Warszawa, dnia 23 stycznia 2020 r.

Poz. 1

ZARZĄDZENIE NR 14
KOMENDANTA GŁÓWNEGO PAŃSTWOWEJ STRAŻY POŻARNEJ

z dnia 17 grudnia 2019 r.

w sprawie ustalenia podziału obowiązków współadministratorów danych Systemu Wspomagania Decyzji Państwowej Straży Pożarnej (SWD PSP) oraz minimalnych wymagań dotyczących realizacji zadań w tym zakresie

Na podstawie art. 14ha ust. 2, 3 oraz 6 ustawy z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej (Dz. U. z 2019 r. poz. 1372, 1518 i 1593), w związku z art. 26 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 (Dz. Urz. UE L 119 z 04.05.2016 r., str. 1, z późn. zm.), zarządzam co następuje:

§ 1. 1. Wprowadzam do stosowania w jednostkach organizacyjnych Państwowej Straży Pożarnej (PSP) „Zakres odpowiedzialności oraz podział zadań współadministratorów Systemu Wspomagania Decyzji Państwowej Straży Pożarnej", stanowiący załącznik nr 1 do zarządzenia.

2. Informacje zawarte w załączniku nr 1 do zarządzenia należy opublikować na stronach podmiotowych Biuletynu Informacji Publicznej wszystkich jednostek organizacyjnych PSP oraz dodatkowo na ich stronach www.

§ 2. 1. Wprowadzam do stosowania w jednostkach organizacyjnych PSP „Minimalne wymagania dotyczące realizacji zadań przez współadministratorów Systemu Wspomagania Decyzji Państwowej Straży Pożarnej", stanowiące załącznik nr 2 do zarządzenia.

2. Współadministratorzy zobowiązani są do wdrożenia wymagań technicznych określonych w załączniku nr 2 do zarządzenia w ciągu 12 miesięcy od daty jego wejścia w życie.

§ 3. 1. Zasady określone w rozdziale IV załącznika nr 1 oraz w zakresie w jakim rozdział ten odsyła do załącznika nr 2 do zarządzenia mają odpowiednie zastosowanie wobec jednostek ochrony przeciwpożarowej, o których mowa w art. 14ha ust. 6 ustawy z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej, które uzyskały dostęp do SWD PSP.

2. Zasady określone w rozdziale IV załącznika nr 1 oraz w zakresie w jakim rozdział ten odsyła do załącznika nr 2 do zarządzenia mogą być również stosowane odpowiednio przez inne jednostki ochrony przeciwpożarowej, o których mowa w art. 15 pkt 1a–8 ustawy z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej, które nie uzyskały dostępu do SWD PSP, a przetwarzają dane na jego potrzeby.

§ 4. Zarządzenie wchodzi w życie z dniem podpisania.

Komendant Główny
Państwowej Straży Pożarnej

bryg. Andrzej Bartkowiak

Załącznik nr 1
do zarządzenia nr 14/2019
z dnia 17 grudnia 2019 roku

Zakres odpowiedzialności oraz podział zadań współadministratorów Systemu Wspomagania Decyzji Państwowej Straży Pożarnej

I. Przepisy ogólne

1. Zarządzenie określa zakresy odpowiedzialności związanej z wypełnianiem obowiązków i zadań współadministratorów danych osobowych oraz ich relacje względem siebie, względem osób, których dane dotyczą, względem innych jednostek ochrony przeciwpożarowej, które uzyskały dostęp do Systemu Wspomagania Decyzji Państwowej Straży Pożarnej oraz względem organu nadzorczego, w zakresie danych osobowych przetwarzanych w SWD PSP, funkcjonującego w jednostkach organizacyjnych Państwowej Straży Pożarnej w oparciu o art. 14g, 14h i 14ha ustawy z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej (Dz. U. z 2019 r. poz. 1372 ze zm.).
2. Ilekroć w dokumencie jest mowa o:
   1) **RODO** – rozumie się przez to – 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) **ustawa o ochronie przeciwpożarowej** – rozumie się przez to ustawę z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej (Dz. U. z 2019 r. poz. 1372 ze zm.);
   3) **ustawa o systemie powiadamiania ratunkowego** – rozumie się przez to ustawę z dnia 22 listopada 2013 r. o systemie powiadamiania ratunkowego (Dz. U. z 2019 r. poz. 1077);
   4) **ustawa prawo geodezyjne i kartograficzne** – rozumie się przez to ustawę z dnia 17 maja 1989 r. - Prawo geodezyjne i kartograficzne (Dz. U. z 2019 r. poz. 725 ze zm.);
   5) **ustawa prawo telekomunikacyjne** – rozumie się przez to ustawę – Prawo telekomunikacyjne (Dz. U. z 2018 r. poz. 1954 ze zm.);
   6) **rozporządzenie ksrg** – rozumie się przez to rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 3 lipca 2017 r. w sprawie szczegółowej organizacji krajowego systemu ratowniczo-gaśniczego (Dz. U. poz. 1319 ze zm.);
   7) **administrator** – rozumie się przez to: Komendanta Głównego Państwowej Straży Pożarnej, komendantów wojewódzkich Państwowej Straży Pożarnej, komendantów powiatowych (miejskich) Państwowej Straży Pożarnej, Rektora - Komendanta Szkoły Głównej Służby Pożarniczej, komendantów szkół Państwowej Straży Pożarnej;

8) **współadministratorzy** – rozumie się przez to: Komendanta Głównego Państwowej Straży Pożarnej, komendantów wojewódzkich Państwowej Straży Pożarnej, komendantów powiatowych (miejskich) Państwowej Straży Pożarnej, Rektora - Komendanta Szkoły Głównej Służby Pożarniczej, komendantów szkół Państwowej Straży Pożarnej;
9) **SWD PSP** – rozumie się przez to System Wspomagania Decyzji Państwowej Straży Pożarnej funkcjonujący w oparciu o art. 14 g i 14 h ustawy o ochronie przeciwpożarowej;
10) **PSP** – rozumie się przez to Państwową Straż Pożarną;
11) **SWP** – rozumie się przez to – System Wymiany Plików – oprogramowanie i sprzęt będący w wyłącznej dyspozycji i administracji Komendy Głównej PSP lub komend wojewódzkich PSP, oparty na mechanizmie chmury danych lub innym mechanizmie zapewniającym rozliczalny i bezpieczny dostęp oraz wymianę plików;
12) **IOD** – rozumie się przez to Inspektora Ochrony Danych właściwego dla danej jednostki PSP, wyznaczonego na podstawie art. 37 RODO;
13) **UODO** – rozumie się przez to Urząd Ochrony Danych Osobowych;
14) **OSP** – rozumie się przez to jednostki Ochotniczych Straży Pożarnych;
15) **CPR** – rozumie się przez to centra powiadamiania ratunkowego, o których mowa w art. 3 ust 2 ustawy o systemie powiadamiania ratunkowego;
16) **KDR** – rozumie się przez to kierującego działaniem ratowniczym, o którym mowa w rozporządzeniu ksrg;
17) **Rejestr czynności przetwarzania** – rozumie się przez to rejestr czynności przetwarzania danych osobowych, o którym mowa w art. 30 RODO;
18) **Dane** – rozumie się przez to dane osobowe, o których mowa w art. 4 pkt 1 RODO.

II. Zasady przetwarzania danych osobowych

1. Współadministratorzy zobowiązują się do administrowania danymi osobowymi przetwarzanymi w SWD PSP w zgodzie z obowiązującymi przepisami prawa, w tym w szczególności z postanowieniami RODO.
2. Współadministratorzy zapewniają bezpieczeństwo przetwarzanych danych osobowych oraz wdrażają odpowiednie środki organizacyjne i techniczne służące ochronie danych osobowych, oraz w razie potrzeby, aktualizują te środki. Środki te będą uwzględniać stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania, a także ryzyko naruszenia praw i wolności osób fizycznych.
3. Dane osobowe muszą być zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami.
4. Dane osobowe w SWD PSP są przetwarzane w celu ochrony życia, zdrowia, mienia lub środowiska przed pożarem, klęską żywiołową lub innym miejscowym zagrożeniem, w zakresie niezbędnym do realizacji zadań wynikających z ustawy o ochronie przeciwpożarowej, uzyskane w związku z prowadzeniem działań

ratowniczych oraz obsługą zgłoszeń alarmowych, o których mowa w art. 2 pkt 2 ustawy o systemie powiadamiania ratunkowego, w tym dane osobowe osoby zgłaszającej oraz osób, których zgłoszenie dotyczy.
5. Zbierane dane osobowe muszą być merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane.
6. Zabronione jest zbieranie wszelkich danych nieistotnych, niemających znaczenia, o większym stopniu szczegółowości niż wynika to z określonego celu.
7. Zabronione jest przetwarzanie danych osobowych, dla których zakres, cel przetwarzania i sposoby przetwarzania nie zostały ustalone przez administratora, z wyjątkiem danych osobowych wynikających wprost z przepisów prawa.
8. Dane mogą być przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.
9. Okres przechowywania danych może zostać wydłużony nawet po osiągnięciu celu przetwarzania, jeżeli przepisy ustaw szczególnych takie postępowanie dopuszczają.
10. Dane osobowe mogą być przetwarzane po wcześniejszej rejestracji procesów z tym związanych w Rejestrze czynności przetwarzania.

III. Relacje zachodzące pomiędzy współadministratorami

Państwowa Straż Pożarna jest formacją składającą się z jednostek administracji publicznej, wzajemnie ze sobą powiązanych, mających możliwość wymiany doświadczeń, wiedzy oraz informacji w zakresie wykonywania ustawowych zadań walki z pożarami, klęskami żywiołowymi i innymi miejscowymi zagrożeniami, celem dążenia do ciągłego oraz zharmonizowanego rozwoju wszystkich swoich podmiotów. W związku z powyższym określony został katalog funkcjonalności SWD PSP, umożliwiający we wszystkich jednostkach organizacyjnych:

1) obsługę przyjęcia zgłoszeń i rejestracji zdarzeń;
2) alarmowanie i powiadamianie sił i środków krajowego systemu ratowniczo-gaśniczego oraz innych podmiotów współpracujących z systemem;
3) dysponowanie sił i środków krajowego systemu ratowniczo-gaśniczego oraz innych podmiotów współpracujących z systemem do działań ratowniczych;
4) nadzorowanie i koordynowanie działań ratowniczych;
5) sporządzanie dokumentacji z prowadzonych działań;
6) wymianę informacji i danych między jednostkami organizacyjnymi Państwowej Straży Pożarnej oraz innymi podmiotami współpracującymi z systemem;
7) prowadzenie szczegółowej ewidencji sił i środków Państwowej Straży Pożarnej, Ochotniczej Straży Pożarnej, Zakładowych Straży Pożarnych i Zakładowych Służb Ratowniczych;
8) prowadzenie ewidencji dostępnych dla Państwowej Straży Pożarnej sił i środków innych zasobów pochodzących z instytucji i organizacji wspierających Państwową Straż Pożarną;
9) współpracę z urządzeniami łączności oraz urządzeniami umożliwiającymi śledzenie pojazdów, nadzór, alarmowanie i powiadamianie sił i środków krajowego systemu

ratowniczo-gaśniczego oraz innych podmiotów współpracujących z systemem, a także sterowanie automatyką przemysłową, wykorzystywaną w jednostkach organizacyjnych Państwowej Straży Pożarnej;

10) generowanie analiz, raportów, zestawień i statystyk;
11) pozyskiwanie danych przestrzennych, udostępnianych za pośrednictwem systemu, o którym mowa w art. 40 ust. 3e ustawy – Prawo geodezyjne i kartograficzne, z Głównego Urzędu Geodezji i Kartografii;
12) korzystanie z usług danych przestrzennych, udostępnionych za pośrednictwem systemu, o którym mowa w art. 40 ust. 3e ustawy – Prawo geodezyjne i kartograficzne, z Głównego Urzędu Geodezji i Kartografii;
13) wymianę informacji z CPR za pośrednictwem interfejsu komunikacyjnego, o którym mowa w art. 13 ust. 2 ustawy o systemie powiadamiania ratunkowego;
14) pozyskiwanie i prezentacja danych dotyczących lokalizacji zakończenia sieci, z którego zostało wykonane połączenie do numeru alarmowego, oraz danych dotyczących abonenta, o których mowa w art. 78 ust. 2 ustawy – Prawo telekomunikacyjne, za pośrednictwem centralnego punktu systemu powiadamiania ratunkowego, o którym mowa w art. 78 ust. 4 pkt 1 ustawy – Prawo telekomunikacyjne, lub przekazanych z CPR;
15) współpracę z innymi systemami teleinformatycznymi za pośrednictwem interfejsów zrealizowanych w architekturze otwartej.

Z uwagi na funkcjonalność, pionową strukturę i budowę SWD PSP, wprowadzony zostaje następujący, opisany w poniższej tabeli, podział odpowiedzialności, obowiązków i zadań współadministratorów związanych z przetwarzaniem danych osobowych w tym systemie. Ponadto wprowadza się ograniczenie w dostępie do danych przetwarzanych w SWD PSP na równorzędnych poziomach struktury organizacyjnej PSP. Oznacza to, że administratorzy na danym szczeblu posiadają dostęp do własnych danych oraz do danych jednostek podległych (nadzorowanych), lecz nie posiadają dostępu do danych jednostek z tego samego szczebla organizacyjnego PSP. Wyjątek stanowią dane przetwarzane przez szkoły pożarnicze, do których mają dostęp również jednostki szczebla powiatowego, na których terenie działania funkcjonuje Szkoła oraz przypadki celowego udostępnienia danych w ramach realizacji zadań. Jednocześnie ustala się, że dokonywany podział zadań i obowiązków nie prowadzi, ani też nie będzie prowadził do pozbawienia realnej kontroli nad przetwarzaniem danych osobowych któregokolwiek ze współadministratorów.

A. Podział odpowiedzialności, obowiązków i zadań

LP	Zadanie	Szczebel organizacyjny PSP			
		Komendant Główny PSP	Administratorzy danych osobowych w Szkołach pożarniczych PSP	Komendanci wojewódzcy PSP	Komendanci powiatowi i miejscy PSP
	Wdrożenie odpowiednich środków technicznych i organizacyjnych, w tym zapewnienie realizacji procedur bezpieczeństwa opisanych w przyjętej polityce ochrony danych*	X – w odniesieniu do przetwarzania we własnej jednostce organizacyjnej	X – w odniesieniu do przetwarzania we własnej jednostce organizacyjnej	X – w odniesieniu do przetwarzania we własnej jednostce organizacyjnej	X – w odniesieniu do przetwarzania we własnej jednostce organizacyjnej
2.	Analiza ryzyka w związku z przetwarzaniem danych w systemie	X – w odniesieniu do całości systemu – w odniesieniu do przetwarzania we własnej jednostce organizacyjnej	X – w odniesieniu do przetwarzania we własnej jednostce organizacyjnej	X – w odniesieniu do przetwarzania we własnej jednostce organizacyjnej	X – w odniesieniu do przetwarzania we własnej jednostce organizacyjnej
3.	Ocena skutków dla ochrony danych osobowych	X – w odniesieniu do całości systemu			
4.	Zapewnienie adekwatności danych do celu	X – na etapie projektowania systemu określa zakres danych przetwarzanych w systemie – dokonuje okresowego przeglądu danych w systemie w odniesieniu do celu i usuwa zbędne dane, które uprzednio wprowadził	X – dokonuje okresowego przeglądu danych w systemie w odniesieniu do celu i usuwa zbędne dane, które uprzednio wprowadził	X – dokonuje okresowego przeglądu danych w systemie w odniesieniu do celu i usuwa zbędne dane, które uprzednio wprowadził	X – dokonuje okresowego przeglądu danych w systemie w odniesieniu do celu i usuwa zbędne dane, które uprzednio wprowadził
5.	Zapewnienie rozliczalności operacji przetwarzania	X – w odniesieniu do przetwarzania we własnej jednostce organizacyjnej	X – w odniesieniu do przetwarzania we własnej jednostce organizacyjnej	X – w odniesieniu do przetwarzania we własnej jednostce organizacyjnej	X – w odniesieniu do przetwarzania we własnej jednostce organizacyjnej
6.	Prowadzenie rejestru czynności przetwarzania	X – w odniesieniu do przetwarzania	X – w odniesieniu do przetwarzania	X – w odniesieniu do przetwarzania	X – w odniesieniu do przetwarzania

		we własnej jednostce organizacyjnej	we własnej jednostce organizacyjnej	we własnej jednostce organizacyjnej	we własnej jednostce organizacyjnej
7.	Powierzenie przetwarzania danych w związku ze zlecaniem obsługi technicznej systemu	X – w odniesieniu do całości systemu			
8.	Udostępnianie danych, które nie jest powierzeniem danych	X – w odniesieniu do przetwarzania we własnej jednostce organizacyjnej	X – w odniesieniu do przetwarzania we własnej jednostce organizacyjnej	X – w odniesieniu do przetwarzania we własnej jednostce organizacyjnej	X – w odniesieniu do przetwarzania we własnej jednostce organizacyjnej
9.	Zgłaszanie naruszeń i postępowanie po ich stwierdzeniu	X – w odniesieniu do przetwarzania we własnej jednostce organizacyjnej	X – w odniesieniu do przetwarzania we własnej jednostce organizacyjnej	X – w odniesieniu do przetwarzania we własnej jednostce organizacyjnej	X – w odniesieniu do przetwarzania we własnej jednostce organizacyjnej
10.	Wykonanie obowiązku informacyjnego oraz udostępnienie treści uzgodnień osobom, których dane dotyczą	X w odniesieniu do przetwarzania we własnej jednostce organizacyjnej	X w odniesieniu do przetwarzania we własnej jednostce organizacyjnej	X w odniesieniu do przetwarzania we własnej jednostce organizacyjnej	X w odniesieniu do przetwarzania we własnej jednostce organizacyjnej
11.	Realizacja praw osób, których dane dotyczą, w tym zawiadamianie osoby, której dane dotyczą o naruszeniu ochrony danych osobowych	X – w odniesieniu do przetwarzania we własnej jednostce organizacyjnej	X – w odniesieniu do przetwarzania we własnej jednostce organizacyjnej	X – w odniesieniu do przetwarzania we własnej jednostce organizacyjnej	X – w odniesieniu do przetwarzania we własnej jednostce organizacyjnej
12.	Współpraca z wyznaczonym przez administratora inspektorem ochrony danych i zapewnienie współpracy z organem nadzorczym	X w odniesieniu do przetwarzania we własnej jednostce organizacyjnej	X w odniesieniu do przetwarzania we własnej jednostce organizacyjnej	X w odniesieniu do przetwarzania we własnej jednostce organizacyjnej	X w odniesieniu do przetwarzania we własnej jednostce organizacyjnej
13.	Realizacja zadań punktu kontaktowego dla osób, których dane dotyczą	X – w odniesieniu do przetwarzania we własnej jednostce organizacyjnej	X – w odniesieniu do przetwarzania we własnej jednostce organizacyjnej	X – w odniesieniu do przetwarzania we własnej jednostce organizacyjnej	X – w odniesieniu do przetwarzania we własnej jednostce organizacyjnej
14.	Kontrole i audyty	X – wobec bezpośrednio podległych i nadzorowanych jednostek – wewnętrzne	X – wewnętrzne	X – wobec bezpośrednio podległych i nadzorowanych jednostek – wewnętrzne	X – wewnętrzne
15.	Przestrzeganie obowiązujących przepisów i procedur wewnętrznych	X – w odniesieniu do przetwarzania	X – w odniesieniu do przetwarzania	X – w odniesieniu do przetwarzania	X – w odniesieniu do przetwarzania

		we własnej jednostce organizacyjnej	we własnej jednostce organizacyjnej	we własnej jednostce organizacyjnej	we własnej jednostce organizacyjnej
16.	Przekazywanie danych do państw trzecich	X – w odniesieniu do całości systemu			
17.	Realizacja polityki prywatności domyślnej i prywatności w fazie projektowania	X – w odniesieniu do całości systemu			

* W odniesieniu do zadania pt. „Wdrożenie odpowiednich środków technicznych i organizacyjnych, w tym zapewnienie realizacji procedur bezpieczeństwa opisanych w przyjętej polityce ochrony danych”, każdy ze współadministratorów w swoim zakresie obsługi systemu odpowiedzialny jest za:

1) Wydawanie upoważnień do przetwarzania danych i nadawanie uprawnień do pracy w SWD PSP;
2) Prowadzenie i aktualizowanie ewidencji osób upoważnionych do przetwarzania danych osobowych w SWD PSP;
3) Prowadzenie szkoleń dla użytkowników w zakresie bezpieczeństwa teleinformatycznego oraz ochrony danych osobowych;
4) Regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania. Przeglądy i kontrole bezpieczeństwa w zakresie stosowanych środków technicznych, zarządzanie uprawnieniami i zapewnienie odpowiedniego poziomu wiedzy i świadomości użytkowników;
5) Zapewnienie poufności, integralności, dostępności i odporności systemów i usług przetwarzania, w tym tworzenie zabezpieczeń technicznych, ograniczeń dostępu fizycznego i zdalnego, przestrzeganie zasad zarządzania – administrowania, zarządzanie użytkownikami i uprawnieniami w odniesieniu do serwera, bazy danych, sieci oraz stacji roboczych i oprogramowania końcowego;
6) Zdolność (adekwatnie do zarządzanych zasobów) do szybkiego przywrócenia dostępności danych osobowych w razie incydentu fizycznego lub technicznego odnoszącego się w szczególności do:
   a) Serwera i bazy danych,
   b) Sieci teleinformatycznych i kanałów przesyłu danych,
   c) Stacji roboczych i oprogramowania końcowego.

IV. Odpowiedzialność i zadania innych niż PSP jednostek ochrony przeciwpożarowej mających dostęp do SWD PSP

1. Inne jednostki ochrony przeciwpożarowej, przetwarzające dane w SWD PSP są zobowiązane do:

1) Dopuszczania do pracy w SWD PSP wyłącznie osób spełniających minimalne wymagania odnośnie bezpieczeństwa osobowego określone w dziale IV.1. załącznika nr 2 do zarządzenia;
2) Prowadzenia i aktualizowania ewidencji osób upoważnionych do przetwarzania danych osobowych w SWD PSP;
3) Prowadzenia szkoleń dla użytkowników w zakresie bezpieczeństwa teleinformatycznego oraz ochrony danych osobowych;
4) Regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania;
5) Zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania, w tym tworzenia zabezpieczeń technicznych, ograniczeń dostępu fizycznego i zdalnego, przestrzegania zasad zarządzania – administrowania, zarządzania użytkownikami i uprawnieniami w odniesieniu do sieci oraz stacji roboczych i oprogramowania końcowego;
6) Zapewnienia rozliczalności operacji przetwarzania;
7) Zgłaszania naruszeń i przeprowadzania postępowań po ich stwierdzeniu;
8) Wykonania obowiązku informacyjnego oraz udostępnienia treści uzgodnień strażakom i innym osobom z własnych jednostek, których dane dotyczą;
9) Zapewnienia współpracy z IOD oraz UODO;
10) Przestrzegania obowiązujących przepisów i procedur wewnętrznych.

2. Inne jednostki ochrony przeciwpożarowej są również obowiązane do przestrzegania minimalnych wymagań dotyczących realizacji zadań w zakresie:
   1) Zbierania danych, opisanym w pkt I.1 załącznika nr 2 do zarządzenia;
   2) Utrwalania danych, opisanym w pkt I.2 a–b oraz g–l załącznika nr 2 do zarządzenia;
   3) Przekazywania danych za pomocą środków łączności, opisanym w pkt I.3. c-d załącznika nr 2 do zarządzenia;
   4) Usuwania danych, opisanym w pkt I.9 załącznika nr 2 do zarządzenia;
   5) Zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania, opisanym w pkt IV.5 c-d załącznika nr 2 do zarządzenia;
   6) Zasad napraw urządzeń teleinformatycznych, opisanym w pkt IV.7 załącznika nr 2 do zarządzenia;
   7) Zabezpieczenia przed dostępem fizycznym do obszaru przetwarzania, opisanym w pkt IV.8 załącznika nr 2 do zarządzenia;
   8) Postępowania w sytuacji naruszeń praw i wolności osób fizycznych w związku z przetwarzaniem ich danych osobowych, opisanym w pkt IV.9 załącznika nr 2 do zarządzenia.

Załącznik nr 2
do zarządzenia nr 14/2019
z dnia 17 grudnia 2019 roku

Minimalne wymagania dotyczące realizacji zadań przez współadministratorów Systemu Wspomagania Decyzji Państwowej Straży Pożarnej

I. Organizacja przetwarzania danych

1. Zbieranie danych - osoby pozyskujące dane powinny spełniać minimalne wymagania odnośnie bezpieczeństwa osobowego określone w dziale IV.1.
2. Utrwalanie danych:
   1) Dane zbierane w związku z prowadzonymi działaniami ratowniczymi mogą być pierwotnie utrwalane na nośnikach tradycyjnych – papierowych, skąd niezwłocznie przenoszone są do SWD PSP. Dane utrwalone w formie papierowej (notatki odręcznej) powinny zostać zniszczone, po ich skutecznym przeniesieniu do SWD PSP, chyba, że zostały lub będą włączone do akt sprawy. Odpowiedzialność za te czynności spoczywa na osobie pierwotnie utrwalającej dane;
   2) Wyjątek mogą stanowić notatniki KDR i notatniki dyżurnego stanowiska kierowania PSP (dyżurnego SK), które podlegają rejestracji wiążącej notatnik z konkretną osobą odpowiedzialną. Notatniki te podlegają niszczeniu do 3 miesięcy po upływie roku kalendarzowego, w którym zostały wytworzone. Dokumentacja w postaci notatników KDR i dyżurnych SK powinna być odpowiednio chroniona przed dostępem osób nieupoważnionych;
   3) Dane mogą być także utrwalane w postaci zapisów rozmów na rejestratorach dźwięku w stanowiskach kierowania. Okres przechowywania nagrań powinien zapewnić możliwość wykonania stenogramu rozmów w razie potrzeby związanej z dokumentowaniem zdarzenia, lecz nie powinien być dłuższy niż 3 miesiące. Po tym okresie nagrania podlegają obowiązkowemu usunięciu z rejestratora. Wyjątek stanowią nagrania pochodzące z bezpośredniej obsługi zgłoszeń alarmowych, które powinny być zabezpieczone na zewnętrznym nośniku i przechowywane przez 3 lata;
   4) Dostęp do rejestratorów rozmów powinien być ograniczony i zabezpieczony przed nieuprawnionym dostępem i usunięciem danych. Osoby mające dostęp do rejestratorów powinny spełniać wymagania bezpieczeństwa osobowego określone w dziale IV.1;
   5) Rejestratory powinny spełniać wymagania bezpieczeństwa analogiczne jak określone dla SWD PSP;
   6) Administrator w sytuacji konieczności zabezpieczenia nagrania na potrzeby postępowania, sporządza jego kopię na zewnętrznym nośniku. Zabezpieczenie nagrania może nastąpić także, gdy treść rozmów lub sytuacja, której dotyczyły ma potencjalnie charakter sporny lub roszczeniowy. Nagranie przechowywane jest zgodnie z zasadami określonymi dla przechowywania danych osobowych, przez

okres niezbędny do realizacji celów, dla których zostało zabezpieczone, po czym podlega zniszczeniu lub przekazaniu do właściwego organu prowadzącego postępowanie;

7) Dokumentacja multimedialna (audio, zdjęcia i wideo) powinna być wykonywana za pomocą sprzętu służbowego przez osoby spełniające minimalne wymagania odnośnie bezpieczeństwa osobowego określone w dziale IV.1;
8) Użycie sprzętu prywatnego do wykonywania dokumentacji multimedialnej dozwolone jest wyłącznie za wiedzą i zgodą właściwego administratora;
9) Zabrania się wykorzystywania ogólnie dostępnych systemów informatycznych, w tym mediów społecznościowych w celu przetwarzania dokumentacji ze zdarzenia, a zwłaszcza dokumentacji multimedialnej (audio, zdjęcia, wideo);
10) Podczas zgrywania materiałów z urządzeń w celu ich dalszego przetwarzania, należy dokonać ich przeglądu pod kątem niezbędności ich przechowywania oraz adekwatności zawartości w odniesieniu do celu, jakim jest dokumentowanie działań ratowniczych;
11) Systemy informatyczne, służące do przechowywania materiałów multimedialnych powinny spełniać wymagania bezpieczeństwa analogiczne jak określone dla SWD PSP;
12) Administrator może zdecydować o wykorzystaniu wybranej dokumentacji multimedialnej do celów związanych z działalnością informacyjną oraz do działań związanych z zapobieganiem powstawania i rozprzestrzeniania się pożarów, klęsk żywiołowych lub innych miejscowych zagrożeń w ramach prewencji społecznej;
13) Administrator może zdecydować o wykorzystaniu wybranej dokumentacji multimedialnej (audio, zdjęcia i wideo) w tym także danych utrwalonych w postaci zapisów rozmów na rejestratorach dźwięku w Stanowiskach Kierowania, do celów szkoleniowych, jako materiały dydaktyczne, które mogą zostać wykorzystane w procesie kształcenia, szkolenia i doskonalenia zawodowego. Warunkiem wykorzystania ww. dokumentacji do celów szkoleniowych jest odpowiednie ich zanonimizowanie, w sposób określony w pkt 11 lit. c.

3. Przekazywanie danych za pomocą środków łączności:
   1) Dopuszcza się przekazywanie danych telefonicznie bądź pocztą elektroniczną pomiędzy stanowiskami kierowania komendanta głównego PSP (SK KG PSP), komendantów wojewódzkich PSP (SK KW PSP), komendantów powiatowych PSP lub poprzez funkcję SWP;
   2) Pliki z danymi zawierającymi dane osobowe SWD PSP powinny zostać zabezpieczone środkami ochrony kryptograficznej i hasłem, przekazanym odbiorcy w sposób odrębny lub poprzez inny mechanizm gwarantujący poufność;
   3) Przekazując i przyjmując dane w formie informacji ustnej, za pomocą środków łączności, należy zawsze mieć na względzie ochronę danych osobowych; nie wolno robić tego w obecności osób nieupoważnionych;
   4) Zabronione jest przekazywanie za pomocą niekodowanych środków łączności informacji, które umożliwiają zidentyfikowanie konkretnych osób, w tym obejmujących szczególne kategorie danych osobowych, o których mowa w art. 9 ust 1 RODO.

4. Wprowadzanie danych do SWD PSP - dane do systemu wprowadza osoba spełniająca minimalne wymagania odnośnie bezpieczeństwa osobowego określone w dziale IV.1., niezwłocznie, tzn. w możliwie najkrótszym czasie, na który wpływ mogą mieć jedynie bieżące potrzeby służby.
5. Weryfikacja wprowadzonych danych:
   1) Dokumentacja papierowa zdarzenia przed włączeniem w akta sprawy, powinna uzyskać kontrasygnatę administratora lub osoby przez niego upoważnionej, której celem jest potwierdzenie poprawności i niezaprzeczalności danych;
   2) Korekty danych wprowadzonych do SWD PSP może dokonać osoba uprawniona do sporządzania danego typu dokumentacji, wskazana w rozporządzeniu ksrg;
   3) Weryfikacja danych obejmujących informacje ze zdarzeń realizowana jest dwutorowo:
      - zdarzenia szczególne (według filtrów SWD PSP: między innymi zdarzenia z dużą ilością osób rannych, z ofiarami śmiertelnymi, z udziałem substancji niebezpiecznych, w obiektach użyteczności publicznej, z udziałem znacznych sił i środków jednostek ochrony przeciwpożarowej) powinny być weryfikowane przez służbę dyżurną Stanowiska Kierowania Komendanta Głównego PSP na bieżąco poprzez przeglądanie danych w module przeglądania meldunków oraz w module zestawień SWD PSP,
      - wybrane grupy zdarzeń lub zdarzenia podczas przeprowadzanych analiz oraz wyszukiwania błędów powinny być weryfikowane cyklicznie przez pracowników Wydziału Przetwarzania Danych Operacyjnych KCKRiOL (WPDO KCKRiOL). Poprawa danych może następować poprzez kontakt telefoniczny bądź pocztą elektroniczną ze stanowiskami kierowania komendantów wojewódzkich PSP (SK KW PSP) lub poprzez funkcjonalności SWD PSP;
   4) Weryfikacja danych obejmujących informacje ze zdarzeń odbywa się na podstawie rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie szczegółowej organizacji krajowego systemu ratowniczo-gaśniczego oraz „Zasad ewidencjonowania zdarzeń w SWD PSP”. Informacje ze zdarzeń powinny być weryfikowane w powyższym zakresie na poziomie komend powiatowych, miejskich i wojewódzkich PSP;
   5) Weryfikacja danych w zakresie bazy sił i środków dokonywana jest poprzez sprawdzanie poprawności przyporządkowania sił i środków do odpowiednich miejsc katalogu. Weryfikacja powinna dotyczyć kompletności danych zgodnie z określonymi przez KG PSP zakresem parametrów sił i środków. Dane powinny być sprawdzane cyklicznie.
6. Wykonywanie kopii danych i zarządzanie wydrukami:
   1) Wszelkie wykonywanie kopii winno mieć swoje uzasadnienie. Wszystkie kopie, które nie podlegają archiwizacji, należy po wykorzystaniu trwale zniszczyć;
   2) Przekazywanie nośników elektronicznych z zapisanymi na nich danymi osobowymi poza obszar przetwarzania danych, powinno odbywać się w sposób zapewniający poufność i integralność tych danych, wyłącznie dla realizacji czynności służbowych, za wiedzą i zgodą administratora lub bezpośredniego przełożonego użytkownika SWD PSP. Plik z danymi zawierającymi dane osobowe

SWD PSP powinien zostać zabezpieczony środkami ochrony kryptograficznej i opatrzony hasłem, przekazanym odbiorcy w sposób odrębny;
3) Wydruki i dokumentację należy przechowywać poza zasięgiem wzroku osób trzecich;
4) Niedozwolone jest pozostawianie wydruków w drukarce;
5) Niedozwolone jest przekazywanie wydruków osobom nieuprawnionym;
6) Wszelkie wydruki nadmiarowe lub nieprzydatne należy niszczyć za pomocą niszczarki przewidzianej do likwidacji dokumentów zawierających dane osobowe;
7) Dokumenty, których nie można zniszczyć z uzasadnionych przyczyn, powinny być składowane w miejscu z ograniczonym dostępem, systematycznie weryfikowane, a następnie archiwizowane zgodnie z obowiązującymi w tym zakresie przepisami.

7. Udostępnianie danych dla podmiotów uprawnionych oraz w celu wykonania obowiązków prawnych:
1) Dane osobowe mogą być udostępniane w następujących przypadkach:
- na podstawie przepisów prawa organom publicznym, w szczególności w ramach konkretnego postępowania,
- na podstawie wniosku od podmiotu uprawnionego do otrzymania danych na podstawie przepisów prawa,
- na podstawie umowy z odbiorcą danych lub współadministratorem danych, w ramach, której istnieje konieczność udostępnienia danych;

2) Dane utrwalone w SWD PSP w związku ze zdarzeniem mogą być udostępniane tylko na pisemny, zaakceptowany przez administratora, wniosek:
- udostępnianie powinno odbywać się w sposób zapewniający poufność i integralność danych,
- pliki zawierające dane osobowe powinny zostać zabezpieczone środkami ochrony kryptograficznej i hasłem, przekazanym odbiorcy w sposób odrębny,
- każdorazowe udostępnienie powinno być odnotowane w rejestrze udostępnień danych innym podmiotom,
- Udostępnienie powinno zostać udokumentowane, co najmniej w zakresie: daty, zakresu, odbiorcy oraz podstawy prawnej udostępnienia danych.

8. Wykonywanie kopii bezpieczeństwa:
1) Dopuszcza się do celów przywracania sytemu po awarii wykonanie obrazu partycji systemowej za pomocą specjalistycznego oprogramowania lub innych programów do wykonywania kopii zapasowych, będących na wyposażeniu jednostki lub komórki organizacyjnej PSP;
2) Proces wykonywania kopii danych dokonywany jest na centralnych bibliotekach;
3) Ze względu na założenie wysokiej dostępności środowiska, wszystkie kopie bezpieczeństwa baz danych wykonywane są w trybie online (tzn. bez konieczności zatrzymania pracujących aplikacji);
4) Kopie zapasowe muszą być zabezpieczone przed dostępem osób nieuprawnionych, nieautoryzowaną modyfikacją i zniszczeniem oraz powinny być przechowywane w zamykanych na klucz metalowych szafach, szufladach lub sejfach;

5) Dane w postaci kopii elektronicznej przechowywane mogą być maksymalnie przez okres 3 miesięcy od dnia ich sporządzenia.

9. Archiwizowanie danych, które mogą zostać zakwalifikowane do materiałów archiwalnych lub dokumentacji niearchiwalnej w rozumieniu przepisów ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2019 r. poz. 553 ze zm.), następuje zgodnie z obowiązującymi w tym zakresie uregulowaniami.
10. Usuwanie danych z SWD PSP może nastąpić wyłącznie w przypadkach określonych w art. 17 RODO, na pisemny wniosek osoby, której dane dotyczą lub z inicjatywy administratora.
11. Zapewnienie retencji danych zgodnej z przepisami:
    1) Dane osobowe w katalogu sił i środków należy weryfikować i aktualizować na bieżąco i w razie potrzeby usuwać wpisy dotyczące osób, których dane nie są już potrzebne;
    2) Dane osobowe podlegają przeglądowi nie rzadziej, niż co 5 lat od dnia ich uzyskania;
    3) W ramach przeglądu, administrator anonimizuje dane osobowe utrwalone w SWD PSP zawarte w dokumentacji zdarzenia, starsze niż 5 lat oraz usuwa nieaktualne dane w katalogu sił i środków. Anonimizacja polega w szczególności na trwałym usunięciu wybranych danych, w taki sposób, że osób, których dane dotyczą, w ogóle nie można zidentyfikować lub już nie można zidentyfikować.

II. Realizacja praw osób, których dane dotyczą

1. Administratorzy w ramach własnej działalności realizują: Prawo dostępu do danych (art. 15 RODO), Prawo do sprostowania danych (art. 16 RODO), Prawo do usunięcia danych (art. 17 RODO), Prawo do ograniczenia przetwarzania (art. 18 RODO), Informowanie o sprostowaniu lub usunięciu (art. 19 RODO), Prawo do sprzeciwu (art. 21 RODO).
2. Wnioski w sprawie skorzystania z praw osoby, której dane osobowe dotyczą rozpatruje właściwy administrator.
3. Sposób rozpatrzenia wniosków powinien zostać udokumentowany.
4. W przypadku wątpliwości, co do zgodności z prawem przyjętego postępowania, a w szczególności w sytuacji wątpliwości w zakresie treści odpowiedzi, administrator może zasięgnąć opinii właściwego Inspektora Ochrony Danych.
5. W celu ułatwienia korzystania z praw przez osobę, której dane dotyczą, administrator umożliwia jej także kontakt z Inspektorem Ochrony Danych poprzez umieszczeniu adresu poczty elektronicznej do niego na stronie internetowej jednostki.
6. Informacja o danych przetwarzanych w SWD PSP dla osoby, której te dane dotyczą, powinna być przekazana w ciągu 1 miesiąca. Istnieje możliwość przedłużenia przekazania tej informacji o kolejne 2 miesiące, jeżeli wniosek/żądanie ma skomplikowany charakter.

III. Obowiązek informacyjny

1. Informowanie strażaków i innych osób, których dane są przetwarzane w ramach katalogu sił i środków:
   1) Każdy administrator wypełnia obowiązek informacyjny wobec strażaków PSP i pracowników własnej jednostki, których dane są przetwarzane w SWD PSP;
   2) Każdy administrator wypełnia obowiązek informacyjny wobec specjalistów ds. ratownictwa, z którymi zawarł umowę.
2. Obowiązek informacyjny wobec pozostałych osób, których dane przetwarzane są w związku z prowadzonymi działaniami ratowniczymi, a także wobec strażaków OSP, których dane są przetwarzane w SWD PSP, jest spełniany poprzez udostępnienie informacji w Biuletynie Informacji Publicznej na swojej stronie podmiotowej lub na stronie internetowej oraz w widocznym miejscu w siedzibie.
3. W klauzuli informacyjnej należy uwzględnić zakres określony odpowiednio w art. 13 lub 14 RODO oraz dodatkowo informacje o danych pozostałych współadministratorów oraz o zakresie odpowiedzialności i podziale zadań współadministratorów określonym w załączniku nr 1 do zarządzenia.
4. Każdy administrator udostępnia w Biuletynie Informacji Publicznej informacje o ograniczeniach związanych z wypełnianiem obowiązku informacyjnego, o którym mowa w ust 2 oraz dodatkowych warunkach realizacji prawa dostępu do danych, wynikającego z art. 15 RODO, opisanych w art. 14h ust 3 ustawy o ochronie przeciwpożarowej.

IV. Mechanizmy i procedury bezpieczeństwa

1. Bezpieczeństwo osobowe:
   1) Każda osoba mająca przetwarzać dane, które będą trafiały do SWD PSP powinna:
      - posiadać imienne upoważnienie pisemne do przetwarzania danych osobowych wydane przez właściwego administratora,
      - podpisać oświadczenie o poufności zawierające dodatkowo informację o zapoznaniu się z procedurami, przepisami i instrukcjami oraz zobowiązanie do ich przestrzegania,
      - odbyć szkolenie obejmujące zasady przetwarzania w systemach teleinformatycznych oraz ochrony danych osobowych;
   2) Każda osoba mająca przetwarzać dane w SWD PSP powinna posiadać dodatkowo dokument zatwierdzony przez administratora, upoważniający do przetwarzania danych w systemie teleinformatycznym łączący jego nazwę oraz nazwę użytkownika, pod którą dozwolone jest przetwarzanie danych dla danej osoby.
2. Przyznawanie uprawnień do pracy w SWD PSP, kontrola dostępu do kont uprzywilejowanych:
   1) Zakres uprawnień związanych z kontem użytkownika powinien być ściśle związany z rolą, jaką pełni w systemie wynikającą z zakresu zadań przydzielonych przez kierownika jednostki;

2) Użytkownik, w sytuacji wykonywania różnych zadań w ramach SWD PSP, związanych z zasadniczo różnymi uprawnieniami (np. administrator i dyżurny operacyjny), powinien je wykonywać z użyciem różnych identyfikatorów lub ról, zapewniających rozliczalność wykonanych czynności;
3) Liczba kont uprzywilejowanych, umożlwiających wprowadzenie istotnych zmian w strukturze danych oraz uprawnieniach użytkowników powinna być ograniczona do minimum niezbędnego dla zachowania ciągłości pracy.

3. Szkolenia dla użytkowników:
   1) Szkolenia powinny obejmować zagadnienia związane z bezpieczeństwem teleinformatycznym oraz zasadami i procedurami ochrony danych osobowych obowiązującymi w jednostce;
   2) Szkolenia powinny być prowadzone przez osoby posiadające odpowiednią wiedzę i kwalifikacje, w zakresie objętym szkoleniem;
   3) Przed dopuszczeniem do pracy w SWD PSP szkoleniem należy objąć każdego nowego użytkownika;
   4) Wymagane są cykliczne szkolenia dla stałych użytkowników SWD PSP (dyżurnych stanowisk kierowania i dowódców), nie rzadziej niż raz na 3 lata.
4. Regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania:
   1) Dla każdego systemu lub grupy systemów teleinformatycznych wykorzystywanych do przetwarzania danych w ramach SWD PSP należy przygotować analizę ryzyka związaną z bezpieczeństwem przetwarzanych danych osobowych oraz wpływem na prawa i wolności osób, których dane dotyczą;
   2) Analiza powinna podlegać okresowej weryfikacji, nie rzadziej niż raz na 5 lat lub w przypadku wprowadzenia istotnych dla jej wyników zmian w sprzęcie, oprogramowaniu lub procedurach;
   3) Przygotowywane analizy podlegają obowiązkowemu opiniowaniu właściwego terytorialnie Inspektora Ochrony Danych;
   4) Wymagany jest coroczny przegląd uprawnień i kont użytkowników;
   5) Przeglądy powinny zostać udokumentowane w sposób umożliwiający zapewnienie ich rozliczalności, a ich wyniki zaakceptowane przez właściwego administratora;
   6) W ramach prowadzonych kontroli i audytów należy uwzględniać tematykę związaną z ochroną danych osobowych.
5. Zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów ·i usług przetwarzania (adekwatnie do zarządzanych zasobów):
   1) W zakresie funkcjonowania serwera i baz danych:
      - pomieszczenie z serwerem musi być zabezpieczone przed dostępem osób nieuprawnionych,
      - serwer musi być wyposażony w zabezpieczenia przed nieautoryzowanym dostępem zdalnym w postaci: login i hasło oraz odseparowany od sieci publicznej przy pomocy zapory sieciowej,
      - dostęp do serwera i bazy danych pod kątem administracji technicznej ograniczony do niezbędnej liczby osób,

- sprzęt i oprogramowanie musi być zabezpieczone przed złośliwym oprogramowaniem, z systematycznie aktualizowanymi definicjami mechanizmów bezpieczeństwa,
- sprzęt musi być wyposażony w mechanizm zasilania awaryjnego zapewniający jego ciągłość działania i wymagane parametry techniczne zasilania,
- niezbędne jest regularne tworzenie kopii bezpieczeństwa systemu i bazy danych, w tym na nośniku zewnętrznym zlokalizowanym w innym pomieszczeniu niż serwer, przechowywanym w bezpiecznym miejscu;

2) W zakresie funkcjonowania sieci teleinformatycznej i kanałów transmisji danych:
- pomieszczenie z urządzeniami aktywnymi sieci powinno być zabezpieczone przed dostępem osób nieuprawnionych,
- urządzenia sieciowe muszą być wyposażone w zabezpieczenia przed nieautoryzowanym dostępem zdalnym w postaci loginu i hasła,
- dostęp do urządzeń sieciowych pod kątem administracji technicznej ograniczony do niezbędnej liczby osób,
- infrastruktura sieciowa powinna być wyposażona w mechanizm zasilania awaryjnego zapewniający jego ciągłość i wymagane parametry techniczne;

3) W zakresie funkcjonowania stacji roboczych i oprogramowania końcowego:
- urządzenia muszą być zlokalizowane w pomieszczeniach spełniających wymogi bezpieczeństwa fizycznego dla przetwarzania danych osobowych,
- sprzęt oraz oprogramowanie na nim używane musi być wyposażone w zabezpieczenia przed nieautoryzowanym dostępem zdalnym w postaci: login i hasło oraz odseparowany od sieci publicznej przy pomocy zapory sieciowej,
- wymagana jest praca użytkowników pod indywidualnym identyfikatorem,
- dopuszczalna jest praca na wspólnym loginie w stanowiskach kierowania pod warunkiem zapewnienia innego mechanizmu rozliczalności operacji przetwarzania danych,
- wskazane jest rozdzielenie uprawnień użytkownika od uprawnień administracyjnych i technicznych;

4) W zakresie przetwarzania w formie papierowej:
- kopie papierowe z danymi osobowymi muszą być przechowywane w zamykanych na klucz szafach, szufladach lub sejfach,
- obowiązuje tzw. „zasada czystego biurka”, czyli niepozostawianie dokumentów z danymi osobowymi w trakcie nieobecności w pomieszczeniu bez odpowiedniego ich zabezpieczenia,
- dopuszcza się przechowywanie danych osobowych w niezamykanych szafach lub regałach tylko w pomieszczeniu archiwum lub pomieszczeniu do przechowywania informacji niejawnych zabezpieczonym zgodnie z odrębnymi przepisami.

6. Procedury zapewnienia ciągłości działania i zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego, które powinny zostać opracowane i wdrożone w jednostkach przetwarzających dane w SWD PSP (adekwatnie do zarządzanych zasobów):

1) Postępowanie w sytuacji awarii serwera i bazy danych obejmujące przywracanie systemu z kopii bezpieczeństwa;
2) Postępowanie w sytuacji awarii sieci/kanałów dostępu do systemu;
3) Postępowanie w sytuacji awarii stacji roboczych i oprogramowania końcowego obejmująca przywracanie z kopii bezpieczeństwa;
4) Zasady korzystania z urządzeń mobilnych i nośników wymiennych;
5) Zasady wykonywania kopii bezpieczeństwa i kopii archiwalnych.

7. Zasady napraw urządzeń teleinformatycznych:
   1) Urządzenia teleinformatyczne powinny być oddawane do naprawy po usunięciu z nich nośników pamięci zawierających dane osobowe lub po trwałym skasowaniu tych danych;
   2) W przypadku, gdy naprawa dotyczy samego nośnika, a nie jest możliwe usunięcie z niego danych, administrator jest zobowiązany podpisać umowę powierzenia przetwarzania danych osobowych z podmiotem dokonującym naprawy.
8. Zabezpieczenie dostępu fizycznego do obszaru przetwarzania:
   1) Administrator definiuje obszar, w którym dozwolone jest przetwarzanie danych osobowych oraz zasady przebywania w nim osób postronnych, nieupoważnionych do przetwarzania danych;
   2) Administrator określa zasady dostępu do pomieszczeń i obszarów, gdzie są przetwarzane dane osobowe, które zapewniają poufność przetwarzanych danych oraz rozliczalność w zakresie osób w nich przebywających;
   3) Pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane na czas nieobecności w nich osób dopuszczonych do danych osobowych, w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym;
   4) Przetwarzanie danych osobowych poza wyznaczonymi pomieszczeniami i obszarami powinno się odbywać wyłącznie na polecenie administratora lub osoby przez niego upoważnionej, przy zachowaniu adekwatnym do ryzyka, zasad i procedur bezpieczeństwa. Procedury te powinny być co najmniej tak skuteczne jak stosowane do wyznaczonych pomieszczeń i obszarów.
9. Postępowanie w sytuacji naruszeń praw i wolności osób fizycznych w związku z przetwarzaniem ich danych osobowych:
   1) Administrator po stwierdzeniu lub uzyskaniu informacji o naruszeniu ochrony danych osobowych powinien:
      - przystąpić do identyfikacji rodzaju zdarzenia, a w szczególności do określenia skali zniszczeń, danych osobowych, do których uzyskano nieuprawniony dostęp itp.,
      - powiadomić IOD, a także przekazać mu wszelkie niezbędne informacje do realizacji jego obowiązków,
      - podjąć odpowiednie kroki w celu zminimalizowania szkód i rozmiarów zdarzenia oraz zabezpieczenia przed usunięciem śladów zdarzenia,
      - opisać zdarzenie w prowadzonej dokumentacji naruszeń (również takie, które nie wymaga zgłoszenia do UODO),

- w terminie 72 godzin przesłać do UODO zgłoszenie naruszenia ochrony danych osobowych, jeżeli skutkowało ono ryzykiem naruszenia praw i wolności osób fizycznych,
- zgodne z art. 34 RODO, bez zbędnej zwłoki zawiadomić osobę, której dane dotyczą o naruszeniu, jeżeli skutkowało ono dużym ryzykiem naruszenia praw i wolności osób fizycznych;

2) W przypadku zdarzenia mającego związek z systemem informatycznym należy dodatkowo:
   - dokonać szczegółowej analizy systemu w celu potwierdzenia lub wykluczenia faktu naruszenia,
   - wygenerować, wydrukować dokumenty, raporty lub zestawienia, które mogą pomóc w ustaleniu okoliczności zdarzenia, opatrując je datą i podpisem,
   - w razie konieczności dokonać fizycznego odłączenia urządzenia, segmentu sieci, które mogły umożliwiać dostęp do bazy danych osobowych osobie nieupoważnionej,
   - wylogować użytkownika podejrzewanego o naruszenie ochrony danych osobowych,
   - dokonać zmiany haseł na kontach, poprzez które uzyskano nielegalny dostęp,
   - przywrócić normalne działanie systemu, przy czym, jeżeli nastąpiło uszkodzenie bazy danych, przywrócić ją z ostatniej kopii awaryjnej z zachowaniem środków ostrożności przed ponownym dostępem tą samą drogą przez osobę nieupoważnioną.