GIODO

Generalny Inspektor
Ochrony Danych Osobowych

Wskazówki i wyjaśnienia dotyczące obowiązku rejestrowania czynności i kategorii czynności przetwarzania określonego w art. 30 ust. 1 i 2 RODO

Wskazówki i wyjaśnienia przygotowali pracownicy Biura Generalnego Inspektora Ochrony Danych Osobowych:

dr inż. Andrzej Kaczmarek - dyrektor Departamentu Informatyki,

Monika Młotkiewicz - zastępca dyrektora Departamentu Rejestracji,

Michał Mazur - informatyk w Departamencie Informatyki.

Spis treści

1. Informacje ogólne.

Obowiązek prowadzenia rejestru czynności wynika z art. 30 ust. 1 ogólnego rozporządzenia o ochronie danych (RODO)[1], który stanowi że „Każdy administrator oraz – gdy ma to zastosowanie – przedstawiciel administratora prowadzą rejestr czynności przetwarzania danych osobowych, za które odpowiadają". W rejestrze tym, zgodnie z dalszą treścią ww. artykułu, powinny znaleźć się następujące informacje:

a) imię i nazwisko lub nazwa 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.

Natomiast podmioty przetwarzające, oraz – gdy ma to zastosowanie – ich przedstawiciele, zgodnie z art. 30 ust. 2 RODO, zobowiązani są do prowadzenia rejestru kategorii czynności przetwarzania wykonywanych w imieniu zlecających im je administratorów danych. W rejestrze kategorii czynności przetwarzania powinny być zawarte:

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.

Przytoczone przepisy wskazują obligatoryjne składniki rejestrów. Jednak wątpliwości może budzić znaczenie poszczególnych pojęć użytych w powołanych przepisach, a także stopień szczegółowości rejestrów i sposób ich prowadzenia.

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), https://giodo.gov.pl/pl/569/9276.

Dla ułatwienia realizacji tego zadania Generalny Inspektor Ochrony Danych Osobowych (GIODO), przygotował **szablony rejestru czynności przetwarzania i rejestru kategorii czynności wraz z przykładami ich uzupełnienia oraz objaśnienia dotyczące sposobu realizacji obowiązków określonych w art. 30 RODO.** W przypadku szablonu rejestru czynności przykłady czynności przetwarzania dotyczą kilku, wybranych czynności przetwarzania prowadzonego przez szkołę podstawową jako administratora danych:

1. Rekrutacja pracowników pomocniczych, administracyjnych oraz nauczycieli.
2. Prowadzenie rejestru pracowników, akt pracowniczych i ewidencji czasu ich pracy.
3. Zgłoszenie pracowników i członków ich rodzin do ZUS, aktualizacja zgłoszonych danych i przekazywanie danych o zwolnieniach.
4. Prowadzenie rozliczeń w zakresie wypłaty wynagrodzeń pracownikom, naliczania obciążeń oraz naliczania i odprowadzania składek do ZUS.
5. Rekrutacja uczniów do szkół podstawowych.
6. Prowadzenie ewidencji uczniów.
7. Prowadzenie dziennika lekcyjnego.

W przypadku rejestru kategorii czynności – przykłady kategorii czynności mogą dotyczyć dowolnego podmiotu przetwarzającego i są to:

1. Udostępnienie i utrzymywanie zdalnej platformy programistycznej do prowadzenia sklepu internetowego w środowisku sprzętowo-programowym wynajętym przez przetwarzającego.
2. Udostępnienie i utrzymywanie zdalnej platformy programistycznej do prowadzenia rekrutacji pracowników w środowisku sprzętowo-programowym wynajętym przez przetwarzającego.
3. Dostarczenie usługi wsparcia technicznego (instalacji, konfiguracji, naprawy, odzyskania po awarii, przygotowania raportów z bazy danych, itp.) dla systemu Kadry-Płace-ABZ w środowisku sprzętowo-programowym administratora.
4. Udostępnienie i utrzymywanie zdalnej platformy programistycznej do prowadzenia dziennika lekcyjnego w środowisku sprzętowo-programowym przetwarzającego.
5. Dostarczenie licencji systemu do prowadzenia dziennika elektronicznego wraz z usługą wsparcia technicznego w zakresie instalacji, konfiguracji, zabezpieczenia, odzyskania danych po awarii, w środowisku sprzętowo programowym administratora (szkoły).

Podkreślenia wymaga, że **przedstawionych szablonów rejestrów nie należy traktować jako jedynych prawidłowych wzorów**. Ze względu na różnorodność administratorów, sektorów, w których działają i procesów przetwarzania danych, które prowadzą oraz innych czynników, w praktyce może występować wiele różnych modeli (struktur) rejestru czynności. Ważne, żeby w każdym przypadku, administrator lub podmiot przetwarzający był w stanie przedstawić wymagane w art. 30 ust. 1 i 2 RODO elementy w odniesieniu do wszystkich prowadzonych procesów przetwarzania danych osobowych, w sposób czytelny i przejrzysty.

2. Jaki jest cel obowiązku prowadzenia rejestrów?

Motyw 82 RODO określa dwie podstawowe funkcje obowiązku prowadzenia rejestru:

1. Zachowanie przez administratora i podmiot przetwarzający zgodności z RODO.

2. Umożliwienie organowi nadzorczemu monitorowania prowadzonego przetwarzania.

Celem obowiązku określonego w art. 30 jest zatem zapewnienie - zarówno przez administratora oraz podmioty przetwarzające, jak i przez organ nadzorczy - zgodności z RODO (art. 5 ust. 2 RODO), czyli z wskazanymi w tym akcie prawnym zasadami i warunkami przetwarzania danych osobowych.

Prowadzone przez administratorów i przetwarzających rejestry pozwalają im usystematyzować wykonywane czynności oraz całościowo spojrzeć na wykonywane operacje przetwarzania danych osobowych pod względem zgodności zarówno z celami biznesowymi, jak i wymaganiami prawnymi. Dzięki zebranym w tych rejestrach informacjom, administratorzy i podmioty przetwarzające mogą również ocenić, w jakim zakresie dotyczą ich inne obowiązki wynikające z rozporządzenia ogólnego, np. obowiązek przeprowadzenia oceny skutków przetwarzania dla ochrony danych, która jest na gruncie rozporządzenia przewidziana m.in. w sytuacji przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 RODO, lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o których mowa w art. 10 RODO. Wykonywanie obowiązku określonego w art. 30 RODO pozwala na stałą weryfikację swojej działalności w zakresie przetwarzania danych osobowych oraz poddawanie ocenie każdego nowo wprowadzanego lub modyfikowanego procesu już na jego najwcześniejszym etapie.

Z drugiej zaś strony rejestry mają ułatwić organowi nadzorczemu kontrolę wszystkich procesów przetwarzania danych w organizacji. Na żądanie organu nadzorczego informacje o prowadzonym przez administratora i podmiot przetwarzający przetwarzaniu będą udostępniane organowi w sposób jednolity, czytelny i uproszczony, umożliwiający dokonanie ich szybkiego przeglądu i wstępnej weryfikacji. Rejestry dotyczą wszystkich czynności przetwarzania danych osobowych, a określona w art. 30 ust. 1 i ust. 2 RODO klasyfikacja zawiera wiele istotnych dla sprawowania nadzoru kryteriów. Zapoznanie się z takimi rejestrami może być jednym z pierwszym z działań podejmowanych w celu przeprowadzenia przez organ nadzorczy kontroli przestrzegania przepisów RODO, nie tylko w ramach audytów, o których mowa w art. 58 ust. 1 lit. b RODO, ale także w innych prowadzonych przez organ postępowaniach.

3. Kto jest obowiązany do prowadzenia rejestru czynności i rejestru kategorii czynności?

Obowiązek prowadzenia rejestru czynności spoczywa na **administratorze**, czyli osobie fizycznej lub prawnej, organie publicznym, jednostce lub innym podmiocie, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Obowiązek prowadzenia rejestrów kategorii czynności został nałożony zaś na **podmioty przetwarzające**, czyli osoby fizyczne lub prawne, organy publiczne, jednostki lub inne podmioty, które przetwarzają dane osobowe w imieniu administratora.

Warto zauważyć, że większość podmiotów przetwarzających będzie zobowiązana do prowadzenia zarówno rejestru kategorii czynności przetwarzania, jak i rejestru czynności przetwarzania danych, za które odpowiadają jako administratorzy (np. danych osób zatrudnionych).

Obowiązek prowadzenia rejestrów w określonych przypadkach spoczywa też na **przedstawicielach administratora i podmiotu przetwarzającego**. Zgodnie z art. 27 w związku z art. 3 ust. 2 RODO, obowiązek wyznaczenia swojego przedstawiciela mają administrator i podmiot przetwarzający nieposiadający jednostek organizacyjnych w Unii wówczas, jeżeli prowadzone przez nich czynności przetwarzania wiążą się z oferowaniem towarów lub usług takim osobom, których dane dotyczą, w Unii – niezależnie od tego, czy

wymaga się od tych osób zapłaty; lub monitorowaniem ich zachowania, o ile do zachowania tego dochodzi w Unii.

W przypadku **współadministratorów i procesów przetwarzania danych, w zakresie których wspólnie ustalają oni cele i sposoby przetwarzania danych**, przyjąć należy, że obowiązek prowadzenia rejestru ciąży na każdym z nich. Wskazuje na to zarówno brzmienie art. 30 ust. 1 RODO, zgodnie z którym do prowadzenia rejestru zobowiązany jest „każdy" administrator danych, a ponadto cel tego obowiązku, jakim jest zapewnienie - zarówno przez administratora, jak i przez organ nadzorczy - zgodności z RODO. W takim przypadku w rejestrze każdego ze współadministatorów powinien się znaleźć opis procesów przetwarzania objętych współadministrowaniem .

Ze względu na swoją zawartość **rejestry** czynności i kategorii czynności **mogą być** również **instrumentem** monitorowania zgodności przetwarzania danych z prawem **przydatnym dla inspektorów ochrony danych.** Wprawdzie z art. 30 rozporządzenia ogólnego bezsprzecznie wynika, że obowiązek prowadzenia rejestrów nie jest adresowany do inspektora ochrony danych, niemniej z pewnością może on w tym zakresie doradzać administratorowi i jednocześnie wykorzystywać zawarte w rejestrze informacje w swojej pracy (więcej na ten temat w serwisie ABI-Informator w sekcji Zadania inspektora ochrony danych oraz Pytania i odpowiedzi/Inspektor ochrony danych.)

Zgodnie z art. 30 ust. 5 RODO, obowiązek prowadzania rejestru czynności i rejestru kategorii czynności nie ma zastosowania do przedsiębiorcy lub podmiotu zatrudniającego mniej niż 250 osób, chyba że czynności przetwarzania, które wykonują:

1) mogą powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą,
2) nie mają charakteru sporadycznego lub obejmują szczególne kategorie danych osobowych, o których mowa w art. 9 ust. 1, lub
3) dotyczą wyroków skazujących i naruszeń prawa, o czym mowa w art. 10.

W motywie 13 preambuły RODO wskazano, że wyjątek dotyczący rejestrowania czynności przetwarzania dla podmiotów zatrudniających mniej niż 250 pracowników przewidziano ze względu na szczególną sytuację mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw. W związku z licznymi pytaniami dotyczącymi stosowania tego wyłączenia od obowiązku prowadzenia rejestru czynności i rejestru kategorii czynności w najbliższym czasie Grupa Robocza Art. 29, w pracach której uczestniczy GIODO, opublikuje swoje stanowisko.

4. Jak należy rozumieć pojęcie „czynności przetwarzania" w kontekście obowiązku prowadzenia rejestru czynności?

RODO nie definiuje pojęcia „czynności przetwarzania", jednak posługuje się nim w kilku przepisach lub motywach w różnych kontekstach, np. „Zgoda powinna dotyczyć wszystkich czynności przetwarzania dokonywanych w tym samym celu lub w tych samych celach." (motyw 32), „Aby stwierdzić, czy czynność przetwarzania można uznać za monitorowanie zachowania osób, których dane dotyczą, należy ustalić, czy osoby fizyczne są obserwowane w Internecie, w tym także czy później potencjalnie stosowane są techniki przetwarzania danych polegające na profilowaniu osoby fizycznej, w szczególności w celu podjęcia decyzji

jej dotyczącej lub przeanalizowania lub prognozowania jej osobistych preferencji, zachowań i postaw." (motyw 24).

Samo pojęcie „przetwarzanie" zostało zdefiniowane w art. 4 pkt 2 jako operacja lub zestaw operacji na danych, takich jak: *zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie*. Powstaje zatem pytanie, jak należy interpretować pojęcie „czynności przetwarzania danych" biorąc pod uwagę ww. definicję oraz fakt, że rejestr takich czynności odnosi się nie tylko do pojedynczych czynności przetwarzania, ale, jak wynika również z angielskiej wersji dokumentu („records of procesing activities") do czynności w liczbie mnogiej.

W kontekście obowiązku określonego w art. 30 ust. 1 RODO przyjąć należy, że **czynności przetwarzania to zespół powiązanych ze sobą operacji na danych, wykonywanych przez jedną lub kilka osób, które można określić w sposób zbiorczy, w związku z celem, w jakim te czynności są podejmowane.**

Tytułem przykładu: w przypadku rekrutacji pracowników, jeden cel będzie obejmował wiele cząstkowych operacji niewymagających szczegółowego ich opisywania w rejestrze, takich jak. pozyskiwanie informacji o kandydatach z ofert nadesłanych w wyniku ogłoszenia, dokonywanie ich selekcji, uzyskiwanie dodatkowych informacji w ramach przeprowadzania wywiadów z wybranymi osobami, usunięcie danych osób, które nie zostały wskazane do zatrudnienia itp. Nie ma konieczności opisywania każdej poszczególnej operacji wykonywanej na danych w procesie określonym zbiorczo „rekrutacja pracowników", bo nie jest to konieczne dla scharakteryzowania przetwarzania w świetle wskazanych w art. 30 ust. 1 RODO kryteriów. Podobnie w przypadku przetwarzania danych w celu obsługi umów sprzedaży określonych towarów i usług jako „czynność przetwarzania" wskazać można ogólnie np. „obsługa umów sprzedaży", bez konieczności wpisywania do rejestru cząstkowych operacji wykonywanych w ramach tego procesu, takich jak: rejestrowanie danych nabywcy (klienta), wystawienie faktury, wydanie klientowi oryginału faktury, przechowywanie kopii faktury w systemie sprzedaży, zapis danych z faktury w rejestrze VAT czy też po zakończeniu każdego miesiąca generowanie pliku JPK-VAT, a po jego weryfikacji i podpisaniu - wysłanie do urzędu skarbowego.

Przy wyodrębnianiu poszczególnych procesów (zespołów czynności) **zasadne jest uwzględnienie rzeczywistego podziału zadań pomiędzy poszczególnymi komórkami organizacyjnymi lub osobami w danej jednostce**. W dużych podmiotach, o złożonej strukturze organizacyjnej często wydziela się oddzielny zespół do spraw kadr i oddzielny do spraw płac. Zespół Kadr wykonuje najczęściej takie czynności przetwarzania, jak: prowadzenie ewidencji pracowników, czasu ich pracy, szkoleń, urlopów, zwolnień lekarskich itp. Do zadań tego zespołu należy też wykonywanie takich czynności, jak zgłaszanie pracowników i członków ich rodzin do ZUS oraz zgłaszanie aktualizacji dotyczących ich informacji. Zespół Płac natomiast prowadzi takie czynności przetwarzania, jak: wyliczanie wynagrodzeń i ich wypłata, a także wyliczanie składek na ubezpieczenie emerytalne, rentowe, chorobowe, wypadkowe i przekazywanie tych informacji do ZUS wraz z imiennymi raportami miesięcznymi ZUS RCA o należnych składkach i wypłaconych świadczeniach.

W małych jednostkach może być z kolei tak, że wszystkie wymienione wyżej operacje wykonuje jedna, ta sama osoba i z tego względu mogą być one pogrupowane inaczej, np. wszystkie operacje wykonywane przy użyciu programów „Kadry i Płace" mogą być ujęte jako jeden proces nazwany „Prowadzenie ewidencji pracowników i rozliczeń z pracownikami", pozostałe zaś wykonywane przy użyciu programu „Płatnik" jako „Prowadzenie obsługi ubezpieczeniowej pracowników". Proces związany z obsługą ubezpieczeniową pracowników będzie obejmował wówczas zarówno zgłaszanie pracowników i członków ich rodzin do ubezpieczenia, jak i zgłaszanie deklaracji rozliczeniowych, imiennych raportów o wynagrodzeniu i naliczonych składkach na poszczególne rodzaje ubezpieczenia.

Podsumowując: określona w art. 30 ust. 1 RODO zawartość rejestru czynności nie wskazuje na obowiązek opisywania każdej poszczególnej operacji wykonywanej na danych, takiej jak np. zbieranie, utrwalanie, porządkowanie, modyfikowanie, usuwanie (czy innej wskazanej w art. 4 pkt 2 RODO). Rejestr powinien obejmować opis poszczególnych zespołów operacji związanych zbiorczo z realizacją określonego celu przetwarzania.

Warto zaznaczyć, że takie rozumienie pojęcia „czynność przetwarzania" przyjmują również inne organy nadzorcze w Europie, między innymi organy ochrony danych w Niemczech, Belgii i Wielkiej Brytanii. W projekcie rejestru czynności przetwarzania organ brytyjski jako przykłady czynności związanych z zatrudnieniem wskazuje takie, jak: obsługa płac pracowników, prowadzenie księgowości, przechowywanie danych w chmurze.

5. Czy w zakresie „kategorii odbiorców" należy wpisywać do rejestru podmioty działające z upoważnienia administratora wewnątrz jego struktury organizacyjnej?

Znaczenie pojęcia „odbiorcy danych" na gruncie RODO różni się od tego, jakie ma ono zgodnie z art. 7 pkt 6 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Zgodnie z art. 4 pkt 9 RODO, za odbiorcę uznaje się osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, z wyjątkiem organów publicznych, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego.

Na potrzeby realizacji obowiązku określonego w art. 30 ust. 1 przyjąć należy, że podmiotami objętymi definicją odbiorcy będą podmioty przetwarzające, natomiast nie będą nimi inne podmioty działające z upoważnienia administratora, w jego imieniu i na jego polecenie wewnątrz struktury organizacyjnej. Jak wskazano w komentarzu do art. 4 ust. 9 *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz Bielak-Jomaa Edyta (red.), Lubasz Dominik (red.),* „Przyjęcie koncepcji, w której odbiorcą danych jest także osoba funkcjonująca w strukturze administratora, prowadzi do znacznego utrudnienia realizacji obowiązków przez administratora, a jednocześnie nie wzmacnia praw osób, których dane dotyczą. Zapewnienie podmiotowi danych wiedzy na temat przepływu danych w ramach struktury administratora mogłoby naruszać również zasadę proporcjonalności, ze względu na wrażliwość tego typu informacji, bez uzasadnienia w postaci podniesienia poziomu ochrony danych osobowych. Z tego względu opowiedzieć się należy za koncepcją uznania za odbiorcę podmiotu przetwarzającego, ale już nie innych podmiotów działających z upoważnienia administratora, w jego imieniu i na jego polecenie wewnątrz struktury organizacyjnej. Taki pogląd prezentowany jest także w doktrynie niemieckiej." (Chomiczewski Witold, Czerniawski Michał, Drobek Piotr,

Góral Urszula, Kuba Magdalena, Lubasz Dominik, Makowski Paweł Witkowska-Nowakowska Katarzyna, Komentarz do art. 4, w: E. Bielak-Jomaa, D. Lubasz (red.), RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, LEX).

6. Czy rejestr czynności może obejmować inne elementy niż wskazane w art. 30 ust. 1 RODO?

Wskazane w art. 30 ust. 1 RODO składniki rejestru (kryteria klasyfikacji przetwarzanych danych osobowych) są obligatoryjne. Jednak wskazany w tym przepisie zakres informacji o operacjach wykonywanych w ramach danej czynności nie ma charakteru zamkniętego. Zatem mogą się w nim znaleźć inne elementy, które administrator uzna za zasadne, uwzględniając wiele specyficznych dla niego czynników, takich jak np.:

- wskazanie podstawy prawnej przetwarzania,
- wskazanie źródła pozyskania danych,
- wskazanie użytego do przetwarzania systemu informatycznego,
- informacje dotyczące przeprowadzonej oceny skutków dla ochrony danych itp.

W niektórych przypadkach uzasadnione może okazać się odnotowanie w rejestrze dodatkowo takich informacji, jak np.:

- określenie tzw. właścicieli procesów, czyli osób odpowiedzialnych u administratora za konkretne czynności przetwarzania (np. kierownik określonej komórki w organizacji, wydzielone stanowisko itp.), oraz
- dane kontaktowe podmiotu przetwarzającego oraz podmiotów, którym podpowierzono wykonywanie określonych czynności przetwarzania danych lub określonych operacji w ramach tych czynności (art. 28 ust. 4 RODO).

Zamieszczenie innych danych niż wymagane w art. 30 ust. 1 RODO może być przydatne szczególnie w kontekście wykazania zgodności wykonywanych czynności przetwarzania z przepisami RODO. Jeśli zatem w rejestrze tym dla każdej czynności wskażemy np. przepis prawa dający podstawę przetwarzania danych w ramach danej czynności, czy np. w odniesieniu do informacji wysyłanej drogą elektroniczną wskażemy sposób jej zabezpieczenia, wówczas łatwiej w przypadku kontroli będzie wykazać zgodność z zasadami RODO. Ponadto rejestr taki, podczas jego tworzenia, aktualizacji i przeglądania będzie przypominał samemu administratorowi o obowiązku zapewnienia określonych w RODO zasad i warunków przetwarzania.

Tworzenie rozszerzonego o dodatkowe elementy rejestru czynności przetwarzania zalecane jest obecnie między innymi przez organy nadzorcze w Belgii[2] i Wielkiej Brytanii[3].

[2] www.privacycommission.be/fr/canevas-de-registre-des-activites-de-traitement

[3] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/documentation/how-do-we-document-our-processing-activities

7. Jak należy rozumieć pojęcie „kategorii czynności przetwarzania" oraz „kategorii przetwarzań" w kontekście obowiązku prowadzenia rejestru kategorii czynności, o którym mowa w art. 30 ust. 2 RODO?

RODO nie definiuje ani pojęcia „**kategorii czynności przetwarzania**", ani pojęcia „**kategorii przetwarzań**", o których mowa w art. 30 ust. 2 lit. b RODO. Do pojęć tych nie odnosi się też preambuła RODO, co dodatkowo stwarza trudności w zakresie interpretacji tego pojęcia.

Zgodnie z art. 30 ust. 2 RODO, rejestr czynności ma obejmować wszystkie kategorie czynności przetwarzania dokonywanych w imieniu wszystkich administratorów. Ma zawierać m.in. określenie (imię, nazwisko lub nazwę) każdego administratora, w imieniu którego działa podmiot przetwarzający oraz **kategorie przetwarzań dokonywanych w imieniu każdego z administratorów**. W odniesieniu do każdego z administratorów wskazane jest zatem nazwanie poszczególnych powierzeń (zleceń), a zatem rodzaju usług, jakie podmiot przetwarzający na podstawie zawartych umów wykonuje na rzecz poszczególnych administratorów. Uporządkowanie czynności wykonywanych w ramach powierzenia w kategorie, czyli ich pogrupowanie pod względem rodzaju usług świadczonych przez podmiot przetwarzający, umożliwi łatwy przegląd „powierzeń" zwłaszcza w przypadku podmiotów, które działają na rzecz wielu administratorów danych lub świadczą wiele różnych usług w zakresie przetwarzania danych.

Powyższe względy wskazują, że na potrzeby wykonania obowiązku określonego w tym przepisie należy przyjąć, że:

Kategoria czynności przetwarzania (kategoria przetwarzań) to rodzaj usługi realizowanej przez podmiot przetwarzający na zlecenie administratora związanej ze zleconymi czynnościami przetwarzania.

Jak wskazuje praktyka, rodzajami takich usług mogą być np.:

1) przechowywanie danych klienta (administratora) rozumiane jako udostępnienie zamawiającemu określonej przestrzeni dyskowej w infrastrukturze przetwarzającego na przechowywanie danych, którymi zlecający (administrator) sam zarządza i decyduje o tym, jakie dane tam przechowuje – np. wykonuje kopie zapasowe danych elektronicznych;
2) udostępnianie klientowi (administratorowi) mocy obliczeniowej procesorów, przestrzeni pamięci operacyjnej i dyskowej lub innych usług na potrzeby instalacji i eksploatacji usług przetwarzania, którymi zamawiający w pełni zarządza – dostarczanie infrastruktury informatycznej;
3) udostępnienie klientowi (administratorowi) określonej platformy programistycznej (np. serwera www wraz z odpowiednim oprogramowaniem do prowadzenia własnej strony internetowej);
4) wykonywanie na zamówienie klienta (zamawiającego) określonych usługi w zakresie konfiguracji sprzętowej, programowej, w tym zabezpieczeń udostępnionych mu serwerów, innych urządzeń komputerowych oraz oprogramowania – usługi administracyjne i konserwacyjne;
5) wykonywanie na zamówienie klienta (zamawiającego) usług programistycznych, w tym aktualizacji oprogramowania na okoliczność zmieniających się przepisów prawnych lub wymagań klienta – usługi programistyczne itp.
6) samo przechowywanie dokumentacji podatkowej, księgowej, kadrowej i medycznej;
7) prowadzenie dokumentacji podatkowej, księgowej, kadrowej;
8) archiwizacja danych elektronicznych;

9) skanowanie i digitalizacja danych;
10) niszczenie nośników informacji.

8. Odnotowywanie w rejestrach przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej.

Zarówno administrator danych w rejestrze czynności, jak i podmiot przetwarzający w rejestrze kategorii czynności powinni odnotowywać fakt przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej (art. 30 ust. 1 lit. e oraz art. 30 ust. 2 lit. c RODO), wskazując nazwę tego państwa trzeciego lub organizacji międzynarodowej.

Natomiast obowiązek dokumentowania zabezpieczeń wynika z art. 30 ust. 1 lit. e, jak i z art. 49 ust. 6 RODO, zgodnie z którym administrator lub podmiot przetwarzający dokumentują ocenę oraz odpowiednie zabezpieczenia, o których mowa w art. 49 ust. 1 akapit drugi, w rejestrze czynności i rejestrze kategorii czynności. Należy pamiętać, że obowiązek odnotowania w rejestrze odpowiednich zabezpieczeń jest przewidziany w sytuacji, kiedy przekazanie danych do państwa trzeciego lub organizacji międzynarodowej nie następuje na podstawie wydanej przez Komisję Europejską decyzji stwierdzającej adekwatny stopień ochrony w państwie trzecim lub organizacji międzynarodowej (art. 45 ust. 3 RODO), ani z wykorzystaniem odpowiednich mechanizmów ochrony (o których mowa w art. 46 RODO), oraz gdy nie zachodzą szczególne sytuacje wymienione w art. 49 ust. 1 akapit pierwszy RODO.

Ponadto warto mieć na uwadze, że **dotychczas przyjęte przez Komisję Europejską decyzje na podstawie art. 25 ust. 6 dyrektywy 95/46/WE[4], w myśl art. 45 ust. 4 i 5 RODO, pozostają w mocy do czasu ich zmiany, zastąpienia lub uchylenia przez Komisję Europejską (biorąc pod uwagę kryteria wskazane w art. 45 ust. 2 RODO).**

Przykładowo: Decyzja Komisji Europejskiej w sprawie właściwej ochrony danych osobowych w Szwajcarii (2000/518/WE) pozostaje w mocy od 25 maja 2018 r. W związku z tym, w przypadku przekazania danych do Szwajcarii nie zachodzi konieczność umieszczania w rejestrze informacji o zastosowanych środkach bezpieczeństwa w rozumieniu art. 30 ust. 2 lit. c RODO. Pozostaje jednak konieczność zamieszczenia informacji o fakcie przekazywania danych do kraju trzeciego, jakim jest Szwajcaria. Nie zwalnia to jednak przetwarzającego (czy administratora) z zamieszczenia w rejestrze ogólnego opisu technicznych i organizacyjnych środków bezpieczeństwa przez samego administratora (art. 30 ust. 2 pkt g RODO).

9. Dlaczego rejestr kategorii czynności przetwarzania z art. 30 ust. 2 RODO nie obejmuje tych samych elementów, co rejestr czynności z art. 30 ust. 1 RODO?

W odróżnieniu od rejestru czynności – rejestr kategorii czynności **nie obejmuje celów przetwarzania; opisu kategorii osób, których dane dotyczą, kategorii danych osobowych; oraz kategorii odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych.** Określenie tych okoliczności jest obowiązkiem administratora lub

[4] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady WE, https://giodo.gov.pl/pl/568/603

współadministratora jako podmiotów, które zgodnie z definicją zawartą w art. 4 pkt 7 RODO decydują o celach i sposobach przetwarzania danych, chyba że cele te i sposoby określone są w przepisach prawa, na podstawie których działa administrator lub współadministrator.

10. Jakie inne elementy niż „kategorie przetwarzań" może obejmować rejestr kategorii czynności?

Tak jak rejestr czynności, tak i rejestr kategorii czynności może obejmować inne elementy niż wskazane w art. 30 ust. 2 RODO, w szczególności takie, które podmiot przetwarzający uznaje za potrzebne i uzasadnione dla zapewnienia zgodności z prawem przetwarzania danych, które zostało mu powierzone.

Fakultatywnymi elementami rejestru mogą być następujące przykładowe elementy:
- wskazanie użytego do przetwarzania systemu informatycznego,
- czas trwania umowy (ze wskazaniem daty),
- dane kontaktowe podmiotów, którym podpowierzono dane osobowe (art. 28 ust. 4 RODO).

Te informacje jako pomocne w zapewnieniu zgodności z prawem przetwarzania, za które jest odpowiedzialny podmiot przetwarzający, mogą być fakultatywnie wpisywane do rejestru kategorii czynności.

11. Jak powinien wyglądać „ogólny opis technicznych i organizacyjnych środków bezpieczeństwa", o których mowa w art. 32 ust. 1 lit. d i art. 30 ust. 2 lit. d RODO"?

W rejestrze czynności przetwarzania i rejestrze kategorii czynności przetwarzania zamieszcza się - jeżeli jest to możliwe - ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO. Opis może mieć charakter ogólny i wskazywać najważniejsze założenia czy elementy przyjętych systemów lub koncepcji w zakresie bezpieczeństwa danych osobowych. Jest to uzasadnione zwłaszcza w przypadkach, gdy koncepcje te obejmują wiele elementów i rozwiązań, które uszczegółowione są w innym miejscu, np. konkretnej dokumentacji, polityce lub procedurach. Wówczas należy zamieścić w rejestrze ogólną informację o rodzaju zastosowanych zabezpieczeń (np. kontrola dostępu w oparciu o identyfikator i hasło, zastosowanie certyfikatów, szyfrowanie komunikacji itp.) oraz odesłanie do dokumentacji opisującej szczegóły zarządzania danego rodzaju zabezpieczeniami.

W odniesieniu do informatycznych nośników danych oraz danych przetwarzanych w systemach informatycznych, a w szczególności w odniesieniu do danych przekazywanych za pośrednictwem publicznie dostępnych sieci telekomunikacyjnych, opis ten powinien zawierać również informacje o zastosowanych środkach kontroli dostępu do przetwarzanych danych, a także zastosowanych środkach ochrony kryptograficznej. Przykładem takiego opisu może być następujące wskazanie rodzaju zabezpieczeń:

- do kontroli dostępu do danych przetwarzanych w systemie informatycznym zastosowano kontrolę dostępu bazującą na wydawanych kartach z certyfikatami dostępu oraz przekazanych ich użytkownikom kodach PIN;
- w przypadku zabezpieczenia poufności korespondencji można wskazać, że informacje szyfrowane są przy użyciu określonego narzędzia za pomocą publicznego klucza jej adresata.

W każdym przypadku jednak opis ten ma umożliwiać administratorowi i podmiotowi przetwarzającemu oraz organowi nadzorczemu wstępną ocenę zastosowanych środków w odniesieniu do poszczególnych czynności i kategorii czynności zamieszczonych w rejestrze.

Trzeba przy tym pamiętać, że administratorzy, powierzając przetwarzanie, powinni korzystać jedynie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą (art. 28 ust. 1 RODO). Każdy podmiot przetwarzający zobowiązany jest stosować odpowiednie środki techniczne i organizacyjne zgodnie z art. 32 ust. 1 RODO. Jak wskazuje art. 28 ust. 3 lit. f RODO, podmiot przetwarzający - zgodnie z umową lub innym instrumentem prawnym, na podstawie którego powierzenie jest dokonywane - zobowiązany jest pomagać administratorowi wywiązać się z obowiązku wdrożenia odpowiednich środków technicznych i organizacyjnych, o których mowa w art. 32 RODO. Ogólny opis zastosowanych środków - o ile to możliwe - podmiot przetwarzający zobowiązany jest zamieścić w rejestrze kategorii czynności przetwarzania.

12. W jakiej formie należy prowadzić rejestr czynności i kategorii czynności?

RODO nie narzuca układu informacji wymaganych w rejestrach. Stanowi jedynie, że **rejestry powinny być prowadzone w formie pisemnej** (art. 30 ust. 3). RODO nie narzuca również wymagań dotyczących postaci, w jakiej rejestry powinny być prowadzone, wskazując, że może to być postać zarówno papierowa, jak i elektroniczna.

Brak szczegółowego wskazania układu wymaganych informacji w poszczególnych rejestrach oznacza, że administrator danych lub podmiot przetwarzający może przyjąć dowolny układ informacji dotyczących poszczególnych czynności przetwarzania. Na przykład w odniesieniu do pozycji wskazanej w art. 30 ust. 1 lit. e RODO w rejestrze czynności przetwarzania dotyczącej informacji o przekazaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej, administrator może podzielić te informacje na mniejsze jednostki, np. na dwie podpozycje, takie jak:

1) informacji o przekazaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej ze wskazaniem nazw tych państw/organizacji oraz
2) informacji o zastosowanych zabezpieczeniach w przypadku przekazania na podstawie art. 49 ust. 1 akapit drugi RODO.

Biorąc pod uwagę fakt, że dany administrator prowadzi **rejestr wszystkich czynności przetwarzania**, które wykonywane są w jego organizacji, rejestr czynności powinien być tak skonstruowany, aby dla każdej czynności nie było potrzeby powtarzania informacji o nazwie i danych kontaktowych administratora, a także - gdy ma to zastosowanie - o nazwie i danych kontaktowych przedstawiciela administratora oraz inspektora ochrony danych. Ponadto mając na uwadze fakt, że dany administrator może wykonywać jedne czynności jako ich administrator, inne zaś jako współadministrator, celowe jest, aby:

1) informacje o nazwie administratora danych, jego danych kontaktowych, nazwie przedstawiciela i jego danych kontaktowych, a także nazwisku i danych kontaktowych inspektora ochrony danych umieścić jednorazowo, np. na stronie tytułowej rejestru.

2) dla każdego wpisu w rejestrze czynności na pierwszej pozycji umieścić nazwę lub opis czynności przetwarzania, a następnie pozostałe informacje o danej czynności wymienione w art. 30 ust. 1 punkty od b) do g) oraz inne dodatkowe informacje, o których mowa w punkcie 6.

W przypadku **rejestru kategorii czynności przetwarzania**, poszczególne wpisy (rekordy) tego rejestru powinny być uporządkowane według kategorii przetwarzania, tj. rodzaju usług świadczonych na rzecz administratorów. Z drugiej strony, biorąc pod uwagę fakt, że każdy taki rejestr odnosi się do kategorii czynności przetwarzania świadczonych przez jeden podmiot, który go prowadzi, celowe jest, aby:

1. informacje o nazwie podmiotu przetwarzającego, jego danych kontaktowych, nazwie i danych kontaktowych jego przedstawiciela, a także nazwisku i danych kontaktowych jego inspektora ochrony danych umieścić jednorazowo np. na stronie tytułowej przedmiotowego rejestru.
2. dla każdego wpisu w rejestrze kategorii czynności przetwarzania na pierwszej pozycji umieścić nazwę danej „kategorii czynności przetwarzania" (rodzaj usługi) jako wartość pozwalającą pogrupować wszystkie wpisy, a następnie nazwę i dane kontaktowe administratora danych, dla którego dana usługa jest wykonywana, nazwę i dane kontaktowe, przedstawiciela administratora – jeśli dotyczy oraz, nazwisko i dane kontaktowe wyznaczonego przez niego inspektora ochrony danych. W kolejnych pozycjach należy zamieścić informacje wskazane w art. 30 ust. 2 lit. c i d, oraz inne dodatkowe informacje, o których mowa w punkcie 8.

Szablony rejestru czynności przetwarzania i rejestru kategorii czynności przygotowane przez GIODO obejmują następujące informacje:

REJESTR CZYNNOŚCI PRZETWARZANIA:

I. STRONA TYTUŁOWA:

1. **Nazwa i dane kontaktowe administratora**:
   a) nazwa administratora
   b) adres
   c) email
   d) nr telefonu/faksu
2. **Inspektor Ochrony Danych (gdy ma to zastosowanie):**
   a) nazwa inspektora
   b) adres
   c) email
   d) nr telefonu/faksu
3. **Przedstawiciel (gdy ma to zastosowanie):**
   a) nazwa przedstawiciela
   b) adres
   c) email
   d) nr telefonu/faksu

II. INFORMACJE O POSZCZEGÓLNYCH CZYNNOŚCIACH PRZETWARZANIA:

a) Nazwa czynności przetwarzania
b) Jednostka organizacyjna

c) Cel przetwarzania
d) Kategorie osób
e) Kategorie danych
f) Podstawa prawna
g) Źródło danych
h) Planowany termin usunięcia kategorii danych
i) Nazwa współadministratora i dane kontaktowe
j) Nazwa podmiotu przetwarzającego i dane kontaktowe
k) Kategorie odbiorców
l) Nazwa systemu lub oprogramowania
m) Ogólny opis techniczny i organizacyjny środków bezpieczeństwa
n) DPIA
o) Transfer do kraju trzeciego lub organizacji międzynarodowej:
    - Transfer do kraju trzeciego lub organizacji międzynarodowej
    - Dokumentacja odpowiednich zabezpieczeń w przypadku transferu

***Kolorem czerwonym oznaczono informacje wymagane w rejestrze zgodnie z art. 30 ust. 1 RODO.**

REJESTR KATEGORII CZYNNOŚCI PRZETWARZANIA:

I. STRONA TYTUŁOWA:

1. **Nazwa i dane kontaktowe przetwarzającego**:
    a) nazwa administratora
    b) adres
    c) email
    d) nr telefonu/faksu
2. **Inspektor ochrony danych (gdy ma to zastosowanie):**
    a) nazwa inspektora
    b) adres
    c) email
    d) nr telefonu/faksu
3. **Przedstawiciel (gdy ma to zastosowanie):**
    a) nazwa przedstawiciela
    b) adres
    c) email
    d) nr telefonu/faksu

II. INFORMACJE O POSZCZEGÓLNYCH KATEGORIACH CZYNNOŚCI PRZETWARZANIA:

a) Kategorie przetwarzania
b) Ogólny opis techniczny i organizacyjny środków bezpieczeństwa
c) Administrator:

- Nazwa i dane kontaktowe administratora
- Nazwa i dane kontaktowe współadministratora (gdy ma to zastosowanie)
- Nazwa i dane kontaktowe przedstawiciela administratora (gdy ma to zastosowanie)
- Inspektor ochrony danych administratora (gdy ma to zastosowanie)

d) Czas trwania przetwarzania

e) Nazwy państw trzecich lub organizacji międzynarodowych, do których dane są przekazywane

f) Dokumentacja odpowiednich zabezpieczeń danych osobowych

g) Podprzetwarzający:
   - Nazwa i dane kontaktowe podprzetwarzającego
   - Kategorie podpowierzonych przetwarzań

***Kolorem czerwonym oznaczono informacje wymagane w rejestrze zgodnie z art. 30 ust. 2 RODO**

13. Czy informacje zawarte w rejestrach i wykazach zbiorów prowadzonych na podstawie ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych mogą być wykorzystane do tworzenia rejestrów, o których mowa w art. 30 RODO?

Dla większości podmiotów bazą do realizacji obowiązku określonego w art. 30 ust. 1 i 2 RODO będą ewidencje danych osobowych oraz systemów służących do ich przetwarzania prowadzone na podstawie ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych i przepisów wykonawczych do tej ustawy, w tym przede wszystkim wykazy będące elementami polityki bezpieczeństwa, takie jak lokalne rejestry zbiorów prowadzone przez administratorów bezpieczeństwa danych czy wykazy danych, które są przekazywane między poszczególnymi systemami bądź zbiorami danych.