Informacja o przetwarzaniu danych osobowych w związku z prowadzeniem działań ratowniczych przez jednostki ochrony przeciwpożarowej

Jednostki organizacyjne ochrony przeciwpożarowej, o których mowa w art. 15 ustawy o ochronie przeciwpożarowej, przetwarzają dane osobowe w związku z prowadzonymi działaniami ratowniczymi, w tym dane, które trafiają do systemu teleinformatycznego zwanego Systemem Wspomagania Decyzji Państwowej Straży Pożarnej (SWD PSP), o którym mowa w art. 14g ww. ustawy. Niniejszy dokument jest związany z wypełnieniem obowiązków określonych w art. 13 ogólnego 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 (RODO).

Współadministratorzy danych

Współadministratorami danych osobowych przetwarzanych w SWD PSP są: Komendant Główny Państwowej Straży Pożarnej, komendanci wojewódzcy Państwowej Straży Pożarnej, komendanci powiatowi (miejscy) Państwowej Straży Pożarnej, Rektor-Komendant Szkoły Głównej Służby Pożarniczej i komendanci szkół Państwowej Straży Pożarnej.

Informacje o siedzibach i danych kontaktowych poszczególnych współadministratorów są dostępne na stronie https://www.straz.gov.pl/kontakt/jednostki_organizacyjne_psp.

Wspólne uzgodnienia między Współadministratorami

Współadministratorzy uzgodnili zakres odpowiedzialności oraz podział zadań związanych z przetwarzaniem danych osobowych w ramach Systemu Wspomagania Decyzji Państwowej Straży Pożarnej. Szczegóły uzgodnień są dostępne na stronie *(wpisać adres własnej strony z opublikowanym podziałem zadań)*

Punkt kontaktowy

Współadministratorzy ustali wspólny punkt kontaktowy do którego można zwracać się z wszelkimi sprawami dotyczącymi przetwarzania danych osobowych w Systemu Wspomagania Decyzji Państwowej Straży Pożarnej. Zapytania należy kierować na adres poczty elektronicznej iod@kgpsp.gov.pl

Niezależnie od powyższego możliwe jest realizowanie wszelkich praw osób związanych z przewarzaniem ich danych osobowych wynikających z RODO wobec każdego ze współadministratorów odrębnie.

Cel, podstawa, sposób i zakres przetwarzania

Dane osobowe są przetwarzane w oparciu art. 6 ust 1 lit c, d i e RODO – w celu 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 z dnia 22 listopada 2013 r. o systemie powiadamiania ratunkowego,

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:

1. 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.
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 z właściwej jednostki PSP oraz UODO.
10. 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

- 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.:

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 2018 r. poz. 620, 1669, z 2019 r. poz. 730).

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 2018 r. poz. 620, 1669, z 2019 r. poz. 730);
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;

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;

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	X w odniesieniu do przetwarzania we własnej jednostce organizacyjnej	X w odniesieniu do przetwarzania we własnej jednostce	X w odniesieniu do przetwarzania we własnej jednostce	X w odniesieniu do przetwarzania we własnej jednostce

b. Sieci teleinformatycznych i kanałów przesyłu danych;
c. Stacji roboczych i oprogramowania końcowego.