(R)ewolucja w ochronie danych osobowych

Od 25 maja 2018 r. we wszystkich krajach należących do Unii Europejskiej zaczną być stosowane przepisy Ogólnego Rozporządzenia o Ochronie Danych, zwanego w skrócie RODO.

Obowiązki administratora w zakresie ochrony danych

Przepisy RODO, w przeciwieństwie do obecnie obowiązujących rozwiązań nie wskazują wprost, jakie działania powinien podjąć administrator w celu zapewnienia danym osobowym należytej ochrony. Konieczne jest uwzględnienie takich okoliczności jak:

- charakter,
- zakres,
- kontekst,
- cele przetwarzania,
- ryzyko naruszenia praw lub wolności osób fizycznych.

Oceniając ryzyko należy wziąć pod uwagę prawdopodobieństwo oraz istotność potencjalnych zagrożeń, jakie mogą być związane z przetwarzaniem danych osobowych. Jeżeli planowane przez administratora działania mogą powodować wysokie ryzyko naruszenia praw osób, których dane są przetwarzane, powinna zostać przeprowadzona ocena skutków dla ochrony danych (ang. *Data Protection Impact Assessment*, DPIA). Ocena taka powinna zawierać m.in. określenie środków bezpieczeństwa jakie zostaną wykorzystane w celu zminimalizowania wystąpienia zagrożeń. Środki te mogą polegać np. na szyfrowaniu czy pseudonimizacji danych.

Podstawa prawna: art. 4, 24, 32, 35 RODO

Od tego dnia podmioty przetwarzające dane osobowe, niezależnie od tego czy mają charakter prywatny czy publiczny, powinny stosować się do obowiązków wynikających z przepisów RODO. Zgodnie z treścią nowych przepisów dane osobowe to informacje, które identyfikują albo w sposób pośredni lub bezpośredni umożliwiają identyfikację osoby fizycznej. Przykładem takich danych jest imię i nazwisko, numer PESEL czy adres email. Jednak taki charakter będą też miały mniej oczywiste informacje takie jak dane o lokalizacji, identyfikatory internetowe, kod genetyczny czy nawet preferencje zakupowe.

Z drugiej strony nowe przepisy wprowadzają jednolite na terenie całej Unii mechanizmy, dające możliwość łatwiejszego respektowania praw osobom fizycznym, których dane są przetwarzane.

Mimo, że rozporządzenie, jako instrument prawa wspólnotowego będzie stosowane bezpośrednio, to w pewnych sferach (np. związanych z przetwarzaniem szczególnych kategorii danych, tzw. danych wrażliwych) pozostawiono możliwość doprecyzowania przepisów państwom członkowskim. Jednocześnie dostosowania wymagają obecnie funkcjonujące rozwiązania prawne, co wymusza zmianę wielu przepisów sektorowych.

Prawa osób fizycznych

Przepisy Ogólnego Rozporządzenia o Ochronie Danych wprowadzają jednolity w całej Unii poziom ochrony dla wszystkich osób, których dane są przetwarzane.
Wśród uprawnień można wskazać:

- prawo do informacji o operacjach przetwarzania,
- prawo dostępu do danych,
- prawo do sprostowania danych,
- prawo do bycia zapomnianym,
- prawo do przenoszenia danych,
- prawo do sprzeciwu,
- prawo do decydowania o zautomatyzowanym podejmowaniu decyzji,
- prawo do bycia informowanym o naruszeniu danych osobowych.

Większość z powyższych uprawnień przysługuje już na gruncie obecnie obowiązujących przepisów. Należy pamiętać, że co do zasady niektóre prawa, takie jak prawo do informacji przysługiwać będą wszystkim uprawnionym, inne aktualizować się będą w określonych sytuacjach. Na zakres przysługujących uprawnień może wpływać np. podstawa prawna, umożliwiająca przetwarzanie danych. Trzeba także zaznaczyć, że prawa te mogą zostać ograniczone dla ochrony takich interesów jak np. bezpieczeństwo narodowe, publiczne czy zapobieganie przestępczości.
Podstawa prawna: art. 12 - 22, 34, 23 RODO

Biometria

Zgodnie z przepisami RODO *dane biometryczne oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne.* Definicja ta jest neutralna technologicznie – nie odwołuje się do konkretnych rozwiązań, dzięki czemu może pozostać aktualna pomimo postępu technicznego.

Kwestia przetwarzania danych biometrycznych przez pracodawców jest jednym z obszarów jakie zostaną uregulowane przepisami wprowadzającymi zmiany związane z RODO. Obecnie przetwarzanie tego rodzaju danych wiąże się z korzystaniem z systemów kontroli dostępu. Projektowane rozwiązanie dopuszcza *przetwarzanie przez pracodawcę danych biometrycznych obejmujących tylko dane osobowe pracownika, jeśli dotyczą one stosunku pracy i pracownik wyrazi na to zgodę w oświadczeniu złożonym w postaci papierowej lub elektronicznej.*
Użycie przez pracodawcę danych biometrycznych będzie wymagało dobrowolnej zgody pracownika – jej brak nie może być jednak przyczyna odmowy nawiązania lub rozwiązania stosunku pracy. Dane te zostały bowiem uznane za szczególne kategorie danych, tzw. dane wrażliwe. Szczegółowe rozwiązania określające sposób gromadzenia i zabezpieczenia danych biometrycznych określone zostaną w osobnym rozporządzeniu.
Podstawa prawna: art. 4, 9 RODO

Privacy by default oraz privacy by design

Przepisy RODO wprowadzają dwa nowe pojęcia wpływające na podejście do przetwarzania danych osobowych.
Zasada *privacy by default* zakłada domyślną ochronę prywatności. Domyślnie powinny być przetwarzane wyłączni te dane, które są niezbędne dla osiągnięcia celu przetwarzania. Zmiana ustawień programu lub aplikacji polegająca na przetwarzaniu większej ilości danych lub innych kategorii danych powinna wymagać aktywności użytkownika. Zmiana ustawień powinna następować świadomie i wymagać aktywnego działania użytkownika. Zasada *privacy by design* nakazuje, aby już na etapie projektowania systemu lub aplikacji uwzględnione

Obowiązek informacyjny

W motywie 60 preambuły RODO wskazano, że osoba, której dane dotyczą, musi być poinformowana o prowadzeniu operacji przetwarzania i o jej celach. Administrator powinien w sposób zwięzły, przejrzysty i zrozumiały przekazać informacje, mogące m.in. pozwolić na podjęcie świadomej decyzji co do udzielenia zgody na przetwarzanie danych. Administrator powinien poinformować o:

- swojej tożsamości i danych kontaktowych ewentualnie o tożsamości i danych kontaktowych swojego przedstawiciela, jeżeli go ustanowił,
- danych kontaktowych inspektora ochrony danych, jeżeli został ustanowiony,
- celach i podstawach prawnych przetwarzania danych osobowych,
- prawnie uzasadnionych interesach administratora,
- odbiorcach danych osobowych lub o kategoriach odbiorców,
- zamiarze przekazania danych osobowych do państwa trzeciego,
- okresie, przez który dane osobowe będą przechowywane,
- przysługujących prawach,
- prawie wniesienia skargi do organu nadzorczego,
- dobrowolności lub obowiązku podania danych osobowych, w szczególności czy jest to wymóg ustawowy,
- zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, jeżeli działania takie są stosowane.

Wyróżnione elementy stanowią nowość w odniesieniu do obecnie obowiązujących przepisów. Klauzula informacyjna powinna być sporządzona prostym językiem, w szczególności gdy będzie ona kierowana do dziecka. Dodatkowo może być opatrzona znakami graficznymi, które w zrozumiały sposób przedstawią sens zamierzonego działania, np. piktogram monitoringu. Należy tylko pamiętać, że jeżeli znaki te są przedstawione elektronicznie, muszą się nadawać do odczytu maszynowego.

Podstawa prawna: art. 12, 13 RODO

zostały rozwiązania zapewniające ochronę danych osobowych. Rozwiązania te mogą być związane ze sposobem pobierania danych (np. walidacja), przechowywania (np. szyfrowanie), dostępu do danych (np. pseudonimizacja czy poprzez poziomy dostępu użytkowników). Jednym ze środków pozwalających na zabezpieczenie przetwarzanych danych osobowych jest pseudonimizacja. Jest to rozwiązanie polegające na takim przetworzeniu danych osobowych, że nie można ich przypisać określonej osobie bez użycia dodatkowej, przechowywanej osobno informacji. Ta dodatkowa informacja jest kluczem umożliwiającym powiązanie dostępnych informacji z konkretną osobą fizyczną. Klucz musi być również odpowiednio zabezpieczony środkami technicznymi i organizacyjnymi.

Mimo, że zasady te można odnieść bezpośrednio do rozwiązań informatycznych, to powinny zostać uwzględnione przy tworzeniu każdego systemu ochrony danych osobowych wykorzystywanego przez administratora. Zasady te nakazują bowiem uwzględniać nie tylko możliwość wynikające ze stanu techniki, ale również środki organizacyjne.

Podstawa prawna: art. 4, 25 RODO

Zgłaszanie naruszeń

W przypadku gdy administrator stwierdzi naruszenie ochrony danych osobowych powinien on poinformować organ nadzoru – Prezesowi Urzędu Ochrony Danych Osobowych, który zastąpi dotychczas funkcjonujący organ – Generalnego Inspektora Ochrony Danych Osobowych. Zgłoszenie powinno zostać dokonane w ciągu 72 godzin, od chwili, w której administrator stwierdził naruszenie. Przepisy RODO określają naruszenie danych osobowych przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych. Oznacza to, że nawet utrata danych osobowych w wyniku awarii zasilania czy zalania może wiązać się z koniecznością informowania organu nadzoru. Nie oznacza to jednak, że należy informować organ o każdym zdarzeniu takiego rodzaju. Konieczność przesłania zawiadomienia nie dotyczy sytuacji, w których jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Jeżeli naruszenie nastąpiło w związku z przetwarzaniem danych przez podmiot działający na zlecenie administratora (tzw. procesor, czyli podmiot, któremu administrator powierzył przetwarzanie danych osobowych), podmiot ten powinien niezwłocznie poinformować o zdarzeniu administratora. Jeżeli jednak naruszenie ochrony danych związane jest z wysokim ryzykiem naruszenia praw i wolności osób fizycznych, to w szczególnych przypadkach, może wystąpić konieczność poinformowania, poza organem, także osób, których dane osobowe dotyczą.

Podstawa prawna: art. 4, 33, 34 RODO

Sankcje

Przepisy RODO kształtują odpowiedzialność na różnych płaszczyznach. Rozporządzenie wprowadza m.in. wysokie administracyjne kary pieniężne za naruszenie jego postanowień. Maksymalna wysokość kary pieniężnej zależy od dokonanego naruszenia. Przewidziane zostały dwa przedziały określające wysokość kar, w zależności od naruszenia:

do 10 000 000 EUR, a w przypadku przedsiębiorstwa - w wysokości do 2 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa,

do 20 000 000 EUR, a w przypadku przedsiębiorstwa - w wysokości do 4 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa.

WYBRANE NARUSZENIA ZASAD PRZETWARZANIA DANYCH OSOBOWYCH I SANKCJE

ARTYKUŁ RODO	ZASADA	KARA
Art. 8	Wyrażanie zgody przez dziecko w związku z usługami społeczeństwa informacyjnego	**Do 10 milionów euro** lub do 2% wartości rocznego światowego obrotu przedsiębiorstwa
Art. 25	Zasada domyślnej ochrony danych (privacy by default) oraz ochrony danych osobowych w fazie projektowania (privacy by design)	
Art. 28	Powierzenie przetwarzania danych osobowych	
Art. 30	Rejestrowanie czynności przetwarzani	
Art. 31	Współpraca z organem nadzorczym	
Art. 32	Bezpieczeństwo przetwarzania	
Art. 37	Wyznaczenie inspektora ochrony danych	
Art. 6, 9	Podstawy przetwarzania danych	**Do 20 milionów euro** lub do 4% wartości rocznego światowego obrotu przedsiębiorstwa
Art. 12–22	Naruszenie praw przysługujących uprawnionym	

Materiał powstał we współpracy
z p. Pawłem Tańskim,
radcą prawnym w Kancelarii SDO

Decydując o nałożeniu kary administracyjnej oraz jej wysokości organ indywidualnie podchodzi do każdego przypadku zwracając uwagę m.in. na:

- charakter, wagę i czas trwania naruszenia,
- umyślny lub nieumyślny charakter naruszenia,
- działania podjęte w celu zminimalizowania szkody poniesionej przez osoby, których dane dotyczą,
- stopień odpowiedzialności,
- wszelkie stosowne wcześniejsze naruszenia,
- stopień współpracy z organem nadzorczym w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych negatywnych skutków,
- kategorie danych osobowych, których dotyczyło naruszenie,
- sposób, w jaki organ nadzorczy dowiedział się o naruszeniu.

Niezależnie od kar administracyjnych, każdy kto poniósł szkodę w wyniku naruszenia niniejszego rozporządzenia, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie. Aby zwolnić się z odpowiedzialności to przetwarzający dane będą musieli udowodni, że w żaden sposób nie ponoszą winy za zdarzenie, które doprowadziło do powstania szkody.
Przepisy rozporządzenia dopuszczają także wprowadzenie przez poszczególne kraje innych rodzajów sankcji, np. sankcji karnych. Polski ustawodawca zamierza skorzystać z tego uprawnienia przewidując w projekcie ustawy o ochronie danych osobowych karę grzywny, ograniczenia wolności lub pozbawienia wolności do 2 lat w przypadku przetwarzanie danych nie jest dopuszczalne lub dokonywane jest bez uprawnienia. Kara może wynieść do 3 lat pozbawienia wolności, jeżeli przetwarzanie dotyczyć będzie tzw. danych wrażliwych, np. biometrycznych.

Podstawa prawna: art. 82, 83, 84 RODO

Regionalne Centrum Innowacji
i Transferu Technologii
Zachodniopomorski Uniwersytet
Technologiczny w Szczecinie
tel./fax: +48 91 449 43 54
e-mail: innowacje@zut.edu.pl
www.innowacje.zut.edu.pl

Komisja Europejska ani żadna osoba działająca w jej imieniu nie ponosi odpowiedzialności za wykorzystanie informacji zawartych w niniejszej publikacji. Informacje i poglądy zawarte w opracowaniu są poglądami autora i nie muszą odzwierciedlać ofcjalnego stanowiska Komisji Europejskiej.