Prywatność zawsze na pierwszym miejscu

Privacy by design oraz *privacy by default,* czyli uwzględnienie ochrony danych w fazie projektowania oraz domyślna ochrona danych, to podstawowe zasady wprowadzone przepisami *Ogólnego rozporządzenia o ochronie danych*. Ich przestrzeganie jest kluczowe podczas tworzenia i utrzymania systemu ochrony danych osobowych w organizacji. Zasady te są silnie powiązane z zasadą, na której opiera się cała konstrukcja *Ogólnego rozporządzenia o ochronie danych*, czyli tzw. *risk-based approach* (podejście oparte na ryzyku). Stosując się do tych zasad, administrator powinien uwzględniać między innymi poziom ryzyka naruszenia praw i wolności osób fizycznych, czyli prawdopodobieństwo wystąpienia naruszenia oraz wagę zagrożenia.

O prywatności, jako jednym z podstawowych elementów tworzenia rozwiązań, muszą pamiętać jednak nie tylko administratorzy. Każdy produkt czy też usługa, która swoim zakresem obejmuje procesy przetwarzania danych osobowych, powinna powstawać w duchu omawianych zasad.

Koncepcja *privacy by design* w fazie jej opracowywania

Koncepcja *privacy by design* nie jest rozwiązaniem nowym, które pojawiło się wraz z *Ogólnym rozporządzeniem o ochronie danych*. Jej początków należy upatrywać już pod koniec XX wieku. Pojęcie *privacy by design* zostało zaproponowane w 1995 r. przez A. Cavoukiana, Rzecznika Ochrony Informacji i Prywatności Ontario, a następnie opublikowane w raporcie na temat technologii zwiększających prywatność w projektach infrastrukturalnych realizowanych w Kanadzie.

Następnie, ramy ochrony prywatności w fazie projektowania zostały opublikowane w 2009 r. i przyjęte rok później w formie rezolucji w trakcie 32 Międzynarodowej Konferencji Rzeczników Ochrony Danych i Prywatności. Zasadę *privacy by design* uznano wtedy za **niezbędny element podstawowej ochrony prywatności**. Organy ochrony danych zostały zaś zobligowane do wspierania ochrony prywatności w fazie projektowania podczas formułowania polityk i ustawodawstw w ramach swoich działań.

W 2012 r. koncepcja została włączona do projektu *Ogólnego rozporządzenia o ochronie danych*, a od 2018 r., czyli od rozpoczęcia jego stosowania, powinna być realizowana przez wszystkich administratorów, którzy chcą przetwarzać dane osobowe zgodnie z prawem.

By design – czyli jak?

W swoim pierwotnym założeniu koncepcja *privacy by design* powinna opierać się na podejściu **proaktywnym i zaradczym**. Nie obejmuje ona czynności o charakterze naprawczym. Odnosi się do **prywatności jako części wdrażanego lub już realizowanego projektu**. Oznacza to, że prywatność powinna być chroniona nie poprzez dodatki do już funkcjonującego systemu lub projektu, lecz zostać wbudowana w jego konstrukcję w taki sposób, aby stanowić jego część składową.

Zasada *privacy by design* przewiduje **ochronę danych osobowych w całym cyklu ich *życia***, tj. od momentu gromadzenia, aż po moment ich nieodwracalnego usunięcia. Zasada *privacy by design* zakłada również **pełną transparentność i przejrzystość** stosowanych środków i działań administratora na danych osobowych.

W *Ogólnym rozporządzeniu o ochronie danych* koncepcja *privacy by design* opisana została w art. 25 ust. 1. Definiuje ona podstawowe obowiązki administratora podczas określania sposobów przetwarzania danych, jak i w czasie samego przetwarzania. Mówiąc inaczej, definiuje **obowiązki, które administrator musi zrealizować przed rozpoczęciem procesu przetwarzania** danych osobowych, jak również **podczas całego okresu jego trwania**.

Sama koncepcja bazuje na trzech głównych zadaniach, do których realizacji zobowiązany jest administrator, tj.:

1) Dokonanie oceny

Przed rozpoczęciem przetwarzania danych osobowych, administrator, bazując na podejściu opartym na ryzyku, powinien ocenić, **wdrożenia jakich środków technicznych i organizacyjnych będzie wymagało planowane przetwarzanie**.

Oceny dokonuje się **przy uwzględnieniu:**

- stanu wiedzy technicznej,
- kosztów wdrażania,
- charakteru, zakresu, kontekstu i celów przetwarzania,
- ryzyka naruszenia praw lub wolności osób fizycznych.

Przed wdrożeniem nowego procesu przetwarzania danych osobowych, każdy administrator powinien również rozważyć przeprowadzenie oceny skutków dla ochrony danych (*data protection impact assessement*).

Przykład

Administrator chce udostępnić pracownikom samochody służbowe i wdrożyć system zarządzania flotą. W tym celu planuje współpracę z podmiotem zewnętrznym. W tym zakresie administrator powinien dokonać oceny:

- czy i w jakim zakresie występuje ryzyko naruszenia przepisów *Ogólnego rozporządzenia o ochronie danych* lub praw i wolności osób, których dane dotyczą,
- jakie środki organizacyjne powinny zostać wdrożone, aby przetwarzanie danych odbywało się zgodnie z *Ogólnym rozporządzeniem o ochronie danych* i innymi powiązanymi przepisami, co obejmować będzie w szczególności:
  - ustalenie zakresu oraz podstawy prawnej przetwarzania danych osobowych pracowników oraz uzupełnienie rejestru czynności przetwarzania o nowy proces przetwarzania danych osobowych,

  - opracowanie odpowiednich klauzul informacyjnych dla pracowników, których dane osobowe będą przetwarzane w procesie,
  - opracowanie środków umożliwiających realizację praw osób, których dane dotyczą,
  - nadanie upoważnień osobom, które będą przetwarzać dane osobowe w procesie,
  - wybór podmiotu zewnętrznego gwarantującego ochronę powierzonych mu danych osobowych i podpisanie umowy powierzenia przetwarzania danych osobowych.
- jakie środki techniczne powinny zostać wdrożone, aby zapewnić bezpieczeństwo przetwarzanych danych, w tym ich integralność i poufność, co obejmować będzie w szczególności:
  - sposoby zabezpieczenia przepływu danych do podmiotu zewnętrznego,
  - zasady dostępu do systemu zarządzania flotą oraz związane z tym procesy uwierzytelniania,
  - środki zabezpieczenia systemu zarządzania flotą, w tym zasady tworzenia kopii bezpieczeństwa.

2) Wdrożenie środków

Uwzględniając dokonaną ocenę, administrator powinien wdrożyć **odpowiednie** środki techniczne i organizacyjne dla ochrony przetwarzanych w procesie danych osobowych.

Przez odpowiednie środki należy przede wszystkim rozumieć środki zaprojektowane w celu:

- **skutecznej realizacji zasad** ochrony danych przewidzianych w *Ogólnym rozporządzeniu o ochronie danych*,
- **nadania przetwarzaniu niezbędnych zabezpieczeń**, tak by spełnić wymogi *Ogólnego rozporządzenia o ochronie danych* oraz chronić prawa osób, których dane dotyczą.

Artykuł 25 ust. 1 *Ogólnego rozporządzenia o ochronie danych* wskazuje **przykładowe środki**, które może zastosować administrator. Są to w szczególności pseudonimizacja oraz minimalizacja danych. Dla przypomnienia, pod pojęciem pseudonimizacji kryje się takie przetworzenie danych osobowych, by nie można ich było już przypisać konkretnej osobie, bez użycia dodatkowych informacji. Warunkiem jest jednak to, aby takie dodatkowe informacje były przechowywane osobno i zostały objęte środkami uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Należy podkreślić, że **spseudonimizowane dane nadal pozostają danymi osobowymi i podlegają pełnej ochronie**.

Powyższe środki zostały wymienione przykładowo, co oznacza, że w celu spełnienia wymogów *Ogólnego rozporządzenia o ochronie danych* i ochrony praw osób, których dane dotyczą, **możliwe jest zastosowanie także środków innych niż te wymienione**.

Należy przy tym zwrócić uwagę, że *Ogólne rozporządzenie o ochronie danych* nie nakłada na administratora stosowania zabezpieczeń **skutecznych** w każdych okolicznościach. Należy bowiem przyjąć, że ryzyko związane z przetwarzaniem danych osobowych istnieje zawsze, niezależnie od stosowanych środków. Choćby ryzyko wyniesienia bazy danych przez zaufanego pracownika.

Ryzyko to oczywiście można, a nawet trzeba zminimalizować poprzez zastosowanie odpowiednich zabezpieczeń. Należy jednak liczyć się z tym, że jego całkowita eliminacja może okazać się praktycznie niemożliwa.

Przy wdrażaniu odpowiednich środków, administrator powinien zwrócić uwagę w szczególności na ***zasadę rozliczalności***. Oznacza to, że wdrożenie powinno być dokonane w taki sposób, aby wszelkie działania w tym zakresie były odpowiednio udokumentowane. Przede wszystkim dotyczy to zabezpieczeń systemów wykorzystywanych do przetwarzania danych. Administrator zawsze powinien dysponować ich specyfikacją lub przynajmniej mieć możliwość wglądu do niej albo bezpośredniego jej przedstawienia organowi nadzorczemu w przypadku kontroli.

W przypadku, jeżeli w toku dokonanej oceny administrator stwierdzi, że występuje ryzyko naruszenia przepisów *Ogólnego rozporządzenia o ochronie danych* lub praw i wolności osób, których dane dotyczą konieczne będzie podjęcie **działań zmierzających do zmniejszenia jego wystąpienia**.

Przykład

Administrator udostępniający pracownikom samochody służbowe i wdrażający system zarządzania flotą podjął, w szczególności następujące działania:

- określił zakres i podstawy prawne przetwarzania danych w procesie,
- dokonał aktualizacji rejestru czynności przetwarzania,
- wdrożył klauzule informacyjne dla pracowników, których dane osobowe będą przetwarzane w procesie,
- wdrożył środki pozwalające na efektywną realizację praw osób, których dane dotyczą,
- nadał upoważnienia pracownikom mającym dostęp do danych osobowych przetwarzanych w procesie,
- zweryfikował podmiot, któremu chce powierzyć przetwarzanie danych osobowych,
- zawarł umowę powierzenia przetwarzania danych osobowych z podmiotem zewnętrznym,
- określił zakresy dostępu do systemu zarządzania flotą,
- wspólnie z podmiotem przetwarzającym określił środki zabezpieczeń wykorzystywanego systemu informatycznego oraz odebrał w tym zakresie od tego podmiotu stosowne oświadczenia o ich stosowaniu.

3) Stały monitoring

Z uwagi na to, że zasada *privacy by design* obowiązuje nie tylko w kontekście nowych procesów przetwarzania danych, ale **powinna być stosowana przez cały okres jego trwania**, administrator powinien prowadzić **stały monitoring wdrożonych środków ochrony** danych osobowych. W razie konieczności, administrator musi być przygotowany na wdrożenie nowych środków lub aktualizację tych, które wdrożył przy rozpoczęciu procesu przetwarzania.

Większość procesów przetwarzania danych osobowych ma **charakter dynamiczny**. W trakcie ich trwania mogą pojawić się nowe akty prawne, co może mieć wpływ na stosowane przesłanki przetwarzania. Administrator może również chcieć zmienić podmiot przetwarzający z którego usług korzysta. Wreszcie, rozwój nowych technologii może sprawić, że pierwotne wdrożone zabezpieczenia techniczne staną się po prostu przestarzałe i nie będą wystarczająco chronić przetwarzanych danych osobowych.

Przykład

Administrator udostępniający pracownikom samochody służbowe i prowadzący system zarządzania flotą podejmuje następujące działania:

- przeprowadza cykliczne audyty zgodności przetwarzania danych osobowych,
- kontroluje podmiot przetwarzający, któremu powierzono dane pracowników, pod względem zgodności przetwarzania danych z zawartą umową powierzenia oraz przepisami z zakresu ochrony danych osobowych,
- w razie potrzeby wdraża nowe środki ochrony danych osobowych lub aktualizuje środki wcześniej wykorzystywane.

Chcesz być zgodny z RODO *by default*? Zapraszamy na nasz kurs!

Wiedza przekazywana w przystępny sposób przez wykładowców – praktyków (możesz spotkać ich artykuły na naszym blogu ;), kameralne grupy szkoleniowe, praktyczne wzory i szablony dokumentów i procedur, egzamin zakończony wydaniem certyfikatu. To tylko niektóre z zalet naszego kursu. Sprawdź terminy:

SPRAWDŹ

Prywatność w ustawieniach domyślnych

Zasada *privacy by default* stanowi uzupełnienie zasady *privacy by design*. Jej stosowanie powinno prowadzić do sytuacji, w której domyślnie przetwarzane będą wyłącznie te **dane osobowe**, które są **niezbędne dla osiągnięcia konkretnego celu** przetwarzania. Zgodnie z art. 25 ust. 1 *Ogólnego rozporządzenia o ochronie danych* obowiązek ten odnosi się do:

- **ilości** zbieranych danych osobowych,
- **zakresu** przetwarzanych danych osobowych,
- **okresu przechowywania**,

- **dostępności** do danych osobowych.

Zasada ta jest nierozerwalnie związana z innymi podstawowymi zasadami przetwarzania danych osobowych tj. m.in.: ***zasadą ograniczenia celu*** (art. 5 ust. 1 lit. b *Ogólnego rozporządzenia o ochronie danych*), ***zasadą minimalizacji danych*** (art. 5 ust. 1 lit. c *Ogólnego rozporządzenia o ochronie danych*), ***zasadą ograniczenia przechowywania*** (art. 5 ust. 1 lit. e *Ogólnego rozporządzenia o ochronie danych)*.

Zasadę domyślnej ochrony danych należy rozumieć jako postulat uwzględnienia jak **najdalej posuniętych zabezpieczeń prywatności w ustawieniach początkowych każdego systemu**. Domyślnie, czyli bez konieczności jakiejkolwiek aktywności osób, których dane dotyczą.

Co jednak najważniejsze, *privacy by default* oznacza, że **domyślnie powinny być przetwarzane tylko te dane, które są niezbędne do osiągnięcia celu**, dla którego zostały zebrane.

Pierwszym pytaniem, na jakie powinien odpowiedzieć sobie każdy administrator przed rozpoczęciem jakiegokolwiek procesu jest: ***Czy dla prawidłowej realizacji tego rozwiązania, rzeczywiście konieczne jest przetwarzanie danych osobowych?***

Nierzadko bowiem zdarza się, że tak naprawdę nie potrzebujemy w ogóle tego typu informacji, aby osiągnąć założony cel projektu. Jeżeli faktycznie, administrator musi być w stanie zidentyfikować osoby biorące udział w procesie, **gromadzenie i późniejsze przetwarzanie danych powinno zostać ograniczone do minimum**. Bolączką wielu administratorów jest bowiem zbieranie danych „na zapas" w myśl *mogą przydać się „w przyszłości"*.

Przykład

Administrator danych organizuje konkurs. W regulaminie wskazuje, że to on, jako organizator dokona rozliczenia podatku dochodowego od wartości przyznanej nagrody. W związku z tym, już na etapie zgłaszania do konkursu żąda od uczestnika podania dodatkowych informacji takich jak PESEL lub NIP, czy też informacji o właściwym urzędzie skarbowym. Rzeczywiście informacje te będą niezbędne w momencie rozliczania nagrody. Niemniej, na samym etapie wyłaniania zwycięzców, te kategorie danych osobowych nie powinny być gromadzone. Nie są one bowiem niezbędne dla osiągnięcia celu przetwarzania jakim jest wyłonienie zwycięzców. Zebranie tych informacji powinno nastąpić dopiero po ogłoszeniu wyników konkursu i wyłącznie od jego laureatów.

Należy przy tym podkreślić, że obowiązek stosowania zasady *privacy by default* znajdzie pośrednio zastosowanie do **dostawców usług i aplikacji związanych z przetwarzaniem danych**, czyli zasadniczo podmiotów przetwarzających dane na zlecenie administratora.

Zgodnie z motywem 78 preambuły *Ogólnego rozporządzenia o ochronie danych*, jeżeli opracowywane, projektowane, wybierane i użytkowane są aplikacje, usługi i produkty, które opierają się na przetwarzaniu danych osobowych, **należy zachęcać wytwórców tych produktów, usług i aplikacji**, by podczas ich opracowywania i projektowania, wzięli pod uwagę prawo do

ochrony danych osobowych i z należytym uwzględnieniem stanu wiedzy technicznej **zapewnili administratorom i podmiotom przetwarzającym możliwość wywiązania się ze spoczywających na nich obowiązków ochrony danych osobowych**.

Odpowiedzialność

Spełnianie wymogów określonych przez zasadę *privacy by design* oraz zasadę *privacy by default* jest obowiązkiem wynikającym wprost z *Ogólnego rozporządzenia o ochronie danych*, którego przepisy przewidują sankcje za ich nieprzestrzeganie.

Naruszenie zasad stanowi przesłankę do **nałożenia niższej administracyjnej kary pieniężnej** tj. w wysokości do 10 000 000 euro, a w przypadku przedsiębiorstwa – w wysokości do 2% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego.

Podsumowanie

Koncepcje zasad *privacy by design* oraz *privacy by default* nie stanowią żadnego *novum* wprowadzonego przepisami *Ogólnego rozporządzenia o ochronie danych*. Funkcjonowały one już wcześniej pośród zagadnień związanych z ochroną danych osobowych czy szerzej, prywatnością. Przestrzeganie tych zasad przez administratorów powinno być ich *naturalnym odruchem* przy tworzeniu skutecznych systemów ochrony danych osobowych w ich organizacji.

Warto zauważyć, że zgodnie z art. 25 ust. 3 *Ogólnego rozporządzenia o ochronie danych* stosowanie zasad *privacy by design* oraz *privacy by default* można wykazać między innymi poprzez **wprowadzenie zatwierdzonego mechanizmu certyfikacji**. Niestety do dziś nie została sporządzona żadna lista dokumentów wymaganych, by administrator otrzymał certyfikat lub inny podmiot nabył uprawnienia do nadawania certyfikatów. Prezes UODO nie prowadzi również żadnych prac nad stworzeniem krajowych kryteriów akredytacji oraz certyfikacji. Być może z uwagi na rosnące potrzeby administratorów, jak również wątpliwości środowiska w zakresie ostatnio nałożonej kary finansowej, regulator zdecyduje się podjąć działania w tym zakresie. Do tego czasu jednak, administratorzy muszą bazować na swojej własnej ocenie, w której oczywiście wesprzeć ich mogą zewnętrzni eksperci.

Autor artykułu:

Małgorzata Zdunek, ekspert ds. ochrony danych osobowych

Źródła:

- 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)

- RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, Bielak-Jomaa Edyta (red.), Lubasz Dominik (red.)
- Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz, Litwiński Paweł (red.), Barta Paweł, Kawecki Maciej
- Opinion 5/2018 European Data Protection Supervisor Preliminary Opinion on privacy by design
- https://uodo.gov.pl/427 dostęp 02.10.2019 r.
- https://archiwum.giodo.gov.pl/pl/1520281/10023 dostęp 02.10.2019 r.