Założenia ogólne systemu
rejestru czynności przetwarzania / rejestru kategorii czynności przetwarzania
(Projekt)

1 Podstawa prawna

Podstawą prawną prowadzenia rejestru czynności przetwarzania / rejestru kategorii czynności przetwarzania jest art. 30 ust. 1 oraz art. 30 ust. 2.
Zgodnie z art. 30 ust. 3 rejestry, o których mowa w ust. 1 i 2 (czynności przetwarzania / kategorii czynności przetwarzania), mają formę pisemną, w tym formę elektroniczną.

Minimalny zestaw informacyjny rejestru czynności przetwarzania jest określony w art. 30 ust. 1 RODO i obejmuje :
a) imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych;
b) cele przetwarzania;
c) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
d) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
e) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń;
f) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
g) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1.

Minimalny zestaw informacyjny rejestru kategorii czynności przetwarzania jest określony w art. 30 ust. 2 RODO i obejmuje :
a) imię i nazwisko lub nazwa oraz dane kontaktowe podmiotu przetwarzającego lub podmiotów przetwarzających oraz każdego administratora, w imieniu którego działa podmiot przetwarzający, a gdy ma to zastosowanie – przedstawiciela administratora lub podmiotu przetwarzającego oraz inspektora ochrony danych;
b) kategorie przetwarzań dokonywanych w imieniu każdego z administratorów;
c) gdy ma to zastosowanie –przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń;
d) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1.

2 Rola rejestru

System ma wspierać osobę prowadzącą rejestr (inspektor ochrony danych, jego zastępca lub inna osoba wyznaczona do prowadzenia rejestru) w prowadzeniu rejestrów czynności przetwarzania oraz kategorii czynności przetwarzania. Zgodnie z art. 30 ust. 3 rejestry czynności przetwarzania / kategorii czynności przetwarzania, mają formę pisemną, w tym formę elektroniczną.

Zadaniem systemu jest zgromadzenie potrzebnych danych w formie elektronicznej. Wydruki z rejestru mają pełnić rolę wersji papierowej. Eksport do pliku Excel'a mają pełnić rolę wersji elektronicznej.

2.1 Rola prowadzącego rejestr

Prowadzący rejestr wykonuje czynności :
- wpisu do rejestru,
- wyrejestrowania z rejestru poprzez ustawienie flagi aktywności
- klonowania dowolnej pozycji z rejestru w celu utworzenia nowej
- edycję rejestru
- przeglądanie rejestru

Prowadzący rejestr powinien móc:
- przeglądać wykaz czynności prowadzonych w izbie
- przeglądać wykaz czynności prowadzonych w komórkach izby i urzędu
- edytować (dopisywać / usuwać) stosowane w komórkach środki ochrony

2.2 Rola kierownika komórki

Rejestr służy kierownikom komórek organizacyjnych IAS do zapoznania się z aktualnym stanem rejestru w celu ustalenia, czy zgłosić prowadzącemu rejestr:
1) nową czynność przetwarzania do rejestracji
2) zakończenie czynności przetwarzania celem jej wyrejestrowania / wyłączenia aktywności
3) propozycję zmiany / edycji czynności przetwarzania w zakresie kolumn opisujących czynność przetwarzania

Dla poszczególnych rejestrów system powinien zapewniać możliwość wydruku wszystkich pozycji lub ich podzbioru wg zadanego kryterium w postaci kart czynności przetwarzania.

Kierownik komórki powinien móc:
- przeglądać wykaz czynności prowadzonych w izbie
- przeglądać wykaz czynności, w których uczestniczy jego komórka
- edytować dane specyficzne dla kierowanej komórki, w tym co najmniej stosowane ochrony.

2.3 Inne role

Na razie nie określono.

3 Projektowany zestaw informacyjny rejestrów

3.1 Rejestr czynności

1) Nazwa ogólna czynności przetwarzania
2) imię i nazwisko lub nazwę oraz dane kontaktowe administratora
3) Jedna lub więcej nazwa współadministratorów/ przedstawiciela administratora + inspektora ochrony danych;
4) Aktywność pozycji

5) Jedna lub więcej nazwa komórki organizacyjnej IAS uczestniczącej w przetwarzaniu
6) Jedna lub więcej podstawa prawna przetwarzania
7) Cel przetwarzania
8) Podstawa zgodności z prawem z art. 6 ust. 1 lit. a do e RODO
9) Jedna lub więcej kategorii osób, których dane dotyczą ← Jedna lub więcej kategorii danych osobowych
10) Jedna lub więcej podstawa przetwarzania danych o szczególnym charakterze ← Jedna lub więcej kategoria danych o szczególnym charakterze
11) Źródło danych ← {Od osoby, której dane dotyczą / od innej osoby}
12) Termin usunięcia danych wynikający z przepisów (maksymalny)
13) Jedna lub więcej nazwa współadministratora ← ich dane kontaktowe
14) Jedna lub więcej nazwa podmiotu przetwarzającego ←i dane kontaktowe
15) Jedna lub więcej kategorii odbiorców (nazwa, adres – nie dotyczy własnych jednostek i komórek)
16) Jeden lub więcej sposobów przetwarzania ← nazwa systemu lub oprogramowania
17) Jeden lub więcej opis technicznych i organizacyjnych środków ochrony ← (z polityki ochrony danych osobowych)
18) Transfer do krajów trzecich i organizacji międzynarodowych ← Jedno lub więcej zabezpieczeń dla transferu do krajów trzecich
19) Proces główny z architektury procesów KAS
20) Jedna lub więcej przesłanek wysokiego ryzyka (z komunikatu UODO)

3.2 Rejestr kategorii czynności

1) Nazwa ogólna kategorii czynności przetwarzania
2) Jedna lub więcej nazwa podmiotu przetwarzającego lub podmiotów przetwarzających oraz każdego administratora, w imieniu którego działa podmiot przetwarzający, a gdy ma to zastosowanie – przedstawiciela administratora lub podmiotu przetwarzającego oraz inspektora ochrony danych
3) kategorie przetwarzań dokonywanych w imieniu każdego z administratorów;
4) Transfer do krajów trzecich i organizacji międzynarodowych ← Jedno lub więcej zabezpieczeń dla transferu do krajów trzecich
5) Jeden lub więcej opis technicznych i organizacyjnych środków ochrony ← (z polityki ochrony danych osobowych)

4 Słowniki

Operacje na pozycjach słownika wykonuje osoby prowadzące rejestr. Do słownika można dodawać nowe rodzaje danych oraz usuwać istniejące.

4.1 Rodzaje danych osobowych

Słownik rodzajów danych osobowych zawiera co najmniej:

nazwisko i imiona,
imiona rodziców,
data urodzenia,
miejsce urodzenia,
adres zamieszkania lub pobytu,
numer identyfikacyjny PESEL,
Numer Identyfikacji Podatkowej (NIP),
zawód,

wykształcenie,
seria i numer dowodu osobistego,
numer telefonu,
adres e-mail;
numer konta

4.2 Rodzaje danych o szczególnym charakterze

Słownik danych o szczególnym charakterze zawiera co najmniej:

dane dotyczące stanu zdrowia,
pochodzenie rasowe lub etniczne,
poglądy polityczne,
przekonania religijne lub światopoglądowe,
przynależność do związków zawodowych
dane genetyczne,
dane biometryczne w celu identyfikacji osób,
seksualność lub orientacja seksualna,
wyroki skazujące i naruszenia prawa

4.3 Przesłanki wysokiego ryzyka (z komunikatu UODO)

1. Ewaluacja lub ocena, w tym profilowanie i przewidywanie (analiza behawioralna) w celach wywołujących negatywne skutki prawne, fizyczne, finansowe lub inne niedogodności dla osób fizycznych;
2. Zautomatyzowane podejmowanie decyzji wywołujących skutki prawne, finansowe lub podobne istotne skutki;
3. Systematyczne monitorowanie na dużą skale miejsc dostępnych publicznie wykorzystujące elementy rozpoznawania cech lub właściwości obiektów, które znajdą się w monitorowanej przestrzeni. Do tej grupy systemów nie są zaliczane systemy monitoringu wizyjnego, w których obraz jest nagrywany i wykorzystywany tylko w przypadku potrzeby analizy incydentów naruszenia prawa;
4. Przetwarzanie szczególnych kategorii danych osobowych i dotyczących wyroków skazujących i czynów zabronionych (danych wrażliwych wg opinii WP 29);
5. Dane przetwarzane na dużą skalę;
6. Przeprowadzanie porównań, ocena lub wnioskowanie na podstawie analizy danych pozyskanych z różnych źródeł;
7. Przetwarzanie danych dotyczących osób, których ocena i świadczone im usługi są uzależnione od podmiotów lub osób, które dysponują uprawnieniami władczymi i/lub oceniającymi;
8. Innowacyjne wykorzystanie lub zastosowanie rozwiązań technologicznych lub organizacyjnych
9. Gdy przetwarzanie samo w sobie uniemożliwia osobom, których dane dotyczą, wykonywanie prawa lub korzystanie z usługi lub umowy.