

Warszawa, dnia piątek, 10 maja 2024 r.

Poz. 5

**ZARZĄDZENIE**  
**PREZESA URZĘDU OCHRONY KONKURENCJI**  
**I KONSUMENTÓW**

z dnia 9 maja 2024 r.

**w sprawie wprowadzenia Polityki ochrony danych osobowych w Urzędzie Ochrony**  
**Konkurencji i Konsumentów**

Na podstawie § 1 ust. 2 statutu Urzędu Ochrony Konkurencji i Konsumentów, stanowiącego załącznik do zarządzenia nr 272 Prezesa Rady Ministrów z dnia 20 grudnia 2019 r. w sprawie nadania statutu Urzędowi Ochrony Konkurencji i Konsumentów (M.P. z 2023 r. poz. 271) w związku z art. 24 ust. 1 i 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) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.<sup>1)</sup>) zarządza się, co następuje:

**§ 1.** W Urzędzie Ochrony Konkurencji i Konsumentów, zwanym dalej „Urzędem”, wprowadza się Politykę ochrony danych osobowych, stanowiącą załącznik nr 1 do zarządzenia.

---

<sup>1)</sup> Zmiany wymienionego rozporządzenia zostały ogłoszone w Dz. Urz. UE L 127 z 23.05.2018, str. 2 oraz Dz. Urz. UE L 74 z 04.03.2021, str. 35.

§ 2. Upoważnienia do przetwarzania danych osobowych wydane przed dniem wejścia w życie niniejszego zarządzenia zachowują moc do czasu wydania nowych upoważnień.

§ 3. Rejestr czynności przetwarzania danych osobowych w Urzędzie opracowany na podstawie przepisów dotychczasowych podlega dostosowaniu do wymogów niniejszego zarządzenia w terminach określonych w harmonogramie przygotowanym przez Inspektora Ochrony Danych Urzędu.

§ 4. Pracownicy Urzędu są zobowiązani do zapoznania się z treścią Polityki ochrony danych osobowych i złożenia oświadczenia stanowiącego załącznik nr 2 do zarządzenia w terminie 14 dni od dnia wejścia w życie niniejszego zarządzenia.

§ 5. Traci moc zarządzenie nr 19/2017 Prezesa Urzędu Ochrony Konkurencji i Konsumentów z dnia 1 sierpnia 2017 r. w sprawie Polityki Bezpieczeństwa Przetwarzania Danych Osobowych w Urzędzie Ochrony Konkurencji i Konsumentów zmienione zarządzeniem nr 14/2018 z dnia 24 maja 2018 r., zarządzeniem nr 9/2019 z dnia 12 marca 2019 r. i zarządzeniem Prezesa Urzędu Ochrony Konkurencji i Konsumentów z dnia 9 września 2022 r. (Dz. Urz. UOKiK poz. 6).

§ 6. Zarządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

**PREZES URZĘDU OCHRONY  
KONKURENCJI I KONSUMENTÓW**

*Tomasz Chróstny*

Załączniki do zarządzenia Prezesa Urzędu  
Ochrony Konkurencji i Konsumentów  
z dnia 9 maja 2024 r.

Załącznik nr 1

## **Polityka ochrony danych osobowych w Urzędzie Ochrony Konkurencji i Konsumentów**

### **Rozdział 1**

#### **Przepisy ogólne**

§ 1. 1. Polityka ochrony danych osobowych, zwana dalej „Polityką”, określa zasady przetwarzania danych osobowych, dla których Prezes Urzędu Ochrony Konkurencji i Konsumentów, zwany dalej „Prezesem Urzędu”, jest administratorem.

2. Politykę stosuje się w siedzibie głównej Urzędu Ochrony Konkurencji i Konsumentów, zwanego dalej „Urzędem”, w budynkach delegatur i laboratoriów oraz poza tymi lokalizacjami, w szczególności w ramach prowadzonych kontroli i przeszukań.

3. Politykę stosuje się do danych osobowych przetwarzanych:

- 1) w sposób całkowicie lub częściowo zautomatyzowany, w szczególności w systemach teleinformatycznych, poczcie elektronicznej, informatycznych nośnikach danych;
- 2) w sposób inny niż zautomatyzowany, stanowiących część zbioru danych lub mających stanowić część zbioru danych;
- 3) w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych oraz dokumentach Urzędu, stanowiących zbiory danych w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), zwanego dalej „RODO”.

4. Politykę stosuje się także do przetwarzanych w Urzędzie danych osobowych, których administratorem nie jest Prezes Urzędu, chyba że zawarte przez Prezesa Urzędu umowy lub porozumienia z administratorami danych stanowią inaczej.

§ 2. Polityka ma zapewniać zgodność przetwarzania danych osobowych w Urzędzie z przepisami prawa w zakresie ochrony danych osobowych, w szczególności z:

- 1) RODO;
- 2) ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781);

3) Systemem Zarządzania Bezpieczeństwem Informacji i przepisami wewnętrznymi obowiązującymi w Urzędzie mającymi wpływ na przetwarzanie danych osobowych.

§ 3. 1. Przetwarzanie danych osobowych odbywa się zgodnie z ogólnymi zasadami przetwarzania danych osobowych, o których mowa w art. 5 RODO, a w szczególności aby dane te były:

- 1) przetwarzane zgodnie z prawem, w oparciu o co najmniej jedną przesłankę legalności przetwarzania danych osobowych wskazaną w art. 6 lub art. 9 RODO (zasada legalności);
- 2) przetwarzane rzetelnie, rozumiane jako obowiązek starannego działania i należytego wypełniania obowiązków, ale także postępowanie uczciwe (zasada rzetelności);
- 3) przetwarzane w sposób przejrzysty dla osoby, której dane dotyczą (zasada przejrzystości), w szczególności poprzez realizowanie obowiązków informacyjnych wynikających z art. 13 i art. 14 RODO oraz w ramach uprawnień przysługujących osobom, których dane dotyczą wynikających z art. 15-22 RODO;
- 4) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami ze wskazaniem odpowiedniej podstawy dopuszczalności przetwarzania danych, o których mowa w art. 6, art. 9 i art. 10 RODO (zasada ograniczenia celu);
- 5) adekwatne, stosowne i ograniczone do tego, co niezbędne do celów, w których są przetwarzane (zasada minimalizacji danych);
- 6) prawidłowe i w razie potrzeby uaktualniane, w szczególności w trybie art. 16 RODO (zasada prawidłowości);
- 7) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą przez okres nie dłuższy, niż jest to niezbędne do osiągnięcia celów, w których są one przetwarzane, przy czym po osiągnięciu celu dane powinny zostać usunięte lub zanonimizowane (zasada ograniczenia przechowywania);
- 8) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem zgodnie z przepisami wewnętrznymi obowiązującymi w Urzędzie regulującymi zabezpieczenia techniczne i organizacyjne (zasada integralności i poufności).

2. Przetwarzanie danych osobowych powinno odbywać się w taki sposób, aby można było wykazać przestrzeganie zasad, o których mowa w ust. 1, zgodnie z zasadą rozliczalności.

§ 4. Politykę stosują wszystkie osoby, które na polecenie administratora przetwarzają dane osobowe w Urzędzie, w tym pracownicy, praktykanci, stażyści, wolontariusze oraz inne osoby wykonujące zadania na rzecz Prezesa Urzędu w ramach zawartych umów, porozumień lub innych zobowiązań.

§ 5. Środki techniczne i organizacyjne zapewniające bezpieczeństwo danych osobowych przetwarzanych w Urzędzie zostały określone w przepisach wewnętrznych obowiązujących w Urzędzie.

§ 6. Użyte w Polityce określenia i skróty oznaczają:

- 1) Administrator – Prezesa Urzędu;
- 2) dane osobowe – dane osobowe w rozumieniu art. 4 pkt 1 RODO;
- 3) IOD (Inspektor Ochrony Danych) – pracownika Urzędu wyznaczonego na podstawie art. 37 ust. 1 lit. a RODO;
- 4) kierujący komórką organizacyjną – dyrektora lub zastępcę dyrektora departamentu, biura lub delegatury Urzędu;
- 5) komórka organizacyjna – departament, biuro lub delegaturę Urzędu;
- 6) organ nadzorczy – Prezesa Urzędu Ochrony Danych Osobowych;
- 7) podmiot przetwarzający – osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora;
- 8) pracownik – osobę zatrudnioną w Urzędzie na podstawie umowy o pracę, mianowania, powołania, stażystę, wolontariusza, praktykanta lub osobę świadczącą usługi na podstawie umów, porozumień lub innych zobowiązań;
- 9) przetwarzanie danych osobowych – przetwarzanie w rozumieniu art. 4 pkt 2 RODO;
- 10) rejestr czynności przetwarzania danych osobowych – rejestr czynności przetwarzania danych osobowych w rozumieniu art. 30 ust. 1 RODO;
- 11) rejestr kategorii czynności przetwarzania danych osobowych – rejestr kategorii czynności przetwarzania danych osobowych w rozumieniu art. 30 ust. 2 RODO;
- 12) system teleinformatyczny – zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (D. U. z 2024 r. poz. 34);
- 13) umowa powierzenia przetwarzania danych osobowych – umowę lub porozumienie w sprawie powierzenia przetwarzania danych osobowych;
- 14) współadministrator – jeden z co najmniej dwóch administratorów wspólnie ustalających cele i sposoby przetwarzania, o którym mowa w art. 26 RODO.

## Rozdział 2

### Organizacja systemu bezpieczeństwa przetwarzania danych osobowych

§ 7. Za prawidłowość przetwarzania danych osobowych i ich ochronę w Urzędzie odpowiada Administrator.

§ 8. 1. W celu zapewnienia przestrzegania przepisów o ochronie danych osobowych w Urzędzie funkcjonuje IOD wyznaczony przez Administratora.

2. Administrator może wyznaczyć osobę zastępującą IOD, wykonującą zadania, o których mowa w ust. 3, wyłącznie w czasie nieobecności IOD.

3. IOD wykonuje zadania, o których mowa w art. 39 RODO, w szczególności:

- 1) informuje Administratora, podmiot przetwarzający oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów Unii Europejskiej lub przepisów krajowych o ochronie danych osobowych i doradza im w tej sprawie;
- 2) monitoruje przestrzeganie przepisów z zakresu ochrony danych osobowych, w tym RODO i Polityki;
- 3) udziela na żądanie zaleceń co do oceny skutków dla ochrony danych osobowych oraz monitoruje jej wykonanie, zgodnie z art. 35 RODO;
- 4) współpracuje z organem nadzorczym;
- 5) pełni funkcję punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych osobowych, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzi konsultacje w innych sprawach;
- 6) opiniuje projekty dokumentów rządowych, projekty wewnętrznych aktów prawnych i innych dokumentów związanych z ochroną danych osobowych;
- 7) opiniuje projekty umów i porozumień o współadministrowaniu danymi osobowymi oraz projekty umów powierzenia przetwarzania danych osobowych;
- 8) przygotowuje wzory umów powierzenia przetwarzania danych osobowych;
- 9) prowadzi rejestry, o których mowa w § 24 ust. 1, § 26 ust. 3 i § 43 ust. 1;
- 10) opracowuje roczny plan audytów, realizuje ten plan oraz sporządza z niego sprawozdanie;
- 11) sporządza i przekazuje Administratorowi raz na rok, do końca pierwszego kwartału za rok ubiegły, sprawozdanie z wykonywania zadań z zakresu ochrony i sposobu przetwarzania danych osobowych;
- 12) współpracuje z kierującymi komórkami organizacyjnymi w sprawach z zakresu ochrony danych osobowych;
- 13) zapewnia obsługę adresu e-mail: [iod@uokik.gov.pl](mailto:iod@uokik.gov.pl).

§ 9. 1. Kierujący komórką organizacyjną, w zakresie ochrony danych osobowych, w kierowanej komórce organizacyjnej, w szczególności:

- 1) sprawuje bieżący nadzór nad przetwarzaniem danych osobowych;
- 2) wdraża oraz nadzoruje przestrzeganie Polityki;
- 3) realizuje obowiązek informacyjny, o którym mowa w rozdziale 8;
- 4) informuje IOD o:
  - a) zdarzeniu, w którym doszło do naruszenia ochrony danych osobowych lub mogło dojść do naruszenia ochrony danych osobowych,
  - b) zmianach w zakresie, sposobie lub rodzaju przetwarzania danych osobowych,
  - c) pracach dotyczących planowania, projektowania lub przygotowania przedsięwzięć o charakterze programowym, projektowym lub legislacyjnym, jeżeli ich realizacja będzie związana z przetwarzaniem danych osobowych, w tym umożliwia IOD włączenie się w te prace;
- 5) identyfikuje i aktualizuje czynności przetwarzania danych osobowych w celu uwzględnienia w rejestrach, o których mowa w § 11 ust. 1 i § 12 ust. 1;
- 6) dokonuje przeglądu upoważnień do przetwarzania danych osobowych w celu zapewnienia ich aktualności;
- 7) przeprowadza analizę planowanego powierzenia przetwarzania danych osobowych;
- 8) przygotowuje projekty umów i porozumień o współadministrowanie danymi osobowymi oraz projekty umów powierzenia przetwarzania danych osobowych;
- 9) prowadzi rejestry, o których mowa w § 11 ust. 1 i § 12 ust. 1;
- 10) przeprowadza analizę ryzyka naruszenia praw lub wolności osób fizycznych, o której mowa w § 44 ust. 3 pkt 1;
- 11) przeprowadza ocenę skutków dla ochrony danych osobowych;
- 12) uwzględnia zalecenia IOD.

#### 2. Pracownicy:

- 1) przestrzegają przepisów z zakresu ochrony danych osobowych, w tym RODO i Polityki;
- 2) składają oświadczenie o zapoznaniu się z Polityką oraz o zobowiązaniu do zachowania w tajemnicy przetwarzanych danych osobowych;
- 3) przetwarzają dane osobowe zgodnie z zasadami, o których mowa w § 3 ust. 1;
- 4) przetwarzają dane osobowe w zakresie swojego upoważnienia i zgodnie z celami przetwarzania;
- 5) zgłaszają IOD zdarzenia, w których doszło do naruszenia ochrony danych osobowych lub mogło dojść do naruszenia ochrony danych osobowych;

6) biorą udział w audycie, o którym mowa w rozdziale 13, w tym umożliwiając IOD przeprowadzenie czynności w toku audytu.

3. Oświadczenie, o którym mowa w ust. 2 pkt 2, jest dołączane do akt pracowników.

**§ 10.** Nieprzestrzeganie Polityki może skutkować odpowiedzialnością dyscyplinarną lub inną odpowiedzialnością wynikającą z przepisów prawa.

### **Rozdział 3**

#### **Rejestr czynności przetwarzania danych osobowych i rejestr kategorii czynności przetwarzania danych osobowych**

**§ 11.** 1. Kierujący komórką organizacyjną, we współpracy z IOD, identyfikuje i aktualizuje czynności przetwarzania w celu uwzględnienia w rejestrze czynności przetwarzania danych osobowych, którego wzór określa załącznik nr 1 do Polityki.

2. Wzór zgłoszenia czynności przetwarzania danych osobowych określa załącznik nr 2 do Polityki.

**§ 12.** 1. Kierujący komórką organizacyjną, we współpracy z IOD, identyfikuje i aktualizuje czynności przetwarzania w celu uwzględnienia w rejestrze kategorii czynności przetwarzania danych osobowych, którego wzór określa załącznik nr 3 do Polityki.

2. Wzór zgłoszenia kategorii czynności przetwarzania danych osobowych określa załącznik nr 4 do Polityki.

**§ 13.** 1. IOD dokonuje przeglądu rejestrów, o których mowa w § 11 ust. 1 i § 12 ust. 1, w szczególności w przypadku zmian w przepisach powszechnie obowiązujących lub wprowadzenia istotnych zmian organizacyjnych w Urzędzie.

2. Rejestry, o których mowa w § 11 ust. 1 i § 12 ust. 1, są prowadzone w formie elektronicznej.

### **Rozdział 4**

#### **Udzielanie upoważnień do przetwarzania danych osobowych i ewidencja osób upoważnionych**

**§ 14.** 1. Do przetwarzania danych osobowych mogą być dopuszczone jedynie osoby posiadające imienne upoważnienie w formie pisemnej lub elektronicznej udzielone przez Administratora albo osobę przez niego upoważnioną, z zastrzeżeniem ust. 2.

2. Administrator upoważnia:

- 1) Wiceprezesów Urzędu, Dyrektora Generalnego Urzędu, kierujących komórkami organizacyjnymi, IOD do przetwarzania danych osobowych w zakresie wynikającym z realizacji powierzonych zadań;
- 2) pracowników do przetwarzania danych osobowych w zakresie wynikającym z realizacji powierzonych zadań dotyczących:



- a) petycji, skarg, wniosków,
  - b) interwencji, interpelacji, zapytań poselskich i oświadczeń senatorskich,
  - c) wniosków o udostępnienie informacji publicznej,
  - d) wniosków i wystąpień o charakterze ogólnym;
- 3) pracowników w komórce organizacyjnej właściwej do spraw obsługi prawnej do przetwarzania danych osobowych w zakresie wynikającym z realizacji powierzonych zadań.
3. Wzór upoważnienia, o którym mowa w ust. 1, określa załącznik nr 5 do Polityki.

**§ 15.** 1. Do złożenia wniosku o udzielenie upoważnienia do przetwarzania danych osobowych jest obowiązany kierujący komórką organizacyjną, w której zatrudniony jest pracownik objęty wnioskowaniem.

2. Upoważnienie, o którym mowa w § 14 ust. 1, jest udzielane na podstawie wniosku zatwierdzonego przez kierującego komórką organizacyjną.

3. Wzór wniosku określa załącznik nr 6 do Polityki.

**§ 16.** 1. Na wniosek kierującego komórką organizacyjną Administrator albo osoba przez niego upoważniona może odwołać udzielone upoważnienie, o którym mowa w § 14 ust. 1, w szczególności w przypadku niewłaściwego przetwarzania danych osobowych przez osobę upoważnioną.

2. Wzór wniosku określa załącznik nr 7 do Polityki.

**§ 17.** 1. Upoważnienie, o którym mowa w § 14 ust. 1, traci moc w przypadku:

- 1) ustania stosunku pracy;
- 2) przeniesienia pracownika do innej komórki organizacyjnej w Urzędzie;
- 3) zmiany zakresu obowiązków pracownika powodujących zaprzestanie czynności przetwarzania danych osobowych, do którego upoważnienie posiada;
- 4) wygaśnięcia upoważnienia wydanego na czas określony.

2. Kierujący komórką organizacyjną niezwłocznie informuje Administratora albo osobę przez niego upoważnioną o okolicznościach, o których mowa w ust. 1.

**§ 18.** 1. Administrator albo osoba przez niego upoważniona prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych, której wzór określa załącznik nr 8 do Polityki.

2. Ewidencja jest prowadzona w formie elektronicznej.

## **Rozdział 5**

### **Powierzenie przetwarzania danych osobowych**

**§ 19.** 1. Powierzenie przetwarzania danych osobowych odbywa się zgodnie z art. 28 RODO.

2. Określenie zadań i obowiązków Administratora i podmiotu przetwarzającego wymaga zawarcia umowy w formie pisemnej lub elektronicznej.

3. W Urzędzie funkcjonuje wzór umowy powierzenia przetwarzania danych osobowych, który jest dostępny na stronie intranetowej Urzędu.

**§ 20.** 1. Kierujący komórką organizacyjną konsultuje z IOD konieczność zawarcia umowy powierzenia przetwarzania danych osobowych.

2. Kierujący komórką organizacyjną przygotowuje projekt umowy powierzenia przetwarzania danych osobowych i jest obowiązany uzyskać opinię IOD.

3. Kierujący komórką organizacyjną jest obowiązany uzyskać opinię IOD także w przypadku projektu umowy, w którym wprowadzono istotne modyfikacje względem wzoru umowy, o którym mowa w § 19 ust. 3, w szczególności dokonano zmiany elementów umowy, które nie zostały przewidziane do modyfikacji.

**§ 21.** 1. Kierujący komórką organizacyjną, realizując zadania skutkujące powierzeniem przetwarzania danych osobowych innemu podmiotowi, odpowiada za wybór podmiotu przetwarzającego, który zapewni wystarczającą gwarancję wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie chroniło prawa osób, których dane dotyczą.

2. Warunkiem dopuszczalności powierzenia przetwarzania danych osobowych jest poddanie planowanego powierzenia analizie wskazującej, że wybór podmiotu przetwarzającego zostanie uzależniony od zapewnienia gwarancji, o których mowa w ust. 1. Przeprowadzając analizę kierujący komórką organizacyjną dokonuje oceny podmiotu przetwarzającego na podstawie:

- 1) arkusza oceny podmiotu przetwarzającego;
- 2) oświadczeń podmiotu przetwarzającego o określonej treści;
- 3) sprawdzenia przedwdrożeniowego stosowania przez podmiot przetwarzający określonych standardów, praktyk, certyfikatów, norm;
- 4) innego sposobu umożliwiającego dokonanie oceny podmiotu przetwarzającego.

3. W Urzędzie funkcjonuje arkusz oceny podmiotu przetwarzającego, który jest dostępny na stronie intranetowej Urzędu.

4. Arkusz oceny podmiotu przetwarzającego może być przekazany temu podmiotowi na każdym etapie wykonywania umowy powierzenia przetwarzania danych osobowych.

5. Analiza planowanego powierzenia przetwarzania danych osobowych jest przeprowadzana we współpracy z IOD.

**§ 22.** Kierujący komórką organizacyjną sprawuje nadzór nad podmiotem przetwarzającym w zakresie wynikającym z umowy powierzenia przetwarzania danych osobowych.

**§ 23.** Oryginał umowy powierzenia przetwarzania danych osobowych przechowuje komórka organizacyjna zawierająca umowę, chyba że przepisy wewnętrznie obowiązujące w Urzędzie dotyczące przechowywania umów określają inny tryb, a jej kopię niezwłocznie udostępnia IOD.

- § 24.** 1. IOD prowadzi rejestr zawartych umów powierzenia przetwarzania danych osobowych.
2. Wzór rejestru określa załącznik nr 9 do Polityki.
  3. Rejestr jest prowadzony w formie elektronicznej.

## **Rozdział 6**

### **Współadministrowanie danymi osobowymi**

**§ 25.** 1. Współadministrowanie danymi osobowymi odbywa się zgodnie z art. 26 RODO.

2. Współadministrowanie danymi osobowymi wymaga zawarcia umowy lub porozumienia w formie pisemnej lub elektronicznej.

**§ 26.** 1. Kierujący komórką organizacyjną przygotowuje projekt umowy lub porozumienia o współadministrowanie i konsultuje go z IOD.

2. Oryginał umowy lub porozumienia o współadministrowanie przechowuje komórka organizacyjna, która je zawiera, a ich kopię niezwłocznie udostępnia IOD.

3. IOD prowadzi rejestr zawartych umów i porozumień o współadministrowanie danymi osobowymi.

4. Wzór rejestru określa załącznik nr 9 do Polityki.
5. Rejestr jest prowadzony w formie elektronicznej.

## **Rozdział 7**

### **Przekazanie danych osobowych do państw trzecich lub organizacji międzynarodowej**

**§ 27.** Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych może odbywać się jedynie zgodnie z zasadami wskazanymi w rozdziale V RODO.

**§ 28.** 1. Kierujący komórką organizacyjną jest obowiązany uzyskać opinię IOD czy istnieje podstawa prawna uprawniająca do przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej przed dokonaniem przekazania.

2. W przypadku braku podstawy prawnej stwierdzającej zapewnienie odpowiedniego stopnia ochrony danych, kierujący komórką organizacyjną, po zasięgnięciu opinii IOD, może przekazać dane osobowe do państwa trzeciego lub organizacji międzynarodowej wyłącznie, gdy zapewnią odpowiednie zabezpieczenia w rozumieniu art. 46 ust. 2 RODO, i pod warunkiem, że obowiązują egzekwowlalne prawa osób, których dane dotyczą, i skuteczne środki ochrony prawnej.

## Rozdział 8

### Obowiązek informacyjny

**§ 29 . 1.** Administrator podejmuje niezbędne środki w zakresie wypełnienia obowiązku informacyjnego, o którym mowa w art. 13 i art. 14 RODO, wobec osoby, której dane dotyczą tak, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, niespecjalistycznym językiem przekazać informacje, o których mowa w art. 13 RODO (w przypadku zbierania danych osobowych od osoby, której dane dotyczą) i art. 14 RODO (w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą).

2. Informacji, o których mowa w ust. 1, udziela się w formie pisemnej lub elektronicznej.

**§ 30. 1.** Obowiązek informacyjny jest realizowany poprzez dołączenie klauzuli informacyjnej właściwej dla danego procesu przetwarzania danych osobowych.

2. Klauzule informacyjnie są dostępne na stronie intranetowej Urzędu.

3. Za aktualność i zgodność z przepisami klauzul informacyjnych funkcjonujących w Urzędzie odpowiada kierujący komórką organizacyjną.

4. Treść klauzul informacyjnych jest uzgadniana z IOD.

**§ 31. 1.** Za realizację obowiązku informacyjnego odpowiada kierujący komórką organizacyjną, w której dane osobowe będą przetwarzane.

2. Realizacja obowiązku informacyjnego jest wykonywana we współpracy z IOD.

3. Kierujący komórką organizacyjną dokumentuje realizację obowiązku informacyjnego, zgodnie z zasadą rozliczalności.

4. W przypadku właściwości kilku komórek organizacyjnych, obowiązek informacyjny realizuje komórka udzielająca zbiorczej odpowiedzi.

**§ 32. 1.** W przypadku zbierania danych osobowych bezpośrednio od osoby, której dane dotyczą, kierujący komórką organizacyjną jest obowiązany do wypełnienia wobec tej osoby obowiązku informacyjnego przez przekazanie podczas pozyskiwania danych klauzuli informacyjnej zawierającej informacje, o których mowa w art. 13 RODO.

2. W przypadku zbierania danych osobowych nie od osoby, której dane dotyczą, kierujący komórką organizacyjną jest obowiązany do wypełnienia wobec tej osoby obowiązku informacyjnego, o którym mowa w art. 14 RODO, przez przekazanie klauzuli informacyjnej:

1) w rozsądnym terminie po pozyskaniu danych osobowych - najpóźniej w ciągu miesiąca - mając na uwadze konkretne okoliczności przetwarzania danych osobowych;

- 2) jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą - najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą;
- 3) jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu.

**§ 33.** Obowiązek informacyjny nie jest realizowany, jeżeli istnieją przesłanki zwalniające z tego obowiązku, o których mowa w art. 13 ust. 4 i art. 14 ust. 5 RODO.

## **Rozdział 9**

### **Realizacja praw osób, których dane osobowe dotyczą**

**§ 34.** 1. Każda osoba, której dane osobowe są przetwarzane w Urzędzie, ma prawo do informacji o fakcie i zakresie przetwarzania tych danych. Urząd realizuje to prawo wypełniając obowiązek informacyjny.

2. Zakres danych przekazywanych w ramach realizacji obowiązku informacyjnego zależy od sposobu pozyskania danych osobowych.

**§ 35.** 1. Administrator umożliwia osobom, których dane dotyczą wykonywanie praw przysługujących im na mocy przepisów RODO, w tym postępowania w przypadku złożenia przez osobę, której dane dotyczą żądania realizacji jej praw przysługujących na mocy art. 7 i art. 15-22 RODO oraz postępowania w przypadku konieczności zawiadomienia osoby fizycznej o naruszeniu jej danych osobowych na mocy art. 34 RODO (prawo do bycia poinformowanym o naruszeniu danych osobowych).

2. Osobie, której dane dotyczą przysługuje prawo do żądania:

- 1) dostępu do danych;
- 2) kopii przetwarzania danych;
- 3) sprostowania danych i bycia poinformowanym o sprostowaniu danych;
- 4) usunięcia danych (prawo do bycia zapomnianym) i bycia poinformowanym o usunięciu danych;
- 5) ograniczenia przetwarzania danych i bycia poinformowanym o ograniczeniu przetwarzania danych;
- 6) przenoszenia danych;
- 7) złożenia sprzeciwu na przetwarzanie danych;
- 8) niepodlegania zautomatyzowanemu podejmowaniu decyzji;
- 9) bycia poinformowanym o naruszeniu danych osobowych;
- 10) wycofania zgody na przetwarzanie danych osobowych;
- 11) bycia poinformowanym o administratorze danych, o celach oraz okresie przetwarzania danych osobowych (klauzula informacyjna).

3. Realizacja praw, o których mowa w ust. 2, odbywa się na podstawie wniosku osoby, której dane dotyczą, w formie pisemnej lub elektronicznej.

## **Rozdział 10**

### **Postępowanie w przypadku naruszenia ochrony danych osobowych lub ich bezpieczeństwa**

**§ 36.** 1. Pracownik jest obowiązany do natychmiastowego zgłoszenia IOD każdego zdarzenia stanowiącego naruszenie ochrony danych osobowych lub mogącego stanowić naruszenie ochrony danych osobowych na adres [iod@uokik.gov.pl](mailto:iod@uokik.gov.pl).

2. Pracownik o zgłoszeniu informuje także bezpośredniego przełożonego i kierującego komórką organizacyjną, w której jest zatrudniony.

3. Wzór zgłoszenia określa załącznik nr 10 do Polityki.

**§ 37.** Naruszeniem ochrony danych osobowych, o którym mowa w § 36 ust. 1, mogą być w szczególności przypadki, gdy:

- 1) dane osobowe są przetwarzane bez upoważnienia lub niezgodnie z jego zakresem;
- 2) nastąpiło nieuprawnione udostępnienie danych osobowych lub nastąpiła kradzież danych;
- 3) wystąpiło zniszczenie, uszkodzenie, utrata, modyfikacja lub nieuprawnione kopiowanie danych;
- 4) stwierdzono nieprzestrzeganie zasad ochrony danych osobowych.

**§ 38.** 1. Pracownik po dokonaniu zgłoszenia, o którym mowa w § 36 ust. 1, jest obowiązany w szczególności do:

- 1) powstrzymania się od rozpoczęcia lub kontynuowania pracy, jak również do podejmowania jakichkolwiek czynności mogących mieć wpływ na ustalenie przyczyn zaistniałego zdarzenia;
- 2) podjęcia niezbędnych działań w celu zapobieżenia dalszym naruszeniom;
- 3) udzielenia IOD niezbędnych wyjaśnień dotyczących zaistniałego zdarzenia;
- 4) zebrania danych, dokumentów i dowodów mających na celu umożliwienie przeprowadzenia postępowania wyjaśniającego.

2. Pracownik, który dokonał zgłoszenia podejmuje wraz z IOD niezbędne czynności w celu udokumentowania zdarzenia stanowiącego naruszenie ochrony danych osobowych lub mogącego stanowić naruszenie ochrony danych osobowych, w tym okoliczności wystąpienia zdarzenia, jego skutki oraz podjęte działania zaradcze.

**§ 39.** 1. Po otrzymaniu zgłoszenia, o którym mowa w § 36 ust. 1, IOD niezwłocznie wszczyna i prowadzi postępowanie wyjaśniające.

2. IOD podejmuje działania w celu oceny czy zgłoszone zdarzenie stanowi naruszenie ochrony danych osobowych oraz oceny wagi naruszenia, a także czy wymaga poinformowania organu nadzorczego oraz osób, których dane dotyczą.

3. IOD, w ramach przeprowadzanego postępowania wyjaśniającego, jest uprawniony w szczególności do:

- 1) wystąpienia o dodatkowe wyjaśnienia do pracownika, który dokonał zgłoszenia oraz do innych osób, których wyjaśnienia mogą mieć wpływ na ocenę zdarzenia, wskazując termin na przekazanie wyjaśnień;
- 2) żądania przekazania przez właściwą komórkę organizacyjną dowodów wystąpienia zdarzenia stanowiącego naruszenie ochrony danych osobowych lub mogącego stanowić naruszenie ochrony danych osobowych;
- 3) dokonania sprawdzenia, w szczególności uzyskania dostępu do pomieszczeń, urządzeń i systemów teleinformatycznych lub dokumentacji, z uwzględnieniem zachowania prywatności;
- 4) nakazania powstrzymania się od kontynuowania pracy w zakresie przetwarzania danych osobowych;
- 5) czasowego odebrania lub ograniczenia uprawnień wskazanym użytkownikom lub wszystkim użytkownikom danego systemu teleinformatycznego.

**§ 40.** 1. Z przeprowadzonego postępowania wyjaśniającego oraz dokonanej oceny wagi naruszenia ochrony danych osobowych IOD sporządza notatkę i niezwłocznie przedkłada Administratorowi oraz do wiadomości Dyrektorowi Generalnemu Urzędu.

2. W przypadku naruszenia ochrony danych osobowych, Administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia - zgłasza je organowi nadzorcemu.

3. Kierujący komórką organizacyjną, we współpracy z IOD, zawiadamia osoby, których dane dotyczą o naruszeniu ochrony danych osobowych, zgodnie z art. 34 RODO.

**§ 41.** 1. IOD, w imieniu Administratora, przekazuje zalecenia zawarte w notatce, o której mowa w § 40 ust. 1, kierującemu komórką organizacyjną, w której doszło do naruszenia ochrony danych osobowych i kierującemu komórką organizacyjną, której zakres realizowanych zadań może mieć wpływ na minimalizację ryzyka wystąpienia naruszenia w przyszłości.

2. Kierujący komórką organizacyjną, w terminie 7 dni kalendarzowych od dnia otrzymania zaleceń, ustala sposób i termin ich realizacji, powiadamiając o tym w formie pisemnej IOD.

3. W przypadku odmowy realizacji zaleceń, kierujący komórką organizacyjną przedstawia, w terminie 7 dni kalendarzowych od dnia otrzymania zaleceń, swoje stanowisko w formie pisemnej IOD i Administratorowi.

4. W sytuacji, o której mowa w ust. 3, Administrator podejmuje decyzję dotyczącą realizacji zaleceń, informując o tym kierującego komórką organizacyjną i IOD.

**§ 42.** W przypadkach gdy po dokonaniu zgłoszeniu, o którym mowa w § 36 ust. 1, IOD nie stwierdzi naruszenia ochrony danych osobowych, sporządza notatkę i niezwłocznie przedkłada Administratorowi oraz do wiadomości Dyrektorowi Generalnemu Urzędowi.

**§ 43.** 1. IOD, w imieniu Administratora, prowadzi rejestr incydentów i naruszeń ochrony danych osobowych, w którym dokumentuje zdarzenia mogące stanowić naruszenie ochrony danych osobowych oraz w których stwierdzono naruszenie ochrony danych osobowych, w szczególności okoliczności zdarzenia, jego skutki oraz podjęte działania zaradcze.

2. Wzór rejestru stanowi załącznik nr 11 do Polityki.

3. Rejestr jest prowadzony w formie elektronicznej.

## **Rozdział 11**

### **Analiza ryzyka w zakresie ochrony danych osobowych**

**§ 44.** 1. W Urzędzie przetwarzanie danych osobowych odbywa się z uwzględnieniem ryzyka naruszenia praw lub wolności osób fizycznych.

2. Analizę ryzyka naruszenia praw lub wolności osób fizycznych przeprowadza się podczas:

- 1) planowania nowej czynności przetwarzania danych osobowych;
- 2) planowania zmian w zarejestrowanej czynności przetwarzania danych osobowych;
- 3) naruszenia ochrony danych osobowych.

3. Analiza ryzyka naruszenia praw lub wolności osób fizycznych jest przeprowadzana przez:

- 1) kierującego komórką organizacyjną odpowiadającą za realizację czynności przetwarzania danych osobowych, we współpracy z IOD - w przypadkach określonych w ust. 2 pkt 1 i 2;
- 2) Administratora, po zasięgnięciu opinii IOD - w przypadku określonym w ust. 2 pkt 3.

**§ 45.** Analizy ryzyka naruszenia praw lub wolności osób fizycznych dokonuje się nie rzadziej niż raz w roku oraz w przypadku wprowadzenia istotnych zmian w czynności przetwarzania danych osobowych, w szczególności dotyczących:

- 1) rozszerzenia zakresu przetwarzanych danych osobowych;
- 2) zmiany celu przetwarzania danych osobowych;
- 3) zmiany podstawy prawnej przetwarzania danych osobowych;
- 4) zmiany środków organizacyjnych i technicznych;
- 5) zmiany otoczenia prawnego.

**§ 46.** Analizę ryzyka naruszenia praw lub wolności osób fizycznych przeprowadza się zgodnie z przepisami wewnętrznymi obowiązującymi w Urzędzie.



## **Rozdział 12**

### **Przeprowadzenie oceny skutków dla ochrony danych osobowych**

§ 47. 1. Ocenę skutków dla ochrony danych osobowych planowanych procesów przetwarzania przeprowadza się, jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii - ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych.

2. Ocena skutków dla ochrony danych osobowych jest przeprowadzana przez kierującego komórką organizacyjną Urzędu, w której będzie odbywało się lub odbywa się przetwarzanie danych osobowych wymagające przeprowadzenia tej oceny.

3. Kierujący komórką organizacyjną realizujący proces wskazany w ust. 1 konsultuje z IOD zasadność przeprowadzenia oceny skutków dla ochrony danych osobowych.

4. Ocenę skutków dla ochrony danych osobowych konsultuje się z IOD i dokonuje się zgodnie z jego zaleceniami.

§ 48. Jeżeli przeprowadzona ocena skutków dla ochrony danych osobowych wskaże, że przetwarzanie powodowałoby wysokie ryzyko naruszenia praw i wolności osób fizycznych, gdyby Administrator nie zastosował środków w celu zminimalizowania tego ryzyka, przed rozpoczęciem przetwarzania Administrator konsultuje się z organem nadzorczym, zgodnie z art. 36 RODO.

## **Rozdział 13**

### **Audyty zgodności przetwarzania danych osobowych**

§ 49. Audyt zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz Polityki jest przeprowadzany przez IOD.

§ 50. 1. IOD opracowuje roczny plan audytów, który przedstawia do wiadomości Administratorowi najpóźniej do końca roku kalendarzowego poprzedzającego rok objęty tym planem.

2. Roczny plan audytów określa:

- 1) przedmiot, zakres oraz termin przeprowadzenia poszczególnych audytów;
- 2) czynności przetwarzania danych osobowych objęte audytem;
- 3) konieczność weryfikacji zgodności przetwarzania danych osobowych z:
  - a) zasadami przetwarzania danych osobowych,
  - b) zasadami dotyczącymi zabezpieczenia danych osobowych,
  - c) zasadami przekazywania danych osobowych.

§ 51. 1. IOD zawiadamia kierującego komórką organizacyjną objętą audytem o zakresie planowanych czynności w terminie co najmniej 7 dni przed dniem przeprowadzenia czynności.

2. IOD dokumentuje czynności przeprowadzone podczas audytu w komórce organizacyjnej objętej audytem.

3. Materiały dokumentujące czynności przeprowadzane podczas audytu są sporządzane w formie pisemnej lub elektronicznej.

**§ 52.** 1. Z przeprowadzonego audytu IOD sporządza sprawozdanie zawierające w szczególności ocenę i zalecenia w odniesieniu do zakresu objętego audytem.

2. Sprawozdanie, o którym mowa w ust. 1, jest przedkładane kierującemu komórką organizacyjną objętą audytem.

**§ 53.** IOD przedkłada Administratorowi roczne sprawozdanie z przeprowadzonych audytów w terminie do końca marca następnego roku kalendarzowego.

## **Rozdział 14**

### **Szkolenia**

**§ 54.1.** Administrator zapewnia szkolenia dla pracowników w zakresie obowiązujących przepisów oraz podstawowych zagrożeń związanych z przetwarzaniem danych osobowych.

2. Szkolenia prowadzi IOD lub podmiot zewnętrzny posiadający wiedzę z zakresu ochrony danych osobowych.

Załączniki do Polityki  
ochrony danych osobowych  
w Urzędzie Ochrony Konkurencji  
i Konsumentów

Załącznik nr 1

**Wzór**

<b>Rejestr czynności przetwarzania danych osobowych w Urzędzie Ochrony Konkurencji i Konsumentów</b>
--

<b>Nazwa i dane kontaktowe Administratora Danych</b>	
<b>Nazwa</b>	
<b>Adres</b>	
<b>Email</b>	
<b>Telefon</b>	

<b>Inspektor Ochrony Danych</b>	
<b>Nazwa</b>	
<b>Adres</b>	
<b>Email</b>	
<b>Telefon</b>	

<b>Lp.</b>	<b>INFORMACJE ZNAJDUJĄCE SIĘ W REJESTRZE ORAZ PODSTAWA PRAWNA Z RODO</b>		
1.	<b>Nazwa czynności przetwarzania</b>		
2.	<b>Komórka organizacyjna</b>		
3.	<b>Cel przetwarzania</b>	art. 30 ust. 1 pkt b	
4.	<b>Kategorie osób</b>	art. 30 ust. 1 pkt c	
5.	<b>Kategorie danych osobowych</b>	art. 30 ust. 1 pkt c	
6.	<b>Podstawa prawna</b>		
7.	<b>Źródło danych (dane zbierane bezpośrednio lub z innych źródeł)</b>		
8.	<b>Planowany termin usunięcia danych osobowych</b>	art. 30 ust. 1 pkt f	
9.	<b>Nazwa współadministratora i dane kontaktowe</b>	art. 30 ust. 1 pkt a	
10.	<b>Nazwa podmiotu przetwarzającego (procesora) i dane kontaktowe</b>	art. 30 ust. 1 pkt d	
11.	<b>Kategorie odbiorców danych</b>	art. 30 ust. 1 pkt d	
12.	<b>Nazwa systemu teleinformatycznego lub oprogramowania</b>		
13.	<b>Ogólny opis organizacyjnych i technicznych środków bezpieczeństwa zgodnie z art. 32 ust. 1 RODO</b>	art. 30 ust. 1 pkt g	
14.	<b>Ocena skutków dla ochrony danych osobowych (jeśli tak lokalizacja raportu)</b>	art. 35	
15.	<b>Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu)</b>	art. 30 ust. 1 pkt e	
16.	<b>Jeśli transfer i art. 49 ust. 1 akapit drugi - dokumentacja odpowiednich zabezpieczeń</b>	Art. 30 ust. 1 pkt e	

Załącznik nr 2

## Wzór

## Zgłoszenie czynności przetwarzania danych osobowych

<b>DANE CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH</b>	
<b>Nazwa czynności przetwarzania</b>	
<b>Komórka organizacyjna (jednostki wewnętrzne)</b>	
<b>Cel przetwarzania</b>	
<b>Kategorie osób</b>	
<b>Kategorie danych</b>	
<b>Podstawa prawna</b>	
<b>Źródło danych</b>	
<b>Planowany termin usunięcia kategorii danych (jeśli jest to możliwe)</b>	
<b>Nazwa współadministratora i dane kontaktowe (jeśli dotyczy)</b>	
<b>Nazwa podmiotu przetwarzającego i dane kontaktowe</b>	
<b>Kategorie odbiorców danych</b>	
<b>Nazwa systemu teleinformatycznego lub oprogramowania</b>	
<b>Ogólny opis organizacyjnych i technicznych środków bezpieczeństwa zgodnie z art. 32 ust. 1 RODO</b>	
<b>Ocena skutków dla ochrony danych osobowych (jeśli tak lokalizacja raportu)</b>	
<b>Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu)</b>	

(data i podpis kierującego komórką organizacyjną)

Załącznik nr 3

**Wzór**

<b>Rejestr kategorii czynności przetwarzania danych osobowych w Urzędzie Ochrony Konkurencji i Konsumentów</b>
--

<b>Nazwa i dane kontaktowe podmiotu przetwarzającego</b>	
--	--

<b>Nazwa</b>	
<b>Adres</b>	
<b>Email</b>	
<b>Telefon</b>	

<b>Inspektor Ochrony Danych</b>	
---------------------------------	--

<b>Nazwa</b>	
<b>Adres</b>	
<b>Email</b>	
<b>Telefon</b>	

<b>Lp.</b>	<b>INFORMACJE ZNAJDUJĄCE SIĘ W REJESTRZE ORAZ PODSTAWA PRAWNA Z RODO</b>		
1.	<b>Nazwa kategorii przetwarzania</b>	<b>art. 30 ust. 2 lit. b</b>	
2.	<b>Administrator danych (nazwa i dane kontaktowe administratora, nazwa i dane kontaktowe współadministratora – jeśli dotyczy, nazwa i dane kontaktowe przedstawiciela administratora, IOD administratora (jeśli dotyczy))</b>	<b>art. 30 ust. 2 lit. a</b>	
3.	<b>Komórka organizacyjna</b>		
4.	<b>Cel przetwarzania</b>		
5.	<b>Kategorie osób</b>		
6.	<b>Kategorie danych osobowych</b>		
7.	<b>Podstawa prawna</b>		
8.	<b>Źródło danych (dane zbierane bezpośrednio lub z innych źródeł)</b>		
9.	<b>Planowany termin usunięcia danych osobowych</b>		
10.	<b>Nazwa współadministratora i dane kontaktowe</b>		
11.	<b>Nazwa podmiotu przetwarzającego (procesora) i dane kontaktowe</b>		
12.	<b>Kategorie odbiorców danych</b>		
13.	<b>Nazwa systemu teleinformatycznego lub oprogramowania</b>		
14.	<b>Ogólny opis organizacyjnych i technicznych środków bezpieczeństwa zgodnie z art. 32 ust. 1 RODO</b>	<b>art. 30 ust. 2 lit. d</b>	
15.	<b>Ocena skutków dla ochrony danych osobowych (jeśli tak lokalizacja raportu)</b>		
16.	<b>Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu)</b>	<b>art. 30 ust. 2 lit. c</b>	
17.	<b>Jeśli transfer i art. 49 ust. 1 akapit drugi - dokumentacja odpowiednich zabezpieczeń</b>	<b>art. 30 ust. 2 lit. c</b>	

Załącznik nr 4

**Wzór****Zgłoszenie kategorii czynności przetwarzania danych osobowych**

<b>DANE KATEGORII CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH</b>	
<b>Nazwa kategorii przetwarzania</b>	
<b>Nazwa administratora danych</b>	
<b>Komórka organizacyjna (jednostki wewnętrzne)</b>	
<b>Cel przetwarzania</b>	
<b>Kategorie osób</b>	
<b>Kategorie danych</b>	
<b>Podstawa prawna</b>	
<b>Źródło danych</b>	
<b>Planowany termin usunięcia kategorii danych (jeśli jest to możliwe)</b>	
<b>Nazwa współadministratora i dane kontaktowe (jeśli dotyczy)</b>	
<b>Nazwa podmiotu przetwarzającego i dane kontaktowe</b>	
<b>Kategorie odbiorców danych</b>	
<b>Nazwa systemu teleinformatycznego lub oprogramowania</b>	
<b>Ogólny opis organizacyjnych i technicznych środków bezpieczeństwa zgodnie z art. 32 ust. 1 RODO</b>	
<b>Ocena skutków dla ochrony danych osobowych (jeśli tak lokalizacja raportu)</b>	
<b>Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu)</b>	

(data i podpis kierującego komórką organizacyjną)



Załącznik nr 5

**Wzór**



Prezes Urzędu Ochrony  
Konkurencji i Konsumentów

**Warszawa, .....**

**UPOWAŻNIENIE  
DO PRZETWARZANIA DANYCH OSOBOWYCH**

.....  
**(znak sprawy)**

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.) w

**URZĘDZIE OCHRONY KONKURENCJI i KONSUMENTÓW**

.....  
otrzymuje Pani/Pan: [imię i nazwisko]  
zatrudniona/zatrudniony w: [komórka organizacyjna]

z dniem ..... upoważnienie do przetwarzania danych osobowych. Upoważnienie obejmuje przetwarzanie danych osobowych w formie papierowej i elektronicznej w zakresie niezbędnym do realizacji zadań wynikających z umowy, obejmujące następujące czynności przetwarzania:

- .....
- .....
- .....
- .....
- .....
- .....
- .....
- .....
- .....
- do innych czynności niezbędnych do wykonywania zadań zleconych przez przełożonego.

Upoważnienie jest ważne na czas zatrudnienia w komórce organizacyjnej i wykonywania wskazanych czynności. Pracownik zapoznał się z Polityką ochrony danych osobowych oraz zobowiązał się do zachowania tajemnicy składając na tę okoliczność oświadczenie według wzoru stanowiącego załącznik nr 2 do zarządzenia Prezesa Urzędu Ochrony Konkurencji i Konsumentów z dnia ..... w sprawie wprowadzenia Polityki ochrony danych osobowych w Urzędzie Ochrony Konkurencji i Konsumentów.

.....  
(podpis Administratora danych osobowych)

Załącznik nr 6

**Wzór**

**WNIOSEK O UDZIELENIE UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH**  
dla

.....  
(imię i nazwisko)

Zgodnie z art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.)

Dane	
Nazwa komórki organizacyjnej	
Rodzaj zatrudnienia/inny stosunek prawny (pracownik, praktykant, stażysta, zleceniobiorca, inna [jaka?])	
<b>Zakres upoważnienia powinien objąć dane osobowe niezbędne do wykonywania następujących czynności przetwarzania danych osobowych (należy wskazać poszczególne czynności przetwarzania zwarte w rejestrze czynności przetwarzania danych osobowych dla danej komórki organizacyjnej):</b> <ul style="list-style-type: none"> <li>➤ .....</li> <li>➤ .....</li> <li>➤ .....</li> <li>➤ .....</li> <li>➤ .....</li> </ul>	
Wnioskowana data rozpoczęcia obowiązywania upoważnienia	<b>dd-mm-rrrr</b>
Wnioskowana data zakończenia obowiązywania upoważnienia	<input type="checkbox"/> <b>dd-mm-rrrr (w przypadku umowy zlecenia, umowy na staż, praktykę i wolontariat)</b>
	<input type="checkbox"/> <b>Upoważnienie na czas wykonywania obowiązków we wnioskującej komórce organizacyjnej w Urzędzie Ochrony Konkurencji i Konsumentów</b>
Akceptacja kierującego komórką organizacyjną inną niż komórka organizacyjna wnioskująca*	<input type="checkbox"/> <b>Należy zaznaczyć, jeżeli akceptacja została uzyskana</b>

\*dotyczy wyłącznie wniosku o udzielenie upoważnienia do poszczególnych czynności przetwarzania danych osobowych zawartych w rejestrze czynności przetwarzania danych osobowych dla innej komórki organizacyjnej

.....  
(data i podpis kierującego komórką organizacyjną)

Załącznik nr 7

**Wzór**

**WNIOSEK O ODWOŁANIE UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH**  
dla

.....  
(imię i nazwisko)

Zgodnie z art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.)

Dane	
Nazwa komórki organizacyjnej	
Rodzaj zatrudnienia/inny stosunek prawny (pracownik, praktykant, stażysta, zleceniobiorca, inna [jaka?])	
Wnioskowana data odwołania upoważnienia do przetwarzania danych osobowych	<b>dd-mm-rrrr</b>
Data i numer odwoływanego upoważnienia do przetwarzania danych osobowych	<b>Upoważnienie z dnia dd-mm-rrrr nr .....</b>

\_\_\_\_\_  
(data i podpis kierującego komórką organizacyjną)

**Wzór**

**Ewidencja osób upoważnionych do przetwarzania danych osobowych  
w Urzędzie Ochrony Konkurencji i Konsumentów**

<b>Lp.</b>	<b>Znak sprawy</b>	<b>Imię i nazwisko</b>	<b>Komórka organizacyjna*</b>	<b>Zakres upoważnienia</b>	<b>Data udzielenia upoważnienia</b>	<b>Data złożenia oświadczenia przez pracownika</b>	<b>Data wygaśnięcia upoważnienia</b>	<b>Uwagi</b>

\* komórka organizacyjna, w której pracownik jest zatrudniony lub wykonuje oznaczone czynności na rzecz Urzędu



**Wzór**

**Zgłoszenie zdarzenia\* ochrony danych osobowych**

Dane zgłoszenia	
Imię i nazwisko osoby zgłaszającej zdarzenie	
Data i godzina zgłoszenia zdarzenia	
Opis zdarzenia	
Okoliczności zdarzenia	
Przeprowadzenie działań wyjaśniających przyczyny zaistnienia zdarzenia	
Skutki wywołane zdarzeniem	
Podjęte działania zaradcze	

\*zdarzenie stanowiące naruszenie ochrony danych osobowych lub mogące stanowić naruszenie ochrony danych osobowych

(data i czytelny podpis)

Załącznik nr 11

**Wzór**  
**Rejestr incydentów i naruszeń ochrony danych osobowych**  
**w Urzędzie Ochrony Konkurencji i Konsumentów**

Lp.	INFORMACJE ZNAJDUJĄCE SIĘ W REJESTRZE					
1.	Miejsce wystąpienia zdarzenia*					
2.	Data i godzina wystąpienia zdarzenia*					
3.	Data i godzina powzięcia informacji o zdarzeniu*					
4.	Pracownik zgłaszający zdarzenie*/nazwa komórki organizacyjnej					
5.	Okoliczności wystąpienia zdarzenia*					
6.	Stwierdzenie naruszenia					
7.	Waga naruszenia					
8.	Skutki i konsekwencje wywołane naruszeniem					
9.	Podjęte środki zaradcze					
10.	Decyzja o zgłoszeniu do organu nadzorczego lub uzasadnienie niezgłoszenia naruszenia					
11.	Data i godzina zgłoszenia do organu nadzorczego					
12.	Decyzja o zawiadomieniu osoby, której dane dotyczą o naruszeniu lub uzasadnienie niezawiadomienia osoby					
13.	Data i godzina zawiadomienia osoby, której dane dotyczą					
14.	Uwagi					

\*zdarzenie stanowiące naruszenie ochrony danych osobowych lub mogące stanowić naruszenie ochrony danych osobowych

Załącznik nr 2

### Oświadczenie

#### **o zapoznaniu się z Polityką ochrony danych osobowych oraz zobowiązanie do zachowania w tajemnicy przetwarzanych danych osobowych**

Oświadczam, że zapoznałam(-łem) się z obowiązującą w Urzędzie Ochrony Konkurencji i Konsumentów Polityką ochrony danych osobowych i zobowiązuję się do przestrzegania zasad przetwarzania danych osobowych w niej określonych.

Oświadczam, że zapoznałam (-łem) się z przepisami 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) i ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

Zobowiązuję się do:

- 1) zachowania w tajemnicy przetwarzanych danych osobowych, z którymi zapoznałam(-łem) się oraz sposobów ich zabezpieczenia, zarówno w okresie trwania umowy, jak również po ustaniu stosunku prawnego łączącego mnie z Urzędem Ochrony Konkurencji i Konsumentów;
- 2) niewykorzystywania danych osobowych w celach pozasłużbowych;
- 3) stosowania instrukcji, procedur i zaleceń dotyczących ochrony danych osobowych przyjętych w Urzędzie Ochrony Konkurencji i Konsumentów;
- 4) przetwarzania danych osobowych jedynie w zakresie udzielonego upoważnienia, zgodnie z poleceniami administratora;
- 5) niezwłocznego zgłaszania każdego zdarzenia stanowiącego naruszenie przetwarzania danych osobowych lub mogącego stanowić naruszenie przetwarzania danych osobowych.

Przyjmuję do wiadomości, że naruszenie zasad poufności oraz zasad Polityki ochrony danych osobowych obowiązującej w Urzędzie Ochrony Konkurencji i Konsumentów może spowodować wobec mnie odpowiedzialność dyscyplinarną, cywilną oraz karną.

---

(data i czytelny podpis)