Zasadnicza treść uzgodnień oraz informacje związane z współadministrowaniem danymi osobowymi w wspólnie użytkowanych systemach teleinformatycznych wykorzystywanych w Komendzie Wojewódzkiej Państwowej Straży Pożarnej w Warszawie oraz jednostkach nadzorowanych przez Mazowieckiego Komendanta Wojewódzkiego Państwowej Straży Pożarnej

Niniejsza informacja jest związana z wypełnieniem obowiązków określonych w szczególności w art. 26 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), zwanego dalej także RODO.

Współadministratorzy danych i ich dane kontaktowe

Współadministratorami danych osobowych przetwarzanych w wspólnie użytkowanych systemach teleinformatycznych wykorzystywanych w Komendzie Wojewódzkiej Państwowej Straży Pożarnej w Warszawie oraz jednostkach nadzorowanych przez Mazowieckiego Komendanta Wojewódzkiego Państwowej Straży Pożarnej są Mazowiecki Komendant Wojewódzki Państwowej Straży Pożarnej oraz komendanci powiatowi (miejscy) Państwowej Straży Pożarnej województwa mazowieckiego, zwani dalej łącznie „Współadministratorami", a osobno „Współadministratorem".
Informacje o siedzibach i danych kontaktowych poszczególnych współadministratorów są dostępne na stronie https://www.gov.pl/web/kwpsp-warszawa/komendy-powiatowe-psp .
Dla każdego z Współadministratorów wyznaczony został Inspektor Ochrony Danych. Można się z nim skontaktować pisząc na adres poczty elektronicznej:

- w przypadku Komendy Miejskiej Państwowej Straży Pożarnej m. st. Warszawy - dpo@warszawa-straz.pl,
- w przypadku pozostałych Współadministratorów - ochrona.danych@mazowsze.straz.pl.

Wspólne uzgodnienia między Współadministratorami

Współadministratorzy, w drodze porozumienia, uzgodnili zakres odpowiedzialności oraz podział zadań związanych z przetwarzaniem danych osobowych w ramach wspólnie użytkowanych systemach teleinformatycznych. Zasadnicza treść uzgodnień jest dostępna na stronie internetowej każdego z współadministratorów oraz w jego siedzibie.

Cel, sposób i zakres przetwarzania

W wspólnie użytkowanych systemach informatycznych przetwarzane są dane osobowe pozyskane w związku z realizacją działań Współadministratorów prowadzonych w oparciu o przepisy prawa, w tym wynikające z zapisów art. 6 ust. 1 RODO. Celem działania jest zwiększenie efektywności działań przewidzianych w przepisach prawa realizowanych przez każdego z Współadministratorów, zmniejszenie obciążeń związanych z realizacją uprawnień i obowiązków przewidzianych w przepisach prawa, zapewnienie redukcji kosztów funkcjonowania, a także racjonalnego gospodarowania funduszami publicznymi. Cele zostały określone w oparciu o zapisy ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne i aktów wykonawczych do tej ustawy.

W ramach wspólnie użytkowanych systemów teleinformatycznych przetwarzane są dane osobowe pracowników i funkcjonariuszy zatrudnionych lub pełniących służbę u każdego z Współadministratorów, a także uczestników realizowanych przez Współadministratorów zadań z zakresu czynności kontrolno-rozpoznawczych w obiektach i na terenach, oraz z zakresu rozpoznawania zagrożeń innych miejscowych.

Każdy z Współadministratorów jest zobowiązany do wykonywania obowiązku informacyjnego w procesie pozyskiwania danych osobowych i ich dalszego przetwarzania, a także udostępnienia zasadniczej treści uzgodnień związanych z współadministrowaniem, osobom, których dane dotyczą.

Do wspólnie użytkowanych systemów teleinformatycznych zalicza się programy kadrowo-płacowe, programy związane z ewidencją majątku, umundurowania, odzieży specjalnej, środków ochrony indywidualnej i ekwipunku osobistego, a także programy wspierające realizację zadań z zakresu czynności kontrolno-rozpoznawczych w obiektach i na terenach oraz z zakresu rozpoznawania zagrożeń innych miejscowych wskazane w załączniku do porozumienia zawartego między Współadministratorami w sprawie współadministrowania danymi osobowymi przetwarzanymi w wspólnie użytkowanych systemach teleinformatycznych w jednostkach nadzorowanych przez Mazowieckiego Komendanta Wojewódzkiego Państwowej Straży Pożarnej.

Zasady przetwarzania danych osobowych

1. Współadministratorzy zobowiązują się do administrowania danymi osobowymi 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. Zbierane dane osobowe muszą być merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane.
5. Zabronione jest zbieranie wszelkich danych nieistotnych, niemających znaczenia, o większym stopniu szczegółowości niż wynika to z określonego celu.
6. 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.
7. Dane mogą być przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.
8. Okres przechowywania danych może zostać wydłużony nawet po osiągnięciu celu przetwarzania, jeżeli przepisy ustaw szczególnych takie postępowanie dopuszczają.
9. Dane osobowe mogą być przetwarzane po wcześniejszej rejestracji procesów z tym związanych w Rejestrze czynności przetwarzania.

Podział obowiązków współadministratorów oraz zakres ich odpowiedzialności

LP	Zadanie	Szczebel organizacyjny PSP	
		Mazowiecki Komendant Wojewódzki PSP	**Komendanci powiatowi i 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
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
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
5.	Zapewnienie rozliczalności operacji przetwarzania	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
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
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
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
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
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
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
14.	Kontrole i audyty	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
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 danym systemie teleinformatycznym;*
2. *prowadzenie szkoleń dla użytkowników w zakresie bezpieczeństwa teleinformatycznego oraz ochrony danych osobowych;*
3. *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;*
4. *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;*