

**ZARZĄDZENIE NR 10/2025**  
**DYREKTORA URZĘDU**  
**ŻEGLUGI ŚRÓDLĄDOWEJ WE WROCŁAWIU**  
**z dnia 21 maja 2025 r.**  
**w sprawie wprowadzenia Polityki Bezpieczeństwa**  
**Ochrony Danych Osobowych**  
**Urzędu Żeglugi Śródlądowej we Wrocławiu**

Na podstawie § 12 ust. 2 pkt. 1 i 10 oraz ust. 3 pkt. 8 Regulaminu Organizacyjnego Urzędu Żeglugi Śródlądowej we Wrocławiu wprowadzonego Zarządzeniem nr 13/2024 Dyrektora Urzędu Żeglugi Śródlądowej we Wrocławiu z dnia 11 grudnia 2024 r. oraz art. 24 ust. 1 i 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 95/94/WE (ogólne rozporządzenie o ochronie danych), (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.), zarządza się co następuje:

**§ 1.**

Wprowadza się Politykę Bezpieczeństwa Ochrony Danych Osobowych Urzędu Żeglugi Śródlądowej we Wrocławiu, stanowiącą załącznik do niniejszego Zarządzenia.

**§ 2.**

Politykę Bezpieczeństwa Ochrony Danych Osobowych Urzędu Żeglugi Śródlądowej we Wrocławiu stanowi dokument wewnętrzny, niepodlegający publikacji.

**§ 3.**

Traci moc zarządzenie nr 7/2023 Dyrektora Urzędu Żeglugi Śródlądowej we Wrocławiu z dnia 19 kwietnia 2023 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Ochrony Danych Osobowych w Urzędzie Żeglugi Śródlądowej we Wrocławiu.

**§ 4.**

Zarządzenie wchodzi w życie z dniem podpisania.

Załącznik do Zarządzenia nr 10/2025  
Dyrektora Urzędu Żeglugi Śródlądowej we  
Wrocławiu z dnia 21 maja 2025 r. w sprawie  
wprowadzenia Polityki Bezpieczeństwa Ochrony  
Danych Osobowych Urzędu Żeglugi Śródlądowej  
we Wrocławiu

## **Polityka Bezpieczeństwa Ochrony Danych Osobowych**

### **Urzędu Żeglugi Śródlądowej we Wrocławiu**

Wrocław 2025 r.

## **Rozdział I**

### **Postanowienia ogólne**

**§ 1.** Celem Polityki Bezpieczeństwa Ochrony Danych Osobowych Urzędu Żeglugi Śródlądowej we Wrocławiu, dalej zwanej Polityką Bezpieczeństwa jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych, sposobu przetwarzania w Urzędzie Żeglugi Śródlądowej we Wrocławiu informacji zawierających dane osobowe, a przede wszystkim zapewnienie ochrony przetwarzania danych osobowych przed wszelkiego rodzaju zagrożeniami, wewnętrznymi i zewnętrznymi. Dodatkowym priorytetem Polityki Bezpieczeństwa jest zapewnienie należytych działań, oceny i udokumentowania możliwych naruszeń bezpieczeństwa danych osobowych, następnie rozpoczęcie odpowiedniego trybu postępowania zmierzającego do przywrócenia stanu właściwego.

**§ 2.** Polityka Bezpieczeństwa została utworzona w związku z wymaganiami zawartymi w:

- 1) rozporządzeniu 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 95/94/WE (ogólne rozporządzenie o ochronie danych), (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.), dalej RODO.
- 2) ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r. poz. 1781), dalej ustawa o ochronie danych osobowych.

**§ 3.** Polityka Bezpieczeństwa odnosi się do danych osobowych przetwarzanych zgodnie z RODO i ustawą o ochronie danych osobowych.

**§ 4.** Uczestnikami procesu przetwarzania danych osobowych w Urzędzie Żeglugi Śródlądowej we Wrocławiu może być:

- 1) osoba zatrudniona w Urzędzie Żeglugi Śródlądowej we Wrocławiu,
- 2) osoba wykonująca zadania w ramach umowy cywilnoprawnej zawartej z Urzędem Żeglugi Śródlądowej we Wrocławiu,
- 3) praktykant, stażysta lub wolontariusz.

**§ 5.** Polityka Bezpieczeństwa ma zastosowanie do przetwarzania danych osobowych:

- 1) w dokumentach papierowych (w tym wnioskach, świadectwach, zaświadczeniach etc.), aktach, kartotekach, wykazach, rejestrach i innych zbiorach ewidencyjnych,
- 2) w systemie Elektronicznego Zarządzania Dokumentacją (dalej EZD), w innych stosowanych systemach informatycznych, poczcie elektronicznej i nośnikach danych.

**§ 6.** Polityka Bezpieczeństwa w Urzędzie Żeglugi Śródlądowej we Wrocławiu określa:

- 1) środki organizacyjne i techniczne niezbędne do zapewnienia poufności, integralności i rozliczalności w procesie przetwarzania danych osobowych,
- 2) zakres zadań Inspektora ds. Ochrony Danych,

- 3) obowiązki uczestników procesów przetwarzania danych osobowych,
- 4) sposób przetwarzania danych osobowych,
- 5) sposób postępowania w przypadku naruszenia ochrony danych osobowych,
- 6) sposób realizacji praw osób, których dane są przetwarzane,
- 7) sposób przeprowadzenia oceny skutków dla ochrony danych osobowych,
- 8) procedurę przeprowadzania analizy ryzyka.

**§ 7.** Zastosowanie Polityki Bezpieczeństwa i zabezpieczeń z nią związanych ma na celu zapewnienie:

- 1) przetwarzania zgodnego z prawem, rzetelnego i przejrzystego,
- 2) ograniczenia celu przetwarzania – przetwarzanie danych osobowych odbywa się tylko w konkretnym i prawnie uzasadnionym celu,
- 3) minimalizacji danych osobowych – przetwarzania danych adekwatnych, stosowanych oraz ograniczonych do niezbędnych celów,
- 4) prawidłowości danych osobowych – systematyczne aktualizowanie danych osobowych oraz ich sprostowanie lub usuwanie jeżeli są wykorzystywane w nieprawidłowy sposób, niezgodny z celem ich przetwarzania,
- 5) ograniczenia przechowywania – przechowywanie nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania,
- 6) integralności danych osobowych – dane osobowe nie są zmieniane lub niszczone w sposób nieautoryzowany,
- 7) poufności danych osobowych – dane osobowe są przetwarzane w sposób zapewniający ich bezpieczeństwo, a także są chronione przed niedozwolonym lub niezgodnym z prawem przetwarzaniem.

**§ 8.** Administratorem Danych Osobowych w Urzędzie Żeglugi Śródlądowej we Wrocławiu jest Dyrektor Urzędu Żeglugi Śródlądowej we Wrocławiu.

## **Rozdział II**

### **Definicje**

**§ 9.** Przez użyte w Polityce Bezpieczeństwa określenia należy rozumieć:

- 1) Administrator Danych Osobowych – Dyrektora Urzędu Żeglugi Śródlądowej we Wrocławiu, dalej jako Administrator Danych;
- 2) Baza danych osobowych – zbiór o określonej strukturze, uporządkowanych i powiązanych ze sobą tematycznie danych przechowywanych w określonym miejscu np. w pamięci wewnętrznej komputera;

- 3) Dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
- 4) Inspektor ds. Ochrony Danych – osobę wyznaczoną przez Administratora Danych do nadzorowania zasad ochrony danych osobowych zgodnie z RODO i ustawą o ochronie danych osobowych;
- 5) Odbiorca – osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, którym ujawnia się dane osobowe, niezależnie od tego czy jest stroną trzecią; organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii Europejskiej lub prawem państwa członkowskiego, nie są uznawane za odbiorców;
- 6) Organizacja międzynarodowa – organizację i organy jej podlegające działające na podstawie prawa międzynarodowego publicznego lub inny organ powołany w drodze umowy między co najmniej dwoma państwami lub na podstawie takiej umowy;
- 7) Państwo trzecie – państwo niebędące członkiem Unii Europejskiej oraz nienależące do Europejskiego Obszaru Gospodarczego (EOG);
- 8) Podmiot przetwarzający – osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora danych osobowych;
- 9) Polityka Bezpieczeństwa – zastosowaną Politykę Bezpieczeństwa Ochrony Danych Osobowych w Urzędzie Żeglugi Śródlądowej we Wrocławiu;
- 10) Prezes Urzędu Ochrony Danych Osobowych – organ nadzorczy z zakresu ochrony danych osobowych, dalej PUODO.
- 11) Przetwarzanie danych – wszystkie operacje jakim poddawane są dane, w szczególności: zbieranie, przechowywanie, udostępnianie, zmienianie, przekazywanie, utrwalanie, opracowywanie, usuwanie i profilowanie danych osobowych;
- 12) System informatyczny – zespół powiązanych i współpracujących ze sobą urządzeń, programów, narzędzi programowych oraz procedur w celu przetwarzania danych osobowych;
- 13) System tradycyjny – zespół procedur organizacyjnych mających na celu przetwarzanie danych osobowych w formie papierowej;
- 14) Urząd – Urząd Żeglugi Śródlądowej we Wrocławiu;
- 15) Usuwanie danych – niszczenie danych osobowych lub ich modyfikacja w taki sposób, aby nie była możliwa identyfikacja tożsamości osoby, której informacje dotyczą;
- 16) Użytkownik – pracownika Urzędu, stażystę, wolontariusza, praktykanta, osobę upoważnioną przez Administratora Danych do przetwarzania danych osobowych zgodnie z RODO, w tym osoby świadczące pracę na podstawie umów cywilnoprawnych;

- 17) Zabezpieczenie danych – wdrożenie odpowiednich środków organizacyjnych i technicznych zapewniających ochronę danych przed nieuprawnionym dostępem;
- 18) Zgoda – dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którą wyraziła osoba, której dane są przetwarzane przez Urząd.

§ 10. Dla niezidentyfikowanych pojęć, przyjmuje się ich znaczenie przedstawione w RODO i ustawie o ochronie danych osobowych.

### **Rozdział III**

#### **Inspektor ds. Ochrony Danych**

§ 11. Administrator Danych wyznacza Inspektora ds. Ochrony Danych.

§ 12. Inspektor ds. Ochrony Danych podlega bezpośrednio Dyrektorowi Urzędu Żeglugi Śródlądowej we Wrocławiu.

§ 13. Administrator Danych zapewnia Inspektorowi ds. Ochrony Danych odpowiednie środki, organizacyjną odrębność i niezależność w wykonywaniu powierzonych zadań.

§ 14. Do zadań Inspektora ds. Ochrony Danych należy:

- 1) informowanie Administratora Danych i użytkowników o obowiązkach spoczywających na nich na mocy przepisów o ochronie danych osobowych,
- 2) doradztwo w zakresie przestrzegania przepisów o ochronie danych osobowych,
- 3) monitorowanie przestrzegania zasad ochrony danych osobowych,
- 4) udzielanie zaleceń co do oceny skutków dla ochrony danych oraz ich monitorowanie,
- 5) nadzorowanie, opracowywanie i aktualizacja dokumentacji opisującej sposób przetwarzania danych osobowych,
- 6) zapoznanie osób upoważnionych do przetwarzania danych osobowych z obowiązującymi przepisami w zakresie ochrony danych osobowych,
- 7) prowadzenie rejestrów zgodnych z RODO i Polityką Bezpieczeństwa,
- 8) prowadzenie analiz przypadków naruszeń bezpieczeństwa danych osobowych oraz stworzenie w tym zakresie zaleceń dla Administratora Danych Osobowych,
- 9) monitorowanie analizy ryzyka ochrony danych osobowych,
- 10) współpraca z PUODO,
- 11) pełnienie funkcji punktu kontaktowego dla PUODO.

§ 15. W trakcie realizacji swoich zadań Inspektor ds. Ochrony Danych posiada, w niezbędnym zakresie, dostęp do wszystkich danych osobowych przetwarzanych w Urzędzie.

## **Rozdział IV**

### **Zakres zastosowania Polityki Bezpieczeństwa**

§ 16. Polityka Bezpieczeństwa określa zasady przetwarzania danych osobowych, dla których Dyrektor Urzędu Żeglugi Śródlądowej we Wrocławiu jest administratorem danych osobowych w rozumieniu art. 4 ust. 7 RODO.

§ 17. Politykę Bezpieczeństwa stosuje się także do przetwarzanych danych osobowych w Urzędzie, dla których administratorem danych osobowych nie jest Dyrektor Urzędu Żeglugi Śródlądowej we Wrocławiu.

§ 18. Politykę Bezpieczeństwa stosuje się przede wszystkim w związku z realizacją:

- 1) zadań wynikających z przepisów prawa krajowego oraz Unii Europejskiej, zwłaszcza ustawy z dnia 21 grudnia 2000 r. o żegludze śródlądowej (t.j. Dz. U. z 2025 r. poz. 18) i określonych szczegółowo w regulaminie organizacyjnym Urzędu,
- 2) obowiązków pracodawcy w rozumieniu ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (t.j. Dz. U. z 2025 r. poz. 277),
- 3) umów cywilnoprawnych,
- 4) umów o organizację staży, praktyk, wolontariatów,
- 5) innych zadań niezbędnych do zapewnienia funkcjonowania Urzędu.

§ 19. Polityka Bezpieczeństwa obowiązuje wszystkich pracowników Urzędu, również wolontariuszy, stażystów, praktykantów i inne osoby upoważnione do przetwarzania danych osobowych, w tym osoby, z którymi zawarto umowę cywilnoprawną.

§ 20. Zakresy ochrony danych osobowych określone przez dokument Polityki Bezpieczeństwa mają zastosowanie do systemów tradycyjnych i informatycznych Urzędu, w których są przetwarzane dane osobowe, a w szczególności do:

- 1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są dane osobowe,
- 2) wszystkich lokalizacji Urzędu – budynków i pomieszczeń, w których są lub będą przetwarzane dane osobowe,
- 3) wszystkich użytkowników mających dostęp do danych osobowych, również wykonujących swoje obowiązki w terenie lub w trybie zdalnym.

## **Rozdział V**

### **Obowiązki użytkowników i odpowiedzialność za przetwarzanie danych osobowych**

§ 21. Każdy użytkownik przed rozpoczęciem przetwarzania danych osobowych zobowiązany jest zapoznać się z przepisami i procedurami dotyczącymi ochrony danych osobowych, w tym w szczególności z RODO, ustawą o ochronie danych osobowych oraz Polityką Bezpieczeństwa,

a także innymi wewnętrznymi regulacjami stosowanymi w Urzędzie dotyczącymi ochrony danych osobowych.

**§ 22.** Użytkownicy w szczególności zobowiązani są do:

- 1) przetwarzania danych osobowych zgodnie z przepisami o ochronie danych osobowych, w tym w szczególności z RODO i ustawą o ochronie danych osobowych,
- 2) przetwarzania danych osobowych zgodnie z Polityką Bezpieczeństwa i innymi regulacjami wewnętrznymi obowiązującymi w Urzędzie,
- 3) zachowania tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, również po ustaniu zatrudnienia lub innego zobowiązania wynikającego z zawartych umów,
- 4) zabezpieczenia danych przed ich utratą, uszkodzeniem lub zniszczeniem, zmianą lub udostępnieniem osobom nieupoważnionym poprzez:
  - a) zabezpieczenia dokumentów w postaci papierowej zawierających dane osobowe oraz zabezpieczenie dostępu do danych osobowych przetwarzanych w systemach informatycznych na stanowisku pracy – w pomieszczeniach służbowych, w miejscu wykonywania pracy poza Urzędem oraz podczas pracy zdalnej,
  - b) przestrzeganie procedur właściwego użytkowania systemów informatycznych, w których przetwarzane są dane osobowe,
- 5) przestrzegania zasad czystego biurka,
- 6) przestrzegania zasad bezpieczeństwa określonych w Polityce Bezpieczeństwa Teleinformatycznego Urzędu Żeglugi Śródlądowej we Wrocławiu,
- 7) niszczenia wszystkich nadmiarowych dokumentów niepodlegających archiwizacji,
- 8) uczestnictwa w szkoleniach z zakresu ochrony danych osobowych,
- 9) współpracy z Inspektorem ds. Ochrony Danych przy realizacji jego zadań.

## **Rozdział VI**

### **Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzania danych**

**§ 23.** W celu zapewnienia poufności, integralności i rozliczalności przetwarzania danych w Urzędzie wprowadzono zabezpieczenia organizacyjne poprzez:

- 1) przegląd i aktualizację Polityki Bezpieczeństwa,
- 2) dopuszczenie do przetwarzania danych osobowych wyłącznie osób posiadających upoważnienie nadane przez Administratora Danych, które zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych,
- 3) zobowiązanie osób zatrudnionych przy przetwarzaniu danych osobowych do zachowania ich w tajemnicy,

- 4) szkolenia z zakresu ochrony danych osobowych,
- 5) zawieranie umów powierzenia przetwarzania danych osobowych,
- 6) wdrożenie procedury postępowania w sytuacji naruszenia ochrony danych osobowych,
- 7) prowadzenie rejestrów wynikających z RODO,
- 8) jeżeli jest to konieczne przeprowadzenie oceny skutków dla ochrony danych osobowych,
- 9) przeprowadzenie analizy ryzyka dla ochrony danych osobowych,
- 10) przeprowadzenie audytu i sprawdzenia przez Inspektora ds. Ochrony Danych,
- 11) Politykę Bezpieczeństwa Teleinformatycznego w Urzędzie Żeglugi Śródlądowej we Wrocławiu.

**§ 24.** W celu zapewnienia poufności, integralności i rozliczalności przetwarzania danych w Urzędzie wprowadzono następujące zabezpieczenia techniczne:

- 1) dopuszczenie przebywania osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe tylko w obecności osoby upoważnionej do przetwarzania danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych,
- 2) podczas nieobecności osób uprawnionych pomieszczenia, w których są przetwarzane dane osobowe są zamykane na klucz,
- 3) stosowanie monitoringu, który umożliwia rejestrację zdarzeń,
- 4) pomieszczenia, w których przetwarzane są dane osobowe zabezpieczone są przed skutkami pożaru za pomocą systemu ppoż oraz podręcznymi środkami gaśniczymi,
- 5) dane przetwarzane przy użyciu tradycyjnych nośników (w postaci papierowej) gromadzone są w rejestrach, księgach, zeszytach papierowych oraz segregatorach i przechowywane w zamykanych szafach oraz kasach pancernych,
- 6) każdy dokument papierowy zawierający dane osobowe przeznaczony do wyrzucenia zostaje zniszczony przy pomocy niszczarki w sposób uniemożliwiający jego odczytanie,
- 7) dane w postaci elektronicznej, przetwarzane przy użyciu komputerów pracujących w zewnętrznej sieci komputerowej podczas pracy zdalnej są zabezpieczone oprogramowaniem antywirusowym; w czasie przetwarzania danych urządzenia i są pod ciągłym nadzorem przeszkolonego pracownika,
- 8) dane w postaci elektronicznej przetwarzane są również przy użyciu urządzeń rejestrujących obraz i dźwięk do wykorzystania służbowego, przykładowo: telefon służbowy, które są zabezpieczone oraz są pod ciągłym nadzorem pracowników,
- 9) dane w postaci elektronicznej przetwarzane są również przy użyciu zewnętrznych zabezpieczonych poprzez hasła nośników danych,
- 10) środki ochrony w ramach oprogramowania:

- a) każda jednostka komputerowa zabezpieczona została hasłem wejściowym do systemu operacyjnego lub do profilu użytkownika,
- b) zastosowano identyfikator i hasło dostępu do danych.

## **Rozdział VII**

### **Upoważnienia do przetwarzania danych osobowych**

§ 25. W Urzędzie przetwarzanie danych osobowych odbywa się na podstawie imiennych upoważnień do przetwarzania danych osobowych.

§ 26. Administrator Danych nadaje upoważnienie do przetwarzania danych osobowych zgodnie ze wzorem przedstawionym w załączniku nr 1 do Polityki Bezpieczeństwa.

§ 27. Upoważnienie jest wystawione w dwóch egzemplarzach.

- 1) Jeden z egzemplarzy zamieszczany jest w aktach osobowych użytkownika.
- 2) Drugi egzemplarz otrzymuje użytkownik.

§ 28. Inspektor ds. Ochrony Danych prowadzi rejestr upoważnień do przetwarzania danych osobowych, którego wzór stanowi załącznik nr 2 do Polityki Bezpieczeństwa.

§ 29. Użytkownik otrzymujący upoważnienie do przetwarzania danych osobowych zobowiązana jest do:

- 1) zapoznania się z Polityką Bezpieczeństwa oraz obowiązującymi przepisami prawa dotyczącymi ochrony danych osobowych,
- 2) potwierdzenia faktu zapoznania się z treścią i zakresem upoważnienia do przetwarzania danych osobowych.

## **Rozdział VIII**

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

§ 30. W Urzędzie prowadzony jest rejestr czynności przetwarzania danych osobowych, którego wzór stanowi załącznik nr 3 do Polityki Bezpieczeństwa.

- 1) Przez rejestr czynności przetwarzania danych osobowych rozumie się ewidencję czynności przetwarzania, która jest zespołem powiązanych ze sobą operacji na danych, wykonywanych przez jednostkę lub kilka osób, które można określić w sposób zbiorczy w związku z celem, w jakim te czynności są podejmowane.
- 2) Rejestr zawiera czynności, za które odpowiada Dyrektor Urzędu Żeglugi Śródlądowej we Wrocławiu.

§ 31. W Urzędzie prowadzony jest rejestr kategorii czynności przetwarzania danych osobowych, którego wzór stanowi załącznik nr 4 do Polityki Bezpieczeństwa.

- 1) Przez rejestr kategorii czynności przetwarzania danych osobowych rozumie się ewidencję usług realizowanych na zlecenie administratora danych osobowych związanych ze zleconymi czynnościami przetwarzania.

- 2) Rejestr zawiera czynności dokonywane w imieniu innego administratora danych osobowych niż Dyrektor Urzędu Żeglugi Śródlądowej we Wrocławiu.

**§ 32.** Rejestry są uzupełniane przez użytkowników merytorycznych.

**§ 33.** Inspektor ds. Ochrony Danych dokonuje przeglądu wymienionych rejestrów w § 30 i 31 nie rzadziej niż raz w roku oraz w przypadku wprowadzenia istotnych zmian w zadaniach wykonywanych przez Urząd.

## **Rozdział IX**

### **Powierzenie przetwarzania danych osobowych**

**§ 34.** Urząd realizując zadania skutkujące powierzeniem danych osobowych może być:

- 1) podmiotem, który powierza przetwarzanie danych osobowych w swoim imieniu innemu podmiotowi.
- 2) podmiotem, który w imieniu innego podmiotu, przetwarza powierzone dane osobowe (podmiot przetwarzający).

**§ 35.** Zawarcie umowy powierzenia przetwarzania danych osobowych poprzedzone jest konsultacją z Inspektorem ds. Ochrony Danych i zaakceptowaniem przez niego zapisów projektu umowy.

**§ 36.** Umowa w zakresie powierzenia przetwarzania danych osobowych powinna w szczególności zawierać:

- 1) przedmiot i czas trwania przetwarzania,
- 2) charakter i cel przetwarzania,
- 3) rodzaj danych osobowych i kategorie osób, których dane dotyczą,
- 4) obowiązki i prawa administratora danych osobowych,
- 5) informacje, że przetwarzanie danych osobowych odbywa się jedynie na polecenie administratora danych osobowych, również danych przekazywanych do państwa trzeciego lub organizacji międzynarodowych,
- 6) informacje o sposobie upoważniania osób, które będą przetwarzały dane osobowe i obowiązku zachowania tajemnicy,
- 7) oświadczenie podmiotu przetwarzającego o zapewnieniu wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie powierzonych danych osobowych spełniało wymogi prawem przewidziane i chroniło prawa osób, których dane dotyczą,
- 8) informacje o warunkach podpowierzenia,
- 9) informacje o wsparciu administratora danych osobowych w wywiązywaniu się z obowiązków wynikających z rozdziału III RODO oraz art. 32-36 RODO,
- 10) informacje o sposobach postępowania z danymi osobowymi po zakończeniu realizacji umowy,

11) informacje zasadach dotyczących przeprowadzania audytu lub kontroli w podmiotach przetwarzających dane osobowe w imieniu administratora danych osobowych,

12) informacje o sposobach zgłaszania naruszeń z zakresu ochrony danych.

**§ 37.** Inspektor ds. Ochrony Danych prowadzi rejestr umów powierzenia przetwarzania danych osobowych zgodnie z załącznikiem nr 5 do Polityki Bezpieczeństwa.

**§ 38.** Wszystkie procesy i zadania, które wymagają powierzenia danych osobowych przez Urząd, uwzględniane są w rejestrze czynności przetwarzania danych osobowych.

**§ 39.** Wszystkie procesy i zadania, w których Urząd pełni rolę podmiotu przetwarzającego zawarte są w rejestrze kategorii czynności przetwarzania danych osobowych.

## **Rozdział X**

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

**§ 40.** Realizacja obowiązku informacyjnego.

- 1) Obowiązek informacyjny wynikający z art. 13 i 14 RODO realizowany jest przy pierwszym kontakcie wobec osób, której dane osobowe są przetwarzane w Urzędzie.
- 2) Każda osoba, od której dane zebrano w sposób bezpośredni, informowana jest o:
  - a) nazwie i adresie Administratora Danych;
  - b) danych kontaktowych Inspektora ds. Ochrony Danych;
  - c) celu i podstawie prawnej przetwarzania;
  - d) gdy ma zastosowanie to o prawnie uzasadnionym interesie realizowanym przez Administratora Danych lub przez stronę trzecią,
  - e) odbiorcach danych lub kategoriach odbiorców;
  - f) o zamiarze przekazania danych osobowych do państw trzecich lub organizacji międzynarodowych;
  - g) okresie przechowywania danych osobowych;
  - h) przysługujących prawach;
  - i) prawie do wycofania zgody na przetwarzanie danych osobowych jeżeli została ona wcześniej wyrażona;
  - j) prawie do wniesienia skargi do PUODO;
  - k) ewentualnym zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu;
  - l) obowiązku lub dobrowolności podania danych osobowych.
- 3) W przypadku pozyskania danych w sposób pośredni, nie od osoby, której dane dotyczą, konieczne jest przedstawienie informacji z ust. 1 pkt 1-11, kategorii danych osobowych oraz źródła, z którego uzyskano dane.

- 4) Każda osoba, której dane przetwarza Administrator Danych, ma prawo uzyskać na żądanie informacje, o których mowa w ust. 2 i 3. Odpowiedzi udziela się w terminie 30 dni od dnia złożenia wniosku. Administrator Danych ma prawo odmówić udzielenia informacji, jeśli nie jest możliwe potwierdzenie tożsamości wnioskodawcy.
- 5) Wskazane przez Inspektora ds. Ochrony Danych klauzule informacyjne są dodatkowo zamieszczane na stronie internetowej Urzędu w zakładce „RODO”.

#### **§ 41. Wniosek osoby fizycznej**

- 1) Realizacja prawa dostępu do danych, uzyskania kopii, sprostowania, ograniczenia, sprzeciwu, usunięcia oraz przeniesienia danych osobowych, może nastąpić na pisemny (w tym elektroniczny) wniosek osoby.
- 2) Wniosek rozpatrywany jest przez pracownika merytorycznego wyznaczonego przez Administratora Danych, zgodnie z wykonywanym zakresem zadań.
- 3) Podczas oceny wniosku należy brać pod uwagę przede wszystkim to, czy:
  - a) można ustalić i potwierdzić tożsamość wnioskodawcy;
  - b) dane wnioskodawcy są przetwarzane w zasobach Urzędu;
  - c) wniosek jest zasadny zgodnie z przepisami art. 15 – 22 RODO.
- 4) Jeśli wyznaczony pracownik potwierdzi istnienie okoliczności, o których mowa w ust. 3 realizuje złożony wniosek.
- 5) W przypadku wątpliwości może skonsultować możliwość i sposób realizacji wniosku z Inspektorem ds. Ochrony Danych.
- 6) Po ustaleniu sposobu realizacji wniosku, wyznaczony pracownik nadzoruje jego wykonanie oraz przygotowuje odpowiedź dla wnioskodawcy.
- 7) Wniosek osoby fizycznej o realizację prawa może być składany za pomocą formularza, którego wzór stanowi załącznik nr 6 do Polityki Bezpieczeństwa. Formularz ten jest dostępny na stronie internetowej Urzędu w zakładce „RODO”.
- 8) Inspektor ds. Ochrony Danych rejestruje wnioski oraz ewentualnie sposób i termin ich realizacji w rejestrze udostępnień i realizacji praw, którego wzór stanowi załącznik nr 7 do Polityki Bezpieczeństwa.
- 9) Wszyscy pracownicy zobowiązani są przesyłać Inspektorowi ds. Ochrony Danych kopię każdego otrzymanego wniosku oraz udzielonej odpowiedzi.
- 10) W celu prawidłowej weryfikacji osób wnioskujących o udzielenie informacji lub o realizację praw osób, Urząd ma prawo żądać od osoby wnioskującej dodatkowego potwierdzenia swojej tożsamości.
- 11) W przypadku, gdy osoba wnioskująca wielokrotnie występuje z wnioskiem o udzielenie informacji lub o realizację praw w zakresie niewnoszącym zmian co do sposobu przetwarzania danych, Administrator Danych informuje osobę wnioskującą o wysokości opłaty za udzielenie tych informacji. Jeżeli kontakt z osobą wnioskującą

możliwy jest przy wykorzystaniu kanałów elektronicznych, kontakt z tą osobą może być prowadzony w ten sposób.

#### **§ 42. Zgoda na przetwarzanie danych osobowych**

- 1) W szczególnych przypadkach przewidzianych prawem lub w sytuacjach, gdy wymagane jest przetwarzanie danych osobowych do realizacji zadania, ale nie mają zastosowania przesłanki określone w art. 6 i 9 RODO, przetwarzanie odbywa się na podstawie zgody osoby, której dane dotyczą.
- 2) Pracownik merytoryczny realizujący zadanie określi w jakim zakresie powinna być pozyskana zgoda od osoby, której dane dotyczą.
- 3) W celu realizacji zasady rozliczalności zgoda musi być udokumentowana w formie pisemnej lub elektronicznej.
- 4) Zgoda musi być jasna i czytelna oraz adekwatna do celu w jakim będą przetwarzane dane osobowe.
- 5) Osoba, która wyraża zgodę na przetwarzanie danych osobowych musi zostać poinformowana o możliwości wycofania zgody, w każdym momencie przetwarzania danych osobowych.
- 6) Pracownik merytoryczny informuje Inspektora ds. Ochrony Danych o pozyskanych zgodach na przetwarzanie danych osobowych.
- 7) Inspektor ds. Ochrony Danych prowadzi rejestr zgód zgodnie z załącznikiem nr 8 do Polityki Bezpieczeństwa.

#### **§ 43. Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych**

- 1) Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych może odbywać się jedynie zgodnie z zasadami wskazanymi w rozdziale V RODO.
- 2) Pracownik merytoryczny jest zobowiązany zweryfikować istnienie podstawy prawnej uprawniającej do przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej przed dokonaniem takiego przekazania.
- 3) Pracownik merytoryczny informuje Inspektora ds. Ochrony Danych o dokonaniu przekazania danych osobowych do państw trzecich lub organizacji międzynarodowych.
- 4) Inspektor ds. Ochrony Danych prowadzi rejestr przekazanych danych osobowych zgodnie z załącznikiem nr 9 do Polityki Bezpieczeństwa.

## **Rozdział XI**

### **Zdarzenia mogące naruszać ochronę danych osobowych**

**§ 44.** Do zagrożeń naruszających ochronę danych osobowych można zaliczyć:

- 1) zagrożenia losowe zewnętrzne – w szczególności klęski żywiołowe, przerwy w zasilaniu, których występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu; ciągłość systemu zostaje wprawdzie zakłócona, lecz nie dochodzi do naruszenia poufności danych,
- 2) zagrożenia losowe wewnętrzne – w szczególności niezamierzone pomyłki operatorów, administratora systemu, awarie sprzętowe, błędy oprogramowania, których występowanie może doprowadzić do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu i przy występowaniu których może nastąpić naruszenie poufności danych,
- 3) zagrożenia zamierzone, świadome i celowe – w szczególności nieuprawniony dostęp do systemu z zewnątrz, nieuprawniony dostęp do systemu z jego wnętrza, nieuprawniony przekaz danych, pogorszenie jakości sprzętu i oprogramowania oraz bezpośrednie zagrożenie materialnych składników systemu, których występowanie zazwyczaj nie doprowadza do uszkodzenia infrastruktury technicznej i zakłócenia ciągłości pracy systemu, lecz których zaistnienie może doprowadzić do naruszenia poufności danych.

**§ 45.** Do zdarzeń zakwalifikowanych jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia danych mogą zaliczać się:

- 1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: pożar, wybuch gazu, zalanie pomieszczeń, katastrofa budowlana, działania terrorystyczne itp.,
- 2) niewłaściwe parametry środowiska, takie jak np. nadmierna wilgotność, zbyt wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,
- 3) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu,
- 4) komunikaty alarmujące o próbie naruszenia zabezpieczeń systemu, które zapewniają ochronę danych bądź komunikat o podobnym znaczeniu,
- 5) odstępstwa od prawidłowego stanu danych wskazujące na niewłaściwe działanie systemu lub niepożądaną jego modyfikację,
- 6) naruszenie lub próba naruszenia integralności systemu bazy danych w tym systemie,
- 7) modyfikacja lub próba modyfikacji danych oraz zmiana w strukturze danych dokonana bez odpowiedniego upoważnienia (autoryzacji),
- 8) stwierdzenie niedopuszczalnej manipulacji danymi osobowymi w systemie,
- 9) ujawnienie danych osobowych lub objętych tajemnicą procedur ochrony danych osobowych osobom nieupoważnionym, bądź innych elementów systemu zabezpieczeń,
- 10) funkcjonowanie sieci komputerowej lub praca systemu wykazuje nieprzypadkowe odstępstwo od prawidłowego rytmu pracy wskazujące na zaniechanie

lub przełamanie ochrony danych osobowych – np. praca w sieci lub przy komputerze osoby do tego nieupoważnionej, sygnał o nieautoryzowanym logowaniu, itp.,

- 11) ujawnienie istnienia nieautoryzowanych kont dostępu do danych objętych ochroną lub tzw. „bocznej furtki”,
- 12) zniszczenie lub podmiana nośnika z danymi osobowymi bądź skasowanie lub skopiowanie danych osobowych w sposób niedozwolony lub przez osobę nieupoważnioną,
- 13) naruszenie dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji np. nie wylogowanie się z systemu przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie wykonanie w określonym terminie kopii bezpieczeństwa, praca na danych osobowych w celach prywatnych, itp.,
- 14) stwierdzenie nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), folii, zdjęciach, itp.

## **Rozdział XII**

### **Postępowanie w przypadku naruszenia ochrony danych osobowych**

#### **§ 46. Naruszenia zidentyfikowane w Urzędzie**

- 1) W przypadku podejrzenia naruszenia ochrony danych osobowych, każdy użytkownik obowiązana niezwłocznie powiadomić o tym fakcie bezpośredniego przełożonego oraz Inspektora ds. Ochrony Danych w sposób telefoniczny lub poprzez wiadomość email.
- 2) Osoba zgłaszająca kolejno wypełnia formularz zgłoszenia, którego wzór stanowi załącznik nr 10 do Polityki Bezpieczeństwa i przekazuje Inspektorowi ds. Ochrony Danych.
- 3) W przypadku niemożności zawiadomienia Inspektora ds. Ochrony Danych, należy powiadomić Administratora Danych.
- 4) Do czasu powiadomienia Inspektora ds. Ochrony Danych lub Administratora Danych, należy podjąć następujące działania:
  - a) niezwłocznie podjąć czynności niezbędne do powstrzymania niepożądanych skutków zaistniałego zdarzenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn i sprawców,
  - b) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
  - c) zaniechać o ile to możliwe dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudniać udokumentowanie i analizę,
  - d) podjąć inne stosowne działania przewidziane w instrukcjach technicznych i technologicznych, dokumentacji systemu operacyjnego, dokumentacji bazy

danych lub aplikacji użytkowej właściwej dla objawów i sytuacji towarzyszącej naruszeniu,

- e) udokumentować wstępnie zaistniałego zdarzenia.
- 5) Inspektor ds. Ochrony Danych przy wsparciu bezpośredniego przełożonego użytkownika, który zgłaszał potencjalne naruszenie ochrony danych osobowych:
  - a) zapoznaje się z zaistniałą sytuacją, identyfikuje rodzaj zaistniałego zdarzenia i dokonuje wyboru metody dalszego postępowania celem powstrzymania lub ograniczenia dostępu osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów naruszenia ochrony danych osobowych,
  - b) może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od innych osób mogących posiadać informacje związane z zaistniałym zdarzeniem.
- 6) Inspektor ds. Ochrony Danych dokumentuje zaistniały przypadek poprzez sporządzenie raportu z naruszeń ochrony danych osobowych, którego wzór stanowi załącznik nr 11 do Polityki Bezpieczeństwa oraz odnotowuje zdarzenie w rejestrze naruszeń, którego wzór stanowi załącznik nr 12 do Polityki Bezpieczeństwa.
- 7) Raport z naruszeń ochrony danych osobowych powinien zawierać w szczególności:
  - a) wskazanie osoby powiadamiającej o naruszeniu,
  - b) określenie czasu oraz miejsca naruszenia i powiadomienia,
  - c) określenie okoliczności towarzyszących i rodzaju naruszenia,
  - d) wybór metody postępowania wraz z opisem podjętych działań i przesłanek skłaniających do ich podjęcia,
  - e) wstępną ocenę przyczyn wystąpienia naruszenia,
  - f) ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.
- 8) Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu Inspektor ds. Ochrony Danych zasięga niezbędnych opinii i proponuje postępowanie naprawcze, w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.
- 9) Zaistniałe zdarzenie powinno stać się przedmiotem szczegółowej analizy przeprowadzonej przez Administratora Danych i Inspektora ds. Ochrony Danych.
- 10) Analiza powinna zawierać ocenę zaistniałego zdarzenia, wskazanie osób odpowiedzialnych oraz wnioski nt. ewentualnych przedsięwzięć proceduralnych, organizacyjnych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.
- 11) Jeśli doszło do naruszenia ochrony danych osobowych zgodnie z art. 4 pkt 12 RODO oraz naruszenie to powoduje ryzyko naruszenia praw lub wolności osób fizycznych, Administrator Danych zgłasza taki fakt PUODO w terminie 72 h od powzięcia

informacji o naruszeniu. Zgłoszenie takie powinno zawierać elementy wskazane w art. 33 ust 3 RODO, tj.:

- a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
- b) zawierać imię i nazwisko oraz dane kontaktowe Inspektora ds. Ochrony Danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
- c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
- d) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

12) Jeśli naruszenie powoduje wysokie ryzyko naruszenia praw lub wolności osoby, Administrator Danych bez zbędnej zwłoki zawiadamia osobę, której dane zostały naruszone lub jeśli jest to niemożliwe – wydaje publiczny komunikat o naruszeniu.

#### **§ 47. Naruszenia ochrony danych osobowych zewnętrzne**

- 1) Podmioty, którym Administrator Danych powierzył przetwarzanie danych są zobowiązane poprzez odpowiednie klauzule w umowach, do zgłoszenia naruszenia powierzonych danych, do którego doszło u tych podmiotów – w terminie 48 h.
- 2) Punktem kontaktowym w związku z naruszeniem jest Inspektor ds. Ochrony Danych.
- 3) Inspektor ds. Ochrony Danych odnotowuje naruszenie w rejestrze zewnętrznych naruszeń ochrony danych osobowych, zgodnym ze wzorem zamieszczonym w załączniku nr 13 do Polityki Bezpieczeństwa.
- 4) Inne zewnętrzne naruszenia dotyczące danych osobowych przetwarzanych w Urzędzie również są odnotowywane w rejestrze opisanym w ust. 3.

### **Rozdział XIII**

#### **Ocena skutków dla ochrony danych osobowych**

**§ 48.** Ocena skutków dla ochrony danych osobowych planowanych procesów przetwarzania przeprowadza się jeżeli dany rodzaj przetwarzania (w szczególności z użyciem nowych technologii) ze względu na swój zakres, charakter, kontekst i cel z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych.

**§ 49.** Komórka organizacyjna lub pracownik stanowiska samodzielnie odpowiadający za dany proces przetwarzania danych osobowych przeprowadza ocenę skutków dla ochrony danych osobowych .

**§ 50.** Komórka organizacyjna lub pracownik stanowiska samodzielnie realizująca proces wskazany w § 48 jest zobowiązana skonsultować z Inspektorem ds. Ochrony Danych w szczególności kwestie dotyczące:

- 1) faktu, czy należy przeprowadzić ocenę skutków dla ochrony danych osobowych,
- 2) metodologii przeprowadzenia oceny skutków dla ochrony danych osobowych,
- 3) zabezpieczeń (w tym środków technicznych i organizacyjnych) stosowanych do łagodzenia wszelkich zagrożeń naruszenia praw i wolności osób, których dane dotyczą,
- 4) prawidłowości przeprowadzonej oceny skutków dla ochrony danych osobowych i zgodności jej wyników z RODO (czy należy kontynuować przetwarzanie, czy też nie, oraz jakie zabezpieczenia należy stosować).

**§ 51.** Ocena skutków dla ochrony danych osobowych zawiera co najmniej następujące elementy:

- 1) opis planowanych operacji przetwarzania i celów przetwarzania, jeżeli ma zastosowanie to prawnie uzasadnionych interesów realizowanych przez Administratora Danych,
- 2) ocenę czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów,
- 3) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą,
- 4) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie RODO, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.

**§ 52.** Jeżeli przeprowadzona ocena skutków dla ochrony danych osobowych wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby Administrator Danych nie zastosował środków w celu zminimalizowania tego ryzyka, przed rozpoczęciem przetwarzania Administrator Danych konsultuje się z PUODO.

**§ 53.** Konsultacja odbywa się za pośrednictwem Inspektora ds. Ochrony Danych, przedstawiając następujące informacje:

- 1) odpowiednie obowiązki Administratora Danych, współadministratorów oraz podmiotów przetwarzających uczestniczących w przetwarzaniu,
- 2) cele i sposoby zamierzonego przetwarzania,
- 3) środki i zabezpieczenia mające chronić prawa i wolności osób, których dane dotyczą,
- 4) dane kontaktowe Inspektora ds. Ochrony Danych,
- 5) ocenę skutków dla ochrony danych,
- 6) wszelkie inne informacje, których zażąda PUODO.

## **Rozdział XIV**

## **Analiza ryzyka**

§ 54. Zgodnie z art. 32 RODO Administrator Danych wdraża odpowiednie środki techniczne i organizacyjne, które zapewniają właściwy poziom bezpieczeństwa odpowiadający ryzyku wystąpienia naruszenia praw i wolności osób fizycznych, których dane dotyczą.

§ 55. W Urzędzie analiza ryzyka dla procesów, w których przetwarzane są dane osobowe przeprowadzona jest zgodnie z procedurą opisaną w załączniku nr 14 do Polityki Bezpieczeństwa.

## **Rozdział XV**

### **Monitoring przestrzegania przepisów ochrony danych osobowych**

§ 56. Monitoring przestrzegania przepisów ochrony danych osobowych realizowany jest przez Inspektora ds. Ochrony Danych poprzez:

- 1) audyty i czynności sprawdzające w zakresie zgodności przetwarzania danych osobowych z przepisami prawa powszechnie obowiązującymi oraz wewnętrznymi aktami normatywnymi obowiązującymi w Urzędzie.
- 2) sprawowanie nadzoru nad czynnościami przetwarzania danych osobowych,
- 3) zgłaszanie uwag dotyczących ochrony danych osobowych użytkownikom i Administratorowi Danych,
- 4) zgłaszanie propozycji i opinii z zakresu ochrony danych osobowych odnośnie stosowanych rozwiązań w Urzędzie.

....., dnia.....  
(pieczęć Administratora Danych Osobowych)

### **UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH NR .....**

Na podstawie art. 32 ust 4 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- RODO), (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.), upoważniam Pana/Panią:..... do przetwarzania danych osobowych w związku z wykonywaniem obowiązków pracowniczych i w zakresie wynikającym z zajmowanego stanowiska pracy.

Upoważnienie udzielane jest na czas trwania zatrudnienia (do odwołania).

.....  
podpis Administratora Danych Osobowych

### **OŚWIADCZENIE PRACOWNIKA**

Niniejszym zobowiązuję się do zachowania poufności wszelkich danych, do których mam bądź będę miał/a dostęp podczas wykonywania zadań służbowych, które nie są przeznaczonych do publicznego rozpowszechniania. Oświadczam, że zobowiązuję się do zachowania w tajemnicy danych i informacji o sposobach ich zabezpieczenia również po ustaniu zatrudnienia. Jednocześnie zobowiązuję się do niezwłocznego zwrócenia wszelkich dokumentów po rozwiązaniu umowy.

Potwierdzam, że zapoznałem/am się z:

- regulaminami, instrukcjami i procedurami obowiązującymi na stanowisku pracy, wiążącymi się z ochroną danych osobowych i zobowiązuję się do ich przestrzegania,
- rozporządzeniem 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 95/94/WE (ogólne rozporządzenie o ochronie danych), (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.),
- ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r. poz. 1781).

.....  
podpis osoby upoważnionej

**Rejestr upoważnień do przetwarzania danych osobowych  
w Urzędzie Żeglugi Śródlądowej we Wrocławiu**

Numer upoważnienia	Nazwisko i imię użytkownika	Zakres upoważnienia	Wydział/ Stanowisko	Data nadania upoważnienia	Data cofnięcia/ wygaśnięcia upoważnienia	Informacja o zmianie nazwiska

Data aktualizacji:.....

### Rejestr czynności przetwarzania danych osobowych

Nazwa i dane kontaktowe Administratora Danych	
Nazwa	
Adres	
Email	
Telefon	

Nazwa i dane kontaktowe Inspektora ds. Ochrony Danych	
Nazwa	
Adres	
Email	
Telefon	

**Rejestr czynności przetwarzania danych osobowych**

Lp.	Nazwa czynności przetwarzania	Cel przetwarzania	Kategorie osób	Kategorie danych	Planowany termin usunięcia kategorii danych	Nazwa współadministratora i dane kontaktowe	Nazwa podmiotu przetwarzającego i dane kontaktowe	Kategorie odbiorców	Ogólny opis techniczny i organizacyjnych środków bezpieczeństwa	Transfer do kraju trzeciego lub organizacji międzynarodowej	Dokumentacja odpowiednich zabezpieczeń w przypadku transferu

Data aktualizacji:.....

### Rejestr kategorii czynności przetwarzania danych osobowych

Nazwa i dane kontaktowe Podmiotu Przetwarzającego	
Nazwa	
Adres	
Email	
Telefon	

Nazwa i dane kontaktowe Inspektora ds. Ochrony Danych	
Nazwa	
Adres	
Email	
Telefon	

### Rejestr kategorii czynności przetwarzania danych osobowych

Lp.	Kategorie przetwarzania	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (jeżeli jest to możliwe)	Nazwa administratora danych osobowych				Nazwy państw trzecich lub organizacji międzynarodowych, do których dane są przekazywane	Dokumentacja odpowiednich zabezpieczeń danych osobowych przekazywanych na podstawie art. 49 ust. 1 akapit drugi	Czas przetwarzania
			Nazwa i dane kontaktowe administratora	Nazwa i dane kontaktowe współadministratora (jeżeli dotyczy)	Nazwa i dane kontaktowe przedstawiciela administratora (jeżeli wyznaczono)	Inspektor ochrony danych administratora (jeżeli powołano)			

Data aktualizacji:.....

### Rejestr umów powierzenia przetwarzania danych osobowych

Lp.	Numer umowy świadczenia usług	Nazwa administratora danych osobowych	Nazwa podmiotu, któremu powierzono dane	Data powierzenia	Cel powierzenia	Zakres powierzonych danych

Data aktualizacji:.....

Miejscowość:

Data:

Numer wniosku:

Data wpływu:

### Wniosek o realizację prawa

- Uzyskanie informacji i dostęp do danych.
- Otrzymanie kopii danych.
- Sprostowanie i aktualizacja danych.
- Przeniesienie danych do innego Administratora Danych Osobowych.
- Ograniczenie przetwarzania danych – prawo do sprzeciwu.
- Usunięcia danych – „prawo do bycia zapomnianym”.

#### Dane osoby wnioskującej:

Imię:.....

Nazwisko:.....

Dane kontaktowe:.....

Dodatkowe informacje pomocne przy identyfikacji osoby w zbiorach danych:.....

.....

.....

Wnioskuje o uzyskanie informacji w zakresie .....  
(procesy przetwarzania danych osobowych/zbiory danych osobowych) na podstawie art. 12-22  
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. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.).

Uzasadnienie wniosku:.....

.....

.....

.....

(Podpis osoby wnioskującej)

**Rejestr udostępnień i realizacji praw osób fizycznych**

Lp.	Data wpływu	Typ wniosku	Imię i nazwisko wnioskodawcy	Dane kontaktowe	Data realizacji	Osoba realizująca	Zakres danych	Sygnatura i data odpowiedzi

Data aktualizacji:.....

**Rejestr zgód na przetwarzanie danych osobowych**

Lp.	Imię i nazwisko osoby wyrażającej zgodę	Dane kontaktowe	Zakres wyrażonej zgody	Data wyrażenia zgody	Data wycofania zgody

Data aktualizacji:.....

**Rejestr przekazywanych danych osobowych do państw trzecich lub organizacji  
międzynarodowych**

Lp.	Komórka organizacyjna, która przekazuje dane osobowe	Data przekazania danych osobowych	Podmiot do którego przekazano dane osobowe	Zakres przekazywanych danych osobowych	Okoliczność przekazanych danych osobowych	Podstawę prawną przekazania danych osobowych

Data aktualizacji:.....

**Zgłoszenie naruszenia ochrony danych osobowych  
w Urzędzie Żeglugi Śródlądowej we Wrocławiu**

1. Data zdarzenia: .....Godzina zdarzenia: .....

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

.....

(imię i nazwisko, stanowisko służbowe, komórka organizacyjna)

3. Lokalizacja zdarzenia:

.....

(adres budynku, nr pokoju/pomieszczenia)

4. Opis zdarzenia związanego z naruszeniem ochrony danych osobowych (przebieg zdarzenia,  
opis zachowania uczestników):

.....

5. Podjęte działania:

.....

6. Przyczyny wystąpienia zdarzenia:

.....

7. Kategorie danych, których dotyczy naruszenie:

.....

8. Kategorie osób, których dotyczy naruszenie:

.....

.....  
(data, podpis osoby zgłaszającej naruszenie)

**Raport nr ..... / .....**  
**z naruszenia ochrony danych osobowych w Urzędzie Żeglugi Śródlądowej**  
**we Wrocławiu**

1. Data: ..... Godzina: .....

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

.....

(imię i nazwisko, stanowisko służbowe)

3. Osoba przyjmująca zgłoszenie o zaistniałym zdarzeniu:

.....

(imię i nazwisko, stanowisko służbowe)

4. Lokalizacja zdarzenia:

.....

(nr pokoju/pomieszczenia)

5. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

.....

6. Podjęte działania:

.....

7. Przyczyny wystąpienia zdarzenia:

.....

8. Postępowanie wyjaśniające:

.....

9. Ocena skuteczności przeprowadzonego postępowania naprawczego:

.....

10. Podjęte środki techniczne, organizacyjne i dyscyplinarne w celu zapobiegania  
w przyszłości podobnym naruszeniom ochrony danych osobowych:

.....

.....  
(data, podpis Inspektora ds. Ochrony Danych)

**Rejestr naruszeń ochrony danych osobowych**

Nr naruszenia	Osoba zgłaszająca	Osoba przyjmująca zgłoszenie	Rodzaj naruszenia	Podjęte działania	Wyniki podjętych działań	Data zamknięcia naruszenia

Data aktualizacji:.....

**Rejestr zewnętrznych naruszeń ochrony danych osobowych**

Data otrzymania informacji	Podmiot informujący o naruszeniu	Rodzaj naruszenia	Podjęte działania	Uwagi

Data aktualizacji:.....

## **Procedura przeprowadzenia analizy ryzyka ochrony danych osobowych w Urzędzie Żeglugi Śródlądowej we Wrocławiu**

### **1. Cel procedury**

Procedura analizy ryzyka ma celu ustanowienie jednolitych zasad zarządzania ryzykiem w zakresie przetwarzania danych osobowych.

### **2. Zakres obowiązywania**

Procedura zarządzania ryzykiem ma zastosowanie dla wszystkich siedzib Urzędu Żeglugi Śródlądowej we Wrocławiu.

Wszystkie procesy określone w rejestrze czynności przetwarzania danych osobowych oraz rejestrze kategorii czynności przetwarzania danych osobowych podlegają szacowaniu ryzyka zgodnie z opisaną procedurą.

### **3. Terminologia**

Bezpieczeństwo danych osobowych – zachowanie poufności, integralności, dostępności i zgodności prawnej danych osobowych.

Dostępność danych osobowych – właściwość polegająca na tym, że dane osobowe są możliwe do wykorzystania przez uprawniony podmiot na jego żądanie, w założonym czasie.

Integralność danych osobowych – właściwość polegająca na tym, że dane osobowe nie zostały zmodyfikowane w sposób nieuprawniony.

Poufność danych osobowych – właściwość polegająca na tym, że dane osobowe nie są udostępniane ani ujawniane nieautoryzowanym osobom, podmiotom lub procesom.

Ryzyko – wpływ zagrożenia na bezpieczeństwo danych osobowych.

Zagrożenie – zdarzenie, które może skutkować utratą poufności, integralności, dostępności lub zgodności prawnej danych osobowych.

Zgodność prawna – właściwość polegająca na tym, że dane działanie związane z danymi osobowymi jest zgodne z przepisami powszechnie obowiązującego prawa, któremu podlega urząd.

### **4. Odpowiedzialność i uprawnienia**

Dyrektor Urzędu Żeglugi Śródlądowej we Wrocławiu pełniący funkcję Administratora Danych odpowiedzialny jest za akceptację wyników analizy i szacowania, a także podejmowanie decyzji dotyczących minimalizacji ryzyka.

Do zadań Inspektor ds. Ochrony Danych należy monitorowanie procesu przeprowadzania analizy ryzyka oraz proponowanie rekomendowanych działań, podejmowanych w następstwie analizy ryzyka.

Do zadań użytkownika odpowiadającego za proces opisany w rejestrze czynności przetwarzania danych osobowych oraz rejestrze kategorii czynności przetwarzania danych osobowych należy uzupełnienie arkusza analizy ochrony danych osobowych, a także realizowanie zaleconych działań zmniejszających ryzyko. Użytkownik, który odpowiedzialny jest za szacowanie ryzyka wskazanego procesu pełni funkcję właściciela tego ryzyka.

## **5. Opis postępowania**

### **5.1. Ocena ryzyka**

Ocena ryzyka składa się z trzech etapów:

1. Identyfikacja ryzyka.
2. Analiza ryzyka.
3. Ewaluacja ryzyka.

### **5.2. Identyfikacja ryzyka**

Identyfikacja ryzyka polega na wskazaniu takich zdarzeń, które mają, lub mogą mieć wpływ na zachowanie poufności, integralności i dostępności oraz spełnienie wymogów prawnych w odniesieniu do przetwarzanych danych osobowych. Identyfikacja ryzyka jest prowadzona metodą samooceny użytkowników.

Efektym identyfikacji jest lista zagrożeń, które mają wpływ na zachowanie poufności, integralności i dostępności oraz spełnienie wymogów prawnych w odniesieniu do ustalonego kontekstu analizy.

### **5.3. Analiza ryzyka**

Każde zidentyfikowane zagrożenie podlega analizie, mającej na celu oszacowanie wpływu, czyli skutku wystąpienia zdarzenia, oraz prawdopodobieństwa ryzyka.

1. Określenie wartości skutku w postaci wagi zmaterializowania się zagrożenia, liczonej wg następującego wzoru:

$$S = Sp + Si + Sd + Spr$$

gdzie:

S – wartość skutku.

Sp – skutek dla zachowania poufności informacji i posiada wartość 0,25 jeśli zmaterializowanie się zagrożenia ma wpływ na zachowanie poufności, lub 0, jeśli zagrożenie nie ma wpływu na poufność.

Si – skutek dla zachowania integralności informacji i posiada wartość 0,25 jeśli zmaterializowanie się zagrożenia ma wpływ na zachowanie integralności, lub 0, jeśli zagrożenie nie ma wpływu na integralność.

Sd – oznacza skutek dla zachowania dostępności informacji i posiada wartość 0,25 jeśli zmaterializowanie się zagrożenia ma wpływ na zachowanie dostępności, lub 0, jeśli zagrożenie nie ma wpływu na dostępność.

Spr – skutek dla zachowania zgodności prawnej i posiada wartość 0,25 jeśli zmaterializowanie się zagrożenia ma wpływ na zachowanie zgodności prawnej, lub 0, jeśli zagrożenie nie ma wpływu na zgodność prawną.

2. Określenie prawdopodobieństwa wystąpienia zagrożenia, czyli przewidywanej częstotliwości występowania zagrożenia wg poniższej skali wartości:

Wartość	Prawdopodobieństwo	Uwagi
1	Mało prawdopodobne	Zagrożenie praktycznie niewystępujące, może się urealnić w pewnych wyjątkowych okolicznościach i zakłada się, że będzie to pojedyncze wystąpienie.
2	Rzadkie	Zakłada się, że zagrożenia mogą występować rzadko. Istnieją zapisy lub dowody na wystąpienie zdarzenia w przeszłości.
3	Realne	Zakłada się że zagrożenia mogą się urealnić. Może wystąpić niezależnie od panujących okoliczności. Mogą występować okoliczności zwiększające prawdopodobieństwo wystąpienia konkretnego zdarzenia (scenariusza)
4	Bardzo prawdopodobne	Oczekuje się, że zagrożenia wystąpią w większości przypadków lub okoliczności. Istnieje pełna wiedza dotycząca wystąpień zagrożeń w przeszłości, skutków oraz przyczyn.

3. Wyliczenie wartości ryzyka wg poniższego wzoru:

$$R = P \times S$$

gdzie:

R – wartość ryzyka.

P – prawdopodobieństwo wystąpienia danego zdarzenia.

S – oznacza skutek, czyli konsekwencje całkowite zmaterializowania się danego zagrożenia, przy czym prawdopodobieństwo wystąpienia konkretnego zagrożenia zawsze odpowiada jednemu konkretnemu skutkowi.

Wartość ryzyka jest określana osobno dla każdego zdarzenia. Wyliczenia można dokonać za pomocą ogólnej macierzy wartościowania ryzyka:

Skutek	Prawdopodobieństwo			
	1	2	3	4
0,25	0,25	0,5	0,75	1
0,5	0,5	1	1,5	2
0,75	0,75	1,5	2,25	3
1	1	2	3	4

#### 4. Określenie poziomu ryzyka.

Wyliczenie poziomu ryzyka dla danego zdarzenia odbywa się wg poniższego wzoru:

$$Pr = R \times W$$

gdzie:

R – wartość ryzyka.

W – waga zagrożenia według poniższej skali wartości:

Wartość	Waga zagrożenia	Uwagi
1	Znikoma	Zagrożenie praktycznie nie ma wpływu na bezpieczeństwo informacji, a jego zmaterializowanie nie niesie żadnych strat zarówno dla Urzędu jak i dla podmiotów danych.
2	Mała	Zmaterializowanie się zagrożenia może generować niewielkie straty finansowe i wizerunkowe dla Urzędu i niewielkie straty dla podmiotów danych.
3	Istotna	Zmaterializowanie się zagrożenia istotnie wpłynie na działalność Urzędu poprzez generowanie dużych strat finansowych i wizerunkowych oraz może powodować poważne szkody dla podmiotów danych.

4	Krytyczna	Zmaterializowanie się zagrożenia może uniemożliwić działalność Urzędu, spowodować bardzo duże straty finansowe i wizerunkowe oraz może powodować poważne szkody dla podmiotów danych.
---	-----------	---

Wyliczenia można dokonać za pomocą ogólnej macierzy poziomu ryzyka:

Wartość ryzyka	Waga				
		1	2	3	4
	0,25	0,25	0,5	0,75	1
	0,5	0,5	1	1,5	2
	0,75	0,75	1,5	2,25	3
	1	1	2	3	4
	1,5	1,5	3	4,5	6
	2	2	4	6	8
	2,25	2,25	5	7,75	10
	3	3	6	9	12
	4	4	8	12	16

Poziom ryzyka jest klasyfikowany, jako:

Poziom ryzyka		Zakres
Minimalne		0 – 1
Małe		1,5 – 5
Średnie		6 – 10
Wysokie		12 – 16

#### 5.4.Ewaluacja ryzyka

Ewaluacja ryzyka jest procesem porównania wyników analizy z przyjętymi kryteriami ryzyka w celu podjęcia decyzji o sposobie postępowania z ryzykiem. W Urzędzie przyjęte są następujące sposoby postępowania z ryzykiem:

- **akceptacja** – tolerowanie ryzyka ze względu na trudności z wprowadzeniem środków kontroli lub koszt ich wprowadzenia nie równoważy spodziewanych korzyści;
- **postępowanie** – polega na wprowadzeniu środków kontroli lub wzmocnieniu istniejących, w celu zmniejszeniu poziomu ryzyka do poziomu akceptowalnego. Postępowanie może polegać na zastosowaniu zabezpieczeń lub przeniesieniu odpowiedzialności za dane ryzyko na trzecią stronę (ubezpieczenie, outsourcing);
- **unikanie** – odejście od działań, które powodują nieakceptowalny poziom ryzyka lub rozpoczęcie konsultacji z organem nadzorczym. Decyzja taka musi być formalnie zaakceptowana przez Administratora Danych.

Poniższa tabela prezentuje kryteria akceptacji ryzyka przyjęte w organizacji w odniesieniu do dopuszczalnych sposobów postępowania:

Poziom ryzyka	Postępowanie	Zakres	Uwagi
Minimalne	Akceptacja	0 – 1	Nie wymaga działania
Małe	Akceptacja/Postępowanie	1,5 – 5	Może wymagać redukcji ryzyka
Średnie	Postępowanie	6 – 10	Wymagana redukcja ryzyka
Wysokie	Unikanie	12 – 16	Należy rozważyć unikanie ryzyka

## 6. Ocena skutków dla ochrony danych

Jeśli z analizy ryzyka przetwarzania danych osobowych wynika, że dane zagrożenie powoduje wysokie ryzyko dla bezpieczeństwa przetwarzania danych, należy przeprowadzić ocenę skutków dla ochrony danych zgodnie z rozdziałem XIII Polityki Bezpieczeństwa.

## 7. Monitorowanie analizy ryzyka

Wyniki przeprowadzonej analizy ryzyka przetwarzania danych osobowych przedstawiane są Administratorowi Danych w celu zatwierdzenia i podjęcia decyzji w zakresie realizacji zaproponowanych dalszych działań.

**Arkusz analizy ryzyka ochrony danych osobowych**

IDENTYFIKACJA RYZYKA		ANALIZA RYZYKA											EWALUACJA RYZYKA	Postępowanie z ryzykiem
Ocena bezpieczeństwa danych osobowych		Analiza ryzyka przetwarzania danych osobowych											Rekomendacje w obszarze	
Lp.	Obszar	Waga zagrożenia	Zagrożenie	Poufność	Integry- lność	Dostępność	Prawne	Prawdopo- dobieństwo	Skutek	Wartość ryzyka	Poziom ryzyka	Poziom Ryzyka		

Data aktualizacji:.....

.....

Podpis Administratora Danych