Rejestr czynności przetwarzania

RODO nakłada na osoby, które przetwarzają dane osobowe, wiele obowiązków, w tym konieczność prowadzenia określonej dokumentacji – na przykład rejestru czynności przetwarzania (dalej jako „rejestr") (art. 30 ust. 1 RODO). Do prowadzenia przedmiotowego rejestru został zobowiązany w zasadzie każdy administrator.

Administrator, czyli kto?

Najprościej rzecz ujmując, administratorem jest każdy podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Nie ma znaczenia, czy jest to osoba fizyczna, osoba prawna (np. spółka z o.o.), organ publiczny (np. komornik sądowy), jednostka czy jeszcze inny podmiot.

Czasami administrator musi wyznaczyć swojego przedstawiciela, który również jest zobowiązany do prowadzenia tego rejestru. Dotyczy to administratorów niemających jednostki organizacyjnej w Unii Europejskiej, którzy podlegają przepisom RODO, czyli są zobowiązani do stosowania i przestrzegania przepisów RODO (art. 27 ust. 1 RODO).

Zobacz: Przedstawiciel administratora danych osobowych

Zobacz: Terytorialny zasięg stosowania RODO

W rejestrze należy wskazać wszystkie dane osobowe, za które administrator lub przedstawiciel administratora odpowiadają.

W jakim celu musisz prowadzić taką

dokumentację?

Po pierwsze, prowadząc rejestr czynności przetwarzania, realizujesz z jedną z podstawowych zasad RODO – zasadę rozliczalności (art. 5 ust. 2 RODO), gdyż na podstawie rejestru czynności przetwarzania jesteś w stanie wykazać, że działasz zgodnie z przepisami o ochronie danych osobowych (zob. art. 5 ust. 1 RODO). Po drugie, umożliwiasz organowi nadzorczemu, którym w Polsce jest Prezes Urzędu Ochrony Danych, monitorowanie prowadzonego przez Ciebie przetwarzania.

Wystąpienie któregokolwiek z niżej opisanych wyjątków powoduje, że ciąży na Tobie obowiązek prowadzenia rejestru czynności przetwarzania.

Co to oznacza, że przetwarzanie może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą?

Zgodnie z jedną z generalnych zasad RODO (art. 24 ust. 1 RODO) administrator, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze, wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z RODO. A prościej – jeżeli twierdzisz, że stosujesz jakieś środki techniczne i organizacyjne, to musisz umieć wykazać czy pokazać, że tak właśnie jest. Wykorzystywane przez Ciebie zabezpieczenia powinny być poddawane przeglądom i uaktualniane.

Jako administrator jesteś zobowiązany do zastosowania wybranych przez Ciebie środków bezpieczeństwa, jednak ich wybór musi być poprzedzony analizą ryzyka. Możesz je oszacować na podstawie obiektywnej oceny, w ramach której sam stwierdzisz, czy z operacjami przetwarzania danych osobowych, których dokonujesz, wiąże się ryzyko naruszenia praw lub wolności osób, których dane dotyczą.

Pamiętaj!

Ryzyko należy rozumieć jako wszelkiego rodzaju zagrożenie interesu osoby, której dane osobowe przetwarzasz, a nie zagrożenie Twojego interesu (biznesu) jako administratora.

Dopiero po dokonaniu analizy ryzyka Ty jako administrator jesteś w stanie stwierdzić, czy przetwarzanie danych, którego dokonujesz, może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą.

Czy moje przetwarzanie danych osobowych ma sporadyczny charakter?

Sporadyczny charakter nie ma definicji, więc może budzić wątpliwości w praktyce. Zgodnie ze słownikiem języka polskiego *sporadyczny* to inaczej incydentalny, nieczęsty, odosobniony, pojedynczy, epizodyczny, rzadki czy wyjątkowy. Przeciwieństwem słowa sporadyczny są słowa takie jak: ciągły, cykliczny, częsty, notoryczny, powtarzający się, stały, systematyczny, często spotykany, regularny.

Każdy administrator powinien przeanalizować termin „sporadyczny charakter" pod kątem stanu faktycznego, czyli przetwarzania danych osobowych, którego on dokonuje.

W literaturze dotyczącej przepisów RODO podkreśla się, że nie można mówić o sporadycznym przetwarzaniu danych osobowych swoich pracowników. Jeżeli zatem zatrudniasz chociaż jednego pracownika, to musisz prowadzić rejestr czynności przetwarzania.

Czy przetwarzam szczególne kategorie danych osobowych lub dane osobowe dotyczące wyroków skazujących i czynów zabronionych RODO?

Jako administrator musisz się zastanowić, jakie kategorie danych osobowych przetwarzasz. Wyróżnia się trzy:

- dane osobowe zwykłe,
- szczególne kategorie danych osobowych (kiedyś nazywane danymi wrażliwymi. Pojęcie „dane wrażliwe” cały czas jest stosowane w praktyce),
- dane osobowe dotyczące wyroków skazujących i czynów zabronionych.

Zacznijmy od końca.

Kategoria danych osobowych dotyczących wyroków skazujących i czynów zabronionych odnosi się do wyroków z art. 413 § 2 Kodeksu postępowania karnego lub z art. 82 Kodeksu postępowania w sprawach o wykroczenia. Za wyrok skazujący nie można zatem uznać wyroku umarzającego, warunkowo umarzającego postępowanie czy wyroku uniewinniającego. Jeżeli chodzi o czyn zabroniony, to chodzi m.in. o mandaty karne.

Kategorie danych osobowych wrażliwych zostały określone w art. 9 ust. 1 RODO i mają charakter zamknięty, czyli już nic nie można tam dodać. Do szczególnych kategorii danych osobowych zaliczono:

- pochodzenie rasowe lub etniczne,
- poglądy polityczne,
- przekonania religijne lub światopoglądowe,
- przynależność do związków zawodowych,
- dane genetyczne,
- dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej,
- dane dotyczące zdrowia,
- dane dotyczące seksualności lub orientacji seksualnej osoby.

Do kategorii danych osobowych zwykłych zaliczone są wszystkie dane osobowe, które nie mieszczą się w dwóch powyższych kategoriach.

Jak widzisz, przywilej nieprowadzenia rejestru ma **charakter pozorny**! Większość administratorów (nawet jeśli są przedsiębiorcami lub zatrudniają mniej niż 250 osób) załapie się na jeden z trzech wyjątków wskazanych powyżej; najczęściej będzie to dotyczyło niesporadycznego przetwarzania danych osobowych.

Przykład nr 1:

Jan Kowalski prowadzący jednoosobową działalność gospodarczą pod firmą Biuro Rachunkowe Jan Kowalski, ul. Miejska 5, 80-123 Gdynia. Pan Jan zatrudnia na ½ etatu sekretarkę.

Pan Jan jest przedsiębiorcą i zatrudnia mniej niż 250 osób. Jednak przetwarzanie danych osobowych dotyczących jego pracownika nie ma charakteru sporadycznego. Pan Jan jako administrator musi prowadzić rejestr czynności przetwarzania.

Przykład nr 2:

Pani Martyna Kowalska prowadzi hobbystycznie bloga o kotach. Na swoim blogu ma newsletter. Nikt jej nie pomaga, nie czerpie z tego korzyści finansowych.

Pani Martyna podlega pod RODO. Jeżeli masz wątpliwości, to zobacz Czysto osobisty lub domowy charakter przetwarzania danych osobowych – na przykładzie bloga osobistego.

Pani Martyna nie jest przedsiębiorcą, ale jest podmiotem, który nie zatrudnia więcej niż 250 pracowników. Pani Martyna przetwarza dane osobowe subskrybentów newslettera. Takie przetwarzanie nie ma charakteru incydentalnego, gdyż informacje są przechowywane w sposób ciągły, regularny. Pani Martyna musi prowadzić rejestr czynności przetwarzania.

Forma prowadzenia rejestru czynności

przetwarzania

Rejestr musi być prowadzony w formie pisemnej, w tym elektronicznej. Oznacza to, że możesz go prowadzić np. w Excelu lub tabelce zrobionej w Wordzie.

W rejestrze musisz zawrzeć poniższe informacje:

- **Informacje, z których wynika, kim jesteś:**
  - Twoje dane jako administratora (imię i nazwisko lub nazwę oraz dane kontaktowe),
  - jeżeli ktoś razem z Tobą jest administratorem – dane wszelkich współadministratorów,
  - jeżeli wyznaczyłeś przedstawiciela administratora – jego dane,
  - jeżeli wyznaczyłeś inspektora ochrony danych – jego dane.

- **Informacje, z których wynika, co robisz z tymi danymi**
  - czynność przetwarzania;
  - cele przetwarzania;
  - opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
  - kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
  - odnotowanie przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej;
  - jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
  - jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.

Wskazane powyżej informacje mają charakter obligatoryjny.

Oznacza to, że wyżej informacje muszą znaleźć się w rejestrze.

O ile informacje dotyczące danych administratora, współadministratorów, przedstawiciela administratora czy inspektora danych osobowych nie powinny stanowić problemu, to już pozostała część informacji może być kłopotliwa. Nie jest jednak to takie trudne, jak się wydaje.

Pojęcie czynności przetwarzania nie zostało zdefiniowane w RODO (super, nie?!). Zgodnie ze stanowiskiem PUODO czynność 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.

Najprościej zobrazować to na przykładach:

- rekrutacja pracowników,
- obsługa umów sprzedaży,
- prowadzenie ewidencji pracowników i rozliczeń z pracownikami,
- prowadzenie obsługi ubezpieczeniowej pracowników,
- prowadzenie księgowości,
- przechowywanie danych w chmurze.

Nie musisz opisywać każdej poszczególnej operacji wykonywanej w ramach rekrutacji pracowników. Takie rozdrobnienie zajęłoby niezliczoną liczbę godzin, a co ważniejsze – nie byłoby czytelne ani dla Ciebie, ani dla organu nadzorczego.

Cele przetwarzania danych osobowych

Cele przetwarzania to nic innego jak cele związane z tym, dlaczego przetwarzasz podane informacje, czyli dlaczego jego przechowujesz, analizujesz, zbierasz itp.

Cele przetwarzania są ściśle związane z podstawami prawnymi przetwarzania, które zostały ujęte w art. 6 RODO i do których

zaliczono:

- zgodę osoby, której dane osobowe są przetwarzane;
- niezbędność do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
- niezbędność do wypełnienia obowiązku prawnego ciążącego na administratorze;
- niezbędność do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
- niezbędność do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
- niezbędność do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności, gdy osoba, której dane dotyczą, jest dzieckiem.

Strasznie trudne, co?

Przykład*:*

Jeżeli prowadzisz bloga, masz swój newsletter, to na podstawie ***prawnie uzasadnionego interesu (art. 6 ust. 1 lit. f RODO)*** *przetwarzasz dane osobowe swoich użytkowników* ***w celu:***

- *zarządzania blogiem i tworzenia własnych baz danych*:
  - *prowadzenia analiz statystycznych*;
  - *wysyłania newslettera jako marketingu bezpośredniego własnych produktów lub usług, lub polecanych produktów osób trzecich*;
  - *prowadzenia badań i analiz bloga, między innymi*

pod kątem funkcjonalności i poprawy jego działania, a także satysfakcji z oferowanych usług;
- *kontaktowania się z Tobą, w szczególności przez formularz kontaktowy dostępny na blogu*.

Dodatkowo na ***podstawie zgody osoby, która dane osobowe Ci przekazała (art. 6 ust. 1 lit. a RODO), przetwarzasz je w celu:***

- *zapisywania ich w plikach cookies, wykorzystywania plików cookies na blogu i jego podstronach*:
  - *umożliwienia komentowania wpisów blogowych*,
  - *wysyłania newslettera (art. 10 ustawy o świadczeniu usług drogą elektroniczną i art. 172 ustawy – prawo telekomunikacyjne)*.

Opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych

O typach danych osobowych już wspominałam. Mamy ich trzy: dane osobowe zwykłe, szczególne kategorie danych osobowych oraz kategoria danych osobowych dotyczących wyroków skazujących i czynów zabronionych.

Jeżeli chodzi o opis kategorii osób, to wystarczy, że wskażesz: pracownicy, zleceniodawcy, subskrybenci itp.

Kategorie odbiorców, których dane dotyczą

Odbiorca danych osobowych został zdefiniowany w RODO. Hurra! Odbiorcą danych jest osoba fizyczna lub prawna, organ

publiczny, jednostka 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 (art. 4 pkt 9 RODO). Czyli kto?

Na potrzeby rejestru czynności przetwarzania odbiorcami są wszystkie podmioty przetwarzające dane osobowe, czyli każda osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora, czyli w Twoim imieniu (art. 4 pkt 8 RODO). Podmiotem przetwarzającym będzie zatem biuro rachunkowe, które Cię rozlicza, firma, u której wykupiłeś hosting swojej strony, informatyk, który dorywczo coś u Ciebie robi, a nawet prawnik. Jeżeli jednak wewnątrz Twojej struktury organizacyjnej pracuje informatyk, prawnik czy księgowa, to oni nie są odbiorcami. Aby jeszcze bardziej to uprościć, można powiedzieć, że wszystkie podmioty, z którymi masz zawarte umowy powierzenia przetwarzania danych osobowych, są Twoimi odbiorcami.

RODO nie wymaga od Ciebie wskazywania każdego indywidualnie, a jedynie podania kategorii odbiorców, np. prawnicy, księgowi, informatycy.

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

Jeżeli przekazujesz dane osobowe do państwa trzeciego lub organizacji międzynarodowej, RODO nakłada na Ciebie jako administratora obowiązek odnotowania w rejestrze informacji o takim procesie. W takiej sytuacji w rejestrze należy odnotować nazwę państwa trzeciego lub organizacji międzynarodowej. Czasem jeszcze dodatkowo należy udokumentować stosowane zabezpieczenia (art. 49 ust. 1 akapit drugi RODO). Dotyczy to sytuacji, kiedy przekazywanie 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, ani z wykorzystaniem odpowiednich mechanizmów ochrony, oraz gdy nie zachodzą szczególne sytuacje określone w art. 49 ust. 1 akapit 1 RODO.

Planowane terminy usunięcia poszczególnych kategorii danych

Nie możesz przechowywać danych osobowych w nieskończoność. Zbierasz dane osobowe, a następnie coś z nimi robisz (czyli przetwarzasz) w określonym celu. Kiedyś ten cel przecież zostanie zrealizowany. W rejestrze musisz wskazać, o ile jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych osobowych.

Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa

Jeżeli jest to możliwie, w swoim rejestrze czynności przetwarzania, musisz wskazać ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.

Chodzi o **ogólną informację o zastosowanych rozwiązaniach**. Nie będziesz przecież przepisywał wszystkich swoich procedur, polityk czy innej dokumentacji.

Pamiętaj!

Od rejestru czynności przetwarzania (art. 31 ust. 1 RODO) należy odróżnić rejestr kategorii czynności przetwarzania (art. 31 ust. 2 RODO). Oba rejestry mają charakter wewnętrzny. Żaden przepis prawa nie nakazuje publikowania rejestru czynności przetwarzania lub kategorii czynności przetwarzania

na stronie internetowej administratora. Co więcej, takie działanie naraża organizację na atak np. hakerski, albowiem zawierają one ogólny opis technicznych i organizacyjnych środków bezpieczeństwa stosowanych w Twojej firmie.

Pobierz bezpłatny wzór rejestru czynności przetwarzania **(plik Excel** oraz **plik Word)**.

Niniejszy artykuł ma charakter wyłącznie edukacyjny i nie stanowi porady prawnej ani opinii prawnej. Zapoznaj się z nota prawną.

Jeżeli potrzebujesz indywidualnej pomocy związanej dostosowaniem się do zmian prawnych, napisz na ***napisz@tudzialprawny.pl****.*

Stan prawny na dzień: **19.04.2020 r.**

Bibliografia

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) (Dz. U. UE z 2016 r., L 119/1 ze zm.), https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32016R0679, 18.04.2020 r.
2. N. Stojanowska, *Rejestr czynności przetwarzania*, Nowa

Currenda 3/2018
3. Urząd Ochrony Danych Osobowych, *Wskazówki i wyjaśnienia dotyczące rejestrowania czynności i kategorii czynności przetwarzania określonego w art. 30 ust. 1 i 2 RODO*, https://uodo.gov.pl/pl/file/708, 18.04.2020 r.
4. Stanowisko Grupy Roboczej Artykułu 29 ds. Ochrony Danych w sprawie wyjątków od obowiązku prowadzenia rejestru czynności przetwarzania zgodnie z art. 30 ust. 5 RODO, https://archiwum.giodo.gov.pl/pl/file/13525, 18.04.2020 r.
5. Urząd Ochrony Danych Osobowych, *Czy rejestr czynności prowadzony na podstawie art. 30 ust. 1 RODO musi być udostępniany publicznie?* https://www.uodo.gov.pl/pl/225/636, 18.04.2020 r.

Źródło zdjęcia: Nataliya Vaitkevich, Pexels, https://www.pexels.com/pl-pl/zdjecie/marketing-laptop-przegladanie-stol-7172825/, dostęp: 25.10.2023 r.