoliczności kwalifikują zdarzenie (lub serię zdarzeń) jako:

1) zdarzenie nie mające cech naruszenia bezpieczeństwa informacji;
2) naruszenie ochrony danych osobowych;

3) incydent w podmiocie publicznym;
4) incydent niskiej kategorii – związany z naruszeniem bezpieczeństwa informacji, nie generujący negatywnych skutków w odniesieniu do poufności, integralności lub dostępności informacji lub ciągłości realizacji procesów biznesowych;
5) incydent średniej kategorii – związany z naruszeniem bezpieczeństwa informacji skutkujący pośrednio lub bezpośrednio trudnościami w realizacji procesu biznesowego, niewielkimi stratami finansowymi, konsekwencjami służbowymi, utratą wizerunku, lub wpływający na poufność, integralność lub dostępność informacji wrażliwych;
6) incydent wysokiej kategorii – związany z naruszeniem bezpieczeństwa informacji prawnie chronionych, skutkujący przerwaniem procesów biznesowych, stratami finansowymi, ryzykiem odpowiedzialności prawnej/karnej.

2. Zdarzenie (lub seria zdarzeń), w zależności od swojej natury, zakresu oddziaływania i skutków mogą być zakwalifikowane do wielu kategorii jednocześnie.

3. Osoby, o których mowa w § 1 ust. 1 dokonują analizy informacji dotyczących zdarzenia, w tym we współpracy z ASI oraz AMS oraz dokonują jego docelowej klasyfikacji. W toku tego procesu mogą występować o wszelkie informacje, wyjaśnienia i opinie do komórek organizacyjnych, pracowników w tym kierujących komórkami organizacyjnymi, którzy są zobowiązani do przekazania informacji, wyjaśnień lub opinii bez zbędnej zwłoki, w możliwie najkrótszym terminie.

4. Analiza uwzględnia następujące kryteria:
1) charakter incydentu i jego znaczenie;
2) miejsce wystąpienia incydentu – identyfikacja punktu, w którym nastąpiło zdarzenie (lokalizacja, serwer, stacja robocza itp.) oraz szacunkowy czas jego wystąpienia i trwania;
3) zakres osób, podmiotów, zasobów dotkniętych incydentem;
4) identyfikacja zasobów potrzebnych do dalszych działań w ramach postępowania z incydentem;
5) możliwości rozszerzania się incydentu i sposoby jego ograniczania;
6) szacowane skutki, w tym m.in. finansowe, osobowe, dla mienia, dla praw osób;
7) rodzaj informacji objętej incydentem (jeśli ma zastosowanie – np. dane osobowe);
8) szacunkowy czas, po którym skutki incydentu zostaną usunięte, jeżeli nie ma możliwości natychmiastowego usunięcia stanu nieprawidłowego.

5. W przypadku, gdy skutki zdarzenia przekładają się na zakwalifikowanie go jako naruszenie ochrony danych osobowych lub incydent wysokiej kategorii osoby, o których mowa w § 1 ust. 1 informują Głównego Inspektora.

6. W przypadku, gdy skutki zdarzenia przekładają się na zakwalifikowanie go jako incydent w podmiocie publicznym osoba, o której mowa w § 1 ust. 1 pkt 2 informuje dyrektora BT oraz właściciela danego systemu.

7. W przypadku, gdy zasięg incydentu wykracza poza systemy Inspektoratu, ASI, w porozumieniu z dyrektorem BT i z zastrzeżeniem posiadania stosownej umowy o poufności z właściwymi podmiotami zewnętrznymi, może przekazać do podmiotu zewnętrznego informacje o incydencie zawierające m.in.:

1) typ zdarzenia;
2) informacje o systemie, który może być źródłem naruszenia, w tym nazwy serwerów, adresy IP, identyfikatory użytkowników;
3) inne informacje określone w umowie z podmiotem zewnętrznym.

8. W przypadku, gdy kategoria incydentu uzasadnia potrzebę powiadomienia właściwych organów:

1) dla naruszeń ochrony danych osobowych IOD dokonuje zgłoszenia do PUODO w terminie do 72 godzin od zaistnienia lub wykrycia naruszenia;
2) dla incydentów w podmiocie publicznym Pełnomocnik do spraw bezpieczeństwa cyberprzestrzeni dokonuje zgłoszenia do CSIRT GOV w terminie do 24 godzin od zaistnienia lub wykrycia zdarzenia;
3) dla pozostałych incydentów – jeżeli jest to uzasadnione ich rodzajem i skutkami, Pełnomocnik do spraw bezpieczeństwa informacji lub inny wyznaczony do tego pracownik dokonuje, w porozumieniu z dyrektorem BT, zgłoszenia do właściwych organów ścigania m.in. Centralnego Biura Zwalczania Cyberprzestępczości.

9. Jeżeli incydent bezpieczeństwa dotyczący systemu występuje w okresie wprowadzenia stopni alarmowych CRP, może być wymagane powiadomienie dodatkowych stron, zgodnie z obowiązującym PZK.

Działania IOD w zakresie obsługi naruszeń ochrony danych osobowych

§ 4. 1. IOD dokonuje analizy informacji dotyczących zdarzenia związanego z naruszeniem zasad ochrony danych osobowych. W toku tego procesu IOD może występować o wszelkie informacje, wyjaśnienia i opinie do komórek organizacyjnych, pracowników w tym

kierujących komórkami organizacyjnymi, którzy są zobowiązani do przekazania informacji, wyjaśnień lub opinii bez zbędnej zwłoki, w możliwie najkrótszym terminie.

2. W wyniku analizy IOD stwierdza czy jest prawdopodobne, że stwierdzone zdarzenie skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych oraz szacuje ryzyko z tym związane.

3. W przypadku stwierdzenia występowania ryzyka naruszenia praw i wolności osób fizycznych, w szczególności ryzyka wysokiego i potwierdzenia prawidłowości kwalifikacji zdarzenia jako naruszenie ochrony danych osobowych IOD informuje o tym Głównego Inspektora.

4. IOD odpowiada za zgłoszenie stwierdzonego naruszenia ochrony danych osobowych do PUODO.

5. IOD pełni nadzór nad właściwym wykonaniem czynności poinformowania osób, których dane osobowe są objęte naruszeniem, przez komórki organizacyjne, w których dane naruszenie wystąpiło. Poinformowania osób, których dane osobowe są objęte naruszeniem, wykonują komórki organizacyjne, w których dane naruszenie wystąpiło (pismo na podpis kierującego komórką organizacyjną), konsultując treść informacji z IOD przed jej podpisaniem i wysłaniem.

6. Informację o zrealizowaniu czynności poinformowania umieszcza w rejestrze naruszeń ochrony danych osobowych oraz przekazuje do PUODO, jeżeli tej informacji nie zawierało zgłoszenie naruszenia.

7. IOD pełni nadzór nad obsługą incydentu przez właściwe komórki organizacyjne.

Działania Pełnomocnika do spraw bezpieczeństwa cyberprzestrzeni w zakresie obsługi incydentu w podmiocie publicznym

§ 5. 1. Pełnomocnik do spraw bezpieczeństwa cyberprzestrzeni dokonuje analizy informacji dotyczących zdarzenia związanego z naruszeniem bezpieczeństwa systemu. W toku tego procesu Pełnomocnik do spraw bezpieczeństwa cyberprzestrzeni może występować o wszelkie informacje, wyjaśnienia i opinie do komórek organizacyjnych, pracowników w tym kierujących komórkami organizacyjnymi, którzy są zobowiązani do przekazania informacji, wyjaśnień lub opinii bez zbędnej zwłoki, w możliwie najkrótszym terminie.

2. W wyniku analizy Pełnomocnik do spraw bezpieczeństwa cyberprzestrzeni stwierdza czy jest prawdopodobne, że stwierdzone zdarzenie skutkuje lub może skutkować obniżeniem jakości lub przerwaniem realizacji zadania publicznego.

3. W przypadku stwierdzenia występowania ryzyka obniżenia jakości lub przerwania realizacji zadania publicznego i potwierdzenia prawidłowości kwalifikacji zdarzenia jako incydent w podmiocie publicznym, Pełnomocnik do spraw bezpieczeństwa cyberprzestrzeni informuje dyrektora BT oraz właściciela danego systemu.

4. Pełnomocnik do spraw bezpieczeństwa cyberprzestrzeni odpowiada za zgłoszenie stwierdzonego incydentu w podmiocie publicznym do CSIRT GOV.

5. Pełnomocnik do spraw bezpieczeństwa cyberprzestrzeni pełni nadzór nad obsługą incydentu przez ASI oraz właściciela tego systemu, którego dotyczy incydent.

Działania Pełnomocnika do spraw bezpieczeństwa informacji w zakresie obsługi incydentu bezpieczeństwa informacji

§ 6. 1. Pełnomocnik do spraw bezpieczeństwa informacji dokonuje analizy informacji dotyczących zdarzenia związanego z naruszeniem bezpieczeństwa informacji. W toku tego procesu Pełnomocnik do spraw bezpieczeństwa informacji może występować o wszelkie informacje, wyjaśnienia i opinie do komórek organizacyjnych, pracowników w tym kierujących komórkami organizacyjnymi, którzy są zobowiązani do przekazania informacji, wyjaśnień lub opinii bez zbędnej zwłoki, w możliwie najkrótszym terminie.

2. W wyniku analizy Pełnomocnik do spraw bezpieczeństwa informacji potwierdza wstępnie nadaną kategorię incydentu bezpieczeństwa informacji.

3. W przypadku kwalifikacji zdarzenia jako incydent kategorii wysokiej, Pełnomocnik do spraw bezpieczeństwa informacji informuje Głównego Inspektora.

4. Pełnomocnik do spraw bezpieczeństwa cyberprzestrzeni pełni nadzór nad obsługą incydentu przez właściwe komórki organizacyjne.

Ograniczanie skutków

§ 7. 1. ASI lub właściwe komórki organizacyjne przeprowadzają działania zmierzające do ograniczenia skutków zdarzenia i zidentyfikowania jego źródła.

2. W przypadku, gdy działania obejmują wyłączenie lub ograniczenie funkcjonowania zasobów niezbędnych do realizowania zadań ustawowych, ASI powinien podjąć lub zainicjować działania określone w Planach Awaryjnych lub PCD.

3. Przy ograniczaniu i zapobieganiu rozprzestrzeniania się skutków zdarzenia ASI, w uzgodnieniu z kierującym komórką organizacyjną może korzystać ze wsparcia podmiotów zewnętrznych, np. utrzymujących system, CSIRT lub innych służb.

Odtwarzanie systemu

§ 8. 1. W przypadku takiej konieczności ASI przystępuje do odtworzenia systemu po zidentyfikowaniu i usunięciu lub zablokowaniu źródła incydentu. Decyzję o odtworzeniu systemu podejmuje właściciel lub inna umocowana do podjęcia takiej decyzji osoba (np. w Planie Awaryjnym lub PCD).

2. W przypadku zaistnienia sytuacji, kiedy nastąpiło uruchomienie PCD, odtwarzanie systemu jest realizowane w oparciu o uprzednio opracowane procedury.

3. Odtwarzanie systemu odnosi się do punktu odtworzenia, co do którego istnieje uzasadniona pewność, że nie zawiera źródła incydentu.

4. Zasoby w postaci oprogramowania oraz danych i konfiguracji są odtwarzane z oryginalnych źródeł dystrybucji oprogramowania oraz kopii zapasowych.

5. Główny Inspektor może podjąć decyzję o wznowieniu przetwarzania mimo braku pewności usunięcia źródła incydentu, jeśli szacowane negatywne skutki braku przetwarzania przewyższają potencjalne ryzyko podjęcia działania.

Działania po zakończeniu incydentu w systemie

§ 9. 1. ASI sporządza raport techniczny, zawierający co najmniej:

1) rejestr obsługi incydentu, zawierający szczegółowe zapisy chronologiczne dotyczące kolejnych zdarzeń i podejmowanych działań;
2) opis incydentu w aspekcie technicznym (zakres incydentu, części systemów dotknięte skutkami incydentu, rozmiar bezpośrednich szkód);
3) kopie dzienników (logów zdarzeń, logów audytu) urządzeń, systemów operacyjnych i aplikacji w części systemów, która była dotknięta skutkami incydentu;
4) kopię dziennika administratora z okresu trwania incydentu;
5) informacje o oryginalnych źródłach dystrybucji oprogramowania oraz kopiach zapasowych wykorzystanych do odtworzenia systemu, jeżeli dotyczy;
6) zakres informacji technicznych przekazanych podmiotom zewnętrznym uczestniczącym w działaniach związanych z ograniczaniem skutków incydentu.

2. Jeżeli charakter zdarzenia tego wymaga osoby, o których mowa w § 1 ust. 1 przedstawiają właścicielowi danego systemu rekomendacje w zakresie działań zmierzających do zmniejszenia ryzyka powtórzenia wystąpienia incydentu w przyszłości.

Gromadzenie materiału dowodowego

§ 10. 1. Na każdym etapie postępowania z incydentem, osoby, o których mowa w § 1 ust. 1 nadzorują, jak również mogą uczestniczyć w gromadzeniu materiału dowodowego.

2. Każdy element materiału dowodowego – dokument papierowy, dokument elektroniczny, kopia zapasowa bazy danych lub plików systemowych i konfiguracyjnych, obraz dysku, dzienników (logów) zdarzeń, dzienników audytu – jest gromadzony i przechowywany w sposób gwarantujący jego poufność, integralność, dostępność i kompletność.

3. Każdy element materiału dowodowego jest utrwalany z zachowaniem integralności całego procesu przetwarzania, od utworzenia do ewentualnego przedstawienia jako dowodu w postępowaniu sądowym:

1) dla dokumentów papierowych – oryginał jest bezpiecznie przechowywany wraz z informacją o źródle, czasie i okolicznościach utrwalenia dokumentu;
2) dla zapisów utrwalanych na nośnikach elektronicznych – sporządzenie kopii zapasowej lub obrazu dysku wraz z udokumentowaniem procesu kopiowania oraz bezpieczne ich przechowanie.

4. Zabezpieczenie środków przetwarzania informacji jest przeprowadzane zgodnie z instrukcją zamieszczoną w załączniku nr 1 do PZI.

5. Protokół ze sporządzenia elementu materiału dowodowego lub zabezpieczenia środków przetwarzania informacji jest sporządzany zgodnie ze wzorem zamieszczonym w załączniku nr 2 do PZI.

6. Wszelkie działania w systemie związane z postępowaniem z incydentem mogą być prowadzone wyłącznie z wykorzystaniem kopii zapasowych, obrazów dysków, kopii plików konfiguracyjnych i systemowych, rejestrów systemowych i aplikacji, plików dokumentów, identycznych ze sporządzonymi uprzednio kopiami przechowywanymi jako materiał dowodowy.

Załącznik nr 1 do PZI

Instrukcja zabezpieczania materiału dowodowego z komputerów

1. Odsuń w sposób zdecydowany, ale taktowny inne osoby od komputerów (mogą później być przydatne). Na czas zabezpieczenia zabroń im korzystania z urządzeń komputerowych i łączności.
2. Jeśli urządzenie jest wyłączone, nie wyłączaj go.
3. Jeśli urządzenie jest włączone, nie próbuj zamykać programów ani wyłączać komputera. Nie przerywaj drukowania, zabezpiecz, jeśli to możliwe, wykonane wydruki. Zanotuj dokładnie wszystkie wiadomości, jakie pojawiają się na ekranie.
4. Zanotuj wszystkie parametry połączeń komputera:
    1) w przypadku połączenia modemowego, zanotuj numer telefoniczny, adres IP komputera, adresy bramki wychodzącej oraz serwera DNS;
    2) w przypadku połączenia po sieci kablowej, zanotuj typ połączenia, adres IP komputera, adresy bramki wychodzącej oraz serwera DNS;
    3) w przypadku połączenia po sieci bezprzewodowej, zanotuj ustawienia zabezpieczenia sieci adres IP komputera, adresy bramki wychodzącej oraz serwera DNS.
5. Przed zabezpieczeniem zanotuj, w jaki sposób poszczególne części stanowiska są ze sobą połączone. Zrób zdjęcia, wykonaj szkic (plan połączeń z opisem wyposażenia). Oznacz odpowiednio wszystkie przewody i połączenia.
6. Następnie odłącz wszystkie kable zewnętrzne od komputera. Zanotuj czas odłączenia kabli.
7. Zabezpiecz jednostkę centralną (komputer) oraz inne urządzenia z zainstalowaną na stałe pamięcią masową w wytrzymałych mechanicznie workach foliowych.
8. Zaplombuj worek i wypełnij metryczkę. Metryczka powinna zawierać typ, numer seryjny urządzenia i numer inwentarzowy nadany przez Agencję albo opis jego indywidualnych cech. Wpisz do protokołu wykonane czynności.
9. Pakuj ostrożnie okablowanie i sprzęt (m. in. klawiatury, monitory, drukarki, plotery, skanery, czytniki kart i pamięci, napędy zewnętrzne).

10. Zabezpiecz wszystkie wymienne nośniki komputerowe: pamięci flash, dyskietki, dyskietki ZIP, JAZZ, taśmy streamera, płyty CD, DVD, MO oraz niezamontowane dyski twarde (także uszkodzone). Grupy nośników pakuj zbiorczo (dyskietki, płyty CD itp.). Pakuj, numeruj poszczególne paczki, plombuj i opisz w protokole. Wpisz do protokołu wykonane czynności.

11. Zażądaj od administratora spisu oprogramowania zainstalowanego na komputerze, a następnie zgodnie ze spisem – okazania licencji i oryginalnych nośników oprogramowania lub wskazania miejsca przechowywania lub osoby upoważnionej, która zarządza licencjami i oryginalnymi nośnikami oprogramowania. Jeśli administrator nie ma spisu oprogramowania, to zażądaj okazania wszystkich posiadanych przez niego licencji i oryginalnych nośników oprogramowania. Oznaczenia licencji i nośników wpisz do protokołu, a następnie zabezpiecz jako materiał porównawczy. Wpisz do protokołu wykonane czynności.

12. Zażądaj od administratora przekazania instrukcji programów pisanych na zamówienie lub programów nietypowych. Zabezpiecz jako materiał porównawczy i wpisz do protokołu wykonane czynności.

13. Zażądaj od użytkowników i administratora podania parametrów dostępu do BIOS-u, systemu operacyjnego i oprogramowania (nazw kont, identyfikatorów, haseł do BIOS), a następnie zabezpiecz je przed osobami postronnymi za pomocą bezpiecznej koperty. Wpisz czynność przejęcia parametrów dostępu do protokołu.

14. Przechowuj zabezpieczone materiały (nośniki i sprzęt) w miejscach suchych i chłodnych z daleka od urządzeń emitujących pole elektromagnetyczne, a bezpieczne koperty w sejfie.

NIE PRÓBUJ SAMODZIELNIE BADAĆ KOMPUTERA, ANI ZAWARTOŚCI NOŚNIKÓW DANYCH. KAŻDE TWOJE WŁĄCZENIE KOMPUTERA WYKONANE PO ZAKOŃCZENIU ZABEZPIECZANIA WYWOŁUJE POWSTANIE ŚLADÓW WSKAZUJĄCYCH NA NARUSZENIE INTEGRALNOŚCI MATERIAŁU DOWODOWEGO.

Załącznik nr 2 do PZI

PROTOKÓŁ ZABEZPIECZENIA MATERIAŁU DOWODOWEGO

Wykonano w dniu ..... o godzinie ..... w obecności:

Świadek 1: <imię i nazwisko, stanowisko, komórka organizacyjna>
Świadek 2: <imię i nazwisko, stanowisko, komórka organizacyjna>
Świadek 3: <imię i nazwisko,..……>

I. Rodzaj materiału dowodowego
(zaznaczyć właściwe i wpisać odpowiednie nazwy i oznaczenia)

Dokument papierowy / elektroniczny
Rodzaj i nazwa dokumentu: .....

Kopia zapasowa
System operacyjny
Nazwa i wersja systemu: .....

Aplikacja
Nazwa i wersja aplikacji: .....

Baza danych
Nazwa i wersja bazy: .....

Oznaczenie nośnika .....

Obraz dysku
Lokalizacja dysku: .....
Typ i nr seryjny dysku: .....

Pliki konfiguracyjne i/lub systemowe

Nazwa(y) pliku(ów): .....

Kopie zawartości dzienników (logów) zdarzeń

Nazwa(y) pliku(ów): .....

Kopia zawartości skrzynki pocztowej zewnętrznej / wewnętrznej

Nazwa skrzynki pocztowej: .....
Za okres od: .....

II. Opis czynności
(opisać kolejne czynności z zaznaczeniem Wykonawcy(ów))
.....
.....
.....

III. Wytworzony materiał dowodowy
Wykonano kopie materiału dowodowego w … egzemplarzach, którym nadano etykiety:
....., Egzemplarz nr .."

....., Egzemplarz nr ..”
....., Egzemplarz nr ..”
(wprowadzić krótkie oznaczenie zabezpieczonego materiału dowodowego, zgodnie z kategorią wskazaną w pkt. I, datą i godziną wykonania)

IV. Zabezpieczenie materiału dowodowego
(opisać sposób zabezpieczenia każdego z egzemplarzy)
.....
.....
.....

Protokół sporządził: .....

Podpisano:
Świadek 1 .....
Świadek 2 .....
Świadek 3 .....

Załącznik nr 7 do Polityki Bezpieczeństwa Informacji
Głównego Inspektoratu Transportu Drogowego

Polityka Ochrony Danych Osobowych

Cel i zakres przetwarzania danych osobowych

§ 1. 1. W Inspektoracie dane osobowe są przetwarzane:

1) jeżeli jest to niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
2) jeżeli jest to niezbędne do wypełniania obowiązku prawnego ciążącego na administratorze;
3) jeżeli jest to niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
4) jeżeli jest to niezbędne do realizacji celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora;
5) na podstawie zgody osoby, której dane dotyczą;
6) w przypadku, gdy ich przetwarzanie jest niezbędne do ochrony żywotnych interesów tej osoby lub innej osoby fizycznej.

2. Obszary działalności Inspektoratu, w których dochodzi do przetwarzania danych osobowych (cel przetwarzania):

1) bezpieczeństwo ruchu drogowego m.in. kontrole drogowe, postępowania mandatowe i czynności wyjaśniające w sprawach o wykroczenia ujawnione za pomocą urządzeń rejestrujących naruszenia przepisów ruchu drogowego w zakresie przekraczania dopuszczalnej prędkości oraz niestosowania się do sygnałów świetlnych;
2) kontrola poboru opłat m.in. kontrola uiszczania opłaty elektronicznej za przejazd po drogach krajowych, postępowania administracyjne dotyczące obowiązku uiszczenia opłaty elektronicznej;
3) wydawanie i kontrola uprawnień w międzynarodowym transporcie drogowym m.in. postępowania administracyjne dotyczące licencji, zezwoleń świadectw w obszarze międzynarodowego transportu drogowego;
4) działalność inspekcyjna m.in. kontrola inspekcyjna;
5) postępowania odwoławcze oraz w trybie nadzwyczajnym;
6) aktywność międzynarodowa;

7) zapewnienie narzędzi teleinformatycznych wspierających podstawową działalność Inspektoratu m.in. budowa, utrzymanie i rozwój systemów;
8) zarządzanie infrastrukturą kontrolną;
9) zarządzanie kadrami i finansami;
10) zarządzanie usługami wspierającymi;
11) zamówienia publiczne;
12) działalność edukacyjna, promocyjna i informacyjna.

3. Dane osobowe mogą być przetwarzane w postaci tradycyjnej (np. słownie, w formie papierowej) oraz w systemach Inspektoratu lub systemach innych podmiotów, które Inspektorat wykorzystuje.

4. Administratorem danych osobowych jest Główny Inspektor.

1) Główny Inspektor przetwarza dane osobowe w zakresie niezbędnym do realizacji zadań określonych w przepisach, w tym dane wskazane w art. 9 ust. 1 RODO;
2) w celach, o których mowa w art. 1 pkt 1 Ustawy, Główny Inspektor jest uprawniony do przetwarzania informacji, w tym danych osobowych, oraz ich wymiany z właściwymi organami i instytucjami krajowymi, Unii Europejskiej oraz innych państw, a także organizacjami międzynarodowymi;
3) Główny Inspektor może przekazać dane osobowe państwu trzeciemu lub organizacjom międzynarodowym, na ich wniosek, w przypadku gdy są spełnione warunki przekazywania informacji określone w art. 18a-18d ustawy z dnia 16 września 2011 r. o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej, państw trzecich, agencjami Unii Europejskiej oraz organizacjami międzynarodowymi;
4) Główny Inspektor przetwarza dane osobowe wskazane w art. 9 ust. 1 RODO wyłącznie w przypadku, gdy:
   a. zostały one przekazane dobrowolnie przez stronę w ramach prowadzonego postępowania,
   b. jest to konieczne do weryfikacji prawidłowości przekazanych przez stronę danych, o których mowa w pkt 1,
   c. z przepisu prawa wynika konieczność przetwarzania tych danych,
   d. jest to niezbędne do wykonania wyroku sądu.
5) Główny Inspektor jest uprawniony do wydawania rozstrzygnięć w indywidualnych przypadkach w oparciu o zautomatyzowane przetwarzanie danych, w tym profilowanie

w związku z realizacją zadań, o których mowa w art. 129a ust. 1 pkt 3 lit. b i art. 129g ustawy z dnia 20 czerwca 1997 r. – Prawo o ruchu drogowym;

6) Główny Inspektor wykonuje obowiązek, o którym mowa w art. 13 ust. 1 i 2 RODO, przy pierwszej czynności skierowanej do osoby, której dane dotyczą, chyba że posiada ona te informacje, a ich zakres lub treść nie uległy zmianie;
7) wystąpienie z żądaniem, o którym mowa w art. 18 ust. 1 RODO, nie wpływa na wykonywanie przez Głównego Inspektora zadań, o których mowa w art. 50 ustawy o transporcie drogowym;
8) wystąpienie z żądaniem, o którym mowa w art. 18 ust. 1 RODO, nie wpływa na przebieg kontroli prowadzonych na podstawie przepisów rozdziału 10 ustawy o transporcie drogowym, ani na uprawnienie Głównego Inspektora do nałożenia kary.

Środki podejmowane w celu wykonania obowiązków informacyjnych

§ 2. 1. Na stronie internetowej (https://www.gov.pl/web/gitd) oraz na stronie podmiotowej Biuletynu Informacji Publicznej zostały umieszczone:

1) dane kontaktowe administratora danych;
2) dane kontaktowe IOD;
3) cele przetwarzania danych i podstawy prawne tego przetwarzania;
4) informację o odbiorcach danych lub kategorii odbiorców jeśli występują;
5) informacje o zamiarze przekazania danych osobowych do państwa trzeciego (jeżeli dotyczy);
6) informacje o okresie przechowywania danych;
7) informacje o prawie osoby do żądania informacji, prawie do cofnięcia zgody i sposobie w jaki można to zrobić;
8) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą;
9) informacje o prawie do wniesienia skargi do organu nadzorczego;
10) informacje, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz
11) informacje, czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych.

2. W każdym przypadku, w którym dochodzi lub ma dojść do przetwarzania danych osobowych, m.in. w dokumentacji związanej z udzielaniem zamówień publicznych, w umowach i porozumieniach, w sprawach dotyczących zatrudnienia, w przypadku stosowania dowolnej formy monitoringu należy udostępnić informacje określone w ust. 1 w formie klauzuli informacyjnej.

3. Za realizację obowiązku informacyjnego w odniesieniu do osób, których dane dotyczą odpowiadają pracownicy realizujący zadania służbowe, o których mowa w ust. 2.

4. Jeżeli nie zostało to określone w odrębnej dokumentacji, podpisane klauzule informacyjne są przechowywane przez właścicieli informacji. Do przechowywania podpisanych przez osoby, których dane dotyczą klauzul informacyjnych należy stosować zasady bezpiecznego przechowywania dokumentów oraz wiedzy koniecznej i uzasadnionej.

5. Przykładowe szablony i wzory klauzul informacyjnych zawiera załącznik nr 1 do PODO. Klauzule te należy każdorazowo dostosować do danej sytuacji wymagającej ich zastosowania. Za dostosowanie i zastosowanie klauzul informacyjnych odpowiadają pracownicy, o których mowa w ust. 3.

Wyznaczenie Inspektora Ochrony Danych

§ 3. 1. Główny Inspektor formalnie wyznaczył:

1) IOD;
2) osobę zastępującą IOD w czasie jego nieobecności, która w tym czasie wykonuje zadania przypisane IOD określone w RODO, Ustawie oraz wewnętrznych regulacjach.

2. Na potrzeby kontaktu z IOD funkcjonuje adres e-mail iod@gitd.gov.pl, pod którym pracownicy, personel podmiotów zewnętrznych współpracujących z Inspektoratem, a w szczególności osoby, których dane dotyczą, mogą się kontaktować z IOD w sprawach dotyczących przetwarzania i ochrony danych osobowych.

3. Z IOD można się również kontaktować za pośrednictwem tradycyjnej korespondencji kierowanej na adres siedziby Inspektoratu, jak również za pośrednictwem skrzynki podawczej. Zalecane jest, aby przy kierowaniu korespondencji w takich formach dopisywać na kopercie lub w tytule, że dotyczy spraw związanych z przetwarzaniem lub ochroną danych osobowych.

4. Dane kontaktowe IOD oraz osoby zastępującej są opublikowane na stronie internetowej (https://www.gov.pl/web/gitd) oraz na stronie Biuletynu Informacji Publicznej.

5. Wszyscy pracownicy, w szczególności kierujący komórkami organizacyjnymi mają obowiązek włączać IOD we wszystkie sprawy związane z przetwarzaniem danych osobowych w, w szczególności przed rozpoczęciem takiego przetwarzania.

6. Dane kontaktowe IOD należy zawierać m.in. w dokumentacji udzielania zamówień publicznych, w umowach i porozumieniach których realizacja wiąże się z przetwarzaniem danych osobowych, w lokalizacjach fizycznych w związku z prowadzeniem monitoringu wizyjnego oraz pojazdach służbowych w związku z prowadzeniem monitoringu GPS tych pojazdów.

Realizacja praw osób, których dane dotyczą

§ 4. 1. IOD jest centralnym punktem kontaktowym dla wszystkich osób, które chcą skorzystać ze swoich praw określonych w RODO i Ustawie.

2. Każda korespondencja, niezależnie od formy jej przekazania, dotycząca przetwarzania lub ochrony danych osobowych na podstawie RODO lub Ustawy musi być niezwłocznie przekazana do IOD. Za jej niezwłoczne przekazanie do IOD odpowiedzialna jest komórka organizacyjna, do której taka korespondencja trafiła.

3. Podstawowym terminem udzielenia odpowiedzi na wniosek lub żądanie jest termin „bez zbędnej zwłoki”, przy czym przyjmuje się:

1) dla wniosków i żądań kierowanych na podstawie RODO – termin 1 miesiąca od otrzymania wniosku lub żądania; termin ten może być wydłużony o kolejne 2 miesiące z uwagi na skomplikowany charakter żądania lub liczbę tych żądań;
2) dla wniosków i żądań kierowanych na podstawie Ustawy – termin 1 miesiąca od otrzymania wniosku lub żądania, termin ten może być wydłużony o kolejny miesiąc z uwzględnieniem przepisów kodeksu postępowania administracyjnego.

4. IOD koordynuje udzielenie odpowiedzi na wnioski i żądania osób, których dane dotyczą, w szczególności:

1) IOD zakłada sprawę i określa domyślny termin jej załatwienia;
2) jeżeli do udzielenia odpowiedzi na wniosek lub żądanie niezbędne jest uzyskanie odpowiedzi lub wykonanie określonych czynności przez właściwego dla danej sprawy właściciela informacji, IOD zwraca się do tego właściciela wskazując termin na udzielenie odpowiedzi zwrotnej;
3) jeżeli termin określony przez IOD nie będzie możliwy do dotrzymania, właściciel informacji wskazuje IOD termin udzielenia odpowiedzi wskazując przyczyny tego

przedłużenia, przy czym termin ten nie może być dłuższy niż 2,5 miesiąca (1,5 miesiąca dla spraw dotyczących przetwarzania danych na podstawie Ustawy) od terminu wpływu wniosku lub żądania i termin ten powinien być jak najkrótszy. W takiej sytuacji IOD informuje wnioskodawcę o konieczności przedłużenia terminu na udzielenie odpowiedzi ze wskazaniem przyczyny;

4) jeżeli właściciel informacji identyfikuje, że nie może zrealizować wniosku lub żądania, ma obowiązek niezwłocznie poinformować o tym IOD oraz wskazać powód, w tym powód odmowy udzielenia odpowiedzi, w szczególności wynikający z przepisów obowiązującego prawa;
5) po uzyskaniu wszelkich niezbędnych informacji IOD przygotowuje odpowiedź na wniosek lub żądanie i przekazuje ją do wnioskodawcy bez zbędnej zwłoki, nie później niż w dniu, w którym upływa termin realizacji wniosku lub żądania;
6) W każdym przypadku udzielania odpowiedzi IOD informuje wnioskodawcę o prawie do wniesienia skargi do PUODO, niezależnie od wyniku, jakim sprawa się zakończyła (np. wniosek lub żądanie w pełni zrealizowane, częściowo zrealizowane, odmowa realizacji);
7) IOD zamyka sprawę, korespondencja w sprawie oraz wszelkie materiały IOD powinien dołączyć do sprawy celem zapewnienia rozliczalności realizacji praw osób, których dane dotyczą.

5. Dopuszcza się sytuacje, w których założenie sprawy nie jest wymagane (np. pytania o ogólne informacje). W takiej sytuacji IOD wykonuje czynności z pominięciem tego kroku, przy czym w przypadku korespondencji elektronicznej IOD zachowuje korespondencję przychodzącą oraz wychodzącą.

6. Składając wniosek lub żądanie na podstawie RODO lub Ustawy, wnioskodawca powinien podać informacje, które pozwolą go w sposób jednoznaczny zidentyfikować, jak również zidentyfikować dane i informacje, których wniosek lub żądanie dotyczą oraz wskazać podstawę prawną swojego wniosku lub żądania, co będzie stanowiło jednoznaczne potwierdzenie oczekiwanych działań, które administrator danych powinien w danej sytuacji podjąć, w tym:

1) składając wniosek lub żądanie na podstawie art. 22 ust. 4, art. 23 ust. 1 lub art. 24 ust. 1 ustawy, wnioskodawca jest obowiązany podać co najmniej imię i nazwisko oraz adres korespondencyjny;

2) jeżeli wniosek nie zawiera wymaganych informacji, lub istnieją wyraźnie uzasadnione wątpliwości co do tożsamości osoby, która złożyła wniosek lub oczekiwanych od administratora danych działań, IOD wzywa wnioskodawcę do podania dodatkowych informacji niezbędnych do potwierdzenia tożsamości tej osoby lub jednoznacznego wskazania, jakich działań wnioskodawca oczekuje od administratora danych. W zależności od kontekstu wniosku lub żądania mogą to być dane takie, jak np. numer PESEL, data urodzenia, numer sprawy lub inny jej szczegół, który może znać tylko osoba, której dane dotyczą, a w odniesieniu do oczekiwanych od administratora działań – wskazanie konkretnej podstawy prawnej wniosku lub żądania;
3) jeżeli w dalszym ciągu istnieją uzasadnione wątpliwości co do tożsamości wnioskodawcy, IOD:
   a. udzielając informacji osobom, których dane dotyczą, może ograniczyć się do przekazania ogólnych informacji opublikowanych na stronie internetowej lub wysłanych w formie zawiadomień na indywidualne adresy poczty elektronicznej wskazując, że udzielenie informacji szczegółowych dotyczących przetwarzanych danych wymaga jednoznacznej i nie budzącej wątpliwości identyfikacji wnioskodawcy lub,
   b. odnosząc się do konkretnej osoby, może udzielić informacji o jej kategoriach danych osobowych, których dotyczy wniosek lub żądanie, ale bez podawania konkretnych danych osobowych;
4) jeżeli pomimo wezwania do podania dodatkowych informacji niezbędnych do jednoznacznego potwierdzenia tożsamości wnioskodawca takich informacji nie udzieli, a informacje ogólne dotyczące przetwarzania danych osobowych przez administratora danych nie realizują celu złożonego wniosku lub żądania, IOD informuje wnioskodawcę o odmowie realizacji wniosku lub żądania ze wskazaniem na brak możliwości jednoznacznego i niebudzącego wątpliwości potwierdzenia tożsamości oraz o prawie do wniesienia skargi do PUODO.

Działania podejmowane w celu przejrzystego informowania i komunikacji oraz wykonywania praw osób

§ 5. 1. Informacje kierowane do osób dotyczące przetwarzania ich danych osobowych muszą być sporządzone w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.

2. IOD może udzielić informacji na piśmie lub w inny sposób, w tym w stosownych przypadkach – elektronicznie. Jeżeli osoba tego zażąda, IOD może udzielić informacji ustnie, o ile jednoznacznie potwierdzi tożsamość tej osoby.

3. IOD:

1) udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku z jej wnioskiem lub żądaniem, w terminach określonych w obowiązujących przepisach prawa i przywołanych w niniejszym dokumencie;
2) informuje wnioskodawcę o przedłużeniu terminu realizacji jej wniosku lub żądania, z podaniem przyczyn tego przedłużenia.

4. Jeżeli wnioskodawca złożył swoje żądanie elektronicznie, IOD w miarę możliwości udziela odpowiedzi również elektronicznie, chyba że wnioskodawca zażąda innej formy.

5. W przypadku niepodjęcia przez Inspektorat działań w odniesieniu do złożonego wniosku lub żądania, IOD informuje wnioskodawcę o przyczynach oraz o możliwości wniesienia skargi do PUODO, jak również o możliwości skorzystania ze środków ochrony prawnej przed sądem.

6. Co do zasady Inspektorat nie pobiera opłat za udzielanie informacji w związku z art. 13 i 14 RODO oraz komunikacji i działań podejmowanych w związku z art. 15-22 i 34 RODO, z zastrzeżeniem ust. 8. Powyższe odnosi się również do udzielania informacji oraz komunikacji i działań podejmowanych na podstawie przepisów Ustawy.

7. Jeżeli przedmiot wniosku lub żądania jest ewidentnie nieuzasadniony lub nadmierny, w szczególności ze względu na swój ustawiczny charakter, IOD przekazuje wnioskodawcy informację o odmowie podjęcia działań, przy czym obowiązek wykazania, że wniosek lub żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter, spoczywa na Inspektoracie – obowiązek ten jest realizowany przez właściciela informacji, który miałby podjąć czynności oczekiwane przez wnioskującego i wskazane we wniosku lub żądaniu.

8. W przypadku podjęcia przez Inspektorat decyzji o realizacji wniosku lub żądania, które ma nadmierny charakter i zostało to jednoznacznie wykazane, Inspektorat może pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań. W takiej sytuacji właściciel informacji konsultuje się z BF celem ustalenia wysokości i szczegółów dotyczących wniesienia przez wnioskodawcę opłaty za realizację wniosku lub żądania i przekazuje informację IOD celem jej przekazania do wnioskodawcy. Realizacja wniosku lub żądania następuje po wniesieniu przez wnioskodawcę opłaty, a w przypadku odmowy jej zapłaty wniosek lub żądanie, dla którego

wykazano jednoznacznie jego nieuzasadniony lub nadmierny charakter, pozostaje bez rozpatrzenia – IOD przekazuje wnioskodawcy stosowną informację wraz z pouczeniem o możliwości wniesienia skargi do PUODO lub możliwości skorzystania ze środków ochrony prawnej.

Działania podejmowane w przypadku zbierania danych bezpośrednio od osoby, której dane dotyczą

§ 6. 1. W przypadku zbierania danych bezpośrednio od osób, których dane dotyczą, właściciel informacji ma obowiązek zapewnić, że tej osobie zostaną podane wszystkie niezbędne informacje:

1) tożsamość i dane kontaktowe administratora;
2) dane kontaktowe inspektora ochrony danych;
3) cele przetwarzania danych osobowych oraz podstawę prawną przetwarzania;
4) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f RODO – prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią;
5) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
6) gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony na podstawie art. 45 RODO lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi RODO, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz informację o sposobach uzyskania kopii tych zabezpieczeń lub o miejscu ich udostępnienia.

2. Poza informacjami, o których mowa w ust. 1 powyżej, podczas pozyskiwania danych osobowych, właściciel informacji ma obowiązek zapewnić, że tej osobie zostaną podane następujące inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania:

1) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
2) informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;

3) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a lub art. 9 ust. 2 lit. a RODO – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
4) informacje o prawie wniesienia skargi do PUODO;
5) informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
6) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

3. Jeżeli dane osobowe będą lub mogą być przetwarzane również w celu innym niż cel, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem właściciel tej czynności przetwarzania ma obowiązek poinformować osobę, której dane dotyczą, o tym innym celu oraz udzielić jej wszelkich innych stosownych informacji, o których mowa w ust. 2 powyżej.

4. Ustępy 1, 2 i 3 nie stosuje się, gdy – i w zakresie, w jakim – osoba, której dane dotyczą, dysponuje już tymi informacjami.

5. Do udzielania informacji, o których mowa w ust. 1-3 powyżej, właściciel informacji stosuje klauzule informacyjne. Przykładowe wzory i szablony klauzul informacyjnych zawiera załącznik nr 1 do PODO. Klauzule te należy każdorazowo dostosować do danej sytuacji wymagającej ich zastosowania. Za dostosowanie i zastosowanie klauzul informacyjnych odpowiada pracownik zbierający dane osobowe.

Działania podejmowane w przypadku zbierania danych w sposób inny, niż bezpośrednio od osoby, której dane dotyczą

§ 7. 1. W przypadku zbierania danych osobowych nie od osoby, której dane dotyczą, właściciel informacji ma obowiązek zapewnić, że osobie, której dane dotyczą zostaną podane wszystkie następujące informacje:

1) tożsamość i dane kontaktowe administratora;
2) dane kontaktowe inspektora ochrony danych;
3) cele przetwarzania danych osobowych, oraz podstawę prawną przetwarzania;

4) kategorie odnośnych danych osobowych;
5) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
6) gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony na podstawie art. 45 RODO lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi RODO, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz informację o sposobach uzyskania kopii tych zabezpieczeń lub o miejscu ich udostępnienia.

2. Poza informacjami, o których mowa w ust. 1, właściciel informacji ma obowiązek zapewnić, że osobie której dane dotyczą zostaną podane następujące informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania wobec tej osoby:

1) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
2) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f RODO – prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią;
3) informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
4) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a lub art. 9 ust. 2 lit. a RODO – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
5) informacje o prawie wniesienia skargi do PUODO;
6) źródło pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą ze źródeł publicznie dostępnych;
7) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

3. Informacje, o których mowa w ust. 1 i 2 powyżej, właściciel informacji ma obowiązek podać:

1) w rozsądnym terminie po pozyskaniu danych osobowych – najpóźniej w ciągu miesiąca – mając na uwadze konkretne okoliczności przetwarzania danych osobowych;
2) jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą – najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą; lub
3) jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu.

4. Jeżeli planowane jest dalsze przetwarzanie danych osobowych, o których mowa powyżej, w celu innym niż cel, w którym te dane zostały pozyskane, przed takim dalszym przetwarzaniem właściciel informacji informuje osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji, o których mowa w ust. 1-3 powyżej.

5. Ust. 1-4 nie mają zastosowania, gdy – i w zakresie, w jakim:

1) osoba, której dane dotyczą, dysponuje już tymi informacjami;
2) udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku; w szczególności w przypadku przetwarzania do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem warunków i zabezpieczeń, o których mowa w art. 89 ust. 1 RODO, lub o ile obowiązek informacyjny, o którym mowa w ust. 1 powyżej, może uniemożliwić lub poważnie utrudnić realizację celów takiego przetwarzania. W takich przypadkach właściciel informacji podejmuje odpowiednie środki, by chronić prawa i wolności oraz prawnie uzasadnione interesy osoby, której dane dotyczą, w tym udostępnia informacje publicznie;
3) pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator, przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą; lub
4) dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii lub w prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy.

6. Do udzielania informacji, o których mowa w ust. 1-4 powyżej właściciel informacji stosuje klauzule informacyjne. Przykładowe wzory i szablony klauzul informacyjnych zawiera załącznik nr 1 do PODO. Klauzule te należy każdorazowo dostosować do danej sytuacji wymagającej ich zastosowania. Za dostosowanie i zastosowanie klauzul informacyjnych odpowiada pracownik zbierający dane osobowe.

Środki ochrony danych osobowych w systemach

§ 8. 1. Środki ochrony danych osobowych inne, niż opisane w PODO, określa PBI, załączniki do PBI oraz odrębne dokumentacje SZBI systemów, w których dane osobowe są przetwarzane.

2. Każdy system, w których dochodzi do przetwarzania danych osobowych, musi posiadać ustanowioną i wdrożoną dokumentację dotyczącą przetwarzania danych osobowych, szczegółowo opisującą i adresującą wszystkie zasady i wymagania odnoszące się do przetwarzania danych osobowych z wykorzystaniem nowoczesnych technologii, w szczególności opis środków i zabezpieczeń podjętych w celu ochrony poufności, integralności i dostępności danych osobowych oraz sposób zapewnienia realizacji praw osób, których dane dotyczą i które to dane osobowe są w takim systemie przetwarzane.

Polityki Ochrony Danych Osobowych

§ 9. 1. Zdefiniowane w PODO wymagania i zasady mają zastosowanie do przetwarzania wszelkich danych osobowych i określają, co należy uwzględnić, kiedy należy uwzględnić oraz określają, kto jest za to odpowiedzialny, z wyłączeniem przetwarzania danych osobowych w oparciu o przepisy ustawy o ochronie informacji niejawnych.

2. PODO nie wyklucza możliwości ustanowienia odrębnej polityki dotyczącej ochrony danych osobowych dla danej czynności przetwarzania, w szczególności z zastosowaniem nowoczesnych technologii. Ustanawiając odrębną politykę ochrony danych osobowych dla czynności przetwarzania należy uwzględnić, ponad przepisy o ochronie danych osobowych oraz rozwiązania przyjęte w PODO, również obowiązujące wymagania prawne dotyczące ochrony informacji oraz cyberbezpieczeństwa, w tym ustanowione na ich podstawie inne polityki, tj. PBI oraz załączniki do niej.

3. Zalecane jest, aby w miarę możliwości ustanawiając dokumentację dla czynności przetwarzania, w szczególności tych realizowanych w systemach, utworzyć jeden nadrzędny dokument opisujący cele strategiczne, zakres, kontekst, uwarunkowania, odpowiedzialność itp. elementy odnoszące się do czynności przetwarzania np. „*Polityka Bezpieczeństwa czynności przetwarzania / systemu …*”, „*Polityka ochrony danych osobowych czynności przetwarzania / systemu …*”.

Nadzór nad przetwarzaniem danych osobowych

§ 10. 1. Nadzór nad przetwarzaniem danych osobowych sprawuje IOD w ramach wykonywania swoich zadań służbowych. Kontrolę lub audyt w zakresie prawidłowości przetwarzania danych osobowych może również prowadzić komórka organizacyjna właściwa do spraw kontroli i audytu wewnętrznego – zastosowanie mają przepisy prawa i regulacje wewnętrzne dotyczące audytu wewnętrznego w jednostkach sektora finansów publicznych.

2. IOD jest uprawniony do żądania od wszystkich pracowników wszelkich informacji związanych z prowadzonym przetwarzaniem danych osobowych.

3. IOD monitoruje zgodność przetwarzania danych osobowych z przepisami prawa oraz wymaganiami określonymi w PODO, jak również wspiera Głównego Inspektora w realizacji obowiązków administratora danych. W tym celu IOD realizuje kontrole, jak również uczestniczy oraz udziela wsparcia w zakresie swojej właściwości w kontrolach i audytach prowadzonych przez komórkę organizacyjną właściwą do spraw kontroli i audytu wewnętrznego, w szczególności gdy te obejmują swoim zakresem zadania przypisane IOD.

5. IOD uczestniczy również w kontrolach i audytach wykonywanych przez podmioty zewnętrzne działające na zlecenie Inspektoratu oraz podmioty ustawowo umocowane do takich działań, jeżeli te dotyczą obszaru ochrony danych osobowych, w szczególności w kontrolach PUODO.

6. IOD w związku z pełnionym nadzorem i monitorowaniem zgodności przetwarzania danych osobowych z przepisami prawa i PODO nie realizuje jakichkolwiek zadań, które mogą powodować wystąpienie konfliktu interesów (tj. gdy nadzorowi i kontroli IOD podlega czynność wykonywana lub wykonana przez IOD). W szczególności IOD nie realizuje czynności przypisanych jednoznacznie do administratora danych, m.in.:

1) nie opracowuje i nie akceptuje zapisów umów lub porozumień w zakresie powierzenia przetwarzania danych osobowych, a wyłącznie weryfikuje, czy te zapisy zawierają wszystkie wymagane przez przepisy prawa elementy dotyczące powierzenia przetwarzania danych osobowych podmiotowi przetwarzającemu; za opracowanie zapisów umów lub porozumień w zakresie powierzenia przetwarzania danych osobowych odpowiadają członkowie komisji przetargowych lub inni pracownicy, którym powierzono do realizacji zadania związane z zawarciem takiej umowy lub porozumienia;
2) nie udziela w imieniu administratora danych odpowiedzi na pytania kierowane w postępowaniach o udzielenie zamówień publicznych; reprezentantem administratora

danych – Głównego Inspektora w postępowaniu o udzielenie zamówienia publicznego jest komisja powołana do jego przeprowadzenia lub inne osoby wykonujące czynności zmierzające do udzielenia zamówienia podmiotom zewnętrznym w sytuacjach, gdy komisja powoływana nie jest; rolą IOD jest nadzór, aby w sytuacji powierzenia przetwarzania danych osobowych było ono dokonane w sposób udokumentowany zawierający wszystkie wymagane przepisami o ochronie danych osobowych elementy; IOD może doradzać tym osobom w zakresie spoczywających na nich obowiązków związanych z powierzaniem przetwarzania danych osobowych na mocy przepisów prawa;

3) nie opracowuje zapisów klauzul informacyjnych, a wyłącznie określa, czy te klauzule zawierają wszystkie wymagane przez przepisy prawa elementy; za opracowanie treści klauzul informacyjnych odpowiadają właściciele informacji oraz pracownicy realizujący w ich imieniu zadania związane z pozyskiwaniem danych osobowych;

4) nie określa zabezpieczeń, jakie administrator danych ma wdrożyć w celu ochrony danych osobowych na odpowiednim poziomie, a wyłącznie doradza w tym zakresie, tym bardziej nie wdraża tych zabezpieczeń; za określenie zabezpieczeń w celu ochrony danych osobowych odpowiada właściciel informacji na podstawie przeprowadzonej oceny skutków dla ochrony danych;

5) nie określa celów i podstaw przetwarzania danych osobowych, a wyłącznie prowadzi monitorowanie i nadzór, aby takie cele i podstawy przetwarzania danych osobowych były ustalone dla każdej z czynności przetwarzania danych osobowych; za określenie celów i podstaw przetwarzania danych osobowych odpowiada właściciel informacji;

6) nie dokonuje oceny skutków dla ochrony danych osobowych, a wyłącznie doradza co do sposobu jej prowadzenia i monitoruje, czy dla czynności przetwarzania, które tego wymagają takie oceny skutków zostały przeprowadzone; za przeprowadzenie oceny skutków dla ochrony danych, w tym dobór i wdrażanie na podstawie tej oceny zabezpieczeń odpowiada właściciel informacji;

7) nie podpisuje, nie akceptuje, jak również nie wysyła powiadomień do osób, których dane osobowe są objęte naruszeniami; obowiązkiem IOD jest nadzorować, aby administrator danych (w jego imieniu realizuje to właściwa dla naruszenia komórka organizacyjna oraz kierujący tą komórką) takiej czynności dopełnił w wymaganych prawem przypadkach, oraz aby powiadomienia te zawierały wymagany zakres informacyjny dotyczący naruszenia, IOD doradza w tym zakresie, ale nie wyręcza.

Obowiązek konsultacji wszelkich spraw związanych z przetwarzaniem danych osobowych

§ 11. 1. IOD musi być obowiązkowo włączany w każdą sprawę dotyczącą ochrony danych osobowych w związku z koniecznością zapewnienia, że m.in. czynność przetwarzania jest zgłoszona i opisana w rejestrze czynności przetwarzania lub rejestrze kategorii czynności przetwarzania, jeżeli jest to wymagane została przeprowadzona ocena skutków dla ochrony danych, ustanowiono wymaganą przepisami prawa dokumentację ochrony danych, jeżeli jest to wymagane przeprowadzono konsultacje z PUODO, czy też prawidłowo realizowane są prawa i obowiązki osób, których dane dotyczą lub obowiązki informacyjne.

2. Za włączanie IOD we wszelkie sprawy związane z ochroną danych osobowych odpowiada każdy pracownik. Obowiązkiem kierujących komórkami organizacyjnymi jest zapewnienie, że IOD jest włączany we wszelkie sprawy związane z ochroną danych osobowych realizowane w tej komórce organizacyjnej, m.in. wnioski i żądania osób, których dane dotyczą, ustanawianie nowych czynności przetwarzania w tym z wykorzystaniem systemów, skargi na przetwarzanie danych osobowych, powierzanie danych osobowych do przetwarzania podmiotom zewnętrznym lub przyjmowanie do przetwarzania danych osobowych od innego administratora danych.

3. Włączanie IOD we wszelkie sprawy związane z ochroną danych osobowych obejmuje również projekty wewnętrznych regulacji, takich jak zarządzenia Głównego Inspektora, zarządzenia DG, które pośrednio lub bezpośrednio dotyczą przetwarzania lub ochrony danych osobowych. IOD może być włączany na etapie przygotowania projektu regulacji lub na etapie jej wewnętrznego uzgadniania.

Przetwarzanie danych osobowych na podstawie upoważnienia

§ 12. 1. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby upoważnione przez Głównego Inspektora lub osoby działające w jego imieniu na podstawie upoważnienia.

2. Główny Inspektor upoważnia pracowników BDG – WKR do udzielania w jego imieniu upoważnień do przetwarzania danych osobowych pracownikom.

3. Pracownicy BDG – WKR upoważniają pracowników Inspektoratu do przetwarzania danych osobowych w zakresie niezbędnym do wykonania przez te osoby zadań na zajmowanym stanowisku pracy, w tym upoważniają pracowników do przetwarzania danych w związku z Zakładowym Funduszem Świadczeń Socjalnych i realizacją zadań Komisji

Socjalnej w Inspektoracie. Zakres upoważnienia do przetwarzania danych osobowych pracowników mają obowiązek określić bezpośredni przełożeni pracowników upoważnianych.

4. Upoważnienia do przetwarzania danych osobowych sporządzane są w formie pisemnej, w tym mogą być sporządzane w formie elektronicznej podpisanej kwalifikowanym podpisem elektronicznym lub podpisem zaufanym, z czego:

1) jeden egzemplarz upoważnienia otrzymuje pracownik;
2) drugi egzemplarz upoważnienia, po potwierdzeniu odbioru przechowuje komórka organizacyjna właściwa do spraw kadrowych.

5. Upoważnienia do przetwarzania danych osobowych udzielane są wyłącznie na okres zatrudnienia lub wykonywania zadań członka Komisji Socjalnej i wygasają najpóźniej wraz z zakończeniem zatrudnienia lub zakończeniem realizacji przez pracownika zadań związanych z udziałem w pracach Komisji Socjalnej.

6. Upoważnienie do przetwarzania danych osobowych może być udzielone pracownikowi, który:

1) w ramach powierzonych do realizacji zadań służbowych będzie przetwarzał dane osobowe;
2) został zapoznany przez IOD z przepisami prawa i zasadami ochrony danych osobowych;
3) złożył podpisane przez siebie oświadczenie potwierdzające znajomość i zrozumienie zasad ochrony informacji, w tym danych osobowych.

7. Oświadczenia potwierdzające znajomość i zrozumienie zasad ochrony informacji, w tym danych osobowych przechowuje komórka organizacyjna właściwa do spraw kadrowych.

8. Opcjonalnie – zaleca się rozważenie przez BDG – WKR prowadzenia wykazu pracowników upoważnionych do przetwarzania danych osobowych obejmującego dane identyfikacyjne pracownika, numer upoważnienia jeżeli nadawany np. może być to numer umowy o pracę, datę nadania upoważnienia, datę ustania ważności upoważnienia, zakres upoważnienia określony przez bezpośredniego przełożonego pracownika. W przypadku prowadzenia takiego wykazu przez BDG – WKR, AMS / ASI mają obowiązek umieszczać w nim informacje o zakresie uprawnień w systemach, do których pracownik ma dostęp. Prowadzenie wykazu jest najprostszą metodą wykazywania rozliczalności stosowania RODO.

9. Wzory i szablony upoważnień do przetwarzania danych osobowych określa załącznik nr 2 do PODO. Jeżeli wymagane jest zastosowanie innego, niż określony w PODO wzoru upoważnienia, wzór ten należy dostosować do danej sytuacji i zidentyfikowanych potrzeb.

10. Wzór oświadczenia o zapoznaniu i zrozumieniu zasad ochrony informacji, w tym danych osobowych określa załącznik nr 1 do PBI.

11. Wzory i szablony oświadczeń innych, niż wskazane w ust. 10 określa załącznik nr 3 do PODO. Jeżeli wymagane jest zastosowanie innego, niż określony w PODO wzoru oświadczenia, wzór ten należy dostosować do danej sytuacji i zidentyfikowanych potrzeb.

12. Główny Inspektor oraz upoważnieni przez niego pracownicy BDG – WKR mogą cofnąć lub zawiesić upoważnienie do przetwarzania danych osobowych, w tym także na wniosek bezpośredniego przełożonego, kierującego komórką organizacyjną w której pracownik jest zatrudniony, IOD, pełnomocnika do spraw bezpieczeństwa informacji, pełnomocnika do spraw bezpieczeństwa cyberprzestrzeni, w szczególności w związku z naruszeniem przez taką osobę zasad ochrony danych osobowych, zmianą stanowiska pracy i związaną z tym zmianą zakresu upoważnienia, odwołaniem z funkcji lub z zespołu, długą nieobecnością takiej osoby, lub zakończeniem zatrudnienia.

13. Główny Inspektor może upoważnić innych, niż BDG – WKR, pracowników do udzielania w jego imieniu upoważnień do przetwarzania danych osobowych np. w związku z dostępem do rejestru lub zbioru danych osobowych prowadzonego przez Głównego Inspektora, dla którego wymagane są odrębne upoważnienia do przetwarzania danych osobowych m.in. wynikające z przepisów prawa.

14. Osoby określone w ust. 13 powinny rozważyć prowadzenie wykazu osób upoważnionych do przetwarzania danych osobowych, którym udzielają upoważnień do przetwarzania danych osobowych, w celu wykazywania rozliczalności stosowania RODO.

15. Odrębna dokumentacja może ustanawiać odmienne od opisanych w PODO wymagania m.in. dla wykazu osób i zasad jego prowadzenia, upoważnień i oświadczeń o zachowaniu poufności, w szczególności w sytuacji, gdy Główny Inspektor staje się podmiotem przetwarzającym lub współadministratorem.

Obowiązek zapoznania z przepisami oraz zasadami ochrony danych osobowych przed uzyskaniem upoważnienia do przetwarzania danych osobowych

§ 13. 1. Każdy pracownik przed uzyskaniem upoważnienia umożliwiającego przystąpienie do wykonywania obowiązków służbowych związanych z przetwarzaniem danych osobowych musi zostać zapoznany przez IOD z obowiązującymi w Inspektoracie zasadami ochrony danych osobowych. Zapoznanie następuje najpóźniej w dniu, w którym pracownik rozpoczyna zatrudnienie.

2. Każdy pracownik ma obowiązek złożyć podpisane przez siebie oświadczenie potwierdzające znajomość i zrozumienie zasad ochrony informacji, w tym danych osobowych, co jest warunkiem koniecznym do uzyskania upoważnienia do przetwarzania danych osobowych. Podpisane oświadczenie pracownik przekazuje do komórki organizacyjnej właściwej do spraw kadrowych.

3. Pracownik ma obowiązek przejść szkolenie z przepisów i zasad ochrony danych osobowych. Szkolenie jest organizowane zgodnie z PBO określoną w załączniku nr 3 do PBI.

Informowanie o rozpoczęciu i zakończeniu zatrudnienia

§ 14. 1. Komórka organizacyjna właściwa do spraw rekrutacji informuje IOD, w miarę możliwości z co najmniej 3 dniowym wyprzedzeniem przed datą planowanego zatrudnienia nowego pracownika o tym fakcie na adres iod@gitd.gov.pl, ewentualnie dodatkowo wiadomość może być wysyłana na imienny adres e-mail IOD.

2. BDG – WKR informuje IOD, w miarę możliwości z co najmniej 3 dniowym wyprzedzeniem przed datą planowanego zakończenia zatrudnienia pracownika o tym fakcie na adres iod@gitd.gov.pl lub na imienny adres e-mail IOD / osoby zastępującej.

3. Informacje określone w ust. 1-2 komórki organizacyjne, o których mowa w ust. 1-2 przekazują również do BT oraz – w przypadku ust. 2 – w miarę możliwości i po uzgodnieniu do AMS, w celu zapewnienia, że uprawnienia w systemach zostaną odebrane najpóźniej z chwilą ustania zatrudnienia. Powyższe nie zdejmuje z bezpośrednich przełożonych pracowników kończących zatrudnienie obowiązków określonych w Regulaminie pracy w Inspektoracie związanych z koniecznością wnioskowania o odebranie uprawnień w systemach, do których pracownik miał dostęp.

Szkolenia i zapoznawanie z przepisami oraz zasadami ochrony danych osobowych

§ 15. Zasady i wymagania dotyczące szkoleń i zapoznawania z przepisami i zasadami ochrony danych osobowych określa załącznik nr 3 do PBI.

Obowiązek zgłaszania naruszeń ochrony danych osobowych

§ 16. 1. Każdy pracownik ma obowiązek niezwłocznego zgłoszenia zdarzeń mogących mieć lub mających wpływ na ochronę danych osobowych (naruszeń ochrony danych osobowych). Przez naruszenie ochrony danych osobowych, należy rozumieć naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia,

utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

2. Każdy przypadek naruszenia lub podejrzenia naruszenia ochrony danych osobowych należy zgłosić niezwłocznie do IOD na adres e-mail iod@gitd.gov.pl lub telefonicznie lub na ogólny adres e-mail dedykowany do zgłaszania incydentów bezpieczeństwa informacji incydent@gitd.gov.pl.

Powierzenie przetwarzania danych osobowych innemu podmiotowi

§ 17. 1. Na potrzeby sytuacji powierzania przetwarzania danych osobowych z zastosowaniem przepisów RODO opracowane zostały standardowe zapisy umowy powierzenia przetwarzania danych osobowych, które zawiera załącznik nr 4 do PODO.

2. Na potrzeby sytuacji powierzania przetwarzania danych osobowych z zastosowaniem przepisów Ustawy opracowane zostały standardowe zapisy umowy powierzenia przetwarzania danych osobowych, które zawiera załącznik nr 4 do PODO.

3. W każdym przypadku korzystania z wzorów, o których mowa w ust. 1 i 2, zawarte w nich zapisy należy każdorazowo zweryfikować i dostosować do własnych potrzeb, kontekstu, celów, zakresu powierzenia itp.

4. W sytuacji powierzania przetwarzania danych osobowych z zastosowaniem jednocześnie przepisów RODO i Ustawy, zapisy zawarte we wzorach wskazanych w ust. 1 i 2 można dowolnie łączyć, przy czym należy pamiętać o zachowaniu wszystkich elementów wymaganych przez RODO i Ustawę.

5. Członkowie komisji przetargowych, kierujący komórkami organizacyjnymi i wszyscy pozostali pracownicy, którzy realizują zadania, których celem jest powierzenie przetwarzania danych osobowych innemu podmiotowi zewnętrznemu, mają obowiązek opracować treść umowy powierzenia przetwarzania danych osobowych, jak również poinformować IOD o zamiarze zawarcia takiej umowy ze wskazaniem czynności przetwarzania z rejestru tych czynności, której powierzenie przetwarzania danych osobowych będzie dotyczyć.

6. Pracownicy, o których mowa w ust. 5 mogą skonsultować z IOD projekt umowy powierzenia przetwarzania danych osobowych, czy zawiera wszystkie elementy wymagane przez RODO lub Ustawę, z zastrzeżeniem, że to do nich należy opracowanie treści takiej umowy w szczególności w zakresie merytorycznym. IOD ocenia wyłącznie zgodność projektu umowy z przepisami prawa. IOD powinien otrzymać czas nie krótszy niż 3 dni robocze na analizę i wyrażenie swojej opinii.

7. Pracownicy, o których mowa w ust. 5 mogą skonsultować z IOD projekt zmian już zawartej i obowiązującej umowy powierzenia przetwarzania danych osobowych, czy zmiany nie mają negatywnego wpływu na realizację obowiązków administratora lub nie powodują niezgodności z przepisami prawa pod względem wymaganych w umowie treści.

8. IOD może weryfikować projekt umowy powierzenia przetwarzania danych osobowych przed jej podpisaniem pod względem zgodności z przepisami prawa. IOD nie akceptuje umowy, w tym treści merytorycznej obejmującej w szczególności kategorie i zakres szczegółowy powierzanych danych osobowych, a wyłącznie może zweryfikować, czy te informacje zostały w umowie powierzenia określone.

9. Pracownicy, o których mowa w ust. 5 mają obowiązek informowania bez zbędnej zwłoki IOD o danych podmiotu przetwarzającego po zawarciu umowy powierzenia oraz o czasie jej obowiązywania, celem aktualizacji rejestru czynności przetwarzania. IOD musi być również bez zbędnej zwłoki poinformowany o rozwiązaniu umowy powierzenia, w szczególności przed terminem w niej określonym.

10. Zaleca się weryfikować zdolność podmiotów przetwarzających do ochrony powierzanych im danych osobowych przed zawarciem umowy, np. poprzez zawarcie w dokumentacji postępowania ankiety pozwalającej na weryfikację, czy podmiot daje wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odbywało się zgodnie z RODO i chroniło prawa osób, których dane dotyczą.

11. Negatywna weryfikacja, o której mowa w ust. 10 powinna prowadzić do zaniechania zawarcia umowy powierzenia z podmiotem zewnętrznym, który nie daje wystarczających gwarancji ochrony powierzanych danych osobowych.

Główny Inspektor jako podmiot przetwarzający

§ 18. 1. Członkowie komisji przetargowych, kierujący komórkami organizacyjnymi i wszyscy pozostali pracownicy, którzy realizują zadania, których celem jest powierzenie Głównemu Inspektorowi przetwarzania danych osobowych przez innego administratora danych mają obowiązek włączenia IOD w ten proces pod względem nadzoru nad zgodnością tego powierzenia z przepisami prawa.

2. Zastosowanie mają zapisy § 17 ust. 5-9 z zastrzeżeniem, że ich kontekst dotyczy w tej sytuacji powierzenia Głównemu Inspektorowi przetwarzania danych osobowych przez innego administratora.

3. Właściciel informacji, której dotyczy powierzenie Głównemu Inspektorowi przetwarzania danych osobowych, zapewnia realizację obowiązków określonych w umowie powierzenia przetwarzania danych osobowych (m.in. określanie i wdrażanie zabezpieczeń, udzielanie upoważnień do przetwarzania danych osobowych, realizowanie obowiązków informacyjnych, przeprowadzanie ocen skutków dla ochrony danych, prowadzenie innej wymaganej dokumentacji dotyczącej przetwarzania powierzonych danych osobowych, obowiązki związane z dalszym powierzaniem przetwarzania danych osobowych), z zastrzeżeniem czynności, za których realizację odpowiada IOD na podstawie przepisów prawa i regulacji wewnętrznych (prowadzenie rejestru kategorii czynności przetwarzania, koordynacja zadań związanych z realizacją praw osób, których dane dotyczą, zarządzanie naruszeniami ochrony danych osobowych, monitorowanie i kontrola zgodności przetwarzania i stosowania ustalonych środków ochrony danych osobowych z przepisami prawa).

Przetwarzanie danych osobowych na podstawie zgody

§ 19. 1. Zarządzanie zgodami na przetwarzanie danych osobowych dotyczy wszelkich sytuacji, w których do przetwarzania danych osobowych wymagane jest posiadanie od osoby, której dane dotyczą, dobrowolnie wyrażonej zgody na przetwarzanie jej danych osobowych.

2. Zarządzanie zgodami obejmuje również sytuacje, w których osoba, której dane dotyczą, przekazała dane osobowe i wyraziła zgodę na ich przetwarzanie, pomimo że przekazania tych danych nie oczekiwano.

3. Zarządzanie zgodami może być prowadzone w systemie posiadającym taką funkcjonalność, lub w sposób organizacyjno-proceduralny.

4. W sytuacji zarządzania zgodami w sposób organizacyjno-proceduralny, właściciel informacji jest zobowiązany do prowadzenia, w formie pisemnej (w tym elektronicznej) rejestru zgód na przetwarzanie danych osobowych. Szablon rejestru zgód określający jego minimalną zawartość informacyjną określa załącznik nr 5 do PODO.

5. Właściciel informacji ma obowiązek zapewnić prowadzenie rejestru zgód dla każdej czynności przetwarzania, która obejmuje przetwarzanie danych osobowych na podstawie zgody.

6. Właściciel informacji ma obowiązek zapewnić poufność, integralność i dostępność informacji zawartych w prowadzonych przez siebie rejestrach zgód, niezależnie od formy ich prowadzenia.

7. Właściciel informacji prowadząc przetwarzanie danych osobowych na podstawie zgody ma obowiązek umożliwić osobie, której dane dotyczą wycofanie zgody w dowolnym momencie i w prosty sposób, co najmniej w tej samej formie, w której zgoda została wyrażona oraz w formie pisemnej w każdym przypadku.

8. Dla wszystkich czynności przetwarzania opartych na zgodzie właściciele informacji powinni określić okresy przechowywania zgód z uwzględnieniem np. przedawnienia roszczeń i celowości przechowywania zgód po końcu okresu, w którym zgoda obowiązywała czy z uwzględnieniem okresu zatrudnienia dla zgód wyrażanych przez pracowników.

Ochrona danych w fazie projektowania i domyślna ochrona danych

§ 20. 1. Stosowanie zasad ochrony danych w fazie projektowania oraz domyślnej ochrony danych jest obowiązkowe, w szczególności tam, gdzie mają zastosowanie technologie informatyczne.

2. Stosowanie zasad ochrony danych w fazie projektowania oraz domyślnej ochrony danych szczegółowo opisują wytyczne EROD nr 4/2019 dotyczące art. 25 RODO i uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych. Treść tych wytycznych dostępna jest na stronie EROD pod adresem https://edpb.europa.eu/edpb_pl.

3. Praktyczne stosowanie zasad ochrony danych w fazie projektowania oraz domyślnej ochrony danych podlega obowiązkowemu dokumentowaniu, którego celem jest wypełnienie obowiązkowej zasady rozliczalności określonej w RODO. Dokumentowanie, o którym mowa powyżej polega m.in. na szczegółowym dokumentowaniu czynności przetwarzania, ocen skutków dla ochrony danych, wymagań i założeń dla rozwiązań teleinformatycznych w ich dokumentacji definiujących planowane lub stosowane środki ochrony i zabezpieczenia w celu zapewnienia stosowania zasad określonych w RODO oraz praw i wolności osób fizycznych, dokumentowaniu zadań wykonywanych przez m. in. AMS i ASI.

Rejestrowanie czynności przetwarzania

§ 21. 1. Główny Inspektor powierzył IOD powadzenie rejestru czynności przetwarzania (RODO) i wykazu kategorii czynności przetwarzania (Ustawa) oraz rejestru wszystkich kategorii czynności przetwarzania w przypadku, gdy to Główny Inspektor jest podmiotem przetwarzającym.

2. Rejestry, o których mowa w ust. 1 IOD prowadzi w postaci elektronicznej.

3. IOD ma obowiązek:

1) zapewnić integralność rejestrów i wykazów, o których mowa w ust. 1, a w odniesieniu do opisu zabezpieczeń – również poufność;
2) okresowo – nie rzadziej niż raz w roku – dokonywać weryfikacji, przy udziale właścicieli informacji, czy czynności przetwarzania opisane w rejestrach i wykazach o których mowa w ust. 1 są aktualne oraz jeżeli to wymagane – dokonać aktualizacji rejestru na podstawie informacji przekazanych przez właścicieli informacji;
3) zapewnić dostępność rejestrów i wykazów, o których mowa w ust. 1.

4. Administratorem danych w odniesieniu do czynności przetwarzania opisanych w rejestrze czynności przetwarzania jest Główny Inspektor.

5. Właścicielami czynności przetwarzania opisanych w rejestrze czynności przetwarzania są właściciele informacji – kierujący komórkami organizacyjnymi, którzy są odpowiedzialni za realizację tych czynności na podstawie regulaminu organizacyjnego oraz regulaminów organizacyjnych komórek.

6. Właściciele informacji mają obowiązek:
1) współpracować z IOD przy prowadzeniu rejestrów i wykazów, o których mowa w ust. 1, w tym dostarczać IOD wszelkich niezbędnych informacji umożliwiających jego prowadzenie oraz poprawność zawartych w nich informacji;
2) zapewnić aktualność zapisów w rejestrach i wykazach, o których mowa w ust. 1 oraz przekazywać IOD bez zbędnej zwłoki informacje umożliwiające aktualizację tych rejestrów i wykazów w przypadku zmian w realizowanych czynnościach przetwarzania m.in. zmian celów przetwarzania, kategorii osób, zakresu danych, odbiorców danych, podmiotów przetwarzających.

7. Szablony i wzory rejestrów i wykazów, o których mowa w ust. 1 określa załącznik nr 6 do PODO. Szablony te mogą być rozszerzane o dodatkowe informacje, jeżeli istnieje taka potrzeba np. wynikająca z umowy powierzenia zawartej z innym administratorem.

Współpraca z UODO

§ 22. 1. Osobą upoważnioną przez Głównego Inspektora do bieżących kontaktów z UODO, w tym do udzielania odpowiedzi na wnioski i skargi oraz prowadzenia innej korespondencji w zakresie wynikającym z udzielonych upoważnień jest IOD.

2. Ponadto IOD utrzymuje z UODO robocze kontakty, m.in. w przypadku konieczności uzyskania pomocy lub wyjaśnień dotyczących interpretacji i stosowania przepisów o ochronie danych osobowych.

3. Uprzednie konsultacje z UODO są obowiązkowe zawsze, gdy ocena skutków dla ochrony danych wykaże, że przetwarzanie powodowałoby wysokie ryzyko naruszenia praw osób, zaś Główny Inspektor nie zastosował lub nie może znaleźć środków w celu zminimalizowania tego ryzyka.

4. Niedopuszczalne wysokie ryzyko szczątkowe obejmuje przypadki, w których osoby fizyczne mogą ponieść znaczne lub nawet nieodwracalne konsekwencje, z którymi nie będą mogły sobie poradzić (np. bezprawne uzyskanie dostępu do danych prowadzące do zagrożenia życia lub zdrowia osób, zwolnienia z pracy, zagrożenia o charakterze finansowym, kradzież tożsamości) lub w których wydaje się oczywiste, że wystąpi ryzyko (np. ograniczenie liczby osób mających dostęp do danych nie jest możliwe ze względu na sposób ich udostępniania, wykorzystywania lub rozprowadzania lub gdy luka w zabezpieczeniach, o której istnieniu wiadomo, nie zostanie usunięta).

5. Uprzednie konsultacje są wykonywane zawsze przed rozpoczęciem przetwarzania danych osobowych. Informacji wymaganych do prowadzenia konsultacji z UODO dostarcza właściciel informacji i obejmują one m.in.:

1) cele i sposoby zamierzonego przetwarzania;
2) środki i zabezpieczenia dla ochrony praw i wolności osób, których dane dotyczą;
3) dane kontaktowe IOD;
4) ocenę skutków dla ochrony danych.

6. Uprzednie konsultacje z UODO koordynuje i prowadzi IOD przy udziale właściciela informacji lub jego przedstawiciela. Właściciel informacji ma obowiązek przygotować i udostępnić IOD wszelkie informacje wymagane do prowadzenia konsultacji, w tym określone powyżej oraz inne, jeżeli takich zażąda UODO, odnoszące się do planowanego przetwarzania.

Zarządzanie naruszeniami ochrony danych osobowych

§ 23. 1. IOD, pełnomocnik do spraw bezpieczeństwa cyberprzestrzeni oraz pełnomocnik do spraw bezpieczeństwa informacji mają obowiązek współpracować ze sobą i wymieniać się informacjami na temat zgłaszanych naruszeń ochrony danych osobowych, incydentów cyberbezpieczeństwa oraz incydentów bezpieczeństwa informacji, celem ustalenia, czy:

1) naruszenia ochrony danych osobowych stanowią incydent w podmiocie publicznym i wymagają zgłoszenia do CSIRT w ciągu 24 godzin od ich wykrycia – kryterium klasyfikacji określa ustawa o krajowym systemie cyberbezpieczeństwa oraz procedura zgłaszania incydentów określona w załączniku nr 6 do PBI;

2) incydenty cyberbezpieczeństwa stanowią naruszenie ochrony danych osobowych i wymagają zgłoszenia do PUODO w ciągu 72 godzin od ich wykrycia, ewentualnie powiadomienia osób, których dane są objęte naruszeniem – kryterium klasyfikacji określa RODO, Ustawa oraz procedura zgłaszania incydentów określona w załączniku nr 6 do PBI;
3) incydenty bezpieczeństwa informacji stanowią naruszenie ochrony danych osobowych i wymagają zgłoszenia do PUODO w ciągu 72 godzin od ich wykrycia, ewentualnie powiadomienia osób, których dane są objęte naruszeniem – kryterium klasyfikacji określa RODO, Ustawa oraz procedura zgłaszania incydentów określona w załączniku nr 6 do PBI.

2. Obsługę i wyjaśnianie naruszeń ochrony danych osobowych koordynuje IOD. W ramach tych czynności IOD jest uprawniony do żądania od wszystkich pracowników udzielenia wyjaśnień w związku z obsługiwanym naruszeniem, w tym do uzyskiwania materiałów mogących stanowić dowód w postępowaniu. Do przekazywania informacji wrażliwych lub informacji prawnie chronionych należy stosować wymagania i wytyczne dotyczące zapewnienia poufności informacji, m.in. dostępne mechanizmy szyfrowania.

3. IOD rejestruje wszystkie naruszenia ochrony danych osobowych w rejestrze naruszeń oraz przechowuje uwierzytelnione przez siebie kopie zgłoszeń naruszeń do PUODO.

4. Rejestr naruszeń ochrony danych osobowych prowadzony przez IOD obejmuje następujące informacje:

1) datę i godzinę zgłoszenia faktu naruszenia ochrony danych osobowych;
2) imię i nazwisko osoby zgłaszającej naruszenie;
3) opis lub symptomy naruszenia zabezpieczenia, opis charakteru naruszenia i okoliczności jego wystąpienia, w tym w miarę możliwości wskazanie kategorii i przybliżonej liczby osób, których dane dotyczą, oraz kategorii i przybliżonej liczby wpisów (wykazów) danych osobowych, których dotyczy naruszenie;
4) opis możliwych konsekwencji naruszenia;
5) opis podjętych działań i decyzji, opis środków zastosowanych lub proponowanych przez administratora i podjętych działań naprawczych i zapobiegawczych w celu zaradzenia naruszeniu (usunięcia naruszenia), w tym zminimalizowania jego ewentualnych negatywnych skutków oraz uniknięcia podobnych naruszeń w przyszłości;
6) przebieg wyjaśniania naruszeń, w tym wskazanie, czy informację o wystąpieniu naruszenia przekazywano do osób, których dane są danym naruszeniem objęte.

5. Kopie zgłoszeń naruszeń do PUODO, które stanowią dopełnienie rejestru naruszeń zawierają informacje, o których mowa w pkt. 1-6 – w takiej sytuacji informacji w rejestrze nie dubluje się. Zakres informacyjny rejestru naruszeń może być rozszerzony o dodatkowe informacje, jeżeli IOD lub administrator danych identyfikują taką potrzebę.

6. Rejestr naruszeń ochrony danych osobowych IOD prowadzi w formie elektronicznej i zapewnia jego poufność, integralność oraz dostępność.

7. Zgłoszenia naruszenia ochrony danych osobowych do PUODO dokonuje IOD w imieniu Głównego Inspektora, bez zbędnej zwłoki ale nie później niż w ciągu 72 godzin od jego wykrycia, przekazując w zgłoszeniu co najmniej (jeżeli są dostępne w chwili zgłoszenia) informacje określone w art. 33 ust. 3 RODO lub art. 44 ust. 4 Ustawy – w zależności, którego przetwarzania naruszenie dotyczy.

8. Zgłoszenia IOD dokonuje jednym ze sposobów wskazanych przez UODO. Dokonując zgłoszenia IOD może korzystać z formularzy interaktywnych dostępnych na stronie internetowej UODO lub formularza udostępnionego przez UODO również na stronie internetowej UODO.

9. W przypadku, gdy nie są dostępne wszystkie informacje wymagane w zgłoszeniu naruszenia ochrony danych w chwili jego przekazywania do PUODO, IOD uzupełnia zgłoszenie w miarę możliwości niezwłocznie, po uzyskaniu brakujących informacji dotyczących naruszenia od pracowników zaangażowanych w jego wyjaśnianie i minimalizowanie skutków jego wystąpienia.

10. W przypadku, gdy źródłem informacji o naruszeniu ochrony danych jest osoba lub podmiot zewnętrzny, IOD informuje o naruszeniu Głównego Inspektora, bez zbędnej zwłoki, najpóźniej z chwilą wysyłania zgłoszenia naruszenia do PUODO.

11. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Główny Inspektor bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu. Czynności tej w imieniu Głównego Inspektora dokonuje właściciel informacji, której dotyczy naruszenie, po uprzedniej konsultacji powiadomienia z IOD.

1) Do przypadków, w których poinformowanie jest obowiązkowe należą sytuacje, w których naruszenie prowadzi do dyskryminacji, kradzieży tożsamości, oszustwa, straty finansowej lub uszczerbku na reputacji. Jeżeli naruszenie dotyczy danych osobowych szczególnej kategorii, należy założyć, że jest wysoce prawdopodobne, iż takie naruszenie może prowadzić do wskazanych wyżej szkód. Nie jest konieczne, aby wysokie ryzyko

zmaterializowało się, czyli faktycznie doszło do naruszenia praw lub wolności osoby fizycznej.

2) Obowiązek zawiadomienia należy zrealizować tak szybko, jak pozwalają na to okoliczności danej sprawy. Należy przyjąć, że im poważniejsze jest ryzyko naruszenia praw lub wolności podmiotu danych, tym szybciej powinno nastąpić zawiadomienie.
3) Gdy jest to uzasadnione oraz zgodnie z zaleceniami organów ścigania wysłanie zawiadomienia o naruszeniu do osób fizycznych, na które wywiera ono wpływ może być opóźnione do momentu, w którym takie zawiadomienie nie zaszkodzi takim postępowaniom, zgodnie z art. 45 ust. 6 Ustawy. Jeżeli zawiadomienie o naruszeniu danych osobowych zostało wysłane z opóźnieniem, właściciel informacji ma obowiązek poinformować IOD o powodach tego opóźnienia celem udokumentowania w rejestrze naruszeń.
4) W przypadku, o którym mowa w art. 26 ust. 1 Ustawy zawiadomienie można również ograniczyć lub pominąć (obowiązek poinformowania IOD w celu udokumentowania powodu ograniczenia lub pominięcia zawiadomienia, w rejestrze naruszeń).

12. Zawiadomienie musi zawierać wymagane prawem elementy wskazane poniżej:

1) charakter naruszenia ochrony danych osobowych;
2) imię i nazwisko oraz dane kontaktowe IOD lub innego punktu kontaktowego, od którego można uzyskać więcej informacji;
3) opis możliwych konsekwencji naruszenia ochrony danych osobowych;
4) opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu, w tym w stosownych przypadkach środków w celu zminimalizowania jego ewentualnych negatywnych skutków.

13. Do zawiadomienia stosuje się zasady przejrzystości, prostoty i zrozumiałości informacji.

14. Wybierając środek komunikacji należy pamiętać, że zawiadomienie musi zostać dostarczone adresatowi w możliwie najkrótszym czasie, przy czym wybór środka komunikacji musi uwzględniać informacje teleadresowe o danej osobie, które administrator posiada.

15. Jeżeli właściciel informacji nie jest w stanie zawiadomić danej osoby fizycznej o naruszeniu, ponieważ posiadane dane są niewystarczające do skontaktowania się z tą osobą, w takim szczególnym przypadku właściciel informacji informuje taką osobę tak szybko, jak jest to rozsądnie wykonalne (np. gdy osoba fizyczna skorzysta z przewidzianego

w art. 15 RODO prawa do uzyskania dostępu do swoich danych osobowych i dostarczy dodatkowe informacje wymagane do skontaktowania się z nią).

16. Zawiadomienia właściciel informacji nie wysyła, jeżeli:

1) zastosowane zostały, przed wystąpieniem naruszenia odpowiednie techniczne i organizacyjne środki w celu ochrony danych osobowych, w szczególności środki uniemożliwiające odczyt danych osobom, które nie są uprawnione do dostępu do tych danych;
2) natychmiast po wystąpieniu naruszenia zostały podjęte działania w celu wyeliminowania prawdopodobieństwa powstania wysokiego ryzyka naruszenia praw lub wolności osoby fizycznej;
3) skontaktowanie się z danymi osobami fizycznymi wymagałoby niewspółmiernie dużego wysiłku, z zastrzeżeniem ust. 15.

17. W przypadku, gdy skontaktowanie się z danymi osobami fizycznymi wymagałoby niewspółmiernie dużego wysiłku, Główny Inspektor w porozumieniu z IOD oraz właścicielem informacji wydaje publiczny komunikat lub stosuje podobny środek, aby w równie skuteczny sposób poinformować osoby o naruszeniu dotyczących ich danych osobowych.

18. Do naruszeń danych osobowych, których przetwarzanie zostało powierzone Głównemu Inspektorowi, zastosowanie mają powyższe zasady, ale przede wszystkim wymagania szczegółowo określone w umowach lub porozumieniach z administratorami tych danych osobowych dotyczących danego powierzenia.

Ocena skutków dla ochrony danych

§ 24. 1. Ocenę skutków dla ochrony danych przeprowadza się m.in. w następujących przypadkach:

1) gdy dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych;
2) gdy dany rodzaj operacji przetwarzania znajduje się w wykazie rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych, który jest publikowany przez PUODO.

2. Ponad powyższe, ocena skutków dla ochrony danych powinna być przeprowadzona w każdym przypadku, gdy dotyczy planowanej (nowej) czynności przetwarzania, w tym w szczególności w systemie, jak również:

1) okresowo, nie rzadziej niż raz na rok dla istniejącej czynności przetwarzania, jeżeli dla tej czynności ocena skutków dla ochrony danych osobowych była obowiązkowa;
2) w przypadku planowanej zmiany zabezpieczeń stosowanych do ochrony danych osobowych;
3) w przypadku zmiany celów, zakresu, kontekstu, podstaw przetwarzania, rozszerzenia dotychczasowego katalogu odbiorców danych;
4) w przypadku zaistnienia innych, niż wskazane powyżej, istotnych zmian dotyczących czynności przetwarzania, które mogą wpływać na ochronę danych osobowych;
5) w przypadku wystąpienia naruszenia ochrony danych – co najmniej w obszarze wystąpienia naruszenia.

3. Katalog przypadków określony w ust. 1 i 2 nie jest katalogiem zamkniętym; każdą zmianę, zdarzenie lub inne czynniki zewnętrzne dotyczące ochrony danych osobowych i prowadzonych czynności przetwarzania należy oceniać indywidualnie, czy powodują konieczność przeprowadzenia oceny skutków.

4. Wyniki oceny skutków dla ochrony danych są podstawą do określenia wszystkich niezbędnych, adekwatnych i skutecznych zabezpieczeń, których celem będzie zapewnienie ochrony danych osobowych oraz zagwarantowanie realizacji praw i wolności osób fizycznych w związku prowadzeniem przetwarzania.

5. Ocenę skutków dla ochrony danych przeprowadza się w oparciu o metodykę francuskiego organu nadzorczego pn. „*Ocena wpływu na prywatność*” (*ang. Privacy Impact Assessment*)[9], z uwzględnieniem dokumentu „*WP 248 rev.01 – Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko” do celów rozporządzenia 2016/679.*[10)]”. Do wykonania oceny skutków dla ochrony danych można wykorzystać oprogramowanie PIA lub opracowany na jego podstawie arkusz oceny skutków dla ochrony danych udostępniany zainteresowanym przez IOD lub Pełnomocnika do spraw bezpieczeństwa informacji.

6. W przypadku stosowania innego, niż określone w ust. 5 podejścia do oceny skutków dla ochrony danych, w raporcie z oceny skutków dla ochrony danych należy obowiązkowo opisać zastosowane podejście.

7. Wyniki oceny skutków dla ochrony danych, w szczególności informacje szczegółowo opisujące stosowane zabezpieczenia ochrony danych uznaje się za informacje wrażliwe. Dostęp

[9)] https://www.cnil.fr/en/privacy-impact-assessment-pia
[10)] https://ec.europa.eu/newsroom/article29/items/611236

do dokumentacji oceny skutków dla ochrony danych zawierającej te informacje z uwagi na jej charakter podlega ograniczeniu na zasadach określonych w PBI.

8. Wyniki oceny skutków dla ochrony danych zatwierdza właściciel informacji, który odpowiada za zapewnienie, że zostanie przeprowadzona. Ocenę skutków dla ochrony danych właściciel informacji konsultuje z IOD, którego zadaniem jest udzielanie zaleceń co do tej oceny oraz monitorowanie jej wykonania.

Szczegółowe zabezpieczenia danych osobowych

§ 25. 1. Ogólne organizacyjne, techniczne oraz informatyczne zabezpieczenia danych osobowych stosowane w Inspektoracie oraz ramy i wymagania odnośnie ich stosowania określa PBI oraz załączniki do PBI, w szczególności PODO.

2. Szczegółowe zabezpieczenia danych osobowych określają odrębne polityki bezpieczeństwa systemów oraz inna dokumentacja opisująca sposób zapewnienia ochrony danych osobowych przetwarzanych w Inspektoracie.

3. Dokumentację, o której mowa w ust. 2 uznaje się za zawierającą informacje wrażliwe. Dostęp do tej dokumentacji z uwagi na jej charakter podlega ograniczeniu na zasadach określonych w PBI.

Załącznik nr 1 do PODO

KLAUZULA INFORMACYJNA – ZATRUDNIENIE

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, dalej RODO, informuję, że:

1. Administratorem Państwa danych osobowych jest Główny Inspektor Transportu Drogowego, mający siedzibę w Warszawie (00-807) przy Al. Jerozolimskich 94.
2. Mogą się Państwo z kontaktować z Administratorem w następujący sposób:
   a. listownie na adres siedziby Administratora: 00-807 Warszawa, Al. Jerozolimskie 94;
   b. poprzez ESP: adres skrytki ePUAP: /canard_gitd/skrytka;
   c. e-mailem: info@gitd.gov.pl;
   d. telefonicznie: 22 220 40 00;
   e. faksem: 22 220 48 99.
3. W sprawach dotyczących przetwarzania Państwa danych osobowych przez Administratora, w tym realizacji Państwa praw przez Administratora, mogą się Państwo kontaktować z wyznaczonym przez Administratora inspektorem ochrony danych (IOD) w następujący sposób:
   a. listownie na adres siedziby Administratora: 00-807 Warszawa, Al. Jerozolimskie 94 (z dopiskiem „ochrona danych osobowych”);
   b. poprzez ESP: adres skrytki ePUAP: /canard_gitd/skrytka;
   c. e-mailem: iod@gitd.gov.pl.
4. Podstawą prawną przetwarzania Państwa danych są przepisy prawa, w szczególności przepisy prawa podatkowego, prawa pracy i ubezpieczeń społecznych, w tym również na potrzeby ustalenia Państwa zdolności do pracy – art. 6 ust. 1 lit. c RODO, art. 9 ust. 2 lit. b RODO oraz art. 9 ust. 2 lit. h RODO.
5. Państwa dane będą mogły być również przetwarzane w związku z dochodzeniem / obroną roszczeń (art. 6 ust. 1 lit. f RODO, art. 9 ust. 2 lit. f RODO), jako uzasadniony interes Administratora.
6. Państwa dane osobowe będą przetwarzane w celach:
   a. zawarcia umowy o pracę oraz realizacji stosunku pracy – podstawą prawną przetwarzania danych osobowych są przepisy prawa;
   b. wypełnienia przez Administratora obowiązków nałożonych na niego przez obowiązujące przepisy prawa – podstawą prawną przetwarzania tych danych jest niezbędność do wypełnienia obowiązków prawnych ciążących na Administratorze wynikających z przepisów prawa.
7. Ponadto informujemy, że na podstawie przepisów prawa, w celach zapewnienia bezpieczeństwa pracowników oraz ochrony mienia miejsce pracy jest objęte monitoringiem wizyjnym.
8. Państwa dane nie podlegają zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.
9. Państwa dane osobowe będą udostępnione jedynie podmiotom uprawnionym do tego na podstawie przepisów prawa, bądź podmiotom świadczącym dla Administratora usługi wsparcia w realizacji ustawowych obowiązków. Są to między innymi:
   a. Zakład Ubezpieczeń Społecznych;
   b. Urząd Skarbowy;
   c. podmiot wykonujący usługi wynikające z obowiązkowej profilaktyki zdrowotnej w zakresie medycyny pracy;
   d. podmioty świadczące usługi w zakresie podnoszenia kompetencji zawodowych;
   e. podmioty zapewniające wsparcie dla systemów informatycznych

   w których przetwarzane są dane osobowe.
10. Państwa dane osobowe nie będą przekazywane do państwa trzeciego lub organizacji międzynarodowej.

11. Państwa dane osobowe będą przechowywane do momentu wygaśnięcia obowiązku przechowywania tych danych wynikającego z przepisów prawa, tj. przez cały okres zatrudnienia, a następnie zostaną poddane archiwizacji i będą przechowywane przez okres 50 lat, a od 1 stycznia 2019 r. przez okres 10 lat licząc do końca roku kalendarzowego, w którym stosunek pracy uległ rozwiązaniu lub wygasł.
12. W związku z prowadzonym monitoringiem miejsca pracy, Państwa wizerunek może być nagrywany i przechowywany, nie dłużej jednak niż przez 30 dni od momentu jego zarejestrowania.
13. Przysługuje Państwu prawo dostępu do swoich danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do wniesienia sprzeciwu wobec przetwarzania, a także prawo do przenoszenia danych oraz prawo do złożenia oświadczenia o cofnięciu każdej wyrażonej zgody w każdym czasie. Cofnięcie zgody nie ma wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem.
14. Przysługuje Państwu również prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, adres: Stawki 2, 00-193 Warszawa, telefon: 22 531 03 00.
15. Podanie danych osobowych w zakresie wymaganym Kodeksem Pracy jest obowiązkowe, a w pozostałym zakresie jest dobrowolne. W przypadku niepodania danych, niemożliwe będzie zawarcie umowy o pracę.

……

/data i czytelny podpis osoby potwierdzający zapoznanie się z klauzulą informacyjną/

KLAUZULA INFORMACYJNA – MONITORING SAMOCHODÓW SŁUŻBOWYCH

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, dalej RODO, informuję, że:

1. Administratorem Państwa danych osobowych przetwarzanych w związku z prowadzeniem monitoringu samochodów służbowych w formie lokalizowania w przestrzeni (GPS) jest Główny Inspektor Transportu Drogowego, mający siedzibę w Warszawie (00-807) przy Al. Jerozolimskich 94.
2. Mogą się Państwo z kontaktować z Administratorem w następujący sposób:
    a. listownie na adres siedziby Administratora: 00-807 Warszawa, Al. Jerozolimskie 94;
    b. poprzez ESP: adres skrytki ePUAP: /canard_gitd/skrytka;
    c. e-mailem: info@gitd.gov.pl;
    d. telefonicznie: 22 220 40 00;
    e. faksem: 22 220 48 99.
3. W sprawach dotyczących przetwarzania Państwa danych osobowych przez Administratora, w tym realizacji Państwa praw przez Administratora, mogą się Państwo kontaktować z wyznaczonym przez Administratora inspektorem ochrony danych (IOD) w następujący sposób:
    a. listownie na adres siedziby Administratora: 00-807 Warszawa, Al. Jerozolimskie 94 (z dopiskiem „ochrona danych osobowych”);
    b. poprzez ESP: adres skrytki ePUAP: /canard_gitd/skrytka;
    c. e-mailem: iod@gitd.gov.pl.
4. Będziemy przetwarzać Państwa dane osobowe w celu zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych Państwu samochodów służbowych, oraz samochodów służbowych wykorzystywanych do celów prywatnych, jak również bezpieczeństwa i ochrony Państwa i udostępnionych Państwu samochodów służbowych, także tych wykorzystywanych do celów prywatnych.
5. Zakres przetwarzanych danych obejmuje trasę pojazdu i jego wykorzystanie, np. jakim stylem jazdy porusza się dany kierowca, gdzie się zatrzymuje, gdzie tankuje, gdzie w danej chwili znajduje się monitorowany samochód.
6. Monitoring samochodów służbowych jest prowadzony całodobowo.
7. Podstawę prawną przetwarzania Państwa danych stanowią:
    a. art. 6 ust. 1 lit. c, e i f RODO;
    b. ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych;
    c. ustawa z dnia 26 czerwca 1974 r. Kodeks pracy.
8. Państwa dane osobowe mogą być przekazane wyłącznie podmiotom, które uprawnione są do ich otrzymania przepisami prawa. Ponadto mogą być one ujawnione podmiotom, z którymi Administrator zawarł umowę na świadczenie usług związanych z dostarczeniem i serwisowaniem rozwiązań technicznych i informatycznych wykorzystywanych do prowadzenia monitoringu samochodów służbowych w formie lokalizowania w przestrzeni (GPS).
9. Państwa dane nie będą przekazywane do państwa trzeciego ani organizacji międzynarodowej.
10. Dane pozyskane w związku z prowadzeniem monitoringu samochodów służbowych w formie lokalizowania w przestrzeni (GPS) będą przechowywane przez okres nieprzekraczający 3 miesięcy od dnia ich zarejestrowania, a następnie będą usuwane z systemu w sposób automatyczny.
11. W odniesieniu do danych pozyskanych w związku z prowadzonym monitoringiem samochodów służbowych w formie lokalizowania w przestrzeni (GPS), przysługuje Państwu:
    a. prawo dostępu do jego danych oraz otrzymywania ich kopii,
    b. prawo do ograniczenia przetwarzania,
    c. prawo do usunięcia danych w uzasadnionych przypadkach,

d. prawo do ograniczenia przetwarzania danych, przy czym przepisy odrębne mogą wyłączyć możliwość skorzystania z tego prawa,
e. prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, adres: Stawki 2, 00-193 Warszawa, telefon: 22 531 03 00.

12. Warunkiem wykorzystania samochodu służbowego do celów prywatnych jest wyrażenie przez Państwa zgody na zbieranie i przetwarzanie danych lokalizacyjnych w przestrzeni (GPS) samochodu służbowego objętego monitoringiem, poza godzinami wykonywania przez Państwa zadań służbowych.

……
/data i czytelny podpis osoby potwierdzający zapoznanie się z klauzulą informacyjną/

KLAUZULA INFORMACYJNA – ZAKŁADOWY FUNDUSZ ŚWIADCZEŃ SOCJALNYCH

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, dalej RODO, informuję, że:

1. Administratorem Państwa danych osobowych jest Główny Inspektor Transportu Drogowego, mający siedzibę w Warszawie (00-807) przy Al. Jerozolimskich 94.
2. Mogą się Państwo z kontaktować z Administratorem w następujący sposób:
   a. listownie na adres siedziby Administratora: 00-807 Warszawa, Al. Jerozolimskie 94;
   b. poprzez ESP: adres skrytki ePUAP: /canard_gitd/skrytka;
   c. e-mailem: info@gitd.gov.pl;
   d. telefonicznie: 22 220 40 00;
   e. faksem: 22 220 48 99.
3. W sprawach dotyczących przetwarzania Państwa danych osobowych przez Administratora, w tym realizacji Państwa praw przez Administratora, mogą się Państwo kontaktować z wyznaczonym przez Administratora inspektorem ochrony danych (IOD) w następujący sposób:
   a. listownie na adres siedziby Administratora: 00-807 Warszawa, Al. Jerozolimskie 94 (z dopiskiem „ochrona danych osobowych”);
   b. poprzez ESP: adres skrytki ePUAP: /canard_gitd/skrytka;
   c. e-mailem: iod@gitd.gov.pl.
4. Państwa dane osobowe przetwarzane są w celu realizacji zadań Administratora związanych z działalnością socjalną. Podstawę prawną przetwarzania Państwa danych osobowych stanowi ustawa z dnia 4 marca 1994 r. o zakładowym funduszu świadczeń socjalnych.
5. Państwa dane nie podlegają zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.
6. Państwa dane osobowe mogą być udostępnione jedynie podmiotom uprawnionym do tego na podstawie przepisów prawa.
7. Państwa dane osobowe są przechowywane przez okres nie dłuższy, niż jest to niezbędne w celu przyznania ulgowej usługi i świadczenia oraz dopłaty z funduszu oraz ustalenia ich wysokości, a także przez okres dochodzenia do nich praw lub roszczeń.
8. Przysługuje Państwu prawo do:
   a. dostępu do treści swoich danych osobowych, żądania ich sprostowania lub usunięcia, na zasadach określonych w art. 15-17 RODO;
   b. ograniczenia przetwarzania, w przypadkach określonych w art. 18 RODO;
   c. wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, adres: Stawki 2, 00-193 Warszawa, telefon: 22 531 03 00.
9. Podanie danych osobowych jest dobrowolne, ale jest warunkiem koniecznym do skorzystania ze świadczeń socjalnych finansowanych z zakładowego funduszu świadczeń socjalnych.

……

/data i czytelny podpis osoby potwierdzający zapoznanie się z klauzulą informacyjną/

KLAUZULA INFORMACYJNA – MONITORING WIZYJNY

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, dalej RODO, informuję, że:

1. Administratorem Państwa danych osobowych jest Główny Inspektor Transportu Drogowego, mający siedzibę w Warszawie (00-807) przy Al. Jerozolimskich 94.
2. Mogą się Państwo z kontaktować z Administratorem w następujący sposób:
   a. listownie na adres siedziby Administratora: 00-807 Warszawa, Al. Jerozolimskie 94;
   b. poprzez ESP: adres skrytki ePUAP: /canard_gitd/skrytka;
   c. e-mailem: info@gitd.gov.pl;
   d. telefonicznie: 22 220 40 00;
   e. faksem: 22 220 48 99.
3. W sprawach dotyczących przetwarzania Państwa danych osobowych przez Administratora, w tym realizacji Państwa praw przez Administratora, mogą się Państwo kontaktować z wyznaczonym przez Administratora inspektorem ochrony danych (IOD) w następujący sposób:
   a. listownie na adres siedziby Administratora: 00-807 Warszawa, Al. Jerozolimskie 94 (z dopiskiem „ochrona danych osobowych”);
   b. poprzez ESP: adres skrytki ePUAP: /canard_gitd/skrytka;
   c. e-mailem: iod@gitd.gov.pl.
4. Podstawą prawną przetwarzania Państwa danych jest art. 6 ust. 1 lit. f RODO, tj. przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora.
5. Państwa dane osobowe w postaci wizerunku nagrywane będą w celu zapewnienia bezpieczeństwa pracowników lub ochrony mienia należącego do pracodawcy lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę.
6. Państwa dane osobowe będą udostępnione uprawnionym organom w przypadku wystąpienia lub podejrzenia wystąpienia zdarzenia zagrażającego bezpieczeństwu, życiu i zdrowiu osób, a także niszczeniu i kradzieży mienia zgodnie z przepisami obowiązującego prawa.
7. Dane z monitoringu wizyjnego mogą być również udostępnione osobie trzeciej, która wykaże swój interes prawny, co do otrzymania zapisu.
8. Materiały pozyskane z monitoringu wizyjnego są przechowywane przez okres 30 dni, po upływie którego są niszczone w sposób automatyczny poprzez nadpisanie, w sposób uniemożliwiający ich odtworzenie.
9. W przypadku, gdy dane z monitoringu wizyjnego mogą posłużyć jako materiał dowodowy, mogą być przechowywane przez okres przekraczający 30 dni, tj. okres niezbędny do wyjaśnienia mających miejsce incydentów lub też zakończenia ewentualnie toczących się postępowań.
10. Przysługuje Państwu prawo do:
    a. dostępu do swoich danych osobowych oraz ograniczenia ich przetwarzania;
    b. żądania usunięcia danych osobowych, jeżeli dane osobowe nie są niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
    c. w zakresie udostępnienia danych – do wniesienia sprzeciwu wobec przetwarzania;
    d. wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, adres: Stawki 2, 00-193 Warszawa, telefon: 22 531 03 00.
11. Państwa wizerunek podlega zarejestrowaniu, gdy przebywają Państwo w miejscach instalacji i funkcjonowania kamer monitoringu wizyjnego.

……

/data i czytelny podpis osoby potwierdzający zapoznanie się z klauzulą informacyjną/

KLAUZULA INFORMACYJNA – ZBIERANIE DANYCH BEZPOŚREDNIO OD OSOBY

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, dalej RODO, informuję, że:

1. Administratorem Państwa danych osobowych jest Główny Inspektor Transportu Drogowego, mający siedzibę w Warszawie (00-807) przy Al. Jerozolimskich 94.
2. Mogą się Państwo z kontaktować z Administratorem w następujący sposób:
   a. listownie na adres siedziby Administratora: 00-807 Warszawa, Al. Jerozolimskie 94;
   b. poprzez ESP: adres skrytki ePUAP: /canard_gitd/skrytka;
   c. e-mailem: info@gitd.gov.pl;
   d. telefonicznie: 22 220 40 00;
   e. faksem: 22 220 48 99.
3. W sprawach dotyczących przetwarzania Państwa danych osobowych przez Administratora, w tym realizacji Państwa praw przez Administratora, mogą się Państwo kontaktować z wyznaczonym przez Administratora inspektorem ochrony danych (IOD) w następujący sposób:
   a. listownie na adres siedziby Administratora: 00-807 Warszawa, Al. Jerozolimskie 94 (z dopiskiem „ochrona danych osobowych”);
   b. poprzez ESP: adres skrytki ePUAP: /canard_gitd/skrytka;
   c. e-mailem: iod@gitd.gov.pl.
4. Podstawą prawną przetwarzania Państwa danych osobowych jest:
   a. art. 6 ust 1 lit a RODO, tj. osoba, której dane dotyczą wyraziła zgodę
   b. na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
   c. art. 6 ust 1 lit. b RODO, tj. przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
   d. art. 6 ust. 1 lit. c RODO, tj. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze w związku z ……...
   e. art. 6 ust. 1 lit. e RODO, tj. przetwarzanie jest niezbędne do wykonania zdania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi w związku z ……...
   f. art. 6 ust. 1 lit. f RODO, tj. przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora w związku z ……...
5. Państwa dane osobowe przetwarzane są w celu:
   a. ……...
   b. ……...
   c. ……...
6. Państwa dane osobowe podlegają/nie podlegają zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.
7. Państwa dane osobowe będą udostępnione :
   a. ……...
   b. ……...

   w związku z:
   a. ……...
   b. ……...
8. Państwa dane osobowe będą przechowywane do momentu wygaśnięcia obowiązku przechowywania danych wynikającego z przepisów, tj. przez okres ……

9. Jeżeli przetwarzanie odbywa się na podstawie zgody, przysługuje Państwu prawo do wycofania zgody w dowolnym momencie.
10. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem.
11. Przysługuje Państwu prawo do dostępu do swoich danych osobowych, prawo żądania ich sprostowania oraz ograniczenia ich przetwarzania.
12. Przysługuje Państwu prawo do żądania usunięcia danych osobowych, jeżeli dane osobowe nie są niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane.
13. W zakresie udostępnienia danych przysługuje Państwu prawo do wniesienia sprzeciwu wobec przetwarzania.
14. Przysługuje Państwu prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, adres: Stawki 2, 00-193 Warszawa, telefon: 22 531 03 00.
15. Podanie danych osobowych jest niezbędne do realizacji celu i wynika ze wskazanych przepisów prawa.

……
/data i czytelny podpis osoby potwierdzający zapoznanie się z klauzulą informacyjną/

KLAUZULA INFORMACYJNA ZBIERANIA DANYCH W SPOSÓB INNY NIŻ OD OSOBY, KTÓREJ DANE DOTYCZĄ

Zgodnie z art. 14 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, dalej RODO, informuję, że:

1. Administratorem Państwa danych osobowych jest Główny Inspektor Transportu Drogowego, mający siedzibę w Warszawie (00-807) przy Al. Jerozolimskich 94.
2. Mogą się Państwo z kontaktować z Administratorem w następujący sposób:
   a. listownie na adres siedziby Administratora: 00-807 Warszawa, Al. Jerozolimskie 94;
   b. poprzez ESP: adres skrytki ePUAP: /canard_gitd/skrytka;
   c. e-mailem: info@gitd.gov.pl;
   d. telefonicznie: 22 220 40 00;
   e. faksem: 22 220 48 99.
3. W sprawach dotyczących przetwarzania Państwa danych osobowych przez Administratora, w tym realizacji Państwa praw przez Administratora, mogą się Państwo kontaktować z wyznaczonym przez Administratora inspektorem ochrony danych (IOD) w następujący sposób:
   a. listownie na adres siedziby Administratora: 00-807 Warszawa, Al. Jerozolimskie 94 (z dopiskiem „ochrona danych osobowych”);
   b. poprzez ESP: adres skrytki ePUAP: /canard_gitd/skrytka;
   c. e-mailem: iod@gitd.gov.pl.
4. Podstawą prawną przetwarzania Państwa danych osobowych jest:
   a. art. 6 ust 1 lit a RODO, tj. osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
   b. art. 6 ust 1 lit. b RODO, tj. przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
   c. art. 6 ust. 1 lit. c RODO, tj. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze w związku z ……...
   d. art. 6 ust. 1 lit. e RODO, tj. przetwarzanie jest niezbędne do wykonania zdania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi w związku z ……...
   e. art. 6 ust. 1 lit. f RODO, tj. przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora w związku z ……...
5. Państwa dane osobowe przetwarzane są w celu
   a. ……...
   b. ……...
6. Państwa dane osobowe zostały przekazane przez ……
   a. ……...
   b. ……...
7. Przetwarzanie danych osobowych obejmuje następujące kategorie Państwa danych:
   a. ……...
   b. ……...
8. Państwa dane osobowe nie podlegają zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.
9. Państwa dane osobowe będą udostępnione
   a. ……...
   b. ……...

   w związku z

a. ……...
b. ……...

10. Państwa dane osobowe będą przechowywane do momentu wygaśnięcia obowiązku przechowywania danych wynikającego z przepisów, tj. przez okres ……
11. Jeżeli przetwarzanie odbywa się na podstawie zgody, przysługuje Państwu prawo do wycofania zgody w dowolnym momencie.
12. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem.
13. Przysługuje Państwu prawo do dostępu do swoich danych osobowych, prawo żądania ich sprostowania oraz ograniczenia ich przetwarzania.
14. Przysługuje Państwu prawo do żądania usunięcia danych osobowych, jeżeli dane osobowe nie są niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane.
15. W zakresie udostępnienia danych przysługuje Państwu prawo do wniesienia sprzeciwu wobec przetwarzania.
16. Przysługuje Państwu prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, adres: Stawki 2, 00-193 Warszawa, telefon: 22 531 03 00.
17. Podanie danych osobowych jest niezbędne i wynika z wyżej wskazanych przepisów prawa.

……
/data i czytelny podpis osoby potwierdzający zapoznanie się z klauzulą informacyjną/

KLAUZULA INFORMACYJNA
informacja o przetwarzaniu danych osobowych osób fizycznych – wykonawców w toku postępowania o udzielenie zamówienia publicznego oraz w toku wykonywania umowy

Zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, dalej RODO, informuję, że:

1. Administratorem Państwa danych osobowych przetwarzanych w związku z prowadzeniem postępowania o udzielenie zamówienia publicznego oraz realizacją umowy jest Główny Inspektor Transportu Drogowego.
2. Mogą się Państwo kontaktować z Administratorem w następujący sposób:
    a. listownie na adres: Główny Inspektorat Transportu Drogowego, 00-807 Warszawa, Al. Jerozolimskie 94;
    b. poprzez elektroniczną skrzynkę podawczą: /canard_gitd/skrytka;
    c. poprzez adres e-mail: info@gitd.gov.pl;
    d. telefonicznie: 22 220 04 00;
    e. faksem: 22 220 48 99.
3. Wyznaczyliśmy Inspektora Ochrony Danych, z którym mogą się Państwo kontaktować we wszystkich sprawach dotyczących przetwarzania danych osobowych oraz korzystania z praw związanych z przetwarzaniem danych.
4. Z Inspektorem Ochrony Danych mogą się Państwo kontaktować w następujący sposób:
    a. listownie na adres: Główny Inspektorat Transportu Drogowego, 00-807 Warszawa, Al. Jerozolimskie 94;
    b. poprzez elektroniczną skrzynkę podawczą: /canard_gitd/skrytka;
    c. poprzez adres e-mail: iod@gitd.gov.pl.
5. Państwa dane będą przetwarzane w celu związanym z prowadzonym postępowaniem o udzielenie zamówienia publicznego. Podstawą prawną ich przetwarzania są następujące przepisy prawa:
    a. art. 6 ust. 1 lit. b i c RODO;
    b. Ustawa z dnia 11 września 2019 r. Prawo zamówień publicznych (dalej: PZP);
    c. Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach.
6. W ramach prowadzonego postępowania o udzielenie zamówienia publicznego, będziemy przetwarzać Państwa dane, aby:
    a. przeprowadzić postępowanie o udzielenie zamówienia publicznego pn. „……” (znak sprawy: ……) prowadzone w trybie podstawowym, w tym weryfikacji spełniania warunków udziału w postępowaniu, braku podstaw do wykluczenia z postępowania, potwierdzenia wymogów Zamawiającego dotyczących wykonania przedmiotu zamówienia, spełniania kryteriów oceny ofert. Podstawą prawną przetwarzania danych są nasze prawne obowiązki wynikające z PZP w tym weryfikacja spełnienia warunków udziału w postępowaniu, braku podstaw do wykluczenia, spełnienia kryteriów oceny ofert;
    b. bronić się przed ewentualnymi roszczeniami lub dochodzić ewentualnych roszczeń związanych z postępowaniem o udzielenie zamówienia publicznego – jeżeli powstanie spór. Podstawą prawną przetwarzania danych jest nasz prawnie uzasadniony interes polegający na możliwości obrony przed roszczeniami lub dochodzenia roszczeń;
    c. archiwizować dokumentację postępowania. Podstawą prawną przetwarzania danych są nasze prawne obowiązki wynikające z przepisów o archiwizacji dokumentów oraz przepisów dotyczących zamówień publicznych.
7. Ponadto, w przypadku wyboru Wykonawcy i podpisania umowy, będziemy przetwarzać dane osobowe Wykonawcy, aby:
    a. realizować jej warunki, w tym kontaktować się w bieżących sprawach biznesowych. Podstawą prawną przetwarzania jest zawierana umowa;

b. wypełniać obowiązki związane z rachunkowością i płaceniem podatków, w tym prowadzenie i przechowywanie ksiąg rachunkowych, przechowywanie dowodów księgowych, dokumentacji podatkowej. Podstawą prawną przetwarzania danych są obowiązki prawne wynikające z przepisów o rachunkowości (ustawa o rachunkowości) oraz przepisów podatkowych;
c. bronić się przed ewentualnymi roszczeniami lub dochodzić ewentualnych roszczeń związanych z umową – jeżeli powstanie spór dotyczący umowy. Podstawą prawną przetwarzania danych jest nasz prawnie uzasadniony interes polegający na możliwości obrony przed roszczeniami lub dochodzenia roszczeń;
d. archiwizować dokumentację dotyczącą umowy. Podstawą prawną przetwarzania danych są nasze prawne obowiązki wynikające z przepisów o archiwizacji dokumentów oraz przepisów dotyczących zamówień publicznych.

8. Państwa dane pozyskane w związku z postępowaniem o udzielenie zamówienia publicznego przekazywane będą wszystkim zainteresowanym podmiotom i osobom, gdyż co do zasady postępowanie o udzielenie zamówienia publicznego jest jawne. Państwa dane osobowe mogą być przekazane w szczególności:
   a. osobom lub podmiotom, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 18 oraz art. 74 ust. 1-2 PZP, w tym innym podmiotom biorącym udział w postępowaniu o udzielenie zamówienia publicznego i innym osobom żądającym dostępu do dokumentacji postępowania;
   b. podmiotom, z którymi Zamawiający zawarł lub zawrze umowy na korzystanie z eksploatowanych przez niego systemów informatycznych, w szczególności platformy do obsługi procesu zamówień publicznych. Zakres przekazania danych tym odbiorcom ograniczony jest jednak wyłącznie do możliwości zapoznania się z tymi danymi w związku ze świadczeniem usług określonych w tych umowach. Odbiorców tych obowiązuje klauzula zachowania poufności pozyskanych w takich okolicznościach wszelkich danych, w tym danych osobowych.
9. Będziemy przechowywać Państwa dane osobowe przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia (zgodnie z art. 78 ust. 1 PZP).
10. W przypadku zawarcia umowy, będziemy przechowywać Państwa dane przez cały okres trwania umowy (zgodnie z art. 78 ust. 4 PZP).
11. Przysługują Państwu następujące uprawnienia:
   a. prawo dostępu do danych osobowych Państwa dotyczących; informujemy, że informujemy, że jeżeli odnalezienie Państwa informacji wymagałoby od nas niewspółmiernie dużego wysiłku, możemy od Państwa żądać wskazania dodatkowych informacji mających na celu sprecyzowanie Państwa żądania, w szczególności podania nazwy lub daty postępowania o udzielenie zamówienia publicznego lub konkursu (co wynika z art. 75 PZP);
   b. prawo do żądania sprostowania Państwa danych osobowych; jednakże skorzystanie z tego uprawnienia nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia ani zmianą postanowień umowy ani nie może naruszać integralności protokołu i jego załączników (co wynika z art. 19 ust. 2 i art. 76 PZP);
   c. prawo żądania ograniczenia przetwarzania Państwa danych osobowych, przy czym prawo to przysługuje tylko w określonych okolicznościach; poza tym skorzystanie z tego prawa nie jest możliwe do czasu zakończenia postępowania o udzielenie zamówienia publicznego lub konkursu (co wynika z art. 19 ust. 3 i art. 74 ust. 3 PZP);
   d. prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, adres: Stawki 2, 00-193 Warszawa, telefon: 22 531 03 00.
12. Podanie danych osobowych Wykonawcy w związku udziałem postępowaniem o udzielenie zamówienia publicznego nie jest obowiązkowe, ale jest warunkiem niezbędnym do wzięcia w nim udziału.

KLAUZULA INFORMACYJNA
informacja o przetwarzaniu danych osobowych osób fizycznych, których dane są przekazywane zamawiającemu przez wykonawcę w toku postępowania o udzielenie zamówienia publicznego

Zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, dalej RODO, informuję, że:

1. Administratorem Państwa danych osobowych przetwarzanych w związku z prowadzeniem postępowania o udzielenie zamówienia publicznego oraz realizacją umowy jest Główny Inspektor Transportu Drogowego.
2. Mogą się Państwo kontaktować z Administratorem w następujący sposób:
    a. listownie na adres: Główny Inspektorat Transportu Drogowego, 00-807 Warszawa, Al. Jerozolimskie 94;
    b. poprzez elektroniczną skrzynkę podawczą: /canard_gitd/skrytka;
    c. poprzez adres e-mail: info@gitd.gov.pl;
    d. telefonicznie: 22 220 04 00;
    e. faksem: 22 220 48 99.
3. Wyznaczyliśmy Inspektora Ochrony Danych, z którym mogą się Państwo kontaktować we wszystkich sprawach dotyczących przetwarzania danych osobowych oraz korzystania z praw związanych z przetwarzaniem danych.
4. Z Inspektorem Ochrony Danych mogą się Państwo kontaktować w następujący sposób:
    a. listownie na adres: Główny Inspektorat Transportu Drogowego, 00-807 Warszawa, Al. Jerozolimskie 94;
    b. poprzez elektroniczną skrzynkę podawczą: /canard_gitd/skrytka;
    c. poprzez adres e-mail: iod@gitd.gov.pl.
5. Państwa dane będą przetwarzane w celu w celu związanym z prowadzonym postępowaniem o udzielenie zamówienia publicznego. Podstawą prawną ich przetwarzania są następujące przepisy prawa:
    a. art. 6 ust. 1 lit. c RODO;
    b. Ustawa z dnia 11 września 2019 r. Prawo zamówień publicznych (dalej: PZP);
    c. Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach.
6. W ramach postępowania o udzielenie zamówienia publicznego, będziemy przetwarzać Pani/Pana dane, aby:
    a. przeprowadzić postępowanie o udzielenie zamówienia publicznego pn. „……” (znak sprawy: ……) prowadzone w trybie podstawowym, w tym weryfikacji spełniania warunków udziału w postępowaniu, braku podstaw do wykluczenia z postępowania, potwierdzenia wymogów zamawiającego dotyczących wykonania przedmiotu zamówienia, spełniania kryteriów oceny ofert. Podstawą prawną przetwarzania danych są nasze prawne obowiązki wynikające z PZP, w tym weryfikacja spełnienia warunków udziału w postępowaniu, braku podstaw do wykluczenia, spełnienia kryteriów oceny ofert;
    b. bronić się przed ewentualnymi roszczeniami lub dochodzić ewentualnych roszczeń związanych z postępowaniem o udzielenie zamówienia publicznego – jeżeli powstanie spór. Podstawą prawną przetwarzania danych jest nasz prawnie uzasadniony interes polegający na możliwości obrony przed roszczeniami lub dochodzenia roszczeń;
    c. archiwizować dokumentację postępowania. Podstawą prawną przetwarzania danych są nasze prawne obowiązki wynikające z przepisów o archiwizacji dokumentów oraz przepisów dotyczących zamówień publicznych.
7. Otrzymaliśmy Państwa dane osobowe od wykonawcy biorącego udział w postępowaniu o udzielenie zamówienia publicznego – Państwa pracodawcy, podmiotu, z którym Państwo współpracujecie lub podmiotu, który zwrócił się do Państwa w związku z chęcią wzięcia udziału w postępowaniu.

8. Zakres przekazanych przez wykonawcę danych określa SWZ.
9. Państwa dane pozyskane w związku z postępowaniem o udzielenie zamówienia publicznego przekazywane będą wszystkim zainteresowanym podmiotom i osobom, gdyż co do zasady postępowanie o udzielenie zamówienia publicznego jest jawne. Państwa dane osobowe mogą być przekazane w szczególności:
    a. osobom lub podmiotom, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 18 oraz art. 74 ust. 1-2 PZP, w tym innym podmiotom biorącym udział w postępowaniu o udzielenie zamówienia publicznego i innym osobom żądającym dostępu do dokumentacji postępowania;
    b. podmiotom, z którymi Zamawiający zawarł lub zawrze umowy na korzystanie z eksploatowanych przez niego systemów informatycznych, w szczególności platformy do obsługi procesu zamówień publicznych. Zakres przekazania danych tym odbiorcom ograniczony jest jednak wyłącznie do możliwości zapoznania się z tymi danymi w związku ze świadczeniem usług określonych w tych umowach. Odbiorców tych obowiązuje klauzula zachowania poufności pozyskanych w takich okolicznościach wszelkich danych, w tym danych osobowych.
10. Będziemy przechowywać Państwa dane osobowe przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia (zgodnie z art. 78 ust. 1 PZP).
11. W przypadku zawarcia umowy, będziemy przechowywać Państwa dane przez cały okres trwania umowy (zgodnie z art. 78 ust. 7 PZP).
12. Przysługują Państwu następujące uprawnienia:
    a. prawo dostępu do danych osobowych Państwa dotyczących; informujemy, że jeżeli odnalezienie Państwa informacji wymagałoby od nas niewspółmiernie dużego wysiłku, możemy od Państwa żądać wskazania dodatkowych informacji mających na celu sprecyzowanie Państwa żądania, w szczególności podania nazwy lub daty postępowania o udzielenie zamówienia publicznego lub konkursu (co wynika z art. 75 PZP);
    b. prawo do żądania sprostowania Państwa danych osobowych; jednakże skorzystanie z tego uprawnienia nie może skutkować zmianą wyniku postępowania lub konkursu ani zmianą postanowień umowy, ani nie może naruszać integralności protokołu i jego załączników (co wynika z art. 19 ust. 2 i art. 76 PZP);
    c. prawo żądania ograniczenia przetwarzania Państwa danych osobowych, o ile nie ogranicza przetwarzania danych osobowych prawo to przysługuje tylko w określonych okolicznościach; poza tym skorzystanie z tego prawa nie jest możliwe do czasu zakończenia postępowania o udzielenie zamówienia publicznego lub konkursu (co wynika z art. 19 ust. 3 i art. 74 ust. 3 PZP);
    d. prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, adres: Stawki 2, 00-193 Warszawa, telefon: 22 531 03 00.
13. Podanie przez wykonawcę danych osobowych w związku z udziałem w postępowaniu o udzielenie zamówienia publicznego jest warunkiem niezbędnym do wzięcia w nim udziału.

Załącznik nr 2 do PODO

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.), art. 129a, art. 129g ust. 1-3 i art. 129h ust. 1-4 ustawy z dnia 20 czerwca 1997 r. – Prawo o ruchu drogowym (Dz. U. z ……..), art. 55a ustawy z dnia 6 września 2001 r. o transporcie drogowym (Dz. U. z ……..), art. 54 ustawy z dnia 24 sierpnia 2001 r. – Kodeks postępowania w sprawach o wykroczenia. (Dz. U. z ……..) oraz art. 41 ustawy z dnia 14 grudnia 2019 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z ……..)

upoważniam Panią/Pana*

……

do przetwarzania danych osobowych w ramach pełnionych obowiązków służbowych, wynikających z nawiązania stosunku pracy / umowy cywilnoprawnej (np. umowy zlecenia, o dzieło) / umowy praktyki / stażu* oraz obowiązków zleconych jednorazowo lub na stałe przez przełożonego.
Zakres i rodzaj przetwarzanych danych osobowych wynika z zakresu zadań danego pracownika / umowy cywilnoprawnej (np. umowy zlecenia, o dzieło) / umowy praktyki / stażu*.
Zakres upoważnienia do przetwarzania danych osobowych w systemach informatycznych jest określany przez indywidualnie przyznawane prawa dostępu do każdego z systemów.

☐ Upoważnienie obejmuje także przetwarzanie danych osobowych, o których mowa w art. 9 ust. 1 RODO**.

Jednocześnie upoważniam wyżej wymienioną / wymienionego* do tworzenia dla potrzeb wykonywanej pracy zestawień, ewidencji oraz rejestrów z danymi osobowymi w plikach programów biurowych (np.: MS Word, MS Excel, MS Access) oraz podręcznych archiwach papierowych z zachowaniem pełnej ich ochrony przy zastosowaniu środków technicznych i organizacyjnych wdrożonych w Głównym Inspektoracie Transportu Drogowego.
Upoważnienie wygasa wraz z rozwiązaniem stosunku pracy lub zakończeniem wykonywania prac określonych umową cywilnoprawną / stażu / praktyki*.
Niniejszego upoważnienia udzielono na podstawie upoważnienia z dnia…...……..20.... r. do nadawania w imieniu Głównego Inspektora Transportu Drogowego upoważnień do przetwarzania danych osobowych pracownikom, współpracownikom, stażystom, praktykantom i wolontariuszom Głównego Inspektoratu Transportu Drogowego oraz odbierania od nich oświadczeń o zachowaniu w tajemnicy danych osobowych (znak: BP.0140…….20.... ……).
Zobowiązuje się Panią/Pana* do zachowania w tajemnicy danych objętych niniejszym upoważnieniem i sposobów ich zabezpieczenia.

……
/data, pieczątka i podpis/

* - niepotrzebne skreślić
** - zaznaczyć X tylko wtedy, jeżeli dotyczy

Potwierdzam odbiór upoważnienia

……
/data i podpis/

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH PRZETWARZANYCH W ZWIĄZKU Z ZAKŁADOWYM FUNDUSZEM ŚWIADCZEŃ SOCJALNYCH

Na podstawie art. 6 ust. 1 lit. c i art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.), w związku z § 2 ust. 7, § 11 i § 12 Regulaminu Gospodarowania Zakładowym Funduszem Świadczeń Socjalnych w Głównym Inspektoracie Transportu Drogowego zwanego dalej: „Regulaminem gospodarowania ZFŚS w GITD", stanowiącego załącznik do zarządzenia nr 26/2020 Dyrektora Generalnego Głównego Inspektoratu Transportu Drogowego z dnia 11 maja 2020 r. w sprawie wprowadzenia Regulaminu Gospodarowania Zakładowym Funduszem Świadczeń Socjalnych w Głównym Inspektoracie Transportu Drogowego, zwanego dalej: „zarządzeniem nr 26/2020" oraz § 6 ust. 3 Regulaminu pracy Komisji Socjalnej, stanowiącego załącznik nr 1 do Regulaminu gospodarowania ZFŚS w GITD oraz § 2 zarządzenia nr 13/2018 Dyrektora Generalnego Głównego Inspektoratu Transportu Drogowego z dnia …… r. w sprawie powołania Komisji Socjalnej w Głównym Inspektoracie Transportu Drogowego

upoważniam Panią/Pana*

……

do przetwarzania danych osobowych w ramach realizacji zadań Komisji Socjalnej w Głównym Inspektoracie Transportu Drogowego, zwanej dalej: „Komisją Socjalną GITD", określonych zarządzeniem nr 26 /2020.
Zakres i rodzaj przetwarzanych danych osobowych obejmuje dane określone szczegółowo w § 16 ust. 1, rozdziale 7 oraz załącznikach nr 3 – 8 do Regulaminu ZFŚS w GITD.
Upoważnienie obowiązuje od dnia wejścia w życie zarządzenia nr 26/2020 przez okres powołania na członka Komisji Socjalnej GITD i traci moc z dniem odwołania niniejszego upoważnienia lub w momencie utraty statusu członka Komisji Socjalnej GITD.
Niniejszego upoważnienia udzielono na podstawie upoważnienia z dnia…...……..20.... r. do nadawania w imieniu Głównego Inspektora Transportu Drogowego upoważnień do przetwarzania danych osobowych pracownikom, współpracownikom, stażystom, praktykantom i wolontariuszom Głównego Inspektoratu Transportu Drogowego oraz odbierania od nich oświadczeń o zachowaniu w tajemnicy danych osobowych (znak: BP.0140…….20.... ……).
Zobowiązuje się Panią/Pana* do zachowania w tajemnicy danych objętych niniejszym upoważnieniem i sposobów ich zabezpieczenia.

……
/data, pieczątka i podpis/

* - niepotrzebne skreślić

Potwierdzam odbiór upoważnienia

……
/data i podpis/

Załącznik nr 3 do PODO

OŚWIADCZENIE O ZAPOZNANIU Z ZASADAMI MONITORINGU SŁUŻBOWEJ POCZTY ELEKTRONICZNEJ ORAZ KOMPUTERÓW SŁUŻBOWYCH I SIECI

Na podstawie art. 22^2 § 8, w związku z art. 22^3 ustawy z dnia 26 czerwca 1976 r. – Kodeks pracy informuje się, że:

1. W celu zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego i bezpiecznego użytkowania udostępnionych pracownikowi narzędzi teleinformatycznych, jak również w celu zapewnienia bezpieczeństwa zasobów informacyjnych Inspektoratu oraz zapewnienia zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę, mogą być prowadzone działania polegające na monitorowaniu służbowej poczty elektronicznej pracowników (monitoring służbowej poczty elektronicznej), dostępu do zasobów teleinformatycznych Inspektoratu, sieci komputerowej Inspektoratu, w tym połączeń do sieci publicznej Internet oraz działań użytkowników na komputerach służbowych.
2. Wszelkie działania pracownika na służbowym sprzęcie komputerowym, w tym działania w sieci Internet wykonywane z sieci wewnętrznej Inspektoratu oraz wiadomości znajdujące się w skrzynce służbowej poczty elektronicznej mogą być monitorowane przez pracodawcę lub upoważnionych przez niego pracowników, zgodnie z Regulaminem pracy w Inspektoracie.
3. Postanowień pkt 2 nie stosuje się do korespondencji pracownika oznaczonej w tytule wyrazem „osobiste", „prywatne", „poufne", „personal", „private", „confidential" lub równoznacznym oraz do korespondencji adresowanej do pracownika, której oznaczenie w tytule uprawdopodabnia, że ma ona charakter prywatny; jeżeli pracodawca wszedł w posiadanie treści korespondencji o charakterze prywatnym w wyniku przekonania, że ma do czynienia z korespondencją prowadzoną w celach służbowych, podejmuje dostępne mu środki mające na celu zachowanie tajemnicy tej korespondencji.
4. Monitorowanie służbowej poczty elektronicznej polega na monitorowaniu treści korespondencji e-mailowej wychodzącej i przychodzącej oraz dokonywaniu wglądu do zawartości służbowych skrzynek e-mailowych pracowników, z wyłączeniem korespondencji pracownika oznaczonej w tytule wyrazem „osobiste", „prywatne", „poufne", personal", „private", „confidential" lub równoznacznym oraz do korespondencji adresowanej do pracownika, której oznaczenie w tytule uprawdopodabnia, że ma ona charakter prywatny. Jeżeli pracodawca wszedł w posiadanie treści korespondencji o charakterze prywatnym, w wyniku przekonania, że ma do czynienia z korespondencją prowadzoną w celach służbowych, podejmuje dostępne mu środki mające na celu zachowanie tajemnicy tej korespondencji.
5. Zabrania się pracownikom wykorzystywania prywatnych skrzynek pocztowych do celów służbowych. Do celów służbowych pracownikowi przydzielana jest firmowa skrzynka pocztowa. Wszelka korespondencja służbowa musi odbywać się za pośrednictwem firmowych skrzynek pocztowych.
6. Zabrania się przekierowywania poczty elektronicznej przychodzącej na wszelkie konta zewnętrzne.
7. Korzystanie z firmowej skrzynki poczty elektronicznej, o której mowa w pkt 5, w celach prywatnych, jest dopuszczalne wyłącznie w sytuacjach uzasadnionych okolicznościami, z zastrzeżeniem wyraźnego podania w tytule korespondencji wyrazu „osobiste", „prywatne", „poufne", „personal", „private", „confidential" lub równoznacznego.
8. Monitoring poczty elektronicznej nie może naruszać tajemnicy korespondencji oraz innych dóbr osobistych pracownika.
9. W celu wykonywania uprawnienia, o którym mowa w pkt 1, pracodawca będzie wykorzystywał rozwiązania teleinformatyczne funkcjonujące w Inspektoracie zapewniające ochronę zasobów wewnętrznych Inspektoratu.
10. Dostęp do materiałów pozyskanych z monitoringu posiadają pracodawca oraz pracownicy, którzy są uprawnieni do przetwarzania zawartych tam danych w związku z realizacją przez te osoby zadań służbowych, w szczególności związanych z zapewnieniem bezpieczeństwa.

Potwierdzam zapoznanie i zrozumienie zasad monitoringu poczty elektronicznej, komputerów i sieci

.....
/data i czytelny podpis pracownika/

OŚWIADCZENIE O ZAPOZNANIU Z ZASADAMI MONITORINGU WIZYJNEGO

Na podstawie art. 22(2) § 8, w związku z art. 22(2) § 1 ustawy z dnia 26 czerwca 1976 r. – Kodeks pracy informuje się, że

1. Na terenie Inspektoratu prowadzony jest całodobowy monitoring wizyjny polegający na rejestrowaniu obrazu przez zamontowane kamery.
2. Monitoring został wprowadzony w celu zapewnienia bezpieczeństwa pracowników lub ochrony mienia należącego do pracodawcy lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę.
3. Pomieszczenia objęte monitoringiem wizyjnym określa szczegółowo załącznik do Regulaminu pracy w Inspektoracie, którego znajomość jest obowiązkiem każdego pracownika.
4. Monitoringiem wizyjnym nie są objęte pomieszczenia sanitarne, pomieszczenia socjalne, w tym stołówki, pomieszczenia udostępniane zakładowej organizacji związkowej, z zastrzeżeniem pkt 5.
5. Pracodawca ma prawo w uzasadnionych przypadkach do monitorowania pomieszczeń, o których mowa w pkt 4, o ile zastosuje techniki uniemożliwiające rozpoznanie przebywających w tych pomieszczeniach osób oraz innych pomieszczeń służbowych, w których świadczona jest praca.
6. Monitoring nie może naruszać prawa pracownika do godności oraz innych dóbr osobistych pracownika, a także zasady wolności i niezależności związków zawodowych.
7. Wejścia do pomieszczeń monitorowanych oznaczone są w sposób widoczny i czytelny.
8. Materiały pozyskane z monitoringu wizyjnego są przechowywane przez okres 30 dni, po upływie którego są niszczone w sposób automatyczny poprzez nadpisanie, w sposób uniemożliwiający ich odtworzenie.
9. Jeżeli materiały pozyskane z monitoringu wizyjnego stanowią dowód w postępowaniu prowadzonym na podstawie przepisów prawa lub pracodawca powziął wiadomość, iż mogą one stanowić dowód w postępowaniu, okres przechowywania ulega przedłużeniu do czasu prawomocnego zakończenia postępowania.
10. Monitorowanie prowadzone jest przez pracodawcę i pracowników, którzy są uprawnieni do przetwarzania zawartych tam danych w związku z realizacją przez te osoby zadań służbowych, w szczególności związanych z zapewnieniem bezpieczeństwa.

Potwierdzam zapoznanie i zrozumienie zasad monitoringu wizyjnego

.....
/data i czytelny podpis pracownika/

OŚWIADCZENIE DOTYCZĄCE WYKORZYSTANIA WIZERUNKU ORAZ PRYWATNYCH DANYCH KONTAKTOWYCH

Ja, ……. wyrażam zgodę na*:
/imię i nazwisko, symbol komórki organizacyjnej/

- ☐ wykorzystanie mojego wizerunku udostępnionego w formie zdjęcia twarzy poprzez umieszczenie go w wewnętrznym komputerowym systemie kadrowo – płacowym Głównego Inspektoratu Transportu Drogowego;
- ☐ wykorzystanie mojego wizerunku udostępnionego w formie zdjęcia twarzy poprzez umieszczenie go na legitymacji pracowniczej pracowników Głównego Inspektoratu Transportu Drogowego;
- ☐ wykorzystanie mojego wizerunku udostępnionego w formie zdjęcia twarzy poprzez umieszczenie go w księdze pracowników Głównego Inspektoratu Transportu Drogowego;
- ☐ wykorzystanie mojego prywatnego numeru telefonu komórkowego …… w celu umożliwienia komunikacji pracodawcy ze mną w sprawach związanych ze stosunkiem pracy;
- ☐ wykorzystanie mojego prywatnego adresu e–mail …… w celu umożliwienia pracodawcy komunikacji ze mną w sprawach związanych ze stosunkiem pracy;
- ☐ przetwarzanie dokumentów przekazanych pracodawcy w trakcie trwania stosunku pracy, których pracodawca nie wymagał.

Udzielona przeze mnie zgoda dotyczy:

- ☐ fotografii przedstawiającej mój wizerunek udostępnionej przeze mnie pracodawcy w formie elektronicznej;
- ☐ mojego wizerunku utrwalonego podczas wydarzeń służbowych, w tym konferencji i szkoleń, w których będę uczestniczyć.

Udzielona przeze mnie zgoda obowiązuje w okresie trwania umowy o pracę / umowy cywilnoprawnej (np. umowy zlecenia, o dzieło) / umowy praktyki / stażu** w Głównym Inspektoracie Transportu Drogowego.

Zostałam/em** poinformowana/y**, że podanie danych jest dobrowolne i przysługuje mi prawo dostępu do treści swoich danych osobowych oraz ich poprawiania, żądania usunięcia, sprostowania lub ograniczenia przetwarzania oraz prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, adres: Stawki 2, 00-193 Warszawa, telefon: 22 531 03 00.

* - zaznaczyć udzielane zgody
** - niepotrzebne skreślić

.....
/data i czytelny podpis pracownika/

POUCZENIE:

Zgodnie z art. 7 ust. 3 RODO pracownik ma prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody powinno być przedstawione pracodawcy w formie pisemnej.

OŚWIADCZENIE O ZOBOWIĄZANIU DO ZACHOWANIA POUFNOŚCI W ZWIĄZKU Z DOSTĘPEM DO INFORMACJI

.....
/imię i nazwisko/

.....
/nazwa podmiotu/

Działając w imieniu ……..…... z siedzibą w ……..……., pod adresem ……..……..... NIP ....., REGON .....,

w związku z...……..... niniejszym oświadczam, że zobowiązuję się do zachowania w tajemnicy informacji prawnie chronionych, w tym danych osobowych, oraz innych informacji, które podlegają ochronie zgodnie z postanowieniami obowiązującej Polityki Bezpieczeństwa Informacji Głównego Inspektoratu Transportu Drogowego, do których mam lub będę miał/a* dostęp, a także sposobów zabezpieczenia tych informacji, zarówno w trakcie wykonywania ……., jak i po zakończeniu realizacji tych zadań.
Oświadczam, że bez upoważnienia nie będę wykorzystywał/a* informacji, w tym danych osobowych ze zbiorów prowadzonych przez Głównego Inspektora Transportu Drogowego, jak i zbiorów powierzonych do przetwarzania Głównemu Inspektorowi Transportu Drogowego przez inne podmioty. Powyższe dotyczy również zewnętrznych zbiorów danych osobowych wykorzystywanych w Głównym Inspektoracie Transportu Drogowego.
Zobowiązuję się do zapewnienia ww. informacjom ochrony przed nieuprawnionym ujawnieniem, modyfikacją oraz ich utratą. Jednocześnie zobowiązuję się wykorzystywać ww. informacje wyłącznie w zakresie niezbędnym do ……
i nie wykorzystywać tych informacji w żadnym innym celu.
Mam świadomość, że naruszenia związane z bezpieczeństwem informacji mogą skutkować odpowiedzialnością karną lub dyscyplinarną na zasadach i w trybie przewidzianym w przepisach prawa, w tym w ustawie z dnia 21 listopada 2008 r. o służbie cywilnej, ustawie z dnia 26 czerwca 1974 r. – Kodeks pracy, ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych oraz ustawie z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.
Powyższe zobowiązanie ma charakter bezterminowy.

Potwierdzam zapoznanie i zrozumienie zobowiązania do zachowania poufności

.....
/data i czytelny podpis osoby składającej oświadczenie/

* - niepotrzebne skreślić

OŚWIADCZENIE O ZOBOWIĄZANIU DO ZACHOWANIA POUFNOŚCI W ZWIĄZKU Z UZYSKANIEM ZDALNEGO DOSTĘPU DO ZASOBÓW

.....
/imię i nazwisko/

.....
/nazwa podmiotu/

Działając w imieniu ……..…... z siedzibą w ……..……., pod adresem ……..…….....
NIP ....., REGON .....,

w związku z wykonywaniem zadań i obowiązków wynikających z ……..……..…
wykonywać będę zdalne prace w sieci wewnętrznej Głównego Inspektoratu Transportu Drogowego.
Oświadczam, że zostałam/em* zapoznana/y* z zasadami zdalnego dostępu do sieci wewnętrznej obowiązującymi w Głównym Inspektoracie Transportu Drogowego oraz zasadami bezpieczeństwa …… i zobowiązuję się do ich przestrzegania.
Oświadczam, że zobowiązuję się do zachowania w tajemnicy informacji prawnie chronionych, w tym danych osobowych, oraz innych informacji, które podlegają ochronie zgodnie z postanowieniami obowiązującej Polityki Bezpieczeństwa Informacji Głównego Inspektoratu Transportu Drogowego, do których mam lub będę miał/a* dostęp w związku z wykonywaniem przeze mnie zdalnych prac w sieci wewnętrznej Głównego Inspektoratu Transportu Drogowego, a także sposobów zabezpieczenia tych informacji, zarówno w trakcie wykonywania zadań, jak i po ich zakończeniu.
Oświadczam, że bez upoważnienia nie będę wykorzystywał/a* informacji, w tym danych osobowych ze zbiorów należących do Głównego Inspektora Transportu Drogowego, jak i zbiorów powierzonych do przetwarzania Głównemu Inspektorowi Transportu Drogowego przez inne podmioty.
Powyższe dotyczy również zewnętrznych zbiorów danych osobowych wykorzystywanych w Głównym Inspektoracie Transportu Drogowego.
Zobowiązuję się do zapewnienia ww. informacjom ochrony przed nieuprawnionym ujawnieniem, modyfikacją oraz ich utratą. Jednocześnie zobowiązuję się wykorzystywać ww. informacje wyłącznie w zakresie niezbędnym do ……
i nie wykorzystywać tych informacji w żadnym innym celu.
Mam świadomość, że przedsiębiorca ponosi wszelką i nieograniczoną odpowiedzialność, w tym za wszelkie szkody lub straty faktyczne lub prawne, jakie poniesie Główny Inspektorat Transportu Drogowego w przypadku naruszenia przeze mnie obowiązujących w Głównym Inspektoracie Transportu Drogowego zasad zdalnego dostępu.
Mam świadomość, że naruszenia związane z bezpieczeństwem informacji mogą skutkować odpowiedzialnością karną lub dyscyplinarną na zasadach i w trybie przewidzianym w przepisach prawa, w tym w ustawie z dnia 21 listopada 2008 r. o służbie cywilnej, ustawie z dnia 26 czerwca 1974 r. – Kodeks pracy, ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych oraz ustawie z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.
Jednocześnie oświadczam, że zostałam/em* poinformowany, że wszelkie działania w sieci wewnętrznej Głównego Inspektoratu Transportu Drogowego wykonywane zdalnie podlegają monitorowaniu na podstawie ustawy z dnia 26 czerwca 1976 r. – Kodeks pracy oraz Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.
Powyższe zobowiązanie ma charakter bezterminowy.

Potwierdzam zapoznanie i zrozumienie zobowiązania do zachowania poufności

.....
/data i czytelny podpis osoby składającej oświadczenie/

* - niepotrzebne skreślić

Załącznik nr 4 do PODO

Umowa powierzenia przetwarzania danych osobowych (RODO)

zawarta dnia _____ w _____ pomiędzy:
Głównym Inspektorem Transportu Drogowego, zwanym dalej „Administratorem danych”, reprezentowanym przez ……;
a
……., zwanym dalej „Podmiotem przetwarzającym” reprezentowanym przez ……;
zwanymi dalej łącznie „Stronami” lub odpowiednio „Stroną”.

§ 1. Definicje

Dla potrzeb niniejszej umowy, Administrator danych i Podmiot przetwarzający ustalają następujące znaczenie niżej wymienionych pojęć:

1. Umowa Powierzenia – niniejsza umowa,
2. Umowa Główna – umowa, w związku z którą zawierana jest umowa powierzenia, tj. _____.
3. RODO – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.).

§ 2. Powierzenie przetwarzania danych osobowych

1. Administrator danych powierza Podmiotowi przetwarzającemu w trybie art. 28 RODO dane osobowe do przetwarzania, na zasadach i w celu określonym w Umowie Powierzenia.
2. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z Umową Powierzenia, RODO oraz innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
3. Podmiot przetwarzający oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi powszechnie obowiązujących przepisów prawa.
4. Podmiot przetwarzający może przetwarzać dane osobowe wyłącznie na podstawie udokumentowanych poleceń Administratora, przy czym za takie udokumentowane polecenia uważa się postanowienia Umowy Powierzenia oraz ewentualne inne polecenia przekazywane przez Administratora drogą elektroniczną na adres _____ lub na piśmie.

§ 3. Zakres, charakter i cel przetwarzania danych

1. Podmiot przetwarzający zobowiązuje się do przetwarzania danych osobowych w celu i zakresie niezbędnym do ……..
2. Podmiot przetwarzający zobowiązuje się do przetwarzania danych osobowych następujących kategorii:
   1) ……..,
   2) ……..,
   3) ……...
3. Zakres powierzonych Podmiotowi przetwarzającemu do przetwarzania danych osobowych obejmuje:
   1) ……..,
   2) ……..,
   3) ……...
4. Powierzone przez Administratora danych dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu realizacji Umowy Głównej w zakresie określonym w umowie powierzenia.

§ 4. Obowiązki Podmiotu przetwarzającego

1. Podmiot przetwarzający zobowiązuje się przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzykom związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 RODO.
2. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
3. Podmiot przetwarzający zobowiązuje się prowadzić rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu Administratora danych, o którym mowa w art. 30 ust. 2 RODO i udostępniać go Administratorowi danych na jego żądanie, chyba że Podmiot przetwarzający jest zwolniony z tego obowiązku na podstawie art. 30 ust. 5 RODO.
4. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji Umowy Głównej.
5. Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy, o której mowa w art. 28 ust. 3 pkt b RODO, przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji Umowy Głównej, zarówno w trakcie współpracy / zatrudnienia ich w Podmiocie przetwarzającym, jak i po ustaniu współpracy / zatrudnienia.
6. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem, zwraca Administratorowi danych wszelkie dane osobowe, a następnie usuwa wszelkie ich istniejące kopie chyba, że prawo unii Europejskiej lub prawo krajowe nakazują przechowywanie danych osobowych.
7. W miarę możliwości Podmiot przetwarzający pomaga Administratorowi danych w niezbędnym zakresie wywiązywać się z obowiązków określonych w art. 32-36 RODO.
8. Podmiot przetwarzający zobowiązuje się pomagać Administratorowi poprzez odpowiednie środki techniczne i organizacyjne, w wywiązywaniu się z obowiązku odpowiadania na żądania osób, których dane dotyczą, w zakresie wykonywania ich praw określonych w art. 15-22 RODO. W szczególności Podmiot przetwarzający zobowiązuje się – na żądanie Administratora – do przygotowania i przekazania Administratorowi informacji potrzebnych do spełnienia żądania osoby, której dane dotyczą, w ciągu 3 dni od dnia otrzymania żądania Administratora danych.
9. Podmiot przetwarzający zobowiązuje stosować się do ewentualnych wskazówek lub zaleceń wydanych przez Administratora danych, organ nadzoru lub unijny organ doradczy zajmujący się ochroną danych osobowych, dotyczących przetwarzania danych osobowych, w szczególności w zakresie stosowania RODO.
10. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora danych o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania powierzonych danych osobowych przez Podmiot przetwarzający, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania powierzonych danych osobowych, skierowanych do Podmiotu przetwarzającego, a także o wszelkich kontrolach i inspekcjach dotyczących przetwarzania powierzonych danych osobowych przez Podmiot przetwarzający, w szczególności prowadzonych przez organ nadzorczy.
11. W sytuacji podejrzenia naruszenia ochrony danych osobowych, Podmiot przetwarzający zobowiązuje się do:
    1) przekazania Administratorowi danych, drogą elektroniczną na adres iod@gitd.gov.pl, informacji dotyczących naruszenia ochrony danych osobowych w ciągu 24 godzin od jego wykrycia, w tym informacji, o których mowa w art. 33 ust. 3 RODO;
    2) przeprowadzenia wstępnej oceny skutków naruszenia praw i wolności osób, których dane dotyczą, i przekazania wyników tej oceny do Administratora danych w ciągu 36 godzin od wykrycia zdarzenia stanowiącego naruszenie ochrony danych osobowych;

3) przekazania Administratorowi danych – na jego żądanie – wszystkich informacji niezbędnych do zawiadomienia osoby, której dane dotyczą, zgodnie z art. 34 ust. 3 RODO, w ciągu 48 godzin od wykrycia zdarzenia stanowiącego naruszenie ochrony danych osobowych.

12. Podmiot przetwarzający, jak i podmiot, który przetwarza dane osobowe w oparciu o § 6 Umowy Powierzenia, jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią Umowy Powierzenia, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.

§ 5. Prawo kontroli

1. Administrator danych jest uprawniony do weryfikacji przestrzegania zasad przetwarzania danych osobowych wynikających RODO oraz Umowy Powierzenia przez Podmiot przetwarzający, poprzez prawo żądania udzielenia wszelkich informacji dotyczących powierzonych danych osobowych, a w szczególności do wykazania spełnienia obowiązków określonych w art. 28 RODO.
2. Administrator danych zgodnie z art. 28 ust. 3 lit. h RODO ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia Umowy Powierzenia oraz są zgodne z przepisami prawa.
3. Administrator danych realizować będzie prawo kontroli w godzinach pracy Podmiotu przetwarzającego i z minimum 3-dniowym jego uprzedzeniem.
4. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora danych nie dłuższym, niż 7 dni.

§ 6. Dalsze powierzenie danych do przetwarzania

1. Podmiot przetwarzający może powierzyć dane osobowe objęte Umową Powierzenia do dalszego przetwarzania podwykonawcom jedynie w celu wykonania Umowy Głównej, po uzyskaniu uprzedniej, pisemnej, pod rygorem nieważności, zgody Administratora danych.
2. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne, pod rygorem nieważności, polecenie Administratora danych chyba, że obowiązek taki nakłada na Podmiot przetwarzający prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora danych o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
3. Podmiot przetwarzający dane osobowe w oparciu o niniejszy paragraf winien spełniać te same gwarancje i obowiązki, jakie zostały nałożone na Podmiot przetwarzający w Umowie Powierzenia.
4. Administratorowi danych będą przysługiwały uprawnienia wynikające z umowy podpowierzenia bezpośrednio wobec podwykonawcy (subprocesora). W przypadku wypowiedzenia lub rozwiązania umowy podpowierzenia, Podmiot przetwarzający poinformuje o tym fakcie Administratora danych w terminie 3 dni od wypowiedzenia lub rozwiązania umowy.
5. Jeżeli Podprzetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych osobowych, pełna odpowiedzialność wobec Administratora danych za wypełnienie obowiązków przez Podprzetwarzającego spoczywa na Podmiocie przetwarzającym.

§ 7. Czas obowiązywania umowy

Administrator danych powierza Podmiotowi przetwarzającemu przetwarzanie danych osobowych na okres obowiązywania Umowy Głównej. Umowa Powierzenia wygasa z chwilą wygaśnięcia Umowy Głównej.

§ 8. Rozwiązanie umowy

1. Administrator danych może rozwiązać niniejszą Umowę Powierzenia ze skutkiem natychmiastowym, gdy Podmiot przetwarzający:
    1) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli, nie usunie ich w wyznaczonym terminie;
    2) przetwarza dane osobowe w sposób niezgodny z Umową Powierzenia oraz obowiązującymi przepisami prawa;
    3) powierzył przetwarzanie danych osobowych innemu podmiotowi bez uprzedniej pisemnej zgody Administratora danych.

§ 9 Postanowienia końcowe

1. W sprawach nieuregulowanych zastosowanie będą miały przepisy powszechnie obowiązujące, w tym Kodeks cywilny oraz RODO.
2. Sądem właściwym dla rozpatrzenia sporów wynikających z Umowy Powierzenia będzie sąd właściwy dla Administratora danych.
3. Wszelkie zmiany Umowy Powierzenia wymagają zachowania formy pisemnej pod rygorem nieważności.
4. Strony zgodnie potwierdzają, że Umowa Powierzenia wiąże od dnia ……. r.
5. Umowa została sporządzona w dwóch … jednobrzmiących egzemplarzach, w tym … dla Administratora danych oraz … dla Podmiotu przetwarzającego.

…… ……

Administrator danych **Podmiot przetwarzający**

Umowa powierzenia przetwarzania danych osobowych (Ustawa)

zawarta dnia _____ w _____ pomiędzy:
Głównym Inspektorem Transportu Drogowego, zwanym dalej „Administratorem danych", reprezentowanym przez ……;
a
……., zwanym dalej „Podmiotem przetwarzającym" reprezentowanym przez ……;
zwanymi dalej łącznie „Stronami" lub odpowiednio „Stroną".

§ 1. Definicje

Dla potrzeb niniejszej umowy, Administrator danych i Podmiot przetwarzający ustalają następujące znaczenie niżej wymienionych pojęć:

1. Umowa powierzenia – niniejsza umowa powierzenia przetwarzania danych osobowych,
2. Umowa główna – umowa, w związku z którą zawierana jest umowa powierzenia, tj. …….....,
3. Ustawa – ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125).

§ 2. Powierzenie przetwarzania danych osobowych

1. Administrator danych powierza Podmiotowi przetwarzającemu, w trybie art. 34 ust. 1 Ustawy, dane osobowe do przetwarzania, na zasadach i w celu określonym w niniejszej Umowie powierzenia.
2. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z Umową główną, Umową powierzenia, Ustawą, oraz innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
3. Podmiot przetwarzający oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi powszechnie obowiązujących przepisów prawa.
4. Podmiot przetwarzający może przetwarzać dane osobowe wyłącznie na podstawie udokumentowanych poleceń Administratora danych, przy czym za takie udokumentowane polecenia uważa się postanowienia Umowy głównej, Umowy powierzenia oraz ewentualne inne polecenia przekazywane przez Administratora danych drogą elektroniczną na adres e-mail [……..] lub na piśmie.

§ 3. Zakres, charakter i cel przetwarzania danych

1. Podmiot przetwarzający zobowiązuje się do przetwarzania danych osobowych w celu i zakresie niezbędnym do realizacji postanowień Umowy głównej.
2. W ramach przetwarzania danych osobowych na podstawie Ustawy Podmiot przetwarzający zobowiązuje się, zgodnie z art. 19 Ustawy, do przetwarzania danych osobowych w ramach następujących kategorii danych:
   1) ……..;
   2) ……..;
   3) ……
3. Zakres powierzonych Podmiotowi przetwarzającemu na podstawie art. 34 ust. 1 Ustawy do przetwarzania danych osobowych obejmuje dane:
   1) ……..,
   2) ……..,
   3) ……

4. Powierzone przez Administratora danych dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu realizacji przedmiotu Umowy głównej w zakresie określonym w umowie powierzenia.

§ 4. Obowiązki Podmiotu przetwarzającego

1. Podmiot przetwarzający zobowiązuje się przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzykom związanym z przetwarzaniem danych osobowych, o których mowa w art. 39 Ustawy. Podmiot przetwarzający oświadcza, że:
   1) przed przystąpieniem do przetwarzania danych powierzonych przez Administratora danych wdrożył i utrzymuje przez czas przetwarzania wszelkie środki i zabezpieczenia związane z przetwarzaniem danych, zgodnie z wymaganiami Ustawy;
   2) dysponuje odpowiednimi rozwiązaniami oraz środkami administracyjnymi, technicznymi i organizacyjnymi, gwarantującymi odpowiedni poziom bezpieczeństwa przetwarzanych danych osobowych. Podmiot przetwarzający zapewnia w szczególności bezpieczeństwo organizacyjne, osobowe i techniczne przetwarzanych danych zgodne z przepisami Ustawy;
   3) przygotował stosowną dokumentację wymaganą od podmiotu, któremu powierzono przetwarzanie danych osobowych, zgodnie z obowiązującymi przepisami.
2. W ramach realizacji obowiązku określonego w art. 40 Ustawy, Podmiot przetwarzający przekazuje Administratorowi danych wycofane z eksploatacji, niepodlegające archiwizacji, informatyczne nośniki danych wykorzystywane do przetwarzania danych osobowych. Ze zniszczenia nośników sporządza się protokół, w którym uwzględnia się wskazanie sposobu ich zniszczenia.
3. Podmiot przetwarzający przetwarzając dane osobowe na podstawie Ustawy zobowiązany jest dopuszczać do przetwarzania danych wyłącznie osoby zapewniające bezpieczeństwo przetwarzanych danych osobowych oraz posiadające upoważnienie do przetwarzania danych osobowych w ramach danej kategorii czynności przetwarzania, spełniające wymogi określone w art. 41 ust. 2 i 3 Ustawy. Podmiot przetwarzający prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych na zasadach opisanych w art. 42 Ustawy.
4. Podmiot przetwarzający przetwarzając dane osobowe na podstawie Ustawy zapewnia ewidencjonowanie operacji przetwarzania w sposób i na zasadach opisanych w art. 36 Ustawy. Podmiot przetwarzający udostępni ewidencję na żądanie Administratora danych lub Prezesa Urzędu Ochrony Danych Osobowych.
5. Podmiot przetwarzający zobowiązuje się prowadzić wykaz wszystkich kategorii czynności przetwarzania dokonywanych w imieniu Administratora danych na podstawie przepisów Ustawy, o którym mowa w art. 35 ust. 3 Ustawy na zasadach opisanych w art. 35 ust. 4-6 Ustawy, a także udostępniać go na żądanie Administratora danych lub Prezesa Urzędu Ochrony Danych Osobowych.
6. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji przedmiotu Umowy głównej.
7. Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy, o której mowa w art. 34 ust. 5 pkt 3 Ustawy, przetwarzane dane oraz informacje dotyczące środków technicznych ich zabezpieczenia przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji przedmiotu Umowy głównej, zarówno w trakcie współpracy/zatrudnienia ich przez Podmiot przetwarzający, jak i po ustaniu współpracy/zatrudnienia.
8. Podmiot przetwarzający ponosi wszystkie koszty utrzymania własnych narzędzi wykorzystywanych do przetwarzania danych osobowych powierzonych Umową powierzenia.
9. W miarę możliwości Podmiot przetwarzający pomaga Administratorowi danych w niezbędnym zakresie wywiązywać się z obowiązków zawartych w art. 31-32 Ustawy.

10. Podmiot przetwarzający zobowiązuje się pomagać Administratorowi danych w wywiązywaniu się z obowiązku odpowiadania na żądania osób, których dane dotyczą w zakresie wykonywania ich praw określonych w art. 22-26 Ustawy. W szczególności Podmiot przetwarzający zobowiązuje się – na żądanie Administratora danych – do przygotowania i przekazania Administratorowi danych informacji potrzebnych do spełnienia żądania osoby, której dane dotyczą w ciągu 7 dni roboczych od dnia otrzymania żądania Administratora danych, pod warunkiem, że uzyskanie takich informacji mieści się w zakresie przedmiotowym Umowy głównej oraz informacje takie są dostępne dla Podmiotu przetwarzającego.
11. Podmiot przetwarzający zobowiązuje się stosować do uzasadnionych wskazówek lub zaleceń, wydanych przez Administratora danych, mających oparcie w przepisach prawa lub stanowisku organów administracji publicznej, organów porządku publicznego lub nadzoru w zakresie ochrony danych osobowych, a także bezpośrednio wydanych przez organ nadzoru lub unijny organ doradczy zajmujący się ochroną danych osobowych, dotyczących przetwarzania danych osobowych, w szczególności w zakresie stosowania Ustawy.
12. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora danych o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania powierzonych niniejszą Umową powierzenia danych osobowych przez Podmiot przetwarzający, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania powierzonych niniejsza Umową powierzenia danych osobowych, skierowanej do Podmiotu przetwarzającego, a także o wszelkich kontrolach i inspekcjach dotyczących przetwarzania powierzonych niniejszą Umową powierzenia danych osobowych przez Podmiot przetwarzający, w szczególności prowadzonych przez organ nadzorczy.
13. W sytuacji podejrzenia naruszenia ochrony danych osobowych, Podmiot przetwarzający zobowiązuje się do:
    1) przekazania Administratorowi danych informacji dotyczących naruszenia ochrony danych osobowych w ciągu 48 godzin od jego wykrycia, w tym informacji, o których mowa w art. 44 ust. 4 Ustawy;
    2) pomagania Administratorowi danych w przeprowadzeniu analizy ryzyka naruszenia praw i wolności osób, których dane dotyczą, pod warunkiem, że uzyskanie takich informacji mieści się w zakresie przedmiotowym Umowy głównej oraz informacje takie są dostępne dla Podmiotu przetwarzającego;
    3) przekazania Administratorowi danych – na jego żądanie – wszystkich informacji niezbędnych do zawiadomienia osoby, której dane dotyczą, zgodnie z art. 45 ust. 1 Ustawy, w ciągu 48 godzin od otrzymania żądania.
14. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią Umowy powierzenia, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.
15. Podmiot przetwarzający jest odpowiedzialny za wszelkie szkody poniesione przez Administratora danych w związku z nienależytym wykonaniem Umowy głównej przez Podmiot przetwarzający w zakresie ochrony danych osobowych. Podmiot przetwarzający w szczególności zwolni Administratora danych z roszczeń osób trzecich zgłaszanych Administratorowi danych, odnoszących się do powierzonych Podmiotowi przetwarzającemu danych, w związku z naruszeniem bezpieczeństwa tych danych.
16. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy danych osobowych oraz informacji poufnych, o których powziął wiadomość w związku z wykonywaniem niniejszej Umowy powierzenia. Obowiązek przestrzegania tajemnicy jest bezterminowy i trwa także po ustaniu niniejszej Umowy powierzenia, niezależnie od przyczyn tego ustania. Podmiot przetwarzający zapewni, aby opisane w Umowie powierzenia obowiązki był należycie realizowane również przez osoby lub podmioty, za pomocą których Podmiot przetwarzający wykonuje niniejszą Umowę powierzenia.
17. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem (w każdym przypadku wygaśnięcia, rozwiązania lub odstąpienia od Umowy powierzenia) zwraca Administratorowi danych wszelkie dane osobowe, a następnie usuwa wszelkie ich istniejące kopie. Podmiot przetwarzający

sporządza protokół potwierdzający usunięcie danych osobowych. Ponadto Podmiot przetwarzający, podwykonawcy oraz osoby trzecie uczestniczące w wykonaniu Umowy głównej zobowiązane są zwrócić Administratorowi danych na jego każde żądanie i usunąć z systemów czy wszelkich posiadanych nośników, dokumentację, dane, informacje oraz korespondencję w terminie nie później niż 5 dni roboczych od otrzymania takiego żądania. Usunięcie to powinno być trwałe oraz polegać na uniemożliwieniu osobom trzecim odzyskania danych, informacji, dokumentacji.

§ 5. Prawo kontroli

1. Administrator danych jest uprawniony do weryfikacji przestrzegania zasad przetwarzania danych osobowych wynikających z Ustawy oraz Umowy powierzenia przez Podmiot przetwarzający, poprzez prawo żądania udzielenia wszelkich informacji dotyczących powierzonych danych osobowych, a w szczególności do wykazania spełnienia obowiązków określonych w art. 34 Ustawy.
2. Administrator danych zgodnie z art. 34 ust. 3 pkt 7 Ustawy ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia Umowy powierzenia oraz są zgodne z przepisami prawa.
3. Administrator danych jest uprawniony do kontrolowania przetwarzania przez Podmiot przetwarzający danych w każdym czasie. Podmiot przetwarzający zobowiązuje się umożliwić Administratorowi danych sprawowanie nadzoru nad przetwarzaniem danych, w tym ich usuwaniem, w szczególności poprzez obecność w miejscach, w których proces ten przebiega.
4. Administrator danych realizować będzie prawo kontroli w godzinach pracy Podmiotu przetwarzającego i z minimum 3 dniowym jego pisemnym uprzedzeniem.
5. Podmiot przetwarzający zobowiązuje się do usunięcia potwierdzonych przez Strony w pisemnym protokole uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora danych nie dłuższym niż 7 dni roboczych.

§ 6. Dalsze powierzenie danych do przetwarzania

1. Administrator danych wyraża zgodę na dalsze przetwarzanie danych osobowych powierzonych niniejszą Umową powierzenia na podstawie art. 34 ust. 6 Ustawy przez podwykonawców (Podmioty podprzetwarzające) wyłącznie na podstawie pisemnej umowy, której treść w zakresie celu, kategorii danych, zakresu przetwarzania danych a także obowiązków Podmiotu podprzetwarzającego dane oraz innych warunków, pozostaje zgodna z Umową powierzenia, z zastrzeżeniem ust. 2 poniżej.
2. Warunki dalszego powierzenia danych do przetwarzania na podstawie Ustawy:
    1) Podmiot przetwarzający może powierzyć dane osobowe objęte Umową powierzenia do dalszego przetwarzania podwykonawcom jedynie w celu wykonania Umowy głównej, w oparciu o pisemną umowę, po uzyskaniu uprzedniej, pisemnej, pod rygorem nieważności, zgody Administratora danych.
    2) Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne, pod rygorem nieważności, polecenie Administratora danych chyba, że obowiązek taki nakłada na Podmiot przetwarzający / podprzetwarzający prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający / podprzetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający / podprzetwarzający informuje Administratora danych o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
    3) Podmiot podprzetwarzający dane osobowe winien spełniać te same gwarancje i obowiązki, jakie zostały nałożone na Podmiot przetwarzający w niniejszej Umowie powierzenia.
    4) Administratorowi danych będą przysługiwały uprawnienia wynikające z umowy podpowierzenia bezpośrednio wobec Podmiotu podprzetwarzającego. W przypadku wypowiedzenia lub rozwiązania umowy podpowierzenia, Podmiot przetwarzający poinformuje

o tym fakcie Administratora danych w terminie 3 dni od wypowiedzenia lub rozwiązania umowy.

5) Jeżeli Podmiot podprzetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych osobowych, pełna odpowiedzialność wobec Administratora danych za wypełnienie obowiązków przez Podmiot poodprzetwarzający spoczywa na Podmiocie przetwarzającym.

§ 7. Czas obowiązywania umowy powierzenia

Administrator danych powierza Podmiotowi przetwarzającemu przetwarzanie danych osobowych na okres obowiązywania Umowy Głównej. Umowa Powierzenia wygasa z chwilą wygaśnięcia Umowy Głównej.

§ 8. Rozwiązanie umowy powierzenia

1. Administrator danych może rozwiązać niniejszą Umowę powierzenia ze skutkiem natychmiastowym, gdy Podmiot przetwarzający:
   1) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli, nie usunie ich w wyznaczonym terminie;
   2) przetwarza dane osobowe w sposób niezgodny z Umową powierzenia oraz obowiązującymi przepisami prawa;
   3) powierzył przetwarzanie danych osobowych innemu podmiotowi bez uprzedniej pisemnej zgody Administratora danych.

§ 9. Postanowienia końcowe

1. W sprawach nieuregulowanych zastosowanie będą miały przepisy powszechnie obowiązujące, w tym Kodeks cywilny oraz Ustawa.
2. Sądem właściwym dla rozpatrzenia sporów wynikających z Umowy powierzenia będzie sąd właściwy dla Administratora danych.
3. Wszelkie zmiany Umowy powierzenia wymagają zachowania formy pisemnej pod rygorem nieważności.
4. Umowa powierzenia została sporządzona w trzech jednobrzmiących egzemplarzach, w tym dwa dla Administratora danych oraz jeden dla Podmiotu przetwarzającego.

…… ……

Administrator danych **Podmiot przetwarzający**

Załącznik nr 5 do PODO

Szablon rejestru zgód na przetwarzanie danych osobowych

L.p.	Dane identyfikacyjne osoby, której danych zgoda dotyczy	Dane kontaktowe osoby (jeśli podano)	Dane adresowe osoby (jeśli podano)	Kanal (forma) pozyskania zgody	Czego dotyczy zgoda (zakres danych, proces)	Data udzielenia zgody	Data obowiązywania zgody	Data wycofania zgody	Kanal (forma) wycofania zgody	Powód wycofania zgody (jeśli podano)
1	*Jan Osobowy*	*jan.osobowy@jakas.domena tel. 123-456-789*	*ul. Osobowa 1 00-000 Osobowo*	*Pisemnie*	*Przetwarzanie wizerunku pracownika w systemie kadrowo – płacowym. Przetwarzanie wizerunku pracownika na legitymacji pracowniczej.*	*01.01.2010*	*Okres związania umową o pracę*			
2	*Jan Telefoniczny*	*tel. 987-654-321*	*-*	*Formularz na stronie abc.pl*	*Przetwarzanie prywatnego numeru telefonu w celach związanych ze stosunkiem pracy.*	*01.01.2010*	*Okres związania umową o pracę*	*31.12.2020*	*E-mail*	*-*

Załącznik nr 6 do PODO

Wzór rejestru czynności przetwarzania – administrator

Imię i nazwisko lub nazwa oraz dane kontaktowe administratora: .....

Imię i nazwisko lub nazwa oraz dane kontaktowe inspektora ochrony danych: .....

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
L.p.	Nazwa procesu / czynności przetwarzania	Jednostka organizacyjna	Nazwa współadministratora, przedstawiciela administratora i dane kontaktowe *(jeśli dotyczy)*	Cele przetwarzania	Kategorie osób	Kategorie danych	Planowany termin usunięcia kategorii danych *(jeżeli jest to możliwe)*	Kategorie odbiorców *(innych niż podmiot przetwarzający)*	Nazwa podmiotu przetwarzającego i dane kontakowe *(jeśli dotyczy)*	Nazwa systemu lub oprogramowania wykorzystywanego do przetwarzania	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa *(jeżeli jest to możliwe)*	Podstawa prawna lub / podstawa przetwarzania	Transfer do kraju trzeciego lub org. międzynarodowej			OSOD / AR (jeśli tak, lokalizacja raportu)	Informacje o stosowaniu profilowania – w przypadku, gdy zostało ono zastosowane
													Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu)	Jeśli transfer i art. 49 ust. 1 akapit drugi - dokumentacja odpowiednich zabezpieczeń	Kategorie przekazanń danych osobowych do państwa trzeciego lub organizacji międzynarodowej – w przypadku gdy przekazanie nastąpło		
			Art. 30 ust. 1 pkt a RODO Art. 35 ust. 2 pkt 1 lit. b Ustawy	Art. 30 ust. 1 pkt b RODO Art. 35 ust. 2 pkt 2 Ustawy	Art. 30 ust. 1 pkt c RODO Art. 35 ust. 2 pkt 4 Ustawy	Art. 30 ust. 1 pkt c RODO Art. 35 ust. 2 pkt 4 Ustawy	Art. 30 ust. 1 pkt f RODO Art. 35 ust. 2 pkt 8 Ustawy	Art. 30 ust. 1 pkt d RODO Art. 35 ust. 2 pkt 3 Ustawy	Art. 30 ust. 1 pkt d RODO Art. 35 ust. 2 pkt 1 lit. d Ustawy		Art. 30 ust. 1 pkt g RODO Art. 35 ust. 2 pkt 9 Ustawy	Art. 35 ust. 2 pkt 7 Ustawy	Art. 30 ust. 1 pkt e RODO Art. 35 ust. 2 pkt 3 Ustawy	Art. 30 ust. 1 pkt e RODO Art. 35 ust. 2 pkt 3 Ustawy	Art. 35 ust. 2 pkt 6 Ustawy		Art. 35 ust. 2 pkt 5 Ustawy

*Kolorem czerwonym oznaczono informacje wymagane w rejestrze przez art. 30 ust. 1 RODO lub art. 35. ust 2 Ustawy

Wzór rejestru (wykazu) kategorii czynności przetwarzania – podmiot przetwarzający

Imię i nazwisko lub nazwa oraz dane kontaktowe podmiotu przetwarzającego: ……

Imię i nazwisko lub nazwa oraz dane kontaktowe inspektora ochrony danych podmiotu przetwarzającego: ……

L.p.	Administrator				Kategorie przetwarzań dokonywanych w imieniu administratora	Gdy ma to zastosowanie –przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń	Ogólny opis technicznych i organizacyjnych środków zapewniających ochronę przetwarzanych danych osobowych, o których mowa w art. 39, jeżeli jest to możliwe
	Imię i nazwisko lub nazwa oraz dane kontaktowe administratora	Nazwa i dane kontaktowe przedstawiciela administratora (jeśli dotyczy)	Nazwa i dane kontaktowe podmiotu przetwarzającego (jeśli dotyczy)	Imię i nazwisko lub nazwa oraz dane kontaktowe inspektora ochrony danych administratora (jeśli powołano)			
	Art. 30 ust. 2 lit a RODO Art. 35 ust. 4 pkt 1 Ustawy				Art. 30 ust. 2 lit b RODO Art. 35 ust. 4 pkt 2 Ustawy	Art. 30 ust. 2 lit c RODO Art. 35 ust. 4 pkt 3 Ustawy	Art. 30 ust. 2 lit d RODO Art. 35 ust. 4 pkt 4 Ustawy
1.							
2.							
3.							
4.							
5.							

*Kolorem czerwonym oznaczono informacje wymagane w rejestrze zgodnie z art. 30 ust 2 RODO oraz art. 35 ust 4 Ustawy

Załącznik nr 8 do Polityki Bezpieczeństwa Informacji
Głównego Inspektoratu Transportu Drogowego

Polityka Bezpieczeństwa Relacji z Podmiotami Zewnętrznymi

§ 1. 1. Umowa z podmiotem zewnętrznym, która wiąże się z możliwością dostępu do informacji, powinna regulować zagadnienia ochrony informacji przez ten podmiot oraz jego wszystkich podwykonawców uczestniczących w realizacji umowy.

2. Umowa z podmiotem zewnętrznym powinna w szczególności adresować następujące zagadnienia:

1) wymagania prawne w zakresie świadczenia usługi w związku z ochroną informacji;
2) określenie sposobu dostępu do informacji;
3) określenie sposobu bezpiecznej wymiany informacji;
4) określenie dopuszczalnego celu przetwarzania przekazanych informacji;
5) określenie zasad bezpiecznego korzystania z systemów oraz infrastruktury teleinformatycznej Inspektoratu i dostępu do tej infrastruktury, w tym systemów na niej funkcjonujących, jeżeli wynika to ze specyfiki świadczenia usługi;
6) ochronę poufności przekazanych informacji (z obowiązku zachowania poufności zwolnione są informacje publicznie dostępne oraz informacje, których ujawnienie wymagane jest przepisami prawa);
7) odpowiedzialność za naruszenie bezpieczeństwa informacji;
8) obowiązkowo określać tryb postępowania w przypadku wystąpienia incydentu naruszenia bezpieczeństwa informacji (tryb ten musi uwzględniać co najmniej powiadomienie Inspektoratu o wystąpieniu incydentu z uwzględnieniem wymogów prawnych, m.in. wynikających z przepisów o ochronie danych osobowych oraz cyberbezpieczeństwa);
9) obowiązek zwrotu otrzymanych nośników informacji przed lub w momencie zakończenia obowiązywania umowy, usunięcia danych wytworzonych w związku z realizacją umowy lub otrzymanych od Inspektoratu w tym drogą elektroniczną oraz protokolarnego udokumentowania usunięcia danych;
10) obowiązek informowania o wszelkich zmianach po stronie podmiotu zewnętrznego, mogących wpłynąć na realizację umowy;
11) specyfikację warunków świadczenia usługi;

12) powierzenie przetwarzania danych osobowych – jeżeli umowa z podmiotem zewnętrznym będzie wymagała przetwarzania przez podmiot zewnętrzny danych osobowych, których administratorem (lub podmiotem przetwarzającym) jest Główny Inspektor.

3. Zagadnienia, o których mowa w ust. 2, nie stanową katalogu zamkniętego. Zagadnienia powinny być każdorazowo analizowane i stosowane z uwzględnieniem specyfiki i przedmiotu zawieranej umowy.

4. Umowa, której przedmiot obejmuje prace rozwojowe w zakresie oprogramowania powinna zawierać klauzule umożliwiające egzekwowanie wymagań określonych w PBI.

5. Wymiana informacji wrażliwych i prawnie chronionych z podmiotem zewnętrznym wymaga ich zabezpieczenia.

6. Wymiana informacji poprzez łącza informatyczne niebędące pod kontrolą Inspektoratu wymaga w szczególności:

1) w przypadku wymiany informacji z wykorzystaniem poczty elektronicznej – zapewnienia szyfrowania przesyłanych informacji; dopuszcza się szyfrowanie wyłącznie załączników, o ile treść wiadomości nie zawiera informacji wymagających ochrony;
2) w przypadku połączenia pomiędzy systemami, a systemem informatycznym dostawcy – zapewnienia przesyłania danych w postaci zaszyfrowanej, w szczególności z wykorzystaniem protokołów zapewniających transfer danych zaszyfrowanych lub poprzez przesyłanie zaszyfrowanych plików.

7. Wymiana informacji przy użyciu dokumentów papierowych odbywa się m.in. osobiście, za pośrednictwem poczty międzyresortowej, operatora pocztowego lub poprzez firmy kurierskie.

8. Sposób bezpiecznej wymiany danych może być określony w umowie lub w oddzielnym porozumieniu z podmiotem zewnętrznym.

9. Kierujący komórkami organizacyjnymi korzystającymi z usług podmiotów zewnętrznych są zobowiązani do monitorowania jakości usług świadczonych przez te podmioty z uwzględnieniem wymagań prawnych oraz zdefiniowanych parametrów świadczenia usług.

10. Częstotliwość monitorowania jakości usług i monitorowane parametry są określane indywidualnie, w zależności od charakteru usługi.

11. W przypadku stwierdzenia, iż jakość usługi nie spełnia wymagań określonych w umowie, kierujący komórką organizacyjną powinien podjąć działania w celu wyegzekwowania warunków umowy zawartej z podmiotem zewnętrznym. W przypadku, gdy egzekwowanie warunków świadczenia usługi nie przynosi oczekiwanych rezultatów powinny zostać podjęte, w ramach możliwych do podjęcia

działań prawnych oraz zgodnie z postanowieniami zawartej umowy, działania w celu zakończenia współpracy z podmiotem zewnętrznym.

Załącznik nr 9 do Polityki Bezpieczeństwa Informacji
Głównego Inspektoratu Transportu Drogowego

Przykładowy wzór udokumentowanego wyznaczenia osoby do pełnienia roli ASI / AMS

Warszawa, dnia …… 20 …. r.

Pan/i*
…….
…….
Biuro ……...
/w miejscu/

Wyznaczam Panią / Pana* na Administratora Systemu Informatycznego / Administratora Merytorycznego Systemu*

……..……..
/nazwa systemu informacyjnego / wspierającego/

…….
/pieczątka i podpis lub podpis elektroniczny
właściciela biznesowego systemu informacyjnego /
właściciela systemu wspierającego/

Powierzone obowiązki przyjmuję:

…….
/data i podpis lub podpis elektroniczny pracownika/

*** niepotrzebne skreślić / usunąć**

Załącznik nr 10 do Polityki Bezpieczeństwa Informacji
Głównego Inspektoratu Transportu Drogowego

Polityka Klasyfikacji i Postępowania z Informacjami

Zasady klasyfikacji i postępowania z informacjami

§ 1. 1. Przyjmuje się następującą klasyfikację informacji oraz ich oznaczenie:

1) informacja jawna, w tym udostępniana w trybie dostępu do informacji publicznej – informacje jawne powszechnie dostępne oraz informacje których obowiązek udostępniania wynika z przepisów prawa, w szczególności informacje publiczne w rozumieniu ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej z wyłączeniem informacji, do których dostęp podlega ograniczeniom w niej wskazanym. Informacje udostępniane w szczególności na stronach internetowych Inspektoratu;

2) informacje prawnie chronione – informacje stanowiące dane osobowe podlegające ochronie na mocy przepisów o ochronie danych osobowych oraz informacje przekazane przez przedsiębiorcę, co do których podjął on działania w celu zachowania ich w poufności, w szczególności niepodane do publicznej wiadomości informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą (tajemnica przedsiębiorstwa) oraz informacje chronione na mocy ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (uregulowane odrębnymi przepisami), oraz inne informacje chronione z mocy prawa (np. tajemnica skarbowa). Dokumenty przychodzące do Inspektoratu zawierające informacje sklasyfikowane w szczególności jako „tajemnica przedsiębiorstwa” oraz „tajemnica skarbowa” powinny być oznaczone, np. na pierwszej stronie w przypadku dokumentów papierowych lub w nazwie pliku w przypadku dokumentów elektronicznych odpowiednio klauzulą: „TAJEMNICA PRZEDSIĘBIORSTWA”. Dokumenty oznaczone klauzulą „TAJEMNICA SKARBOWA” nie powinny być przesyłane do Inspektoratu faksem oraz poprzez pocztę elektroniczną, w tym poprzez Elektroniczną Platformę Usług Administracji Publicznej – ePUAP. Sposób postępowania z informacjami klasyfikowanymi jako informacje niejawne określają właściwe przepisy oraz regulacje wewnętrzne, m.in. POIN. W tej kategorii informacji uwzględnia się dokumenty publiczne w rozumieniu ustawy z dnia 22 listopada 2018 r. o dokumentach publicznych, przy czym zasady postępowania i ochrony dokumentów publicznych określono szczegółowo we

wskazanej ustawie oraz aktach wykonawczych wydanych na jej podstawie oraz innych wewnętrznych aktach normatywnych, zasady określone w PBI należy stosować uzupełniająco;

3) informacje wrażliwe (tajemnica GITD) – informacje wewnętrzne, wytworzone w Inspektoracie lub na jego rzecz, niewchodzące w zakres informacji zaklasyfikowanych do pozostałych grup. Są to informacje dostępne wewnątrz i przeznaczone do użytku wewnętrznego. Informacje te mogą być udostępniane stronom trzecim (osobom lub podmiotom) na zasadzie „wiedzy uzasadnionej", w szczególności w związku z realizacją usług na podstawie zawartych umów, porozumień. Dokumenty zawierające informacje sklasyfikowane jako „tajemnica GITD", w szczególności te udostępniane stronom trzecim, powinno się oznaczać co najmniej na pierwszej stronie (np.: w nagłówku lub stopce dokumentu) w przypadku dokumentów papierowych, lub w nazwie pliku w przypadku dokumentów elektronicznych, informacją np.: „tajemnica GITD", „do użytku wewnętrznego";
4) informacje wymagające klasyfikacji – informacje, których ewentualne udostępnienie poza Inspektorat wymaga złożenia stosownego wniosku oraz analizy prawnej dotyczącej możliwości udostępnienia informacji wskazanych we wniosku oraz analizy ewentualnych konsekwencji związanych z ich udostępnieniem.

2. Wprowadzenie klasyfikacji informacji, o których mowa w ust. 1, nie powoduje konieczności fizycznego oznaczania informacji już udokumentowanych, dokonuje się w nich jedynie odwzorowania literowo-cyfrowego zgodnie z instrukcją kancelaryjną lub oznaczenia identyfikującego dokument w systemie elektronicznego zarządzania dokumentacją.

§ 2. 1. Przyjmuje się następujące zasady postępowania z informacjami:

1) informacja jawna:
   a. przetwarzanie, przechowywanie, przekazywanie – w sposób gwarantujący zachowanie integralności i dostępności informacji,
   b. zmiana klasyfikacji i udostępnianie – na zasadach i w trybie przewidzianym przepisami prawa,
   c. niszczenie – zgodnie z wymogami określonymi w przepisach prawa lub zawartych umowach, instrukcją kancelaryjną oraz niniejszą PBI;
2) informacja prawnie chroniona:
   a. przetwarzanie – w sposób gwarantujący zapewnienie bezpieczeństwa informacji, ze szczególnym uwzględnieniem atrybutów integralności, dostępności i poufności oraz

innych atrybutów bezpieczeństwa, które są wymagane dla danej informacji chronionej na podstawie przepisów prawa,

b. przechowywanie – w sposób gwarantujący zapewnienie bezpieczeństwa informacji,

c. przekazywanie – wyłącznie osobom uprawnionym, w sposób gwarantujący zachowanie integralności i poufności oraz zgodnie z wymaganiami określonymi w przepisach prawa lub zawartych umowach,

d. zmiana klasyfikacji – zgodnie z wymaganiami określonymi w przepisach prawa lub zawartych umowach,

e. udostępnianie – wyłącznie uprawnionym osobom lub podmiotom po uzyskaniu zgody kierującego właściwą komórką organizacyjną lub jego zastępcy,

f. niszczenie – zgodnie z wymogami określonymi w przepisach prawa lub zawartych umowach oraz instrukcją kancelaryjną;

3) informacja wrażliwa:

a. przetwarzanie – w sposób gwarantujący zapewnienie bezpieczeństwa informacji, ze szczególnym uwzględnieniem atrybutów integralności, dostępności i poufności,

b. przechowywanie – w sposób gwarantujący zapewnienie bezpieczeństwa informacji,

c. przekazywanie – wyłącznie osobom uprawnionym (pracownikom, osobom – pracownikom podmiotów, z którymi zawarto umowy), w sposób gwarantujący zachowanie integralności i dostępności informacji oraz zgodnie z wymaganiami określonymi w przepisach prawa lub zawartych umowach,

d. zmiana klasyfikacji – możliwa po podjęciu decyzji przez uprawnione osoby oraz zgodnie z wymaganiami określonymi w przepisach prawa lub zawartych umowach,

e. udostępnianie – wyłącznie po uzyskaniu zgody kierującego właściwą komórką organizacyjną lub jego zastępcy,

f. niszczenie – zgodnie z wymogami określonymi w przepisach prawa lub zawartych umowach oraz instrukcją kancelaryjną;

4) informacja wymagająca klasyfikacji:

a. przetwarzanie – w sposób gwarantujący zachowanie integralności, dostępności i poufności informacji,

b. przechowywanie – w sposób gwarantujący zapewnienie bezpieczeństwa informacji,

c. przekazywanie – możliwe wysyłanie adresatom zewnętrznym po dokonaniu analizy prawnej dotyczącej możliwości udostępnienia informacji oraz analizy ewentualnych konsekwencji z

tym związanych. Przekazywanie wewnątrz na zasadach określonych przez kierującego właściwą komórką organizacyjną lub jego zastępcę,

d. zmiana klasyfikacji – po dokonaniu analizy w tym zakresie,

e. udostępnianie – wyłącznie po uzyskaniu zgody kierującego właściwą komórką organizacyjną lub jego zastępcy,

f. niszczenie – zgodnie z instrukcją kancelaryjną.

3. Klasyfikacja informacji w systemach, jeżeli nie określono inaczej w dokumentacji tych systemów odbywa się w trybie przewidzianym w PBI.

Postępowanie z dokumentami papierowymi

§ 3. 1. Podczas pracy z dokumentami papierowymi wymagane jest zwrócenie szczególnej uwagi na ochronę informacji zawartych w tych dokumentach.

2. Praca z dokumentami odbywa się w pomieszczeniach służbowych, chyba, że charakter wytwarzanego lub przetwarzanego dokumentu wymusza pracę poza tymi pomieszczeniami.

3. Zabronione jest wynoszenie poza Inspektorat dokumentów papierowych bez zgody kierującego komórką organizacyjną lub bezpośredniego przełożonego, chyba, że jest to jednoznacznie związane z wykonywanymi obowiązkami służbowymi i jest niezbędne do wykonania tych obowiązków.

4. Przepis ust. 3 nie dotyczy dokumentów zawierających informacje publicznie dostępne.

5. Podczas pracy z dokumentami należy zwrócić szczególną uwagę na zabezpieczenie przed możliwością zapoznania się z treścią dokumentu przez osoby nieupoważnione.

6. Pracownicy przetwarzający dokumenty papierowe poza pomieszczeniami są zobowiązani do zabezpieczenia tych dokumentów przed ich utratą, w szczególności poprzez bezpośredni nadzór nad dokumentami oraz przechowywanie dokumentów w sposób uniemożliwiający dostęp do nich osobom niepowołanym.

7. Dokumenty papierowe mogą być udostępniane wyłącznie osobom upoważnionym, z racji pełnionych obowiązków służbowych, do zapoznania się z ich treścią.

8. Wytwarzając dokument należy zwrócić szczególną uwagę na poprawność jego treści. W przypadku stwierdzenia błędu w treści dokumentu należy niezwłocznie podjąć działania zapobiegające ewentualnym negatywnym skutkom błędu.

9. Podczas pracy z dokumentami należy zwrócić uwagę na ich zabezpieczenie przed uszkodzeniem lub zniszczeniem na skutek zabrudzenia lub zalania.

10. Drukując dokument należy zapewnić, że wydrukowany dokument nie będzie dostępny dla osoby nieuprawnionej tj. dokument musi być zabrany z drukarki przez osobę uprawnioną niezwłocznie po wydrukowaniu.

11. Kopiowanie lub skanowanie dokumentów odbywa przez pracownika upoważnionego do przetwarzania dokumentu. Po zakończeniu skanowania oryginał, a w przypadku kopiowania również wszystkie kopie dokumentu, muszą być niezwłocznie zabrane z urządzenia.

12. Wszelkie wadliwe wydruki lub kopie muszą być zabrane z urządzenia i zniszczone w przeznaczonych do tego celu niszczarkach dokumentów.

13. W przypadku zacięcia papieru, zadrukowany papier, po jego wyjęciu z urządzenia, podlega zniszczeniu w niszczarce. Papier powinien być wyjęty w sposób uniemożliwiający zapoznanie się przez osoby nieupoważnione z treścią wydruku.

14. Dokumenty papierowe przechowywane są:

1) w zamykanych meblach biurowych lub w innych meblach zapewniających zwiększony poziom ochrony – w przypadku przechowywania dokumentów w pomieszczeniach biurowych,
2) w pomieszczeniach przeznaczonych do przechowywania dokumentacji z zastrzeżeniem ust. 15 i 16.

15. Przechowywanie dokumentów, co do których istnieją prawnie zdefiniowane wymagania tym w zakresie, realizuje się zgodnie z właściwymi przepisami. Obejmuje to m.in. dokumenty publiczne, o których mowa w ustawie z dnia 22 listopada 2018 r. o dokumentach publicznych.

16. Przepis ust. 14 nie dotyczy dokumentów zawierających wyłącznie informacje publicznie dostępne i jawne. Dokumenty zawierające informacje jawne mogą być przechowywane w zamykanych pomieszczeniach biurowych w meblach otwartych oraz nieposiadających zamka lub innego podobnego zabezpieczenia.

17. Zasady grupowania dokumentacji papierowej w miejscach przechowywania reguluje instrukcja kancelaryjna.

18. Zasady przechowywania dokumentacji archiwalnej reguluje instrukcja w sprawie organizacji i zakresu działania archiwum zakładowego.

19. Dokumenty papierowe niepodlegające archiwizacji są niszczone w niszczarkach. Nie dotyczy to dokumentów zawierających wyłącznie informacje przeznaczone do powszechnego udostępniania, chyba że taki dokument nie jest dalej potrzebny, w takiej sytuacji powinien być zniszczony w niszczarce.

20. Zasady brakowania dokumentacji archiwalnej określono w instrukcji w sprawie organizacji i zakresu działania archiwum zakładowego.

21. Przekazanie przez pracownika dokumentacji papierowej w związku z ustaniem stosunku pracy następuje w trybie określonym w obowiązującym regulaminie pracy.

22. Każdy pracownik jest zobowiązany do przestrzegania zasady czystego biurka. Zasada czystego biurka realizowana jest poprzez zapewnienie, że podczas dłuższej nieobecności pracownika na stanowisku pracy dokumenty i informatyczne nośniki danych przechowywane – w miarę możliwości organizacyjno-technicznych – należy przechowywać w odpowiednio zabezpieczonych meblach biurowych lub szafach metalowych, sejfach, itp.

23. Podstawowym narzędziem do niszczenia dokumentów jest niszczarka. Dokumenty przeznaczone do zniszczenia umieszczane są przez pracownika w niszczarce z zachowaniem podstawowych zasad BHP przy obsłudze takiego urządzenia.

24. W sytuacjach wyjątkowych, w szczególności potrzeby zniszczenia dużej ilości dokumentów, kierujący komórką organizacyjną może podjąć decyzję o przekazaniu dokumentów wyspecjalizowanemu podmiotowi zewnętrznemu celem ich zniszczenia. Zniszczenie dokumentacji przez podmiot zewnętrzny odbywa się za zgodą Dyrektora Generalnego. Szczegółowe zasady określają wewnętrzne regulacje, m.in. instrukcja kancelaryjna.

25. Powyższe zasady należy stosować uzupełniająco do zasad i wymagań określonych w ustawie z dnia 22 listopada 2018 r. o dokumentach publicznych oraz aktach wykonawczych wydanych na jej podstawie, w odniesieniu do dokumentów publicznych.

26. Wymagania i zasady dotyczące postępowania z dokumentami i informacjami w postaci elektronicznej określa załącznik nr 4 do PBI.

27. Pracownicy powinni unikać wynoszenia i przechowywania w miejscach wykonywania pracy w formie zdalnej jakiejkolwiek dokumentacji papierowej zawierającej informacje podlegające ochronie prawnej lub wewnętrznej. Pracownik takie dokumenty ma obowiązek zabezpieczyć w sposób nie gorszy, niż ma to miejsce w siedzibie Inspektoratu i przy zastosowaniu co najmniej tożsamych zabezpieczeń fizycznych i organizacyjnych (m.in. zamykane na klucz meble bez dostępu do ich wnętrza (oraz do kluczy) innych osób, nieujawnianie ich treści innym osobom przebywającym w miejscu wykonywania pracy zdalnej. Zidentyfikowany brak stosowania przez pracownika wymaganych i określonych w PBI zabezpieczeń dla dokumentów papierowych zawierających informacje podlegające ochronie prawnej lub wewnętrznej powinien skutkować natychmiastowym odwołaniem pracownika

z pracy zdalnej z obowiązkiem bezpiecznego przetransportowania dokumentów do siedziby Inspektoratu.

28. Pracownik ponosi pełną odpowiedzialność za ujawnienie lub utratę informacji zawartej w dokumentach przechowywanych w miejscu pracy zdalnej.

29. Pracownik lub jego bezpośredni przełożony powinni skonsultować się z IOD w przypadku konieczności korzystania przez pracownika z dokumentacji papierowej wskazanej w ust. 27 w miejscu wykonywania pracy w formie zdalnej w celu poinformowania IOD o sposobie ochrony tych dokumentów (zabezpieczeniach w miejscu pracy zdalnej) przez pracownika w miejscu wykonywania pracy zdalnej.

30. Zabronione jest wynoszenie do miejsc pracy zdalnej i przechowywanie w tych miejscach jakichkolwiek służbowych dokumentów papierowych, które podlegają ochronie i wymagają stosowania zabezpieczeń określonych w ustawie z dnia 22 listopada 2018 r. o dokumentach publicznych oraz aktach wykonawczych wydanych na jej podstawie. Czyn taki stanowi incydent bezpieczeństwa.

Podstawowe zasady ochrony informacji

§ 4. 1. Podstawowe zasady dotyczące ochrony informacji, które należy stosować:

1) zasada wiedzy koniecznej (ograniczonego dostępu do informacji) – pracownicy posiadają dostęp tylko do tych informacji, które są konieczne do realizacji powierzonych im zadań. Zasada ta dotyczy głównie informacji wrażliwych oraz podlegających prawnej ochronie (m.in.: tajemnica przedsiębiorstwa, tajemnica skarbowa, dane osobowe). Zasada ta ma ograniczone znaczenie dla pewnych grup informacji, w szczególności informacji dostępnych publicznie;
2) zasada indywidualnej odpowiedzialności – za utrzymanie odpowiedniego poziomu bezpieczeństwa poszczególnych aktywów lub ich elementów odpowiadają konkretne osoby, w zakresie nałożonych obowiązków i nadanych uprawnień. Zasada ta dotyczy np. wydruków z systemu centralnego wydruku tj. każda osoba odpowiada za sporządzony przez siebie wydruk;
3) zasada niewygody uzasadnionej – bezpieczeństwo co do zasady opiera się na ograniczeniach oraz jest niewygodne. Środki ochrony nie powinny nadmiernie utrudniać realizacji celów i zadań Inspektoratu, z drugiej strony wygoda nie może być czynnikiem, przez który informacje wymagające ochrony będą narażone na wystąpienie zagrożeń, bezpieczeństwo jest w tym przypadku nadrzędne;
4) zasada czystego biurka i czystego ekranu:

a. podczas dłuższej nieobecności pracownika na stanowisku pracy dokumenty i informatyczne nośniki danych należy przechowywać w miarę możliwości organizacyjno-technicznych w odpowiednio zabezpieczonych meblach biurowych lub szafach metalowych, sejfach, przeznaczonych do tego pomieszczeniach,

b. na czas nieobecności pracownika dostęp do komputera jest blokowany, a po zakończeniu pracy komputer jest wyłączany, chyba że dany komputer musi pracować w trybie ciągłym – np.: serwer obsługujący systemy alarmowe, komputery administratorów, serwery do monitoringu. W czasie obecności pracownika monitor powinien być tak ustawiony, aby nie pozwalał na zapoznawanie się z wyświetlanymi treściami przez osoby postronne, nieupoważnione;

5) zasada separacji obowiązków – pojedyncze osoby nie mogą wykonywać krytycznych zadań w całości;

6) zasada dyskrecji (ograniczonego zaufania i odpowiedzialnej konwersacji) – wszelkie informacje służbowe mogą być przekazywane wyłącznie w celu wykonywania zadań w zakresie do tego niezbędnym oraz osobom uprawnionym do pozyskania tych informacji. Zasada ta ma ograniczone znaczenie dla pewnych grup informacji, np. informacji dostępnych publicznie;

7) zasada obecności koniecznej – prawo przebywania w określonych miejscach (istotnych dla bezpieczeństwa informacji) mogą mieć tylko osoby upoważnione. Przebywanie osób nieupoważnionych w tych miejscach jest możliwe wyłącznie w obecności osób upoważnionych. Szczegółowe zasady ochrony fizycznej obiektów i pomieszczeń użytkowanych określają wewnętrzne dokumenty i instrukcje oraz dokumenty, instrukcje i regulaminy udostępniane przez administratora –właściciela budynku, natomiast w odniesieniu do ochrony informacji niejawnych – POIN. Zasady bezpieczeństwa fizycznego określa załącznik nr 3 do PBI;

8) zasada zamykania pomieszczeń – niedopuszczalne jest pozostawienie pod nieobecność pracownika niezabezpieczonego pomieszczenia służbowego, zarówno w godzinach pracy, jak i po jej zakończeniu. Na zakończenie dnia pracy ostatnia wychodząca z pomieszczenia osoba jest zobowiązana zamknąć wszystkie okna i drzwi oraz zabezpieczyć klucze do pomieszczenia. Szczegółowe zasady ochrony fizycznej obiektów i pomieszczeń użytkowanych przez Inspektorat określają wewnętrzne dokumenty i instrukcje oraz dokumenty, instrukcje i regulaminy udostępniane przez administratora – właściciela budynku, natomiast odniesieniu do ochrony informacji niejawnych – POIN. Zasady bezpieczeństwa fizycznego określa załącznik nr 3 do PBI;

9) zasada nadzorowania dokumentów – po godzinach pracy wszystkie dokumenty zawierające informacje podlegające ochronie należy przechowywać w miejscach zabezpieczonych przed dostępem osób nieuprawnionych;
10) zasada stałej gotowości – niedopuszczalne jest tymczasowe wyłączanie mechanizmów zabezpieczających systemy funkcjonujące w Inspektoracie bez zastosowania alternatywnych mechanizmów. Systemy powinny być sprawne i przygotowane na zidentyfikowane zagrożenia;
11) zasada zachowania prywatności kont w systemach – każdy użytkownik zobowiązany jest do pracy w systemach na przypisanych lub udostępnionych mu kontach. Zabronione jest udostępnianie własnych kont osobom trzecim. Poufność ta obejmuje również karty wykorzystywane w systemach kontroli dostępu funkcjonujących w Inspektoracie;
12) zasada poufności informacji uwierzytelniających – każdy użytkownik zobowiązany jest do zachowania poufności udostępnionych mu haseł, kodów dostępu, kodów PIN, w szczególności do systemów;
13) zasada legalnego oprogramowania – na stacjach roboczych zainstalowane jest wyłącznie legalne oprogramowanie. Oprogramowanie powinno posiadać możliwość automatycznej aktualizacji bez dodatkowych działań ze strony użytkownika;
14) zasada zgłaszania incydentów oraz incydentów bezpieczeństwa informacji – każdy użytkownik ma obowiązek niezwłocznie zgłosić wystąpienie lub podejrzenie wystąpienia incydentu mającego lub mogącego mieć wpływ na cyberbezpieczeństwo lub bezpieczeństwo informacji;
15) zasada automatyzacji kopii zapasowych – procesy tworzenia kopii zapasowych powinny być odpowiednio zaplanowane z uwzględnieniem wymogów prawnych i potrzeb, jak również powinny być zautomatyzowane oraz niemożliwe do przerwania;
16) zasada ochrony nośników danych – dane kopiowane na nośniki i wynoszone poza pomieszczenia powinny być odpowiednio zabezpieczone w czasie transportu i przechowywania, co najmniej poprzez szyfrowanie. W szczególności dotyczy to danych prawnie chronionych takich jak tajemnica przedsiębiorstwa, tajemnica skarbowa, dane osobowe oraz innych danych wrażliwych (np. tajemnica GITD);
17) zasada adekwatności zabezpieczeń – używane mechanizmy zabezpieczeń powinny być adekwatne do zagrożeń, podatności, wartości aktywów oraz innych istotnych okoliczności;
18) zasada kompleksowości ochrony – ochrona aktywów systemu przetwarzania informacji powinna opierać się na stosowaniu różnych mechanizmów ochrony, w tym ochrony prawnej, fizycznej, technicznej oraz organizacyjnej;

19) zasada ochrony niezbędnej – minimalny wymagany poziom bezpieczeństwa informacji wynika z obowiązujących przepisów prawa. Zastosowanie wyższych poziomów bezpieczeństwa informacji uzasadniają szczególne potrzeby i wyniki szacowania ryzyka;
20) zasada bezpiecznej współpracy z podmiotami zewnętrznymi – dokumenty regulujące współpracę powinny zawierać stosowne klauzule bezpieczeństwa, w tym o zachowaniu poufności, zasadach postępowania z pozyskaną informacją, niszczenia lub zwrotu dokumentacji po ich wykorzystaniu, gdy wymaga tego przedmiot lub specyfika umowy;
21) zasada doskonalenia – SZBI jest stale monitorowany i dostosowywany do zmieniających się warunków wewnętrznych i zewnętrznych;
22) zasada podwyższonego poziomu ochrony zbiorów informacji – w szczególnie uzasadnionych przypadkach zbiór informacji powinien być bardziej chroniony niż poszczególne informacje, które się na niego składają;
23) zasada czystej tablicy – po zakończonym spotkaniu należy uprzątnąć wszystkie materiały oraz wyczyścić tablice;
24) zasada czystego kosza – dokumenty papierowe, z wyjątkiem materiałów zawierających informacje jawne, muszą być niszczone w sposób uniemożliwiający ich odczytanie. Niedopuszczalne jest wyrzucanie dokumentów zawierających informacje wrażliwe i prawnie chronione, do zwykłego kosza. W celu zniszczenia takich dokumentów należy korzystać z udostępnionych przez Inspektorat niszczarek. Niszczenie nośników elektronicznych należy przeprowadzić zgodnie z zasadami określonymi w PBT lub odrębnej dokumentacji systemu.

Polityka „czystego biurka” oraz „czystego ekranu”

1) Pracownicy zobowiązani są do przechowywania na biurku tylko tych dokumentów i nośników, które są im niezbędne w danym momencie do wykonania bieżących zadań.
2) Po zakończonej pracy pracownik zobowiązany jest odłożyć dokumenty i nośniki zawierające informacje chronione do zamykanej na klucz szafy.
3) W sytuacjach nagłych, związanych m.in. ze stanem zdrowia pracownika lub przedłużającą się nieobecnością, za realizację polityki czystego biurka w jego imieniu odpowiadają solidarnie pracownicy, których stanowiska pracy znajdują się najbliżej, oraz bezpośredni przełożony pracownika.

4) Po zakończonej pracy pracownik powinien pozostawić na biurku jedynie powierzony mu sprzęt komputerowy, telefon oraz materiały biurowe. Na biurku mogą być przechowywane dokumenty jedynie w przypadku, gdy nie zawierają one informacji chronionych.
5) Pracowników obowiązuje zakaz trzymania na biurku wszelkich produktów spożywczych, których posiadanie grozi rozlaniem płynu i uszkodzeniem urządzeń elektronicznych. Należy stosować postanowienia Regulaminu pracy w Inspektoracie.
6) Pracownik zobowiązany jest na bieżąco niszczyć te dokumenty, które przestały mu być potrzebne, jeżeli obowiązek ich przechowywania i archiwizacji nie wynika z odrębnych przepisów. Dokumenty powinny być niszczone w sposób uniemożliwiający odtworzenie zawartych w nich informacji.
7) Konfiguracja komputerów wymusza włączenie wygaszacza ekranu na użytkowanym komputerze po 5 minutach bezczynności użytkownika. W przypadku wznowienia aktywności, powrót do pracy z komputerem jest możliwy jedynie po podaniu hasła (włączenie wygaszacza ekranu powoduje zablokowanie komputera).
8) W przypadku czasowego opuszczenia stanowiska pracy, pracownik jest zobowiązany do każdorazowego blokowania komputera lub wylogowania się z systemu (przyciski Ctrl + Alt + Del → Zablokuj ten komputer lub przyciski lewy logo Windows + L).

Zasada wiedzy koniecznej

1) Każdy pracownik może posiadać dostęp tylko do tych informacji, które są konieczne do realizacji obowiązków służbowych.
2) Każdy pracownik – użytkownik powinien posiadać wiedzę o systemie, do którego ma dostęp, ograniczoną wyłącznie do funkcjonalności, które są konieczne do realizacji obowiązków służbowych.
3) Zapoznanie pracownika – użytkownika z zasadami użytkowania systemu powinno następować przed rozpoczęciem pracy z tym systemem.
4) Zapoznanie pracownika – użytkownika z zasadami użytkowania systemu może następować w dowolnej formie, m.in.: przez szkolenia stacjonarne lub online, e-learning, zapoznanie użytkownika z dokumentacją, samodzielną naukę na środowisku szkoleniowym.
5) AMS lub ASI odpowiadają za udostępnienie pracownikowi – użytkownikowi dokumentacji użytkownika systemu lub przeszkolenie użytkownika z zasad bezpiecznego użytkowania systemu.

Zasada indywidualnej odpowiedzialności

1) Każdy pracownik lub użytkownik odpowiada za bezpieczeństwo powierzonych lub udostępnionych do użytkowania urządzeń, oprogramowania, nośników oraz informacji, które przetwarza.
2) Pracownik lub użytkownik ponosi indywidualną odpowiedzialność za niedopełnienie obowiązków dotyczących ochrony powierzonych lub udostępnionych do użytkowania urządzeń, oprogramowania, nośników, oraz informacji, w szczególności, gdy naruszenie bezpieczeństwa wystąpiło w czasie, gdy pracownik/użytkownik był zalogowany do systemu, w którym wystąpiło naruszenie.
3) Pracownik lub użytkownik ponosi również odpowiedzialność za ujawnienie swoich informacji uwierzytelniających, których poufności ma obowiązek zapewnić.

Zasada niewygody uzasadnionej

1) Zabezpieczenia mają na celu ochronę informacji i mogą powodować w odczuciu użytkownika dyskomfort użytkowania. Konieczność ochrony informacji ma w tym przypadku priorytet, przy czym nie może powodować znaczących utrudnień i opóźnień w realizacji procesów biznesowych, przy zachowaniu spełnienia wymogów prawnych ochrony tej informacji.
2) Zabronione jest obchodzenie zabezpieczeń, ich wyłączanie lub stosowanie wyłącznie niektórych zabezpieczeń w celu podniesienia komfortu pracy. Jakiekolwiek odstępstwa od stosowanych zabezpieczeń muszą być udokumentowane, musi zostać przeprowadzona analiza ryzyka dla tych odstępstw, oraz muszą podlegać zatwierdzeniu.

Zasada obecności koniecznej

1) Przebywanie osób nieuprawnionych w pomieszczeniach serwerowni, węzłów sieci teleinformatycznych, innych wydzielonych ze względu na charakter wykonywanych zadań lub charakter przetwarzanych informacji pomieszczeniach może odbywać się wyłącznie pod nadzorem i w obecności osób do tego uprawnionych.
2) Osoby nieuprawnione przebywając w takich pomieszczeniach nie powinny mieć dostępu do urządzeń oraz możliwości podglądu ekranów, jeżeli nie ma to związku z celem ich przebywania w tych pomieszczeniach (np. prace serwisowe).
3) Za nadzór nad osobami nieuprawnionymi odpowiadają osoby uprawnione.

4) Zalecane jest zapewnienie rozliczalności dostępu osób nieuprawnionych do pomieszczeń poprzez stosowanie elektronicznych systemów kontroli dostępu lub procedur manualnych (np. książka wejść do serwerowni).

Zasada zamykania pomieszczeń

1) Pomieszczenia serwerowni, węzłów sieci teleinformatycznych, inne pomieszczenia wydzielone ze względu na charakter wykonywanych zadań lub charakter przetwarzanych informacji muszą być bezwzględnie zamykane przy ich opuszczaniu. Zabronione jest pozostawianie takich pomieszczeń otwartych i bez nadzoru, gdy w tych pomieszczeniach przebywają osoby nieuprawnione.
2) Powyższa zasada dotyczy również pomieszczeń, w których zlokalizowane są urządzenia wspierające pracę serwerowni, np. elementy systemu klimatyzacji czy UPS.

Zasady nadzorowania dokumentów i ochrony nośników

1) Niniejszą zasadę należy łączyć z zasadą „czystego biurka”.
2) Zabronione jest pozostawianie, bez zabezpieczenia i nadzoru nad nośnikiem informacji, dokumentów i nośników elektronicznych zawierających informacje wrażliwe lub informacje prawnie chronione.
3) Dokumenty i nośniki należy zabezpieczać przed ich utratą lub ujawnieniem zapisanych na nich informacji poprzez chowanie do zamykanych na klucz mebli biurowych lub przeznaczonych do tego celu szaf, sejfów, itp.
4) Dokumenty i nośniki zawierające informacje wrażliwe lub prawnie chronione należy zabezpieczać na czas transportu lub przekazywania poza pomieszczenia Inspektoratu np.: wysyłając pocztą, poprzez stosowanie szyfrowania całych nośników lub zawartych na nich informacji, stosowanie bezpiecznych kopert lub innych środków ochrony.

Zasada stałej gotowości

1) Wszystkie określone i wdrożone zabezpieczenia muszą być cały czas włączone oraz stosowane.
2) Niedopuszczalne jest samodzielne wyłączanie przez pracowników/użytkowników zabezpieczeń elektronicznych lub niestosowanie się do ustanowionych zabezpieczeń proceduralnych.

Zasady zachowania prywatności kont oraz poufności informacji uwierzytelniających

1) Wszelkie informacje uwierzytelniające pracownika/użytkownika (m.in.: karty dostępu, loginy, hasła, kody PIN, wzory zabezpieczające itp.) w systemach kontroli dostępu lub systemach stanowią informację wrażliwą i każdy pracownik/użytkownik jest zobowiązanych je chronić przed ich ujawnieniem innym osobom.
2) Pracownik lub użytkownik odpowiada za ujawnienie informacji uwierzytelniających jego dotyczących.
3) Zabronione są wszelkie formy udostępniania komukolwiek swoich informacji uwierzytelniających.
4) Zabronione jest wykorzystywanie cudzych informacji uwierzytelniających. W sytuacji uzyskania przez pracownika lub użytkownika dostępu do cudzych informacji uwierzytelniających, ma on obowiązek zgłosić incydent bezpieczeństwa.
5) Pracownik/użytkownik, który podejrzewa, że jego informacje uwierzytelniające mogły zostać ujawnione, zostały ujawnione lub wykorzystane przez kogoś innego, ma obowiązek zgłosić incydent bezpieczeństwa.

Zasada legalnego oprogramowania

1) W Inspektoracie może być stosowane wyłącznie legalne oprogramowanie.
2) Jeżeli legalność wykorzystywanego oprogramowania budzi wątpliwości, należy to zgłosić do ASI lub BT.

Zasada podwyższonego poziomu ochrony zbiorów informacji

1) W szczególnie uzasadnionych przypadkach cały zbiór informacji powinien być bardziej chroniony niż poszczególne informacje, które się na niego składają.
2) Ocena wymaganego poziomu ochrony całego zbioru informacji należy do jej właściciela, m.in. poprzez przeprowadzenie analizy ryzyka dla pojedynczych informacji oraz całego ich zbioru.

Zasada czystego kosza

1) Zabronione jest wyrzucanie do kosza wszelkich nośników elektronicznych. Nośniki takie muszą być zniszczone z wykorzystaniem przeznaczonych do tego urządzeń lub przekazane do BT w celu ich zniszczenia.

2) Nośniki optyczne należy niszczyć w przeznaczonych do tego celu niszczarkach dostępnych w przestrzeni ogólnej Inspektoratu – przed umieszczeniem nośnika optycznego w niszczarce należy upewnić się, że jest ona przeznaczona do niszczenia nośników optycznych, aby nie spowodować awarii urządzenia.
3) Inne nośniki danych, jak nośniki przenośne (m. in. dyski przenośne, pamięci USB, karty pamięci), dyski twarde – lub stałe (m. in. HDD, SSD,) należy przekazać do BT w celu ich zniszczenia lub przygotowania do ponownego wykorzystania, jeżeli nośnik się do tego nadaje technicznie.
4) Należy opróżniać zawartość kosza w systemie operacyjnym komputera. Rekomendowanym rozwiązaniem jest stosowanie ustawień automatycznego opróżniania kosza systemowego (np. zgodnie z ustawionym harmonogramem) lub ustawień uniemożliwiających przechowywanie plików w koszu systemowym.

Formalny obowiązek zachowania poufności informacji

1) Obowiązek zachowania poufności informacji przez pracowników należy zapewnić z uwzględnieniem zasad opisanych w PBI.
2) Powyższe dotyczy również praktykantów, stażystów, wolontariuszy oraz każdej innej osoby, która wykonuje w Inspektoracie jakiekolwiek prace i uzyskuje dostęp do systemów i/lub informacji przetwarzanych w jakiejkolwiek postaci.
3) Obowiązek zachowania poufności informacji przez podmioty zewnętrzne należy zapewnić w umowach, porozumieniach lub innych dokumentach regulujących współpracę, z uwzględnieniem zasad opisanych w PBI.

Obowiązek zgłaszania incydentów i naruszeń ochrony danych

1) Wszelkie zdarzenia wpływające na bezpieczeństwo systemów, bezpieczeństwo informacji lub ochronę danych osobowych należy zgłaszać zgodnie z procedurą określoną w PBI.
2) Powyższe dotyczy również sytuacji, w których zdarzenie jeszcze nie wystąpiło, ale jego wystąpienie (uwzględniając prawdopodobieństwo oraz łatwość wykorzystania podatności) może wpłynąć na bezpieczeństwo systemów, bezpieczeństwo informacji lub ochronę danych osobowych.
3) Powyższe obowiązki zgłaszania zdarzeń wpływających lub mogących wpłynąć na bezpieczeństwo systemów, bezpieczeństwo informacji lub ochronę danych osobowych należy obowiązkowo uwzględniać w umowach, porozumieniach lub innych dokumentach regulujących

współpracę podmiotami zewnętrznymi, gdzie dochodzi do przetwarzania informacji, w tym w systemach.