RODO 3, czyli Akt w sprawie sztucznej inteligencji. Co się zmieni? Kogo dotyczy?

Rodzina RODO się powiększa! Niedawno pisaliśmy o Rozporządzeniu ePrivacy, nazywanym RODO 2. Teraz poświęcimy uwagę RODO 3, czyli Aktowi w sprawie sztucznej inteligencji (dalej: jako Akt „SI").

Co to jest sztuczna inteligencja?

Takie pytanie musieli sobie również postawić twórcy RODO 3. Fanów filmów i książek SF muszę niestety zmartwić. Alternatywnie ucieszyć, jeśli obawiacie się sztucznej inteligencji. Na dziś, nie istnieje coś takiego jak sieć SKYNET z filmu „Terminator" (dla starszych widzów), czy superkomputer Roboam z serialu Westworld (dla młodszych widzów).

Sztuczna inteligencja (dalej: „SI" lub „AI" od angielskiego *Artificial intelligence*) wspiera człowieka w nieco mniej widowiskowy sposób. Może się uczyć w oparciu o tzw. sieci neuronowe, które są dostępne (często nieodpłatnie!) w internecie. Kluczem do sukcesu dla systemów SI, są odpowiednio wprowadzone zestawy danych, którą umożliwiają uczenie się. Nie ma to wiele wspólnego ze sztuczną świadomością i wizjami z literatury SF. Może jednak ratować życie, optymalizować procesy biznesowe, pomagać w ściganiu przestępców.

Zdefiniowanie technologii, która powstaje na naszych oczach, nie było proste. Twórcy Rozporządzenia zdecydowali się na definicję dwuetapową.

W samej treści Rozporządzenia, sztuczną inteligencję zdefiniowano bardzo ogólnie:

Art. 3 pkt. 1)

oprogramowanie opracowane przy użyciu co najmniej jednej spośród technik i podejść wymienionych w załączniku I, które może – dla danego zestawu celów określonych przez człowieka – generować wyniki, takie jak treści, przewidywania, zalecenia lub decyzje wpływające na środowiska, z którymi wchodzi w interakcję;

Definicja otwiera drogę do doprecyzowania tego czym jest, a czym nie jest SI. Doprecyzowania będzie mogła dokonać Komisja samodzielnie. Bez uruchamiania skomplikowanej i wielostopniowej unijnej procedury ustawodawczej. Dlaczego? Dzięki temu prawo jest bardziej elastyczne. Nikt nie jest w stanie jednoznacznie przewidzieć kierunku i tempa, w którym będzie się rozwijać SI. Łatwe do modyfikacji prawo, to możliwość uniknięcia absurdów prawnych. A o te łatwo, kiedy próbujemy ująć w ramy prawne nową technologię.

Doprecyzowanie definicji znajduje się w Załączniku nr 1 do Aktu SI. Łatwo modyfikowalny Załącznik mówi o przykładowych podejściach i technikach, takich jak:

(a) podejścia do uczenia maszynowego, w tym nadzorowanego, nienadzorowanego i wzmacniającego uczenie się, z wykorzystaniem szerokiej gamy metod, w tym uczenia głębokiego;

b) podejścia oparte na logice i wiedzy, w tym reprezentacja wiedzy, programowanie indukcyjne (logiczne), bazy wiedzy, silniki wnioskowania i dedukcji, (symboliczne) wnioskowanie i systemy eksperckie;

(c) Podejścia statystyczne, estymacja bayesowska, metody przeszukiwania i optymalizacji

Jeśli więc system, który projektujesz lub który chcesz wdrożyć, zawiera któreś z powyższych podejść lub metod, to podpada pod przepisy RODO 3. Czy to znaczy, że czeka Cię żmudna biurokracja? Niekoniecznie, wszystko będzie zależało od poziomu ryzyka, systemu. Ale o tym jeszcze napiszę w dalszej części tekstu.

Sztuczna inteligencja i prawo do prywatności

Zdefiniowaliśmy zatem sztuczną inteligencję. Tylko co to wszystko ma wspólnego z ochroną danych osobowych?
Po pierwsze, RODO w pewien sposób reguluje obszar dotyczący sztucznej inteligencji. Mam na myśli art. 22 RODO mówiący o tzw. Profilowaniu kwalifikowanym. Nie każdy system profilujący będzie mieścił się w ramach definicji sztucznej inteligencji. Często jednak tak właśnie będzie. W przypadkach tzw. Profilowania kwalifikowanego, RODO każe zastosować szereg dodatkowych obostrzeń. Na przykład konieczne jest zbieranie zgody, wykonanie DPiA etc. Pisaliśmy już na ten temat na łamach naszego bloga.
Po wejściu w życie nowych przepisów, taki system prawdopodobnie będzie musiał spełnić dodatkowe wymogi.

Co z systemami, które przetwarzają dane osobowe, ale nie służą do tworzenia profili? Co z systemami SI, które w ogóle nie przetwarzają danych osobowych, jednocześnie znacząco wpływając na nasze bezpieczeństwo. Choćby tak medialne teraz systemy jazdy autonomicznej, tworzone dla samochodów.
Celem Aktu o SI, jest ujęcie w jego ramach wszystkich sytuacji związanych z budową i wykorzystywaniem SI. A ponieważ SI bardzo często będą służyły do przetwarzania danych osobowych, to jest to jedna z tych regulacji, które warto mieć na oku.

Sztuczna inteligencja made in EU

Obecnie liderami technologii sztucznej inteligencji są Amerykanie i Chińczycy. UE plasuje się na najniższym stopniu podium. Twórcy RODO 3 wyszli z zupełnie innych założeń niż rywale z USA i Chin. W stanach Zjednoczonych, rozwój SI nie jest mocno ograniczany i regulowany. Giganci krzemowej doliny tworzą bardzo silne lobby, które nie chce dopuszczać do zbyt mocnych ograniczeń. USA tradycyjnie już ucieka od regulacji prawnych, krępujących biznes nowych technologii. W Chinach z kolei nie ma bariery polegającej na prawach człowieka. Jeśli SI jest w stanie usprawnić procesy biznesowe, to nikt nie będzie przejmował się np. prawem do prywatności.

UE przyjęło zupełnie inne założenia. Sztuczna inteligencja made in EU, ma wyróżniać się wysokim poziomem bezpieczeństwa, etyki oraz niezawodności. Innymi słowy, SI z UE ma być całkowitym przeciwieństwem tej z Chin. Oczywiście cena rozwiązań z EU, też będzie na pewno wyższa niż tych z Chin czy USA.
Czy to prawidłowy kierunek? Czas pokaże. Przyjrzyjmy się zatem komu i jakie wymogi stawia RODO 3?

Kim jest Dostawca, kim jest Użytkownik?

Akt o sztucznej inteligencji jest adresowany do dwóch kluczowych kategorii organizacji. Po pierwsze, do Dostawców.

„dostawca" oznacza osobę fizyczną lub prawną, organ publiczny, agencję lub inny podmiot, które opracowują system sztucznej inteligencji lub zlecają jego opracowanie w celu wprowadzenia go do obrotu lub oddania go do użytku pod własną nazwą handlową lub własnym znakiem towarowym – odpłatnie lub nieodpłatnie;

Po drugie, do Użytkowników:

„użytkownik" oznacza osobą fizyczną lub prawną, organ publiczny, agencję lub inny podmiot, które korzystają z systemu sztucznej inteligencji pod swoją kontrolą, zwyjątkiem sytuacji, gdy system sztucznej inteligencji jest wykorzystywany w ramach osobistej działalności pozazawodowej;

Co istotne, przepisy wiążą także dostawców i użytkowników z państw trzecich, o ile wyniki działań SI z których korzystają są wykorzystywane w UE.
Jeśli korzystasz z SI i wpływasz nim na rynek unijny, podlegasz pod RODO 3. Podobną konstrukcję dobrze znamy z RODO. Nie ważne, gdzie przetwarzasz dane osobowe. Jeśli przetwarzasz je w związku z działalnością prowadzoną w UE, podlegasz przepisom RODO.

Niedopuszczalne ryzyko

Kolejnym powodem, dla którego Akt o SI jest nazywany również RODO 3, to podejście oparte na ryzyku. Poziomy ryzyka są cztery: niedopuszczalne, wysokie, niskie lub minimalne. Dla każdego z poziomów, system musi spełniać inne kryteria. Zaczniemy od poziomu ryzyka niedopuszczalnego. Systemy kwalifikowane w ten sposób są bezwzględnie zakazane. Tutaj mamy jednak małe zastrzeżenie. RODO 3 nie dotyczy technologii wykorzystywanych jedynie w celach wojskowych (jeśli takie wykorzystanie wchodzi w zakres wyłącznych kompetencji wspólnej polityki zagranicznej i bezpieczeństwa UE).
Jakie systemy znalazły się na cenzurowanym? Na przykład systemy manipulujące emocjami lub wykorzystujące słabości poszczególnych grup (np. osób starszych czy chorych). Zakazano także systemów służących do punktowej oceny społeczeństwa, poprzez pryzmat zachowania jednostki. Takie systemy już funkcjonują, na przykład w Chinach. Za niedopuszczalnie ryzykowne uznano także systemy identyfikacji biometrycznej w czasie rzeczywistym z wykorzystaniem sieci monitoringów miejskich (z pewnymi wyjątkami).
Jeśli system, który chcesz zbudować (lub stosować) spełnia jedną z przesłanek wskazanych w art. 5 Aktu o Sztucznej Inteligencji, to musisz liczyć się z surowymi konsekwencjami.

Wysokie ryzyko

Systemy wysokiego ryzyka zdefiniowano w podobny sposób co samą SI. Mamy więc bardzo ogólną definicję w art. 6 RODO 3, a następnie doprecyzowanie w Załącznikach II i III.
Załącznik nr II zawiera odesłanie do innych unijnych aktów prawnych. Chodzi o systemy przeznaczone do wykorzystywania jako związane z bezpieczeństwem elementu produktu objętego unijnym prawodawstwem harmonizacyjnym wymienionym w Załączniku II lub sam jest takim produktem.

Jakich produktów dotyczy unijne ustawodawstwo harmonizacyjne, wymienione w Załączniku II? Kilka przykładów poniżej:

1. Dyrektywa 2009/48/EC tzw. Dyrektywa zabawkowa, która reguluje kwestie związane z bezpieczeństwem zabawek
2. Rozporządzenie 2017/745 w sprawie wyrobów medycznych
3. Dyrektywa 2014/90/EU w sprawie wyposażenia morskiego

Inne systemy wysokiego ryzyka wymienia Załącznik nr 3, który wskazuje na systemy obsługujące obszary takie jak:

1. identyfikacja i kategoryzacja biometryczna osób fizycznych (np. systemy AI w celu zdalnej identyfikacji biometrycznej osób fizycznych „w czasie rzeczywistym"),
2. zarządzanie infrastrukturą krytyczną i jej eksploatacja (np. systemy AI przeznaczone do kierowania ruchem),
3. kształcenie i szkolenie zawodowe (np. systemy AI mające na celu określenie predyspozycji do kierunku kształcenia),
4. zatrudnienie, zarządzanie pracownikami i dostęp do samozatrudnienia (np. systemy AI przeznaczone dla rekruterów w celu filtrowania, analizy czy segregacji nadesłanych zgłoszeń lub podejmowania decyzji o awansie lub rozwiązania umowy z pracownikiem),
5. dostęp do podstawowych usług prywatnych oraz usług i świadczeń publicznych (np. systemy AI służące analizie zdolności kredytowej przed udzieleniem pożyczki, ustalania priorytetów w wysyłaniu służb ratunkowych),
6. ściganie przestępstw (np. systemy AI służące do analizy możliwości popełnienia przestępstwa przez konkretną osobę , systemy mające na celu wspomaganie organu sądowego w ocenie wiarygodności dowodów),
7. zarządzanie migracjami, azylem i kontrolą graniczną (np. systemy AI przeznaczone do stosowania w celu weryfikacji autentyczności dokumentów podróży poprzez sprawdzenie ich zabezpieczeń),
8. sprawowanie wymiaru sprawiedliwości i procesy demokratyczne (np. systemy AI mające na celu wspomaganie organu sądowego w badaniu i interpretowaniu faktów oraz prawa, a także w stosowaniu prawa do konkretnego stanu faktycznego).

Jeśli działasz w takich obszarach lub tworzysz rozwiązania IT na potrzeby takich branż, musisz liczyć się z dodatkowymi obowiązkami.

Jak legalnie działać na systemie SI wysokiego ryzyka?

Systemy wysokiego ryzyka nie są zabronione. Mogą być tworzone i wykorzystywane, stawia się im jednak pewne wymogi.
W uproszczeniu, sprowadzają się one do:

1) ustanowienia systemu zarządzania ryzykiem. Taki system musi funkcjonować przez cały okres życia systemu.
2) odpowiedniego zarządzania i kontroli nad danymi, które wprowadzane są do AI w celu uczenia maszynowego,
3) posiadania odpowiedniej dokumentacji technicznej systemu,

4) obowiązku rejestrowania zdarzeń związanych z działaniem systemów (przechowywania logów systemowych),
5) zapewnienia przejrzystości działania systemu i udostępniania użytkownikom informacji na jego temat,
6) nadzoru człowieka nad systemem,
7) zapewnienia odpowiedniego poziomu dokładności, solidności i cyberbezpieczeństwa systemu,
8) certyfikacji przez wyznaczony przez państwo organ. Obecnie trudno stwierdzić jednoznacznie czy certyfikacja będzie obowiązkowa i kiedy.

Proste do spełnienia? Trudno powiedzieć w tym momencie. Nie znamy wytycznych dotyczących tego jak w praktyce powinny być realizowane te obowiązki np. dotyczące prowadzenia dokumentacji SI. Niemniej jednak, powyższe wymogi brzmią racjonalnie i zdroworozsądkowo. Nie wydaje się, żeby powyższe wymogi mogły stanowić potężną barierę wejścia dla twórców SI. Na pewno mogą działać jednak zniechęcająco. Zwłaszcza dla środowiska startupów. Trudnością mogą być również spory dotyczące kwalifikowania systemu, do systemów niedopuszczalnego lub wysokiego ryzyka. Z drugiej strony, obywatele UE, mają zyskać pewność i poczucie bezpieczeństwa np. co do tego, że nikt nie będzie manipulował ich emocjami i uczuciami.

Niskie ryzyko

Dla systemów o niskim ryzyku, wymogów jest znacznie mniej. Wystarczy zachowanie przejrzystości. Chodzi o to, żeby osoba wchodząca w interakcję z systemem, wiedziała, że ma do czynienia ze Sztuczną Inteligencją. Na przykład, będzie tak w przypadku kontaktu z chatbotami. W podobny sposób będą musiałby być oznaczone systemy potrafiące wygenerować deepfake. Przykładem deepfake będzie obraz, który nie miał miejsca w rzeczywistości. Wyobraźmy sobie celebrytę i jego zmanipulowaną przez SI wypowiedź. Odbiorca musi wiedzieć, że treść nie jest prawdziwa. Gdyby ktoś chciał zobaczyć jak wygląda technologia deepfake w akcji, proponuję wpisać frazę „Tom Cruise deepfake" w wyszukiwarce YouTube.

Minimalne ryzyko

Zdecydowana większość obecnie funkcjonujących SI zalicza się do tej kategorii. Jeśli grałeś/aś kiedyś na komputerze, to z pewnością rywalizowałeś ze sztuczną inteligencją. Jeśli korzystasz z filtrów antyspamowych, to również masz do czynienia z systemem SI. Tyle, że w tym przypadku twórcy i użytkownicy takich systemów nie muszą spełniać żadnych dodatkowych kryteriów.

Organ Nadzorczy

Przepisy przewidują powołanie nowego europejskiego organu – Europejskiej Rady ds. Sztucznej Inteligencji oraz organów krajowych nadzorczych w państwach członkowskich. W tym zakresie mamy więc rozwiązanie podobne do tego z obszaru ochrony danych osobowych.

Kary

System kar administracyjnych także zbudowano w sposób zbliżony do tego, znanego już z RODO, z tą równicą, że kar nie przewiduje samo Rozporządzenie, lecz mają zostać one przyjęte w przepisach państw członkowskich. Kary nakładane będą przez krajowe Organy Nadzorcze. W najdotkliwszym wariancie kara może wynieść 30 mln EUR lub do 6% światowego rocznego obrotu.

Kiedy Akt w sprawie sztucznej inteligencji wejdzie w życie?

Trudno precyzyjnie przewidzieć datę wejścia w życie aktu SI. Warto jednak wiedzieć, że póki co w projekcie jest mowa o 24 miesięcznym okresie przejściowym (tj. okresem miedzy wejściem w życie przepisów, a rozpoczęciem ich stosowania). Od dnia uchwalenia przez PE, będziemy mieli zatem jeszcze dwa lata na przygotowanie się do nowej regulacji. To kolejne podobieństwo do RODO.

Wiele wskazuje na to, że w przeciwieństwie do ePrivacy, proces ustawodawczy ma szansę być nieco szybszy. Rozwój systemów SI jest tak dynamiczny, że wiele osób czuje silną potrzebę nadania mu pewnych ram.

Co oznacza wejście Aktu SI dla Twojej organizacji?

Jeśli nigdy nie korzystałaś/eś i nie zamierzasz korzystać z SI, to możesz nie przejmować się Rozporządzeniem. Jednak w praktyce SI jest bardzo popularne już teraz. Wszystko wskazuje na to, że w perspektywie kilku lat, trudno będzie znaleźć organizacje w ogóle nie korzystające z SI.

Regulowany obszar:	**Kogo zmiana dotyczy:**
Spełnienie kryteriów stawianych systemom SI wysokiego ryzyka, przede wszystkim dokumentacja, zarządzanie ryzykiem, zarządzanie danymi, nadzór człowieka, przejrzystość i inne.	• Dostawcy systemów (twórcy, producenci, dystrybutorzy). • Użytkownicy systemów (organizacje – biznes i administracja publiczna, zamawiające SI od dostawców).

Podsumowanie

SI dynamicznie wkracza do naszych organizacji. Póki co, korzystanie z takich systemów nie wymaga od nas podejmowania dodatkowych działań prawnych. Wyjątkiem są systemy profilujące lub przetwarzające dane osobowe. W tym przypadku już dzisiaj zastosowanie ma dobrze znane RODO 1.

W przyszłości, korzystając z SI, nawet jeśli nie ma w nich danych osobowych, musisz liczyć się z pewnymi ograniczeniami i obowiązkami.

Sygnałem alarmowym do zainteresowania się Aktem o SI, powinno być dla Ciebie uchwalenie Rozporządzenia przez PE. Od tego momentu musisz zacząć działać.

Zapraszam do śledzenia kolejnych informacji o Akcie o SI na naszym blogu!

Autor artykułu:

Przemysław Zegarek

Źródła:

- Rozporządzenie parlamentu europejskiego i rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze unii https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206