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

Dokument 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 (SWD PSP) 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 (t.j. Dz. U. z 2019 r., poz. 1372 ze zm.).

1. 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) **ustawie o ochronie przeciwpożarowej** - rozumie się przez to - ustawę z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej (t.j. Dz. U. z 2019 r., poz. 1372 ze zm.);
3) **ustawie o systemie powiadamiania ratunkowego** - rozumie się przez to -ustawę z dnia 22 listopada 2013 r. o systemie powiadamiania ratunkowego (tj. Dz. U. z 2018 r. poz. 867, 1115, z 2019 r. poz. 730);
4) **ustawie prawo geodezyjne i kartograficzne** - rozumie się przez to - ustawę z dnia 17 maja 1989 r. - Prawo geodezyjne i kartograficzne (Dz. U. z 2010 r. Nr 193, poz. 1287, z późn. zm.);
5) **ustawie prawo telekomunikacyjne** - rozumie się przez to - ustawę - Prawo telekomunikacyjne (t.j. Dz. U. z 2018 r. poz. 1954, 2245, 2354, z późn. zm.);
6) **rozporządzeniu 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. z 2017 poz. 1319 z późn. zm.);
7) **administratorze** - 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) **współadministratorze** - 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 - Inspektor Ochrony Danych właściwy dla danej jednostki PSP, wyznaczony 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) **Rejestrze czynności przetwarzania** - rozumie się przez to - rejestr czynności przetwarzania danych osobowych, o którym mowa w art. 30 RODO;
18) **Danych** - rozumie się przez to dane osobowe, o których mowa w art. 4 pkt 1 RODO.

Ogólne 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.

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. 3 e 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. 3 e 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. 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.

Podział odpowiedzialności, obowiązków i zadań współad m i n istrato rów

LP	Zadanie	Szczebel organizacyjny PSP			
		Komendant Główny PSP	Administratorzy danych osobowych w	Komendanci wojewódzcy PSP	Komendanci i powiatowi miejscy PSP
1.	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 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
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 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
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:

Wydawanie upoważnień do przetwarzania danych i nadawanie uprawnień do pracy w SWD PSP;

Prowadzenie i aktualizowanie ewidencji osób upoważnionych do przetwarzania danych osobowych w SWD PSP;

Prowadzenie szkoleń dla użytkowników w zakresie bezpieczeństwa teleinformatycznego oraz ochrony danych osobowych;

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;

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;

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.

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

Inne jednostki ochrony przeciwpożarowej, które zostaną dopuszczone do przetwarzania danych w SWD PSP, na mocy odrębnych przepisów, są zobowiązane do:

Dopuszczania do pracy w SWD PSP wyłącznie osób spełniających minimalne wymogi odnośnie bezpieczeństwa osobowego. Oznacza to, że 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. Dodatkowo każda osoba mająca przetwarzać dane w SWD PSP powinna dodatkowo: posiadać dokument zatwierdzony przez administratora, upoważniający do przetwarzania danych w systemie teleinformatycznym łączące jego nazwę oraz nazwę użytkownika, pod którą dozwolone jest przetwarzanie danych dla danej osoby.

Prowadzenia i aktualizowania ewidencji osób upoważnionych do przetwarzania danych osobowych w SWD PSP.

Prowadzenia szkoleń dla użytkowników w zakresie bezpieczeństwa teleinformatycznego oraz ochrony danych osobowych.

Regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

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.

Zapewnienia rozliczalności operacji przetwarzania.

Zgłaszania naruszeń i przeprowadzania postępowań po ich stwierdzeniu.

Wykonania obowiązku informacyjnego oraz udostępnienia treści uzgodnień strażakom i innym osobom z własnych jednostek, których dane dotyczą.

Zapewnienia współpracy z IOD z właściwej jednostki PSP oraz UODO.

Zapewnienia przestrzegania obowiązujących przepisów i procedur wewnętrznych przez własnych członków i pracowników.

Dodatkowo inne jednostki ochrony przeciwpożarowej, są również obowiązane do przestrzegania minimalnych wymogów bezpieczeństwa dotyczących przetwarzania danych osobowych w SWD PSP w zakresie:

1. Zbierania danych, tj.:

a. osoby pozyskujące dane powinny spełniać minimalne wymogi odnośnie bezpieczeństwa osobowego opisane powyżej.

2. Utrwalania danych, tj.:

a. 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;

b. Wyjątek mogą stanowić notatniki KDR i notatniki dyżurnego stanowiska kierowania/punktu alarmowego (dyżurnego), 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 powinna być odpowiednio chroniona przed dostępem osób nieupoważnionych;

c. Dokumentacja multimedialna (audio, zdjęcia i wideo) powinna być wykonywana za pomocą sprzętu służbowego przez osoby spełniające minimalne wymogi odnośnie bezpieczeństwa osobowego;

d. Użycie sprzętu prywatnego do wykonywania dokumentacji multimedialnej dozwolone jest wyłącznie za wiedzą i zgodą właściwego administratora;

e. Zabrania się wykorzystywania ogólnie dostępnych systemów informatycznych, w tym mediów społecznościowych w celu przetwarzania dokumentacji ze zdarzenia, a zwłaszcza dokumentacji multimedialnej (audio, zdjęcia, wideo);

f. 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;

g. Systemy informatyczne, służące do przechowywania materiałów multimedialnych powinny spełniać wymogi bezpieczeństwa analogiczne jak określone dla SWD PSP;

h. 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.

3. Przekazywania danych za pomocą środków łączności, tj.:

a. 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;

b. 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.

Usuwania danych, tj.: usunięcie 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.

Zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania, tj.:

a. 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/punktach alarmowych pod warunkiem zapewnienia innego mechanizmu rozliczalności operacji przetwarzania danych,

wskazane jest rozdzielenie uprawnień użytkownika od uprawnień administracyjnych i technicznych.

b. 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. Zasad napraw urządzeń teleinformatycznych, tj.:

a. Urządzenia teleinformatyczne powinny być oddawane do naprawy po usunięciu z nich nośników pamięci zawierających dane osobowe lub po trwałym skasowaniu tych danych;

b. 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.

7. Zabezpieczenia przed dostępem fizycznym do obszaru przetwarzania, tj.:

a. Administrator definiuje obszar, w którym dozwolone jest przetwarzanie danych osobowych oraz zasady przebywania w nim osób postronnych, nieupoważnionych do przetwarzania danych;

b. 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;

c. 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;

d. 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.

8. Postępowania w sytuacji naruszeń praw i wolności osób fizycznych w związku z przetwarzaniem ich danych osobowych, tj.:

b. Administrator po stwierdzeniu lub uzyskaniu informacji o naruszeniu ochrony danych osobowych powinien:

przystąpić do identyfikacji rodzaju zdarzenia, a w szczególności do określenia skali zniszczeń, dostępu do danych osobowych itp.,

powiadomić właściwego 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.

c. 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.