RODO

Raport Otwarcia

Polskiej Izby Informatyki
i Telekomunikacji

PIIT

Warszawa 2019

Słowo Wstępu

Polska Izba Informatyki i Telekomunikacji (PIIT) działa jako platforma do współtworzenia fundamentów cyfrowego rozwoju Polski. Każda z ponad 130 firm zrzeszonych w PIIT dostosowała się do wymogów rozporządzenia RODO, które weszło w życie 25 maja 2018 r.

Przyjęta w RODO nowa filozofia nie narzuca jednego standardu postępowania. Określa ogólne zasady, jakich trzeba przestrzegać i wskazuje, by administratorzy podchodzili do ochrony danych jak do ciągłego procesu, w którym nieustannie trzeba czuwać, testować rozwiązania i dostosowywać je do zmieniającej się rzeczywistości technologicznej, pewnych zjawisk i zagrożeń.

Dlatego w rok od wejścia w życie rozporządzenia postanowiliśmy sprawdzić, jak wygląda stosowanie RODO w branży IT i Telekomunikacyjnej. Z jakimi problemami spotykają się przedsiębiorcy w tym zakresie? Jak rozporządzenie wpisało się w stosowane w naszym kraju od ponad 20 lat sektorowe i ogólne przepisy dotyczące danych osobowych? Jakie mamy doświadczenia w tym zakresie a jakie jeszcze stoją przed firmami teleinformatycznymi wyzwania?

Liczę na to, że na powyższe i inne pytania, znajdziecie Państwo odpowiedzi w Raporcie Otwarcia RODO przygotowanym przez PIIT pod przewodnictwem Barbary Sawiny, Xawerego Konarskiego i Mariusza Busiło.

Życzę Państwu miłej lektury!

Andrzej Dulka, Prezes Polskiej Izby Informatyki i Telekomunikacji

Wprowadzenie

Ochrona prawna danych osobowych i prywatności w sieciach teleinformatycznych zawsze stanowiła istotny element prowadzenia działalności przez podmioty z sektora ICT. Regulacje te bezpośrednio bowiem wpływają na architekturę tworzonych aplikacji i systemów, jak również realizowane procesy biznesowe przez firmy z tego sektora. Wejście w życie RODO uświadomiło jeszcze bardziej potrzebę znajomości przepisów prawnych z tego zakresu.

Z powyższych przyczyn, w ramach Polskiej Izby Informatyki i Telekomunikacji od lat działa Komitet Ochrony Danych Osobowych i Zarządzania Informacją (KODO). Jego celem jest z jednej strony formułowanie uwag i stanowisk do projektów aktów prawnych z zakresu ochrony informacji, a z drugiej wypracowywanie wśród członków PIIT wykładni przepisów RODO i – docelowo – dobrych praktyk w zakresie stosowania tego prawa. Od 2018 r. w ramach KODO prowadzone są prace nad Kodeksem postępowania i dobrych praktyk w zakresie ochrony danych osobowych, który – po jego zatwierdzeniu przez regulatora – powinien stanowić ważny mechanizm compliance.

Od 2016 roku członkowie KODO spotykali się wielokrotnie, omawiając plany wdrożenia RODO. Poświęcono wiele godzin na dyskusje, w jaki sposób wykonać zobowiązania nałożone na administratorów, z uwzględnieniem specyficznych cech sektora. Po roku stosowania RODO, niektóre kwestie, które budziły wątpliwości zostały wyjaśnione, inne nadal wymagają potwierdzenia. Dlatego też bacznie obserwowane są decyzje oraz wytyczne zarówno Urzędu krajowego jak i pozostałych europejskich.

Pierwsza rocznica obowiązywania RODO jest dobrą okazją do przekazania w ramach niniejszego Raportu doświadczeń członków PIIT w stosowaniu nowego prawa. W pierwszej części przedstawiony został system prawny RODO i jego wpływ na branżę ICT. Następnie opisane są te instytucje prawne Rozporządzenia, których stosowanie jest szczególnie istotne dla firm nowotechnologicznych (realizacja praw podmiotów danych, przetwarzanie danych na potrzeby zautomatyzowanego podejmowania decyzji, transfer danych poza EOG). W dalszej kolejności przedstawiona jest problematyka prawna przetwarzania danych osobowych w rożnych modelach relacji pracowniczych, co jest istotnym elementem działalności firm ICT. I wreszcie na koniec opisana jest wzajemna relacja ochrony danych osobowych i trendów technologicznych, w tym w zakresie przetwarzania danych osobowych w chmurze obliczeniowej.

Xawery Konarski, Wiceprezes PIIT
Barbara Sawina, Przewodnicząca KODO
Mariusz Busiło, Wiceprzewodniczący KODO

SPIS TREŚCI

POLSKA IZBA INFORMATYKI I TELEKOMUNIKACJI

Kim jesteśmy?

PIIT to platforma firm działających na rzecz cyfrowej transformacji gospodarki i modernizacji państwa. Współtworzymy fundamenty cyfrowego rozwoju, realizując następujące działania:

- opiniujemy akty prawne istotne z punktu widzenia firm teleinformatycznych
- współtworzymy w konsultacjach i grupach roboczych warunki do uzgodnień sektorowych dotyczących wspólnych stanowisk oraz nowych inicjatyw branży (poprzez działalność komitetów, grup roboczych, animowanie prac członków nad konkretnymi zagadnieniami)
- budujemy trwałe relacje z administracją publiczną, poprzez organizownie spotkań oraz inicjowanie nowych, wspólnych projektów
- reprezentujemy interesy polskich firm teleinformatycznych na poziomie europejskim, poprzez organizację DIGITALEUROPE

Nasze cele

Sprzyjające warunki dla rozwoju przemysłu teleinformatycznego
Racjonalne regulacje i inicjatywy wspierające wdrażanie cyfrowych innowacji
Partnerska współpraca przemysłu teleinformatycznego i administracji publicznej

Chcesz nas bliżej poznać?

Zadzwoń: **22 628 22 60, 691 119 555**
Napisz: **sekretariat@piit.org.pl**

Polska Izba Informatyki i Telekomunikacji
Al. Jerozolimskie 136 (IX piętro)
Eurocentrum Alfa
02-305 Warszawa

Nowe przepisy o ochronie danych osobowych w Unii Europejskiej i Polsce

Adw. Xawery Konarski, adw. dr Grzegorz Sibiga, Traple Konarski Podrecki i Wspólnicy

Na pakiet normatywny reformujący ochronę danych osobowych w Unii Europejskiej składają się dwa akty prawne:

I) 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, dalej określane jako „RODO" lub „Rozporządzenie")
oraz

II) dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (dalej określana jako „dyrektywa policyjna").

Przepisy RODO obowiązują od 25 maja 2018 r. Rozporządzenie ma zasięg ogólny, wiąże w całości co do wszystkich zawartych w nim postanowień i jest bezpośrednio stosowane we wszystkich państwach członkowskich, bez potrzeby dokonywania implementacji do przepisów krajowych. Taki charakter przepisów Rozporządzenia związany jest z jednym z podstawowych celów uchwalenia RODO tj. likwidacji fragmentaryzacji ochrony danych osobowych w poszczególnych państwach Unii Europejskiej i zapewnienia równorzędnego stopnia ochrony na terytorium całej Unii.

Dyrektywa 2016/680 traktowana jest jako uzupełnienie RODO w zakresie przetwarzania danych osobowych przwez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom. W tym zakresie bowiem RODO wyłącza stosowanie swoich przepisów (tak art. 2 ust.2 lit. d RODO). Prawodawca europejski celowo uregulował powyższe kwestie – ze względu na szczególny charakter takich czynności – w akcie prawnym innej rangi, tj. dyrektywie. Dyrektywa bowiem jako akt prawny zobowiązujący państwa członkowskie do ustanowienia danego porządku prawnego – w przeciwieństwie do rozporządzenia, którego przepisy mają zastosowanie wprost – pozwala na uwzględnienie w przygotowywanych na jej podstawie przepisach odmienności krajowych regulacji w zakresie zapobiegania i zwalczania przestępczości. Przykładem tego rodzaju odmienności w prawie polskim jest chociażby, nie występujące w innych państwach Unii Europejskiej, rozróżnienie czynów karalnych na przestępstwa i wykroczenia. Przepisy Dyrektywy 2016/680 zostały wprowadzone do polskiego porządku prawnego w ustawie z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r. poz. 125). Weszła ona w życie w dniu 6 maja 2019 r., jej postanowienia są omawiane w dalszej części raportu.

Ustawa kompetencyjna i ustawa dostosowująca do RODO

Niezależnie od bezpośredniej stosowalności przepisów RODO, w Rozporządzeniu przewidziano również w pewnym zakresie jego uzupełnienie przepisami krajowymi. W Polsce uzupełnienie tego rodzaju nastąpiło w dwóch aktach prawnych:

I) ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000), tzw. „ustawa kompetencyjna", „uodo", która weszła w życie w dniu 25 maja 2018 r.
oraz

II) ustawie z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 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 (Dz.U. z 2019 r., poz.730), tzw. „ustawa dostosowująca", która weszła w życie w dniu 4 maja 2019 r. W przypadku sektora ICT najważniejsze zmiany wprowadzono na jej podstawie w ustawie o świadczeniu usług świadczonych drogą elektroniczną („uśude") oraz ustawie-Prawo Telekomunikacyjne (odpowiednio art. 63 oraz art. 79 ustawy dostosowującej). Zostaną one omówione w dalszej części raportu (pkt III – „RODO a przepisy sektorowe dotyczące usług łączności elektronicznej".)

Na całość sytemu przepisów RODO składają się więc nie tylko przepisy Rozporządzenia, ale również wydanych w związku z nim ustaw krajowych. Ma to istotne znaczenie prawne, ponieważ naruszeniem przepisów Rozporządzenia, skutkującym między innymi możliwością nałożenia przez Prezesa Urzędu Ochrony Danych Osobowych wysokich kar pieniężnych jako sankcji administracyjnych (art. 83 RODO), będzie również naruszenie przepisów ustaw krajowych, doprecyzowujących RODO.

Ustawa kompetencyjna

W ustawie kompetencyjnej znajdują się przede wszystkim te postanowienia, których przyjęcia w przepisach krajowych wymaga RODO. Do najważniejszych z nich zaliczyć należy określenie sposobu wyboru i kompetencji Prezesa Urzędu Ochrony Danych Osobowych (PUODO) jako organu właściwego w sprawach ochrony danych osobowych (art. 34 i n. uodo) oraz zasad prowadzenia postępowań administracyjnych w sprawie naruszenia przepisów o ochronie danych osobowych (art. 60 i n. uodo). Wiążą się z nimi bezpośrednio przepisy dotyczące postępowania kontrolnego prowadzonego przez PUODO (art. 78 i n. uodo) oraz przesłanek nakładania przez ten organ administracyjnych kar pieniężnych, przewidzianych w RODO (art. 101 uodo). Odrębne przepisy dotyczą uzupełnienia postanowień RODO odnośnie odpowiedzialności cywilnoprawnej z tytułu naruszenia przepisów o ochronie danych osobowych oraz związanych z tym proceduralnych zagadnień dochodzenia roszczeń przed sądami powszechnymi (art. 92 i n. uodo). W ustawie kompetencyjnej wprowadzono również przepisy karne za bezprawne przetwarzanie danych osobowych oraz za utrudnianie prowadzenia kontroli przez PUODO (art. 107-108 uodo).

Nowym, w stosunku do dotychczasowego stanu prawnego, rozwiązaniem przewidzianym w RODO jest możliwość wykazywania przez podmioty przetwarzające dane osobowe zgodności z wymogami Rozporządzenia poprzez stosowanie określnych w nim instrumentów compliance (m.in. kodeks postępowania oraz mechanizmy certyfikacji). W związku z tym w ustawie kompetencyjnej znalazły się przepisy określające warunki i tryb akredytacji podmiotu uprawnionego do certyfikacji w zakresie ochrony danych osobowych („podmiot certyfikujący"), akredytowanego przez Polskie Centrum Akredytacji, oraz trybu dokonywania samej certyfikacji (art. 15 i n. uodo). Podobny charakter mają postanowienia o trybie zatwierdzenia kodeksu postępowania oraz podmiocie monitorującym kodeks postępowania (art. 27 i n. uodo). Doświadczenia innych państw Unii Europejskiej wskazują, że pozyskaniem tego rodzaju certyfikatów szczególnie zainteresowane są podmioty z sektora ICT (np. certyfikat na dany produkt lub usługę IT). Z kolei, kodeksy postępowań wypracowywane są zazwyczaj przez izby gospodarcze, projekt takiego kodeksu przygotowała również Polska Izba Informatyki i Telekomunikacji (PIIT).

Implementacja dyrektywy policyjnej

Dyrektywa policyjna obejmuje przetwarzanie danych osobowych w określonych celach. Ma być ono związane z rozpoznawaniem, zapobieganiem, wykrywaniem i zwalczaniem czynów zabronionych. Celem uchwalenia tzw. dyrektywy policyjnej było między innymi ułatwienie wymiany danych osobowych między państwami członkowskimi Unii Europejskiej, co ma zapewnić skuteczną współpracę wymiarów sprawiedliwości w sprawach karnych i współpracę policji, jak również zapewnienie możliwości przekazania danych do państwa trzeciego (poza Europejski Obszar Gospodarczy), pod warunkiem że celem takiego działania będzie ściganie przestępstw przy jednoczesnym zapewnieniu przez państwo trzecie odpowiedniego poziomu ochrony danych. Dyrektywa policyjna ma również zapewnić transparentność przetwarzania danych przez policję i instytucje zwalczające przestępczość oraz stworzyć mechanizmy, które pozwolą przeciwdziałać ewentualnym nadużyciom ze strony tych służb. Na podstawie nowych przepisów organy państwowe mogą korzystać z danych osobowych wyłącznie w ściśle określonych celach oraz pod kontrolą niezależnego od organu ochrony danych osobowych.

Dyrektywa policyjna została implementowana do polskiego porządku prawnego w ustawie z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r. poz. 125). Ustawa ta określa między innymi jej zakres przedmiotowy i podmiotowy, zadania organu nadzorczego (Prezesa Urzędu Ochrony Danych Osobowych, PUODO), zasady przetwarzania danych osobowych, sposób zabezpieczenia danych osobowych, prawa osób, których dane dotyczą, zasady współpracy PUODO z organami nadzorczymi w innych państwach Unii Europejskiej oraz środki ochrony prawnej przysługujące osobom, których dane są przetwarzane.

Mającej na względzie, że RODO oraz dyrektywa policyjna stanowią część jednego pakietu legislacyjnego reformującego prawo ochrony danych osobowych Unii Europejskiej, brzmienie ustawy policyjnej zostało skorelowane z tekstem RODO w ten sposób, że w obu tych aktach prawnych wprowadzono tą samą terminologię i definicje (art. 4), oba akty prawne bazują na tych samych zasadach ogólnych (art. 13 i n.), ten sam organ (PUODO) czuwa również nad ich przestrzeganiem, z zastrzeżeniem, że w odniesieniu do prokuratury i sądów organ nadzorczy został określony odrębnie, co znalazło odzwierciedlenie w ustawach kompetencyjnych tych podmiotów (art. 5 i n.).

Ustawa policyjna obowiązuje we wszystkich sprawach, w których przetwarzanie danych osobowych odbywa się w jednym z wymienionych celów określonych w jej art. 1 pkt 1 tj. „rozpoznawaniu, zapobieganiu, wykrywaniu i zwalczaniu czynów zabronionych, w tym zagrożeń dla bezpieczeństwa i porządku publicznego, a także wykonywaniu tymczasowego aresztowania, kar, kar porządkowych i środków przymusu skutkujących pozbawieniem wolności". W pozostałych sprawach stosuje się przepisy RODO. To oznacza, że te same podmioty (np. organy ścigania) w zależności od celów przetwarzania danych osobowych mogą być zobowiązane do przestrzegania przepisów ustawy policyjnej, bądź RODO.

Ustawa zawiera dwa istotne wyłączenia przedmiotowe (art. 3). Po pierwsze, wyłącza swoje zastosowanie do danych osobowych znajdujących się w aktach spraw lub czynności lub urządzeniach ewidencyjnych prowadzonych w postępowaniach: a) w stosunku do nieletnich, b) karnych, w tym karnych wykonawczych i karnych skarbowych oraz c) wobec osób z zaburzeniami psychicznymi stwarzającymi zagrożenie dla życia, zdrowia lub wolności seksualnej i innych osób (art. 3 pkt 1). Po drugie, ustawy nie stosuje się w sprawach danych przetwarzanych, w zakresie zapewnienia bezpieczeństwa narodowego, przez Agencję Bezpieczeństwa Wewnętrznego, Agencję Wywiadu, Służbę Kontrwywiadu Wojskowego, Służbę Wywiadu Wojskowego oraz Centralne Biuro Antykorupcyjne (art. 3 pkt 2). W trakcie prac legislacyjnych nad ustawą trafnie zwracano uwagę, że powyższe wyłączenia nie do końca zgodne są z unijnym pierwowzorem tj. dyrektywą 2016/680.

W ustawie policyjnej nie zawarto zamkniętego katalogu podmiotów podlegających jej działaniu. Należy w związku z tym przyjąć, że będą to wszystkie organy przetwarzające dane w związku z realizacją celów określonych w art. 1 pkt 1 ustawy. Tym sam, ustawa obejmuję swoim zakresem nie tylko działalność organów ścigania, lecz również jednostek prokuratury oraz sądów, w zakresie w jakim realizują one te cele.

W ustawie szczegółowo określono obowiązki administratorów i podmiotów przetwarzających dane osobowe (art. 31 i n.). Administratorzy danych między innymi muszą w określonych terminach dokonywać oceny, które z posiadanych przez nich danych są zbędne i należy je usunąć. Mogą przetwarzać dane tylko w uzasadnionych celach, uaktualniać je i przetwarzać w sposób zapewniający odpowiednie bezpieczeństwo danych. Są też zobowiązani do opracowania polityki ochrony danych. W ustawie wskazano również, jakie środki techniczne i organizacyjne powinny być stosowane w celu zapewnienia ochrony danych osobowych (art. 39 i n.).

W ustawie policyjnej zagwarantowano, że osoby, których dane są przetwarzane, mają między innymi prawo dostępu do nich, ich uzupełnienia, uaktualnienia lub sprostowania, a także prawo do usunięcia danych osobowych w przypadku, gdy zostały zebrane lub są przetwarzane z naruszeniem przepisów ustawy (art. 23 i n.).

Ustawa policyjna przewiduje odpowiedzialność:

I) administracyjną (art. 50 i n.),
II) cywilną (art. 53) oraz
III) karną (art. 54) za naruszenie jej przepisów.

Organ regulacyjny w zakresie ochrony danych osobowych

Na podstawie ustawy kompetencyjnej od dnia 25 maja 2018 r. urząd Generalnego Inspektora Ochrony Danych Osobowych (GIODO) został przemianowany na Prezesa Urzędu Ochrony Danych Osobowych (PUODO), Biuro Generalnego Inspektora Ochrony Danych Osobowych stało się natomiast Urzędem Ochrony Danych Osobowych.

Nowy organ nadzorczy w zakresie ochrony danych osobowych otrzymał istotnie szerszy katalog kompetencji, w głównej mierze zdeterminowany przepisami RODO. Do najistotniejszych obszarów działań PUODO zaliczyć należy:

a) prowadzenie ewidencji inspektorów ochrony danych osobowych powołanych przez administratorów (art. 10 uodo),
b) opracowanie kryteriów certyfikacji (art. 16 uodo), o której mowa w art. 42 RODO oraz przeprowadzanie certyfikacji (art. 15 ust. 1 uodo),
c) prowadzenie elektronicznego systemu umożliwiającego administratorom zgłaszanie naruszeń ochrony danych osobowych na podstawie art. 33 RODO,
d) umożliwienie administratorom uprzednich konsultacji w zakresie operacji co do których ocena skutków wykazała wysokie ryzyko, o czym mowa w art. 36 RODO,
e) prowadzenie postępowań kontrolnych przez upoważnionych pracowników Urzędu zgodnie z zatwierdzonym przez Prezesa Urzędu planem kontroli lub na podstawie uzyskanych przez Prezesa informacji (art. 78 i 79 ust. 1 uodo),
f) prowadzenie postępowań w sprawie naruszenia przepisów o ochronie danych osobowych oraz nakładanie administracyjnych kar pieniężnych na podstawie art. 83 ust.2 RODO. Działania w ramach realizacji tego zadania zostały zabezpieczone szeregiem uprawnień dla Prezesa UODO, które mają pomóc w efektywnym podnoszeniu poziomu ochrony danych osobowych (rozdział 7 uodo),

g) zatwierdzanie kodeksów postępowań oraz akredytacja podmiotów monitorujących przestrzeganie zatwierdzonych kodeksów, zgodnie z art. 40 RODO (rozdział 5 UODO),

h) pełnienie roli organu doradczego i opiniotwórczego w zakresie podnoszenia standardów ochrony danych osobowych, m.in. przez wydawanie rekomendacji.

W kontekście kompetencji PUODO należy podkreślić, że Prezes Urzędu ma możliwość nakładania sankcji określonych zarówno w RODO, jak i w ustawach szczególnych – np. na podstawie art. 210a Prawa Telekomunikacyjnego, czy art. 8 ust.2 ustawy policyjnej.

RODO – wpływ na działalność branży ICT.

Nowa filozofia podejścia do ochrony danych osobowych w RODO

Nowy system ochrony danych osobowych ustanowiony w RODO i przepisach odwołujących się opiera się na dwóch podstawowych zasadach.

Po pierwsze, zasadzie rozliczalności (*accountability principle*). Zgodnie z nią, administrator danych powinien być w stanie wykazać, że stosowane przez niego metody są zgodne z RODO oraz skuteczne. W praktyce, zastosowanie się do zasady rozliczalności wymaga wdrożenia odpowiednich procedur i prowadzenia odpowiedniej dokumentacji, nawet jeśli obowiązek ich posiadania nie wynika bezpośrednio z przepisów RODO. Dzięki temu łatwiej będzie wykazać fakt spełniania przewidzianych Rozporządzeniem wymogów, co ma istotne znaczenie, gdyż to na administratorze danych spoczywa ciężar dowodu w tym zakresie, zgodnie bowiem z art. 5 ust.2 RODO *„Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie („rozliczalność")*.

Po drugie, zasadzie podejścia do ochrony danych opartego na ryzyku (*Risk Based Approach, RBA)*. Koncepcja ta zakłada, że im ryzyko związane z przetwarzaniem danych osobowych jest większe, tym większy powinien być zakres obowiązków ciążących na podmiocie przetwarzającym dane. Z takiego podejścia wynikają dwie ważne konsekwencje. Poszczególne zasoby danych wymagają różnego poziomu ochrony, a na podmiocie przetwarzającym dane spoczywa obowiązek dokonania doboru odpowiednich zabezpieczeń techniczno-organizacyjnych zapewniających zgodność z RODO, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia (art. 24 RODO). Istotną różnicę, w stosunku do poprzedniego stanu prawnego, stanowi również brak określenia *a priori* w Rozporządzeniu, jakiego rodzaju środki bezpieczeństwa powinny zostać zastosowane. Ich wymienienie w art. 32 RODO ma bowiem tylko charakter przykładowy i podmioty odpowiadające za dane powinny dokonać samooceny, czy i jakie środki stosować.

RODO – 10 najważniejszych skutków dla działalności przedsiębiorstw

Przepisy RODO istotnie zmieniły sposób funkcjonowania przedsiębiorstw i realizowanych przez nie procesów biznesowych. Dotyczy to również wykorzystywanych przez nie platform technologicznych oraz architektury danych poprzez które zbierane, przechowywane i zarządzane są dane osobowe.

Poniżej przedstawiona została lista 10 najważniejszych skutków obowiązywania RODO.

I) Po pierwsze, przedmiotowy zakres zastosowania przepisów RODO jest szerszy niż miało to miejsce w poprzednim stanie prawnym. Za dane osobowe uznane zostały bowiem wszystkie identyfikatory internetowe takie jak adresy IP, czy identyfikatory plików cookie (art. 4, motyw nr 30 RODO). To samo dotyczy innych

identyfikatorów, takich jak np. znaczniki (tagi) RFID. Ma to istotne znaczenie dla podmiotów działających w Internecie, czy wykorzystujących rozwiązania Internetu rzeczy (IoT). Rozporządzenie swoim zakresem objęło również istotną część relacji B2B, danymi osobowymi są bowiem także informacje o osobach fizycznych prowadzących działalność gospodarczą, samodzielnie lub w formie spółek osobowych (np. spółka cywilna).

II) Po drugie, terytorialny zakres obowiązywania RODO jest również szerszy niż poprzednio. Rozporządzenie znajduję bowiem zastosowanie do szeregu podmiotów nie mających swoich jednostek organizacyjnych w Unii Europejskiej (np. siedziby, oddziału czy przedstawicielstwa). Będzie tak w szczególności wówczas, gdy przetwarzanie dotyczyć będzie danych osobowych osób przebywających w Unii, a czynności przetwarzania wiązać się będą z oferowaniem towarów lub usług takim osobom lub monitorowaniem ich zachowania (art. 3 ust.2 RODO). Takie rozwiązanie jest wynikiem przyjętej w RODO koncepcji „długiego ramienia" ochrony na podstawie przepisów Rozporządzenia, obejmującego w pewnych sytuacjach również przetwarzanie dokonywane poza terytorium Unii Europejskiej.

III) Po trzecie, częściowo inne jest ujęcie przesłanek legalności przetwarzania danych osobowych. Chodzi w szczególności o nowe ujęcie podstawy prawnej przetwarzania danych polegającej na oparciu przetwarzania na przepisach prawa (art. 6 ust.1 pkt c) RODO), a także nowym ujęciu konstrukcji prawnej zgody i warunków jej wyrażania przez podmioty danych (art. 4 pkt 11, art. 6 ust.1 pkt a), art. 7-8 RODO). To samo dotyczy stosowania przesłanki uzasadnionego interesu (art. 6 ust.1 pkt f). Ze zmianami tymi funkcjonalnie powiązana jest modyfikacja obowiązków informacyjnych (art. 13-14 RODO).

IV) Po czwarte, w RODO wprowadzono szczególną regulację dotycząca jednej z operacji na danych tj. profilowania, rozumianego jako *„dowolna formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się."* (art. 4 pkt 4 RODO). W przypadku, gdy profilowanie odbywać się ma na potrzeby „zautomatyzowanych decyzji", a więc decyzji podejmowanych bez udziału człowieka, dopuszczalne jest ono tylko przy spełnieniu warunków określonych w art. 22 RODO, wprowadzających dodatkowe gwarancje zabezpieczenia interesów podmiotów danych poprzez możliwość zakwestionowania automatycznie wydanej decyzji i jej ponownego zweryfikowania przy udziale człowieka (art. 22 ust.3 RODO).

V) Po piąte, w RODO wprowadzono istotnie zmiany w zakresie korzystania ze zleceniobiorców procesów przetwarzania danych osobowych (podmiot przetwarzający na zlecenie administratora, *processor*). *Novum* są obowiązki administratora w zakresie wyboru takiego podmiotu przetwarzającego, który zapewnić ma wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi Rozporządzenia i chroniło prawa osób, których dane dotyczą (art. 28 ust.1 RODO). Istotnie rozbudowane zostały także obowiązkowe elementy treściowe umowy administratora danych z *processorem* (art. 28 ust. 3, ust. 7-9 RODO), a także zasady posługiwania się *podprocessorami* (art. 28 ust. 2 i ust. 4 RODO). Wszystkie te zmiany mają kluczowe znaczenie dla *outsourcingu* różnego rodzaju usług, w tym usług IT.

VI) Po szóste, w RODO istotnie zmodyfikowano dotychczasowe lub ustanowiono zupełnie nowe prawa podmiotów danych. Chodzi tu w szczególności o: prawo dostępu do danych, w tych ich kopii (art. 15 RODO), prawo do bycia zapomnianym (art. 17 RODO), prawo do ograniczonego przetwarzania (art. 18 RODO) oraz prawo do przenoszalności danych (art. 20 RODO). Zapewnienie realizacji tych praw ma istotny wpływ na rodzaj narzędzi IT, z których korzysta dana organizacja. Przykładowo, w przypadku prawa dostępu do danych, organizacje muszą w pierwszej zidentyfikować dane dotyczące konkretnej osoby fizycznej ze wszystkich dostępnych źródeł, takich jakich systemy CRM, HR, czy systemy archiwalne. Konieczna jest w związku implementacja holistycznych narzędzi wyszukiwawczych pozwalających na wyszukiwanie tych danych.

VII) Po siódme, z uwagi na przyjęcie w RODO podejścia opartego na zasadzie ryzyka (*Risk Based Approach*), istotnej zmianie uległy wymogi dotyczące środków bezpieczeństwa danych, które muszą stosować podmioty przetwarzające dane osobowe. W pierwszej kolejności wymienić należy wymóg uwzględnienia ochrony danych osobowych w fazie projektowania (*privacy by design*, art. 25 ust.1 RODO). Z jego realizacją związana może być między innymi analiza statyczna kodu programowania pod kątem ochrony danych. Podobny charakter ma zasada *privacy by default*, zgodnie z którą *„Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania*." (art. 25 ust.2 RODO). Do innych obowiązków z zakresu bezpieczeństwa danych należy zaliczyć obowiązek (art. 32 RODO). W Rozporządzeniu wprowadzono także obowiązek zapewnienia stopnia bezpieczeństwa odpowiadających ryzyku związanemu z zakresem i celem przetwarzania danych, z czym może się wiązać konieczność stosowania np. pseudonimizacji i szyfrowanie danych osobowych (art. 32 ust.1 pkt a RODO). W RODO nałożono również obowiązek dokonania, przed rozpoczęciem przewarzania danych osobowych, oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych, jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych (art. 35 RODO). Jeżeli ta ocena skutków wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby administrator nie zastosował środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania administrator ma obowiązek konsultacji z organem nadzorczym tj. PUODO (art. 36 RODO).

VIII) Po ósme, w RODO wprowadzono rozbudowaną regulację dotyczącą sposobu postępowania w przypadku naruszenia ochrony danych osobowych (art. 33-34 RODO). W zależności od stanu faktycznego, w pewnych sytuacjach aktualizuję się obowiązek powiadamiania organu nadzorczego (PUODO) i podmiotów danych osobowych, a także podjęcia działań zaradczych oraz dokumentowania wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych i jego skutków. Obowiązki te między innymi mają znaczenie w kontekście wdrażanych przez przedsiębiorców polityk (strategii) cyberbezpieczeństwa.

IX) Po dziewiąte, w RODO ustanowiono nowe instrumenty wykazywania zgodności z przepisami o ochronie danych osobowych (*compliance*). Zaliczyć do nich należy kodeksy postępowania oraz mechanizmy certyfikacji (art. 40 i n. RODO). Ich stosowanie istotnie może limitować ryzyka prawne związane z naruszeniem przepisów Rozporządzenia.

X) Po dziesiąte, w RODO przewidziano nowe sankcje administracyjne, w tym wysokie kary pieniężne za naruszenie przepisów o ochronie danych osobowych (art. 58 ust.2, art. 83 RODO). Niezależnie od tego, podmiot przetwarzający może ponosić również odpowiedzialność cywilną (art. 82 RODO).

Wpływ przepisów RODO na rozwój nowych technologii (AI, Blockchain, CC, IoT)

Przepisy o ochronie danych osobowych w istotny sposób wpływają również na rozwój najdynamiczniej rozwijających się innowacji w zakresie nowych technologii tj. sztucznej inteligencji (AI), *blockchain,* chmury obliczeniowej (CC) oraz Internetu rzeczy (IoT). Poniżej przedstawione zostaną najważniejsze problemy prawne związane ze stosowaniem przepisów RODO przy realizacji projektów tego rodzaju. Przed ich omówieniem warto podkreślić, że w prawie unijnym oraz polskim brak jest przepisów pozwalających na wyłączenie czy ograniczenie stosowania zasad ochrony danych osobowych w tych przypadkach, stosowanie tych innowacji nie może również prowadzić do ograniczenia praw przyznanych podmiotom danych na podstawie RODO.

Sztuczna inteligencja (AI)

Anonimizacja danych osobowych

Przetwarzanie informacji na potrzeby sztucznej inteligencji nie zawsze wiąże się z przetwarzaniem danych osobowych w rozumieniu art. 4 pkt 1 RODO. Wyróżnić należy w związku z tym dwie grupy sytuacji. Pierwszą stanowią informacje, które od samego początku są „anonimowe" (np. dane meteorologiczne). Bardziej problematyczna jest ocena drugiej grupy informacji, a więc sytuacji, gdy informacje mające pierwotnie charakter danych osobowych, utraciły następnie ten charakter z uwagi na dokonaną później ich anonimizację.

Dokonanie skutecznej anonimizacji danych często będzie kluczowe dla podmiotów tworzących sztuczną inteligencję, spełnienie wymogów RODO w przypadku danych wykorzystywanych na potrzeby algorytmów AI będzie bowiem często utrudnione. W motywie nr 26 RODO opisany został jedynie proces anonimizacji, bez odwołania się do poszczególnych technik (sposobów) jej dokonania. Podobnie, w Opinii nr 5/2014 Grupy Roboczej art. 29 w sprawie technik anonimizacji, wskazano na dwa podstawowe sposoby anonimizacji tj. randomizację oraz uogólnienie lub osłabienie atrybutów, bez wskazania jednak przykładów tego rodzaju technik. W tym zakresie podmioty tworzące sztuczną inteligencję muszą dokonać samoceny, pomocne w tym zakresie powinny być rekomendacje wydawane przez organy ds. ochrony danych osobowych w poszczególnych państwach Unii Europejskiej (na chwilę obecną w Polsce brak jest jednak takich wytycznych).

W uzupełnieniu powyższych uwag należy dodać, że środkiem prowadzącym do tego samego skutku co anonimizacja danych jest posługiwanie się danymi syntetycznymi, a więc danymi nieprawdziwymi, jednak stworzonymi w oparciu o te same zasady, co dane produkcyjne (np. z użyciem generatora danych).

Zgodność z wymogami RODO

W przypadku, gdy dokonanie anonimizacji danych jest niemożliwe i/lub utrudniałoby realizację celów przetwarzania tych informacji na potrzeby AI, konieczne jest zapewnienie zgodności procesu ich przetwarzania z przepisami RODO. Wiążą się z tym szczególne problemy prawne, których źródłem jest sposób wykorzystywania informacji przez sztuczną inteligencję. Zaliczyć do nich należy:

a) przetwarzanie wszystkich potencjalnie danych, co sprzeczne jest z zasadą minimalizacji danych (art. 5 ust.1 c) RODO),

b) zmiana celu przetwarzania danych, w stosunku do celu dla którego dane zostały zebrane, do której odnosi się zasada celowości (art. 5 ust.1 b RODO),

c) brak przejrzystości przetwarzania danych osobowych z punktu widzenia podmiotu danych, co z kolei stoi w kolizji z zasadą transparentności (art. 5 ust.1 a RODO).

Powyższe ryzyka prawne związane z przetwarzaniem danych na potrzeby AI mogą być limitowane przez stosowanie określonych środków zaradczych. W pierwszej kolejności należy wskazać na pseudonimizację danych, która polega na *przetworzenie danych osobowych w taki sposób, by nie można ich było* już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej" (art. 4 pkt 5 RODO). Pseudonimizację danych od ich anonimizacji różni potencjalna odwracalność procesu deidentyfikacji, z tych przyczyn dane spseudonimizowane objęte są reżimem RODO. Z drugiej strony, w przepisach Rozporządzenia wprowadzono pewne zachęty prawne do korzystania z danych osobowych w tej postaci. Po pierwsze, pseudonimizacja może ułatwić przyjęcie

dopuszczalności „wtórnego" przetwarzania danych mimo zmiany pierwotnego celu przetwarzania danych (art. 6 ust.4 e RODO). Po drugie, stosowanie pseudonimizacji jest w wielu przepisach RODO traktowane jako wykazanie spełnienia wymogu stosowania odpowiednich środków technicznych i organizacyjnych (art. art. 25, 32 RODO).

Złożoność procesu przetwarzania danych osobowych na potrzeby AI przekłada się często na ograniczony zakres informacji przekazywanych podmiotom danych. Zdarza się bowiem, że nie dysponują one informacjami na temat tego, że dane o nich są zbierane oraz jak są one następnie wykorzystywane. Dotyczy to również skutków automatycznych decyzji podejmowanych przez administratorów na podstawie tworzonych przez sztuczną inteligencję algorytmów (art. 22 RODO). Sama okoliczność wykorzystywania danych w tym celu niezwalania podmioty przetwarzające z powinności spełnienia obowiązków informacyjnych określonych w art. 13-14 RODO. Jedynie wyjątkowo będą one mogły powołać się na przesłankę wyłączającą, o której mowa w art. 14 ust.5 pkt b RODO („udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku").

W powyższym kontekście problemów związanych z zapewnieniem wymogu przejrzystości (transparentności) przetwarzania danych osobowych, szczególnego znaczenie nabiera odpowiednie dokonanie oceny skutków przetwarzania danych (art. 35 RODO), a więc oceny jak sztuczna inteligencja wpływa na prawa lub wolności pojedynczych osób czy grup społecznych. Chodzi między innymi o zapobieganie sytuacjom, gdy modele tworzone na podstawie AI prowadziłyby do tendencyjności, uprzedzeń (bias), czy dyskryminacji w traktowaniu osób fizycznych. Z tych przyczyn postuluję się, aby w przypadku tworzenia takich modeli zachowań uwzględniać nie tylko normatywną ochronę praw podstawowych, ale również szereg innych społecznych i etycznych wartości. Wprowadzony w RODO wymóg privacy by design nabiera więc ten sposób charakteru value-oriented design.

Blockchain

Spośród nowych, innowacyjnych technologii, *Blockchain* („łańcuch bloków") niewątpliwie stanowi największe wyzwanie z punktu widzenia zapewnienia zgodności z wymogami RODO. Jego istotą jest bowiem zdecentralizowany charakter, co szczególnie w przypadku tzw. *Blockchaina* publicznego, w którym każdy może wziąć bierny lub czynny udział w budowie tej sieci, utrudnia dokonanie rozliczalności przetwarzania danych i przypisanie roli administratora (współadministratora) danych. To samo dotyczy realizacji praw podmiotów danych. W sieciach zdecentralizowanych nie ma bowiem konkretnego podmiotu przechowującego dane i sprawującego kontrolę nad nim, w tym między innymi w zakresie ich usuwania (np. w ramach realizacji żądania prawa do bycia zapomnianym).

Nie podejmując się rozstrzygnięcia wyżej wskazanych wątpliwości wyrażamy jedynie nadzieję, że zostaną one jak najprędzej rozstrzygnięte przez organy ds. ochrony danych osobowych. Na chwilę obecną bowiem, z uwagi na wczesny wciąż etap rozwoju tej technologii, brak jest oficjalnych wyjaśnień regulatorów, w tym PUODO.

Chmura obliczeniowa

Identyfikacja zagrożeń związanych z przetwarzaniem chmury

Zagrożenia związane z przetwarzaniem danych osobowych w chmurze obliczeniowej można podzielić na dwie podstawowe grupy:

a) brak przejrzystości (transparentności) operacji przetwarzania danych, polegający m.in. na:
- braku informacji o „łańcuchu przetwarzania" w ramach chmury tj. wykonawcy oraz podwykonawcach usługi chmurowej,

- braku informacji o lokalizacjach geograficznych infrastruktury, w ramach której dochodzi do przetwarzania danych osobowych, w tym informacji o tym, czy dane osobowe są przetwarzane poza Europejskim Obszarem Gospodarczym (EOG).

b) brak kontroli nad danymi osobowymi, polegający m.in. na:

- ograniczeniu lub braku możliwości realizacji żądań podmiotu danych (np. w zakresie poprawiania danych),
- ryzyku naruszenia ciągłości działania w przypadku utraty danych,
- braku dostępności danych ze względu na brak interoperacyjności (uzależnienie od jednego dostawcy, *vendor lock-in*),
- brak poufności danych w przypadku realizacji żądań organów z terytorium, na którym przechowywane są dane.

Zgodność z wymogami RODO

W powyższym kontekście określić można listę najważniejszych wymogów prawnych na gruncie RODO, które powinny służyć eliminacji lub ograniczeniu powyższych ryzyk:

a) obowiązki nałożonych bezpośrednio na podmioty przetwarzające dane osobowe na zlecenie administratorów (art. 30, 32, 33 ust.2 RODO)
b) nowe zasady powierzenia i podpowierzenia danych osobowych przez administratorów (art. 28 RODO),
c) obowiązki wsparcia przez dostawcę chmury administratora danych (jako jej użytkownika) w zakresie realizacji zgłoszonych przez podmioty danych – żądań (art. 28 ust.3 e RODO),
d) wykonanie oceny skutków przetwarzania danych osobowych (art. 35 RODO),
e) oparcie transferu danych osobowych do państwa trzeciego na jednej z przesłanek określonych w Rozporządzeniu (art. 44 i n. RODO).

Obowiązki dostawcy chmury obliczeniowej (processor) na gruncie RODO

Do najważniejszych obowiązków podmiotów przetwarzających dane nałożonych przepisami RODO zaliczyć należy:

a) obowiązek prowadzenia rejestru czynności (art. 30 RODO),
b) obowiązki w zakresie bezpieczeństwa danych – m.in. szyfrowanie, pseudonimizacja, ciągłość działania (art. 32 RODO),
c) obowiązek powiadamiania administratora o stwierdzonym naruszeniu ochrony danych (art. 33 ust.2 RODO).

Nowe zasady powierzenia i podpowierzenia danych osobowych

Na gruncie w RODO niezmienione zostają, w stosunku do dotychczasowych przepisów, definicje i konstrukcje prawne administratora danych (art. 4 pkt 7 RODO) oraz processora (art. 4 pkt 8 RODO). W tym kontekście nie budzi wątpliwości, że użytkownika chmury obliczeniowej należy traktować jako administratora danych, a dostawcę chmury jako processora.

Wprowadzone w RODO zmiany w zakresie relacji administrator-*processor* dotyczą natomiast następujących obszarów:

a) wyboru odpowiedniego *processora* (art. 28 ust.1 RODO),
b) treści umowy powierzenia danych osobowych (art. 28 ust.3 RODO),
c) wyraźnego uregulowania podpowierzenia danych osobowych (art. 28 ust.2 i 4 RODO).

Z uwagi na nowy obowiązek z art. 28 ust.1 RODO, przed zawarciem umowy powierzenia przetwarzania administrator powinien dokonać oceny potencjalnego *processora* (dostawcy chmury) zgodnie z kryteriami określonymi w RODO, w szczególności jego motywem nr 81:

Obowiązkowe treści umowy powierzenia danych osobowych określone zostały z kolei w art. 28 ust.3 RODO. Z punktu widzenia projektów chmury obliczeniowej najistotniejsze z nich to:

a) zobowiązanie *processora*, aby biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomagał administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III (art. 28 ust.3 e),

b) zobowiązanie *processora*, aby po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usunął lub zwrócił mu wszelkie dane osobowe oraz usunął wszelkie ich istniejące kopie (art. 28 ust.3 g),

c) zobowiązanie *processora* do umożliwienia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzania audytów udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszym artykule oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich (art. 28 ust.3 h).

Z przetwarzaniem danych osobowych w chmurze obliczeniowej nierozerwalnie związane jest świadczenie usługi przez łańcuch podwykonawców. Istotne znaczenie ma w związku z tym regulacja art. 28 ust. 2 i 4 RODO, w której zawarto szczegółowe wymogi dotyczące podpowierzania przetwarzania danych. Zgodnie z nią processor nie może podpowierzyć przetwarzania bez uprzedniej zgody administratora, a w umowach podpowierzenia powinny być nałożone takie same obowiązki, jakie są nałożone na processora w umowie z administratorem. Mając na względzie specyfikę projektów chmurowych należy podkreślić, że pod warunkiem dochowania wymogu uprzedniej zgody administratora dopuszczalne jest, w trakcie świadczenia usługi chmury, korzystanie z nowych podwykonawców w trakcie trwania umowy (np. nowe centra danych).

Problematyka transferu danych osobowych do państwa trzeciego tj. poza Europejski Obszar Gospodarczy, szerzej została opisana w punkcie raportu omawiającym transfer danych osobowych. W tym miejscu warto jedynie podkreślić, że w mocy pozostały dotychczasowe decyzje Komisji Europejskiej dotyczące przekazywania danych (art. 45 ust.9). Ma to istotne znaczenie dla przetwarzania w chmurze obliczeniowej, w zdecydowanej większości przypadków transfery danych opierane są właśnie na tych klauzulach.

Internet rzeczy (IoT)

Dane osobowe w projektach IoT

Rozwiązania IoT mają coraz szersze zastosowanie – np. dane zbierane z urządzeń medycznych i umożliwiające zdalny monitoring pacjenta, inteligentne liczniki (smart meters), czy różnego rodzaju dane zbierane przez aplikacje inteligentnych domów. Większość z tych informacji, ma charakter danych osobowych w rozumieniu art. 4 pkt 1 RODO. Potwierdza to motyw nr 30 RODO, w którym jako przykład danych osobowych podano identyfikatory generowane przez znaczniki (tagi) RFID.

IoT i najważniejsze wymogi na gruncie RODO

Do najważniejszych wymogów RODO w kontekście Internetu rzeczy zaliczyć należy:

a) określenie podstawy prawnej przetwarzania danych osobowych (art. 6 RODO),
b) spełnienie wymogu *privacy by design* (art. 25 RODO),
c) dokonanie oceny skutków przetwarzania danych osobowych (art. 35 RODO),
d) określenie i przestrzeganie procedury naruszeń ochrony danych osobowych (art. 32 – 33 RODO).

W przypadku projektów IoT podstawą przetwarzania danych osobowych znajdująca najczęstsze zastosowanie jest:

a) zgoda podmiotu danych osobowych (art. 6 ust.1 pkt c RODO), lub
b) prawnie uzasadniony interes (art. 6 ust.1 pkt f RODO).

W przypadku przesłanki zgody, istotne jest przestrzeganie wymogu dobrowolności, określonego w art. 7 ust.4 RODO – „Oceniając, czy zgodę wyrażono dobrowolnie, w jak największym stopniu uwzględnia się, czy między innymi od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy." Jego stosowanie może mieć znaczenie szczególnie wówczas, gdy klauzula zgody ma stanowić dodatkowe postanowienie w umowach (np. w przypadku rozwiązań telematycznych w ubezpieczeniach, czy inteligentnych liczników w energetyce).

W sytuacji, gdy nie jest możliwe pozyskanie zgody, podstawą prawną może być prawnie uzasadniony interes administratora danych. W takim przypadku warto pamiętać o konieczności wykonania tzw. testu równowagi – z jednej strony prawnie uzasadnionych interesów realizowanych przez administratora, a z drugiej – podstawowych praw i wolności osoby, której dane są przetwarzane.

W przypadku projektów IoT, ze względu na sposób pozyskiwania danych, szczególnie aktualny jest wymóg uwzględnienia ochrony danych użytkowników już w fazie projektowania aplikacji do tego służącej (*privacy by design*). Konieczne będzie również wykonanie uprzedniej analizy skutków przetwarzania danych (art. 37 RODO). Warto przy tym podkreślić, że obowiązek wykonania tej analizy przy przetwarzaniu danych osobowych na potrzeby projektów IoT wyraźnie podkreślono w dokumencie Grupy Roboczej art. 29 (WP nr 248, str.10).

Z uwagi na fakt, że w przypadku Internetu rzeczy, dane osobowe są przeważnie generowane przez urządzenia będące w dyspozycji osób fizycznych (konsumentów), większe jest ryzyko ich naruszenia (np. *hacking*). Z tych przyczyn, szczególne znaczenie ma wprowadzenie i przestrzeganie procedury naruszeń ochrony.

RODO a przepisy sektorowe dotyczące usług łączności elektronicznej.

RODO i przepisy sektorowe – różny zakres ochrony

W przypadku RODO podstawowym prawem chronionym jego przepisami jest prawo do ochrony danych osobowych (art. 8 Karty Praw Podstawowych, KPP). Odmiennie przedmiot ochrony został ukształtowany w przepisach dotyczących ochrony praw i wolności w związku ze świadczeniem usług łączności elektronicznej (np. usługi telekomunikacyjne), dalej określanych jako „przepisy sektorowe".

Po pierwsze, ochrona dotyczy prawa do ochrony prywatności i komunikowania się (art. 7 KPP). Zgodnie z tym prawem, informacji przekazywanych między stronami i zewnętrznych elementów takiej komunikacji, w tym danych dotyczących czasu wysłania informacji, miejsca nadania i adresata, co do zasady nie ujawnia się żadnej innej osobie poza stronami zaangażowanymi w dany akt komunikacji. Przepisy chroniące poufność swoim zakresem obejmują zarówno dane pochodzące z łączności elektronicznej tj. treść komunikatów przesyłanych przez użytkowników końcowych (np. głos, tekst, obraz), jak i związane z nim metadane (np. data, godzina, czas trwania oraz rodzaju łączności), a także informacje przechowywane i dotyczące urządzeń końcowych użytkowników.

Po drugie, prawo do prywatności i poufności komunikowania chroni nie tylko – inaczej niż RODO – komunikację elektroniczną z udziałem osoby fizycznej, w którym to przypadku zazwyczaj będzie ona kwalifikowana jako dane osobowe, ale również informacje dotyczące osób prawnych (np. informacje o adresie IP abonenta-osoby prawnej).

Na poziomie unijnym, zasady ochrony prywatności i poufności w związku ze świadczeniem usług droga elektroniczną wprowadzono w dyrektywie 2002/58/WE (dyrektywa o prywatności i łączności elektronicznej), zmienionej częściowo dyrektywą 2009/136/WE. Przepisy te zostały transponowane do polskiego systemu prawnego w dwóch aktach prawnych – W przepisach prawa telekomunikacyjnego (art. 159 i n.), a także w ustawie o świadczeniu usług drogą elektroniczną (m.in. art. art. 6 pkt 2, 10, 18 oraz 19 ust.3 pkt).

Adresatami obowiązków określonych w powyższych przepisach są przede wszystkim dostawcy usług łączności elektronicznej (dostawcy publicznie dostępnych usług telekomunikacyjnych), a więc podmioty świadczące usługi polegające na polegającą głównie na przekazywaniu sygnałów w sieci telekomunikacyjnej. W dwóch grupach sytuacji, zakres podmiotowy regulacji sektorowych będzie szerszy, obejmując swoim zakresem również inne niż dostawcy usług łączności elektronicznej, podmioty. Po pierwsze, będzie tak w przypadku prowadzenia marketingu bezpośredniego za pomocą telekomunikacyjnych urządzeń końcowych (at.172 PT, art. 10 uśude). Po drugie w sytuacji instalowania różnego rodzaju oprogramowania czy danych w urządzeniach końcowych użytkowników (np. pliki cookies). Określone w art. 173 PT, czy art. 6 pkt 2 uśude obowiązki dotyczą bowiem wszystkich podmiotów instalujących tego rodzaju oprogramowania (dane), niezależnie od tego czy świadczą one usługi łączności elektronicznej.

Wzajemna relacja przepisów RODO oraz przepisów sektorowych dotyczących usług łączności elektronicznej

Przepisy sektorowe zaostrzają, w stosunku do RODO, przesłanki dopuszczalnego korzystania z informacji przetwarzanych w związku ze świadczeniem usług łączności elektronicznej, a mających charakter danych osobowych. Istotne znaczenie ma w związku z tym określenie wzajemnych relacji pomiędzy tymi aktami prawnymi oraz wskazanie, które z nich znajdują pierwszeństwo w przypadku wystąpienia kolizji zawartych w nich norm. Wyróżnić należy w związku z tym potencjalnie trzy grupy sytuacji.

Po pierwsze, przypadki, w których nie dochodzi do „kolizji" przepisów, ponieważ postanowienia RODO nie znajdują zastosowania. Będzie tak przykładowo w sytuacji przetwarzania danych o osobach prawnych.

Po drugie, przypadki, w których również nie ma potrzeby wskazywania pierwszeństwa regulacji, ponieważ przetwarzanie danych osobowych zebranych w związku ze świadczeniem usług łączności elektronicznej nie jest objęte przepisami sektorowymi (np. informacje zebrane w wewnętrznych (niepublicznych) sieciach korporacyjnych, do których nie znajdują zastosowania przepisy PT).

Po trzecie, przypadki, w których zastosowanie znajdują zarówno przepisy RODO, jak i przepisy sektorowe. Przykładem jest korzystanie z plików cookies. Z jednej strony, zawarte w nich informacje uznane zostały w RODO za dane osobowe (art. 4, preambuła nr 30), a z drugiej strony – podlegają one szczególnym zasadom przetwarzania określonym w przepisach sektorowych (art. 173 PT).

W kontekście trzeciej, spośród wyżej określonych, grup sytuacji należy stwierdzić, że przepisy sektorowe mają charakter lex specialis względem przepisów RODO jako norm legi generali. W zakresie więc, w jakim przepisy sektorowe będą ograniczać – względem RODO – możliwości przetwarzania danych pochodzących z łączności elektronicznej, będą one „względniejsze". Sytuacja taka może mieć miejsce w szczególności w przypadku ograniczenia – w stosunku do RODO – możliwości posługiwania się poszczególnymi podstawami prawnymi przetwarzania danych. Przykładowo, na gruncie PT brak jest możliwości oparcia się na przesłance prawnie uzasadnionego interesu w sytuacji korzystania z cookies, podmiot korzystający z ciasteczek musi bowiem pozyskać zgodę abonenta lub użytkownika na tego rodzaju działania. Z drugiej strony, charakter RODO jako lex generali w stosunku do PT, przesądza o stosowaniu przepisów Rozporządzenia w zakresie, w którym przepisy sektorowe nie regulują danego rodzaju obowiązków (np. w zakresie realizacji praw podmiotów danych).

Ustawa dostosowująca do RODO – zmiany w uśude i PT

Ustawa o zmianie niektórych ustaw w związku z zapewnieniem stosowania RODO zawiera nowelizacje ponad 160 ustaw. W przypadku sektora ICT najważniejsze zmiany wprowadzono w ustawie o świadczeniu usług drogą elektroniczną („uśude") oraz ustawie-Prawo Telekomunikacyjne (odpowiednio art. 63 oraz art. 79 ustawy dostosowującej).

Zmiany w uśude

Zmiany wprowadzone w ustawie o świadczeniu usług drogą elektroniczną w pierwszej kolejności potwierdzają zasadę, że zgoda usługobiorcy powinna być pozyskiwana na takich zasadach, jak to określono w przepisach o ochronie danych osobowych tj. RODO (art. 4 uśude). Odwołanie to oznacza, iż dla skutecznego pozyskania zgody na przetwarzanie danych osobowych w związku ze świadczeniem usług drogą elektroniczną konieczne jest w szczególności spełnienie warunków określonych w art. 4 ust. 11, art. 7 oraz art. 8 RODO.

Istotnej zmianie uległ dotychczasowy rozdział IV uśude pt. „Zasady ochrony danych osobowych w związku ze świadczeniem usług drogą elektroniczną" (art. 16-22). Z uwagi na bezpośrednie stosowanie RODO uchylono bowiem większość zawartych w nim przepisów tj. art. 16-17, 19 ust.1-2 i 4-5 oraz art. 20-22 uśude. Legalność przetwarzania danych osobowych w sytuacjach opisanych w tych przepisach, oceniana jest więc obecnie na podstawie właściwych przepisów RODO.

W treści rozdziału IV pozostawiono natomiast dwie kategorie przepisów: a) implementujące dyrektywę 2002/58/WE dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej oraz b) regulacje nienaruszające RODO i nieobjęte jego treścią.

Do pierwszej grupy przepisów zaliczyć należy art. 18 ust.4 uśude, który po jego nowelizacji brzmi następująco: *„Usługodawca może przetwarzać, za zgodą usługobiorcy i dla celów reklamy, badania rynku oraz zachowań i preferencji usługobiorców z przeznaczeniem wyników tych badań na potrzeby polepszenia jakości usług świadczonych przez usługodawcę, inne dane dotyczące usługobiorcy, które nie są niezbędne do świadczenia usługi drogą elektroniczną."* Znowelizowana treść tego przepisu budzi istotne kontrowersje interpretacyjne. Zgodnie bowiem z jego literalną treścią, usługodawcy zobowiązani są do pozyskiwania zgody użytkownika (usługobiorcy) na przetwarzanie jego danych osobowych, innych niż niezbędne do świadczenia usług drogą elektroniczną, (np. informacje o odwiedzanych przez nich stronach internetowych). Dotyczy to między innymi sytuacji, gdy dochodzi do przetwarzania tych danych w celach marketingowych czy analitycznych. Stanowi to istotną zmianę w stosunku do dotychczasowego stanu prawnego, w którym obowiązek pozyskania takiej zgody aktualizował się dopiero po „zakończeniu korzystania z usługi świadczonej drogą elektroniczną", a nie w trakcie jej świadczenia (uchylony art. 19 ust.2 uśude).

Do drugiej grupy przepisów pozostawionych w rozdziale IV uśude przepisów zaliczyć należy art. 18 ust.6 uśude, nakładający na usługodawców obowiązek nieodpłatnego udostępniania danych organom państwa, uprawnionym na podstawie odrębnych przepisów, na potrzeby prowadzonych przez nie postępowań oraz art. 19 ust.3 uśude, zgodnie z którym *„Rozliczenie usługi świadczonej drogą elektroniczną przedstawione usługobiorcy nie może ujawniać rodzaju, czasu trwania, częstotliwości i innych parametrów technicznych poszczególnych usług, z których skorzystał usługobiorca, chyba że zażądał on szczegółowych informacji w tym zakresie"*.

Zmiany w PT

Najważniejsze zmiany wprowadzone ustawą dostosowującą w Prawie Telekomunikacyjnym („PT") dotyczą przepisów o: a) podstawie prawnej przetwarzania danych osobowych użytkowników (w tym abonentów) będących osobami fizycznymi (art. 161 ust.2), b) zgodzie abonenta lub użytkownika (art. 174), c) obowiązku stosowania dodatkowych środkach bezpieczeństwa (art. art. 1741) oraz d) obowiązku zgłaszania naruszeń (art. 174a-174 d).

Zmiana wprowadzona w art. 161 ust.2 PT ma na celu jasne rozgraniczenie, kiedy w przypadku przetwarzania danych osobowych użytkownika właściwe są przepisy Prawa Telekomunikacyjnego dotyczące przetwarzania informacji objętych tajemnicą telekomunikacyjną, a kiedy przepisy o ochronie danych osobowych (RODO). Zgodnie z przyjętym rozwiązaniem, objęte regulacją ustawy prawo telekomunikacyjne pozostaje przetwarzanie danych wskazanych w art. 159 ust. 1 lit. 2–5 PT (informacje chronione tajemnicą telekomunikacyjną), także w zakresie w jakim dotyczą one osób fizycznych i mogą być kwalifikowane jako dane osobowe w rozumieniu przepisów RODO. Przetwarzanie danych osobowych użytkownika (osoby fizycznej) – innych niż wskazane w art. 159 ust. 1 pkt 2-5 PT – odbywa się natomiast na podstawie przepisów o ochronie danych osobowych. W trakcie prac nad nowelizacją PT, zrezygnowano ostatecznie ze skreślenia przepisu art. 161 ust.3 PT, którego treść brzmi następująco: *„Oprócz danych, o których mowa w ust. 2, dostawca publicznie dostępnych usług telekomunikacyjnych może, za zgodą użytkownika będącego osobą fizyczną, przetwarzać inne dane tego użytkownika w związku ze świadczoną usługą, w szczególności numer konta bankowego lub karty płatniczej, a także numery telefonów kontaktowych."* Rodzi to istotne kontrowersje interpretacyjne, ponieważ po nowelizacji art. 161 ust.2 PT, w przepisie tym brak jest wymienienia kategorii danych, do których odwołano się w art. 161 ust.3 PT. W ten sposób, zakres danych, które miałyby być przetwarzane na podstawie zgody jest niemożliwy do ustalenia – ust. 3 obejmuje bowiem dane inne niż określone w ust. 2, tymczasem zmieniony ust. 2 nie zawiera już zamkniętego katalogu danych. Stanowi to istotne utrudnienie prowadzenia działalności przez podmioty, do których stosują się przepisy PT.

W znowelizowanym PT przyjęto również, podobnie jak w uśude, zasadę, że zgoda abonenta lub użytkownika końcowego powinna być pozyskana na takich zasadach, jak to określono w przepisach o ochronie danych osobowych tj. RODO (art. 174 PT). Co istotne, wymóg ten odnosi się nie tylko do abonenta lub użytkownika końcowego

będącego osobą fizyczną, ale również osobą prawną. Jest to konsekwencją szerszego zakresu przedmiotowego stosowania Prawa Telekomunikacyjnego, którego ochrona obejmuję – inaczej niż przepisy RODO – również ochronę interesów osób prawnych.

W zmienionym PT wprowadzono także regulację, zgodnie z którą dostawcy publicznie dostępnych usług telekomunikacyjnych obowiązani są wdrożyć dodatkowe, w stosunku do wymogów RODO, techniczne i organizacyjne środki ochrony zapewniające bezpieczeństwo przetwarzania danych osobowych (art. 1741 PT). Przyjęte przez nich środki ochrony powinny co najmniej:

a) zapewnić, aby dostęp do danych osobowych miała osoba posiadająca pisemne upoważnienie wydane przez administratora danych oraz
b) chronić przechowywane lub przekazywane dane osobowe przed przypadkowym lub bezprawnym zniszczeniem, przypadkową utratą lub zmianą oraz nieuprawnionym lub bezprawnym przechowywaniem, przetwarzaniem, dostępem lub ujawnieniem, oraz
c) zapewnić wdrożenie polityki bezpieczeństwa w odniesieniu do przetwarzania danych osobowych.

W dotychczasowym stanie prawnym tj. przed rozpoczęciem obowiązywania RODO, na dostawców publicznie dostępnych usług telekomunikacyjnych nałożone już były określone obowiązki dotyczące postępowania w przypadku naruszenia ochrony danych (art. 174a–174d PT). Było to konsekwencją implementacji art. 2 lit. i oraz art. 4 dyrektywy 2002/58/WE dotyczących bezpieczeństwa przetwarzania danych. Przepisy dyrektywy zostały następnie uzupełnione i uszczegółowione w rozporządzeniu 611/2013 z dnia 24 czerwca 2013 r. w sprawie środków mających zastosowanie przy powiadamianiu o przypadkach naruszenia danych osobowych. Obowiązki te w części zbieżne były z wprowadzonymi w RODO w tego rodzaju sytuacjach (art. 33-34 RODO). Z tych względów w znowelizowanym PT dokonano odpowiednich zmian w art. 174a–174d PT, w szczególności uchylając lub odpowiednio przeredagowując te przepisy ustawy – PT, które powtarzają przepisy Rozporządzenia lub są z nimi niezgodne i jednocześnie nie stanowią implementacji dyrektywy 2002/58/WE.

Konsekwencją wprowadzenia w nowelizacji PT nowych obowiązków w zakresie bezpieczeństwa przetwarzania danych osobowych jest przyjęcie art. 210a PT, regulującego kwestię kar pieniężnych nakładanych przez Prezesa Urzędu Ochrony Danych Osobowych na podmiot, który nie wypełnia obowiązków dotyczących bezpieczeństwa przetwarzania danych osobowych określonych w ustawie – PT. Dotyczy to w szczególności obowiązku:

a) wdrożenia technicznych i organizacyjnych środków ochrony, o których mowa w art. 174,
b) informacyjnego, względem Prezesa Urzędu Ochrony Danych Osobowych, o którym mowa w art. 174a ust. 1,
c) informacyjnego, względem abonenta lub użytkownika końcowego, o którym mowa w art. 174a ust. 3,
d) prowadzenia rejestru naruszeń danych osobowych, o którym mowa w art. 174d ust. 1

Niewykonanie wyżej wymienionych obowiązków daje możliwość nałożenia przez Prezesa Urzędu Ochrony Danych Osobowych w wysokości do 3% przychodu ukaranego podmiotu osiągniętego w poprzednim roku kalendarzowym.

W podsumowaniu powyższych uwag dotyczących sektorowych przepisów zawartych w uśude oraz PT należy podkreślić, że będą one uchylone po wejściu w życie Rozporządzenia o e-Prywatności, nad którym prace legislacyjne nadal trwają.

Projekt Rozporządzenia o e-Prywatności

Cel uchwalenie Rozporządzenia o e-Prywatności

Podstawowym celem strategii jednolitego rynku cyfrowego jest zwiększenie zaufania względem usług cyfrowych i poprawa ich bezpieczeństwa. Służyć temu ma reforma ram ochrony danych, a w szczególności przyjęcie RODO. W ramach tej strategii ogłoszono również przegląd dyrektywy 2002/58/WE, mający na celu zapewnienie wysokiego poziomu ochrony prywatności użytkowników usług łączności elektronicznej. Jego dokonanie było niezbędne z uwagi na konieczność zapewnienia spójności przepisów o prywatności i łączności elektronicznej z nowymi zasadami określonymi w RODO, a także ze względu na potrzebę uwzględnienia istotnych zmian technologicznych i gospodarczych (m.in. nowe modele usług łączności elektronicznej), które nastąpiły od ostatniego przeglądu dyrektywy, mającego miejsce w 2009 r. Wynikiem tego przeglądu było opracowanie przez Komisję Europejską projektu rozporządzenia w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylenia dyrektywy 2002/58/WE. Projekt Rozporządzenia o e-Prywatności został opublikowany przez Komisję Europejską w dniu 10 stycznia 2017 r. („projekt Rozporządzenia o e-Prywatności", „Projekt"). Od tego czasu w Parlamencie Europejskim oraz w Radzie Unii Europejskiej opracowywane są propozycje zmian do projektu, nad którym prace nadal się toczą. W przypadku uchwalenia Rozporządzenia o e-Prywatności zastąpi ono przepisy polskich ustaw, na których wzorowana była dyrektywa 2002/58/WE, a zawarte w Prawie Telekomunikacyjnym oraz ustawie o świadczeniu usług drogą elektroniczną,

Projekt Rozporządzenia o e-Prywatności – najważniejsze postanowienia

Poszerzenie zakresu przedmiotowego stosowania – usługi interpersonalne (OTT)

Jedną z kluczowych zmian w projekcie Rozporządzenia o e-Prywatności, w stosunku do regulacji dyrektywy 2002/58/WE, jest poszerzenie zakresu przedmiotowego jego stosowania. W ślad za definicją usług łączności interpersonalnej w dyrektywie 2018/1972 z dnia 11 grudnia 2018 r., ustanawiającej Europejski Kodeks Łączności Elektronicznej, regulacją rozporządzenia objęto nie tylko usługi dostępu do Internetu, czy usługi polegające w całości lub częściowo na przekazywaniu sygnałów, lecz również tzw. usługi łączności interpersonalnej (*over-the-top, OTT*), takie jak telefonia internetowa (*Voice over IP, VoIP*), różnego rodzaju aplikacje służące jako komunikatory internetowe (*instant messaging apps*), a także usługi poczty elektronicznej w Internecie (webmail). Podstawowym założeniem dla dokonania takiego rozszerzenia jest uznanie, że usługi OTT stanowią funkcjonalne odpowiedniki „tradycyjnych" usług łączności (np. telefonia, SMS/MMS), a więc również spełniają funkcję komunikacyjną i dlatego powinny być objęte projektem Rozporządzenia o e-Prywatności i ustanowionych w nim zasad poufności danych. W tym kontekście zwraca się również uwagę, że zarówno usługi tradycyjne, jak i OTT realizowane są często przy użyciu tego samego urządzenia końcowego (smartphone). Poszerzenie zakresu przedmiotowego Rozporządzenia o e-Prywatności w praktyce oznacza objęcie jego stosowaniem takich usług jak np. WhatsApp, Facebook Messenger, Gmail, czy Skype.

O ile stosowanie przepisów projektu do powyższych usług łączności interpersonalnej, określanych nieraz jako „OTT1", nie budzi kontrowersji, to na obecnym etapie prac nad Rozporządzeniem o e-Prywatności nie do końca jasny jest status usług „OTT2". Chodzi w szczególności o pozwalające na komunikację użytkowników funkcjonalności, zintegrowane z innymi usługami (np. funkcjonalności komunikatorów w aplikacjach „randkowych" czy służących do gier online). To, co je różni od powyżej opisanych usług „OTT1", jest ich pomocniczy (*ancillary*) charakter.

Bez wątpienia w dalszych pracach nad projektem konieczne będzie ostateczne przesądzenie przez prawodawcę, czy i te usługi objęte będą zakresem stosowania Rozporządzenia o e-Prywatności.

Poszerzenie zakresu terytorialnego stosowania

Zmianie ulegnie również sposób określenia zakresu terytorialnego przepisów sektorowych. Celem proponowanej zmiany jest uniknięcie, podobnie jak w art. 3 ust.2 RODO, pozbawienia użytkowników końcowych w Unii Europejskiej skutecznej ochrony. W konsekwencji, w art. 3 ust. 1 projektu Rozporządzenia o e-Prywatności przyjęto rozwiązanie, zgodnie z którym po pierwsze jego przepisy powinny mieć zastosowanie do danych pochodzących z łączności elektronicznej przetwarzanych w związku z zapewnieniem i zastosowaniem usług łączności elektronicznej w Unii, niezależnie od tego, czy przetwarzanie odbywa się na terytorium Unii, a po drugie, że przepisy te powinny stosować się do danych pochodzących z łączności elektronicznej przetwarzanych w związku ze świadczeniem użytkownikom końcowym w Unii usług łączności elektronicznej pochodzących spoza Unii.

Komunikacja M2M oraz Internet rzeczy

W kontekście poszerzenia zakresu obowiązywania Rozporządzenia o e-Prywatności planuję się, że obejmie ono również komunikację związaną z tzw. Internetem Rzeczy (*IoT*). Jak bowiem podkreślono w motywie nr 12 projektu, *„w celu zapewnienia pełnej ochrony prawa do prywatności i poufności komunikacji oraz w celu propagowania zaufanego i bezpiecznego Internetu rzeczy na jednolitym rynku cyfrowym konieczne jest doprecyzowanie, że rozporządzenie powinno mieć zastosowanie do przesyłu komunikatów w trybie maszyna-maszyna"*. Chodzi w szczególności o objęcie zasadą poufności ustanowioną w projekcie Rozporządzeniu o e-Prywatności przesyłów komunikatów w takim zakresie, w jakim tzw. inteligentne urządzenia dostarczają informacje o osobach fizycznych. W praktyce oznaczać to będzie stosowanie się nowych przepisów do np. danych gromadzonych przez różnego rodzaju sensory (czujniki), wbudowane w *smart* urządzenia.

Zmiana przepisów dotyczących plików cookies i innych technik umożliwiających śledzenie urządzeń końcowych użytkowników

W projekcie utrzymano dotychczas obowiązująca zasadę, że urządzenie końcowe użytkowników końcowych sieci łączności elektronicznej oraz wszelkie informacje związane z korzystaniem z takiego urządzenia końcowego stanowią część ich prywatnej sfery. Jak podkreślono, takie urządzenia zawierają lub przetwarzają informacje, które mogą ujawnić szczegóły dotyczące emocji, poglądów politycznych i sytuacji społecznej osoby fizycznej, w tym treść łączności, zdjęcia, lokalizację osób przez dostęp do funkcji GPS urządzenia, listę kontaktów i inne informacje już przechowywane w urządzeniu, informacje związane z takim sprzętem (urządzeniem) wymagają zwiększonej ochrony prywatności (motyw nr 20). Jest to tym bardziej istotne, że dostęp do informacji zgromadzonych w urządzeniach końcowych użytkownika uzyskiwany jest nieraz bez jego zgody, m.in. w celu śledzenia jego aktywności w Internecie czy lokalizacji jego urządzenia końcowego. Służą temu m.in. takie narzędzia jak oprogramowanie szpiegujące, ukryte identyfikatory czy trwałe pliki *cookie*. Co więcej, informacje dotyczące urządzenia użytkownika końcowego mogą być również gromadzone zdalnie w celu identyfikacji i śledzenia z zastosowaniem technik takich jak pobieranie odbitek linii papilarnych przez urządzenie (*device fingerprinting*).

Z powyższych względów w projekcie Rozporządzenia o e-Prywatności przyjęto zasadę, że powyższe działania polegające na ingerencji w urządzenie użytkownika końcowego wymagają jego zgody, wyrażonej w konkretnych i przejrzystych celach (art. 8 ust.1 pkt b). Jedynie wyjątkowo można ich dokonać bez zezwolenia zainteresowanego. Będzie tak m.in. w przypadku tych plików *cookie,* które nie stanowią zagrożenia dla prywatności i ułatwiają użytkownikowi korzystanie ze strony (np. takie, które zapamiętują zawartość koszyka, wybór języka czy ułatwiają

wypełnianie formularzy online na kilku stronach). Zgoda użytkownika nie będzie również potrzebna w przypadku wykorzystywania plików *cookie* w celach analitycznych, np. w celu liczenia wejść użytkowników na daną stronę internetową. Należy w związku z tym zauważyć, że przyjęcie takiego rozwiązania poszerza, w stosunku do dotychczasowego stanu prawnego, możliwości korzystania z *cookie* bez zgody użytkowników końcowych.

Abstrahując od powyższych wyjątków, w zdecydowanej jednak większości przypadków ingerencja w urządzenia końcowe użytkownika dokonywana przez inne osoby będzie wymagała zgody dysponenta tego urządzenia. Do zgody takiej stosować się będą wymogi RODO, w szczególności zawarte w art. 4 ust. 11 i art. 7.

Nowe regulacje dotyczące gromadzenia informacji wysyłanych przez urządzenia końcowe w celu umożliwienia podłączenia ich do innego urządzenia lub sprzętu sieciowego

Od wyżej określonych działań polegających na ochronie informacji przechowywanych w urządzeniu końcowym, odróżnić należy nową regulację zapewniającą ochronę przed przetwarzaniem informacji dotyczących urządzenia końcowego użytkownika (art. 8 ust. 2). Chodzi tu w szczególności o ochronę użytkowników przed procederem określanym jako „śledzenie urządzeń" (*device tracking*). Jak się bowiem zauważa, dostęp do sieci łączności elektronicznej wymaga regularnego wysyłania pewnych pakietów danych w celu odnalezienia lub utrzymania połączenia z siecią lub innymi urządzeniami w obrębie sieci (motyw nr 25). Ponadto, aby urządzenia mogły być rozpoznawane w tej sieci, muszą mieć przypisany niepowtarzalny adres. Standardy rozwiązań bezprzewodowych i telefonii komórkowej podobnie wiążą się z wysyłaniem aktywnych sygnałów zawierających niepowtarzalne identyfikatory, takie jak adres MAC, numer IMEI (międzynarodowy numer fabryczny mobilnego aparatu telefonicznego), IMSI itp. Pojedyncza bezprzewodowa stacja bazowa (tj. nadajnik i odbiornik), taka jak punkt dostępu bezprzewodowego, ma określony zasięg, w jakim można przechwycić takie informacje. W związku z tym, pojawili się dostawcy usług internetowych, którzy oferują usługi śledzenia w oparciu o skanowanie informacji związanych z urządzeniem, które to usługi obejmują różne funkcje, w tym liczenie osób, udostępnianie danych o osobach czekających w kolejce, potwierdzenie liczby osób na konkretnym obszarze itp. Te informacje można wykorzystywać m.in. w celach takich jak wysyłanie informacji handlowych ze spersonalizowanymi ofertami do użytkowników końcowych, np. gdy wchodzą oni do sklepów. Chociaż część tych funkcji nie wiąże się z dużym zagrożeniem dla prywatności, inne mogą wiązać się ze śledzeniem osób przez dłuży czas, w tym ze śledzeniem ponownych wizyt w określonych miejscach. W związku z powyższym, w projekcie wprowadzono rozwiązanie, zgodnie z którym dostawcy usług zaangażowani w takie praktyki powinni wyświetlać widoczne zawiadomienia zamieszczone na granicy obszaru zasięgu, informujące użytkowników końcowych przed wejściem na taki określony obszar, że w danym okręgu funkcjonuje dana technologia, a także wskazujące cel śledzenia, osobę za nie odpowiedzialną oraz istnienie środków umożliwiających użytkownikowi końcowemu urządzenia końcowego ograniczenie lub wstrzymanie gromadzenia danych (art. 8 ust. 2 b). Dodatkowo, gromadzenie takich informacji ma być uzależnione od zastosowania właściwych środków technicznych i organizacyjnych, aby zapewnić poziom bezpieczeństwa właściwy dla ryzyka, jak określono to w art. 32 RODO.

Ochrona przed spamem

Projekt Rozporządzenia o e-Prywatności podtrzymuje dotychczasową zasadę uzyskania uprzedniej zgody użytkownika na prowadzenie działań marketingowych (*opt-in*), bez względu na wykorzystywany w tym celu kanał komunikacyjny (art. 16 ust. 1 projektu).

Zgodnie z art. 16 ust. 2 projektu, dane kontaktowe dotyczące poczty elektronicznej otrzymane przy wysyłaniu materiałów do klienta w związku ze sprzedażą produktu lub usługi, będą mogły zostać wykorzystane do celów

marketingu bezpośredniego własnych podobnych produktów lub usług, pod warunkiem jednak, że klienci będą mieli jasną i wyraźną możliwość wyrażenia – bezpłatnie i w łatwy sposób – sprzeciwu wobec takiego wykorzystania danych (*opt-out*).

Znaczącą zmianą będzie zobowiązanie podmiotów korzystających z telemarketingu do używania możliwego do zidentyfikowania numeru lub stosowania specjalnego prefiksu wskazujący na to, że dana rozmowa ma charakter marketingowy, a także do podawania identyfikatora linii, pod którą można się z nimi skontaktować (art. 16 ust. 3). Niezależnie od tego, państwa członkowskie same będą mogły zastosować rozwiązania oferujące użytkownikom możliwość zastrzeżenia, że nie życzą sobie odbierać połączeń od telemarketerów i wprowadzić np. specjalne publicznie dostępne rejestry pozwalające na zarejestrowanie swojego numeru telefonu jako nieprzyjmującego połączeń marketingowych (art. 16 ust. 4).

Wprowadzenie bardziej dotkliwych kar za naruszenia oraz organ nadzorczy

Podobnie jak RODO, projekt Rozporządzenia o e-Prywatności przewiduje administracyjne kary pieniężne za nieprzestrzeganie jego przepisów. W przypadku naruszenia zasady poufności komunikacji, dozwolonego przetwarzania danych pochodzących z łączności elektronicznej, terminów na usunięcie danych, organ nadzorczy będzie mógł nałożyć kary pieniężne w wysokości do 20 000 000 euro, a w przypadku przedsiębiorstwa – w wysokości do 4% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego (art. 23 ust. 3). W razie naruszenia pozostałych przepisów rozporządzenia organ nadzorczy będzie mógł z kolei nałożyć administracyjną karę pieniężną w wysokości do 10 000 000 euro, a w przypadku przedsiębiorstwa do 2% całkowitego rocznego światowego dochodu z poprzedniego roku obrotowego (art. 23 ust. 2).

Ponadto, każdy użytkownik końcowy będzie mógł skorzystać z środków zaradczych przewidzianych w art. 77, 78 i 79 RODO (prawo do wniesienia skargi do organu nadzorczego, prawo do skutecznego środka ochrony prawnej przed sądem przeciwko organowi nadzorczemu oraz przeciwko podmiotowi dopuszczającemu się naruszeń), a także będzie miał prawo do rekompensat za szkodę materialną i niematerialną poniesioną z tytułu naruszenia, zgodnie z art. 82 RODO. Prawo do wytoczenia powództwa w związku z takimi naruszeniami będzie przysługiwało również podmiotom innym niż użytkownicy końcowi, na które naruszenie miało negatywny wpływ i które mają uzasadniony interes w ustaniu lub zakazaniu naruszeń (art. 21 ust. 1).

Realizacja praw podmiotów danych pod kątem RODO

Autorzy: Bartosz Marcinkowski, Robert Brodzik, Domański Zakrzewski Palinka

Zagadnienie realizacji swych praw przez podmioty danych stanowi centralny punkt regulacji RODO. Należy wszak podkreślić, iż prawo ochrony danych osobowych w pierwszym rzędzie służy zagwarantowaniu ochrony praw i wolności jednostki.

Zatem nie tylko sama regulacja w zakresie ochrony danych osobowych, ale także sposób zapewniający jednostkom (w tym w ujęciu konsumenckim) możliwość skorzystania z uprawnień przyznanych przepisami mają zasadnicze znaczenie dla oceny przyjętych rozwiązań i stopnia a zwłaszcza sposobu wdrożenia RODO w firmie. Co więcej, szereg dylematów praktycznych związanych ze stosowaniem RODO i ustaw towarzyszących można rozstrzygnąć stosując test zapewnienia praw i wolności jednostki.

Powyższe uwagi zasługują na zaakcentowanie, gdyż oddają istotę omawianej regulacji, która nie jest regulacją mającą służyć usprawnieniu prowadzenia działalności gospodarczej, lecz służy wzmocnieniu ochrony praw jednostki.

> **Stąd można spodziewać się, iż w szeregu wypadków rozstrzygnięcia organów ochrony danych osobowych (tak w Polsce, jak i w innych krajach Unii Europejskiej) oraz sądów będą miały charakter proobywatelski i prokonsumencki, co zresztą łączy się z opisywaną w literaturze przedmiotu rzecznikowską funkcją organu ochrony danych.**

W związku z tym metoda realizacji praw podmiotu danych ze wskazanych przyczyn może podlegać szczegółowej analizie i ocenie organów nadzorczych.

Prawa podmiotów danych według RODO

Każda osoba fizyczna uzyskała na gruncie RODO szereg praw. Wśród nich można wyróżnić następujące prawa:

> ***a)*** **do informacji i przejrzystej komunikacji**
> ***b)*** **dostępu do danych osobowych**
> ***c)*** **do sprostowania nieprawidłowych danych**
> ***d)*** **do usunięcia danych *(„prawo do bycia zapomnianym")***
> ***e)*** **do ograniczenia przetwarzania**
> ***f)*** **do przenoszenia danych**
> ***g)*** **do wniesienia sprzeciwu wobec przetwarzania danych**
> ***h)*** **do niepodlegania zautomatyzowanemu podejmowaniu decyzji (prawo do interwencji ludzkiej).**

Część z powyższych to nowe uprawnienia, wprowadzonymi przepisami RODO (np. wywodzące się z dorobku orzeczniczego prawo do bycia zapomnianym czy prawo do przenoszenia danych[1]). Część z kolei, jak na przykład prawo dostępu lub prawo do sprzeciwu, została w nowej regulacji rozszerzona i wzmocniona.

1 Zob. wyrok Trybunału Sprawiedliwości UE z 13 maja 2014 roku – https://eur-lex.europa.eu/legal-content/pl/TXT/PDF/?uri=uriserv%3AOJ.C_.2014.212.01.0004.01.POL

W kontekście realizacji praw, Motyw 59 RODO uzasadnia przyjęcie przez administratorów i processorów procedur dotyczących realizacji praw podmiotów mających za cel ułatwienie ich realizacji.

> **„Należy przewidzieć procedury ułatwiające osobie, której dane doyczą, wykonywanie praw przysługujących jej na mocy niniejszego rozporządzenia, w tym mechanizmy żądania (…)"**

Administrator jest również zobowiązany podjąć odpowiednie kroki, żeby prowadzić komunikację z osobą, której dane dotyczą w związku z realizacją praw. Komunikacja ta musi być w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, wyrażona jasnym i prostym językiem.

Zestawiając powyższe z naczelnymi zasadami RODO – przede wszystkim z zasadami zgodności z prawem, rzetelności i przejrzystości – procedury zdają się naturalnym elementem korporacyjnego systemu ochrony danych osobowych. Konieczność dysponowania procedurami tego rodzaju nie jest wymogiem prawa wyrażonym wprost w przepisach, jednak ich wdrożenie w organizacji może stanowić efektywny środek umożliwiający nie tylko wykazanie zgodności z RODO w myśl zasady rozliczalności, ale też zapewniający faktyczną i efektywną realizację praw przez podmioty danych.

Nie jest jednak przesądzone, jaki powinien być zakres takich procedur. W praktyce spotykane są m.in. procedury dotyczące obsługi żądania podmiotu danych. Innym rozwiązaniem są środki nakierowane na całościowe uregulowanie postępowania związanego z realizacją praw przez podmiot danych. Złożoność, wielorodzajowość i mnogość uprawnień przypisanych podmiotom danych oraz organizacyjna potrzeba systemowego ujęcia omawianej problematyki uzasadnia model opracowywania pełnych ścieżek postępowania w celu realizacji praw osób, których dane dotyczą.

> **W praktyce podejście „od A do Z" oznacza przygotowanie ścieżki składającej się na przykład z następujących kroków:**
>
> 1) **Opracowanie kanałów komunikacji (składania wniosków z żądaniami realizacji praw).**
> 2) **Określenie postępowania na etapie wpłynięcia wniosku z wyszczególnieniem stanowisk / osób odpowiedzialnych za jego obsługę.**
> 3) **Postępowanie weryfikacyjne i ocena formalna wniosku, w tym identyfikacja wnioskodawcy i kwalifikacja zagadnienia.**
> 4) **Ustalenie zasadności żądania oraz jego zakresu (postępowanie decyzyjne).**
> 5) **Określenie wytycznych dotyczących czasu realizacji żądania.**
> 6) **Wszczęcie procedury wykonywania prawa przez administratora (obszar, przedmiot, zakres).**
> 7) **Odpowiedź (optymalnie: możliwie zestandaryzowana), wraz ze zindywidualizowanym uzasadnieniem i typowymi pouczeniami.**
> 8) **Obsługa rejestru żądań.**

Tryb realizacji praw

Obsługa żądania dotyczącego realizacji praw spoczywa na administratorze. Przeprowadzenie tego procesu wymaga podejmowania decyzji w rozmaitych stanach faktycznych. Jednocześnie administrator musi postępować zgodnie z trybem wykonywania praw wyznaczonym przepisami Ogólnego Rozporządzenia. Oznacza to, że:

1) Termin realizacji żądania nie może przekroczyć 30 dni. W wyjątkowych przypadkach, gdy żądanie jest wyjątkowo skomplikowane lub w tym samym czasie spłynie wiele żądań od podmiotów danych, możliwe jest przedłużenie procesu o kolejne dwa miesiące – wówczas należy poinformować podmiot danych, że jego żądanie jest rozpatrywane i wyjaśnić przyczyny przedłużenia procesu.
2) Administrator jest zobowiązany ułatwiać podmiotowi danych realizację praw, czego przejawem może być zwłaszcza stosowanie zestandaryzowanych formularzy kontaktowych, dedykowanych adresów poczty elektronicznej czy uproszczonych procedur usprawniających proces obsługi żądań. Tym sposobem administrator przyjmuje rolę aktywnego organizatora procesu realizacji prawa już na etapie zgłoszenia żądania.
3) Informowanie podmiotów danych, w tym w szczególności w przypadku odmowy realizacji żądania, administrator obowiązany jest poinformować o powodach odmowy, o możliwości wniesienia skargi do organu nadzorczego oraz prawie do skorzystania ze środków ochrony prawnej przed sądem.

Powyższy tryb postępowania (wynikający w szczególności z art. 12 RODO) jest stosowany w odniesieniu do wszystkich praw wskazanych w art. 15 – 22 RODO, co nie wyłącza stosowania szczegółowych wymogów tam, gdzie jest to dodatkowo wymagane przepisami. I tak, na przykład w przypadku realizacji prawa do usunięcia danych, administrator jest dodatkowo zobowiązany do poinformowania o usunięciu danych, jak również poinformowania innych administratorów, którym dane zostały w przeszłości udostępnione, wraz z żądaniem usunięcia ich kopii (art. 17 ust. 2 RODO).

Forma realizacji praw

Równolegle do trybu postępowania, przepisy RODO kładą duży nacisk na warstwę formalną realizacji praw podmiotów danych. Tłem regulacji w tym zakresie jest nie tylko umożliwienie zapoznania się przez adresatów z informacjami, ale również ich zrozumienie. W tym kontekście można wskazać, że:

1) Komunikacja z podmiotami danych powinna być prowadzona w sposób zwięzły, przejrzysty, zrozumiały oraz przy zastosowaniu prostego i jasnego języka. Wszelkie informacje i wszelkie komunikaty związane z przetwarzaniem powinny być adekwatne, stosowne i ograniczone do tego, co jest w danej sytuacji niezbędne. Z kolei jasny i prosty język to taki, który jest jednoznaczny i zrozumiały dla adresata informacji.
2) Informowanie i komunikowanie powinno być uskuteczniane w formie pisemnej, a w stosownych przypadkach w formie elektronicznej. Jeżeli dane są przetwarzane drogą elektroniczną, administrator musi zapewnić możliwość wnoszenia żądań również tą drogą. Na żądanie osoby, której dane dotyczą, omawiana tu komunikacja może następować również ustnie.
3) Udzielanie informacji na gruncie art. 13 oraz art. 14 RODO może być opatrzone znakami graficznymi (infografiki) przedstawiającymi cel i sens przetwarzania. Prawodawca dodatkowo zachęca do takiego rozwiązania w Motywie 58 RODO, wskazując, że *„zasada przejrzystości wymaga, by wszelkie informacje kierowane do ogółu społeczeństwa lub osoby, której dane dotyczą, były zwięzłe (…), a w stosownych przypadkach, dodatkowo wizualizowane*".

RODO kładzie akcent na istotę i komunikatywność przekazu, przez co administratorzy są zobowiązani dostosowywać komunikację do potrzeb danego przypadku, a zwłaszcza kategorii adresatów. W praktyce może to stanowić poważne wyzwanie językowe, głównie ze względu na złożoność problematyki danych osobowych.

Wyłączenia realizacji praw podmiotów – kiedy nie trzeba (czy nawet: nie można) realizować praw

Realizacja praw podmiotów danych na gruncie RODO zleży od szeregu czynników. Otrzymując wniosek z żądaniem realizacji prawa, administrator powinien każdorazowo przeprowadzić analizę tego, czy dany wniosek podlega szczególnym wyłączeniom wskazanym w RODO. Docelowo, analiza tych wyłączeń i warunków realizacji praw może stać się centralnym punktem postępowania w procesie obsługi praw podmiotów danych, ze szczególnym uwzględnieniem ich fakultatywnego albo obligatoryjnego charakteru.

Prawo dostępu

W przypadku prawa dostępu do danych osobowych, administrator jest zobowiązany odmówić dostarczenia kopii danych podlegających przetwarzaniu, gdy realizacja tego prawa może wpłynąć niekorzystnie na prawa i wolności innych. Dokonując wymaganej analizy administrator musi brać pod uwagę zakres przekazywanych informacji i w razie potrzeby – ograniczać zakres udostępnienia danych, jeśli realizacja prawa wpłynęłaby niekorzystnie na prawa i wolności osoby trzeciej.

Prawo do usunięcia danych („do bycia zapomnianym")

Prawo do żądania usunięcia danych przysługuje tylko w określonych wypadkach oraz doznaje wielu ograniczeń.

Podmiot danych może zgłosić żądanie usunięcia jego danych, gdy:

a) dane nie są już niezbędne do celów, w jakich zostały zebrane lub były w inny sposób przetwarzane, lub
b) cofnął zgodę, która była podstawą przetwarzania dany jego dotyczących, lub
c) wniósł sprzeciw wobec przetwarzania jego danych lub
d) dane osobowe były przetwarzane niezgodnie z prawem lub
e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego.
f) Jednakże administrator nie wykonuje żądania usunięcia danych w zakresie, w jakim ich przetwarzanie jest niezbędne:
g) do korzystania z prawa do wolności wypowiedzi i informacji,
h) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa lub do wykonania zadania realizowanego w interesie publicznym,
i) z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego, np. do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej,
j) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, o ile prawdopodobne jest, że wykonanie żądania usunięcia danych podmiotu danych uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania,
k) do ustalenia, dochodzenia lub obrony roszczeń.

Prawo do ograniczenia przetwarzania

Prawo do ograniczenia przetwarzania jako środek tymczasowy, służy zabezpieczeniu interesów podmiotu danych na czas rozpatrywania jego innych żądań lub ustalania, dochodzenia czy obrony roszczeń.

Podmiot danych może żądać ograniczenia przetwarzania jego danych osobowych, jeżeli:

a) kwestionuje on prawidłowość danych osobowych,
b) przetwarzanie jest niezgodne z prawem, a podmiot danych sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,
c) administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne podmiotowi danych do ustalenia, dochodzenia lub obrony roszczeń,
d) w związku ze swoją szczególną sytuacją wniósł on sprzeciw wobec przetwarzania jego danych osobowych.

Prawo do przenoszenia

Prawo do przenoszenia danych ma zastosowanie jedynie w przypadku, gdy dane osobowe podmiotu zgłaszającego żądanie są przetwarzane na mocy:

a) zgody (art. 6 ust. 1 lit. a RODO) lub na podstawie umowy (art. 6 ust. 1 lit. b RODO),
b) a dane te są przetwarzane w sposób zautomatyzowany.

Jeżeli którykolwiek z powyższych warunków nie jest spełniony, administrator może odmówić spełnienia żądania. Ponadto, administrator bezwarunkowo nie może również zrealizować prawa do przenoszenia danych, w zakresie w jakim niekorzystnie by wpłynęło na prawa i wolności innych osób.

Prawo sprzeciwu

Administrator powinien zrealizować żądanie dotyczące sprzeciwu wobec przetwarzania w każdym przypadku, gdy dane osobowe są przetwarzane:

c) na podstawie prawnie usprawiedliwionych interesów administratora,
d) w celu wykonania zadania realizowanego w interesie publicznym.

Jednakże administrator może uwolnić się od zadośćuczynienia żądaniu wykazując, że:

e) istnieją prawnie uzasadnione podstawy przetwarzania danych, które są nadrzędne wobec interesów, praw i wolności osoby, której dane dotyczą, lub
f) dane służą ustaleniu, dochodzeniu lub obronie roszczeń, lub
g) dane są przetwarzane dla celów badań naukowych, historycznych lub statystycznych, a przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

Wyłączenia i warunki realizacji praw są punktem wyjścia dla wdrożenia dalszych procedur obsługi realizacji praw podmiotów danych, w praktyce stanowiąc jądro zautomatyzowanych systemów ochrony danych osobowych. Z punktu widzenia administratora danych istotne jest właściwe „ułożenie" procesów obsługi praw podmiotów poprzez dostosowanie wewnętrznych procedur uwzględniających nie tylko niuanse prawa ochrony danych osobowych, ale też profil i środowisko danego przedsiębiorstwa.

Wdrożenie RODO w sektorze telekomunikacyjnym i IT – realizacja praw osób, których dane dotyczą oraz analiza wpływu na prywatność.

Autorzy: Barbara Sawina, Sławomir Chmielewski, Orange Polska

Jednymi z większych wyzwań z jakimi musieli się zmierzyć administratorzy sektora telekomunikacyjnego i IT było wdrożenie nowego zakresu realizacji praw osób, których dane dotyczą oraz analizy wpływu na prywatność. Członkowie Polskiej Izby Informatyki i Telekomunikacji wzięli udział w anonimowej ankiecie, w której podzielili się swoimi doświadczeniami wdrożenia RODO między innymi w zakresie omawianym w niniejszym Rozdziale.

Prawa osób, których dane dotyczą

Obowiązek informacyjny

Przed 25 maja 2018 r. administratorzy zobowiązani byli do wykonywania wobec podmiotów danych obowiązków informacyjnych zgodnie z art. 10 i 11 dyrektywy 95/46/WE oraz art. 24 i art. 25 Ustawy o ochronie danych osobowych[2]. Rozporządzenie[3] w art. 13 i art. 14 znacznie rozszerzyło katalog informacji dotychczas przekazywanych podmiotom danych.

Rozporządzenie wprowadziło nieznane dotąd obowiązki poinformowania o:

1) tożsamości i danych przedstawiciela administratora;
2) danych kontaktowych inspektora ochrony danych;
3) podstawach prawnych przetwarzania danych;
4) kategoriach przetwarzanych danych osobowych;
5) zamiarze przekazania danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej (w tym o zastrzeżeniu odpowiednich zabezpieczeń, stosowanych wiążących regułach korporacyjnych), przekazaniu niezbędnym ze względu na ważne prawnie uzasadnione interesy realizowane przez administratora, wobec których charakteru nadrzędnego nie mają interesy ani prawa i wolności osoby, której dane dotyczą;
6) okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteriach ustalania tego okresu;
7) prawnie uzasadnionych interesach administratora lub strony trzeciej, o ile stanowią podstawę przetwarzania danych;
8) prawie do żądania od administratora usunięcia lub ograniczenia przetwarzania danych osobowych dotyczących osoby, której dane dotyczą oraz o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
9) jeżeli przetwarzanie odbywa się na podstawie zgody podmiotu danych – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
10) prawie wniesienia skargi do organu nadzorczego;

2 Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U. z 2016 r. poz. 922, z 2018 r. poz. 138, 723)

3 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)

11) źródle pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych;

12) zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu oraz istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Treść nowego obowiązku informacyjnego administratorzy sektora telekomunikacyjnego i IT udostępnili wszystkim podmiotom danych, których dane przetwarzali w dniu 25 maja 2018 r. Różna była forma przekazania informacji.

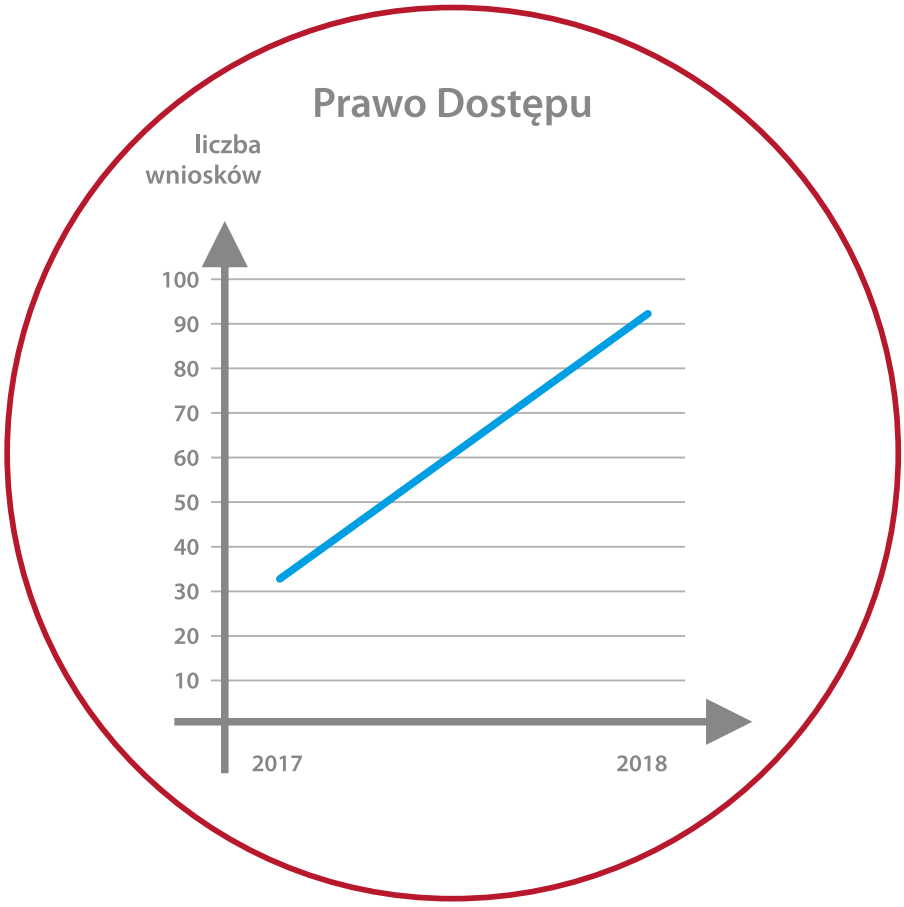
Niektórzy operatorzy usług telekomunikacyjnych wysłali do dotychczasowych Klientów informacje w formie pisemnej. Kilku administratorów zrealizowało obowiązek informacyjny w formie elektronicznej, jeden zamieścił jego treść na samoobsługowych kontach elektronicznych przypisanych poszczególnym klientom.

Kilku administratorów z sektora IT wykonało obowiązek informacyjny wyłącznie na stronie www administratora, w tym w treści polityki prywatności. Należy zwrócić uwagę, że w większości przypadków podmioty te występują w roli pomiotów przetwarzających, a rolę administratora danych pełnią wyłącznie wobec danych swoich pracowników.

Duże wątpliwości w praktyce budzi przekazywanie powyższych informacji, gdy z osobami których dane są przetwarzane nie wiąże administratora żadna umowa. Szczególne trudności powstają w przypadku przetwarzania danych osobowych pracowników / współpracowników podmiotów współpracujących.

Prawo dostępu do danych

Liczne informacje medialne towarzyszące wdrożeniu RODO oraz fakt wysłania przez administratorów dostosowanej do wymogów RODO treści obowiązku informacyjnego były przyczyną nadzwyczajnego zainteresowania podmiotów danych przetwarzaniem ich danych osobowych. Od 25 maja 2018 r. do końca 2018 r. administratorzy otrzymali od 1 do prawie 3 tysięcy wniosków o realizację praw osób, których dane dotyczą.



Najczęściej wnioskodawcy nie wskazują zakresu danych, których dotyczy ich wniosek. Niektóre wnioski zawierają bardzo rozbudowane żądania. Klienci chcieli uzyskać informacje min. o: danych powstałych na skutek aktywności Klienta, w trakcie korzystania przez niego z usług telekomunikacyjnych, w trakcie wizyt w placówkach operatora. Nie wszyscy administratorzy otrzymali wystąpienia odnoszące się do prawa dostępu. Jednak ci do których wpłynęły, zanotowali ich wzrost od 50 % do 500 % w porównaniu z ilością wniosków składanych przed 25 maja 2018 r., gdy istniało prawo do kontroli przetwarzanych danych (wynikające z art. 32 Ustawy o ochronie danych osobowych z 1997 r.).

Prawo do sprostowania danych

Podobnie jak prawo dostępu do danych prawo do sprostowania danych istniało przed 25 majem 2018 r. Art. 24 ust. 1 pkt 3 oraz art. 25 ust. 2 pkt. 4 Ustawy z 1997 r. o ochronie danych osobowych określały je jako prawo dostępu do treści danych oraz ich poprawiania.

Wejście w życie Rozporządzenia (i wysłanie informacji o przetwarzaniu danych osobowych) miało wpływ na liczbę sprostowań danych dokonanych z inicjatywy podmiotów danych do końca 2018 r. W roku 2019 liczba takich wniosków powróciła do stanu sprzed 25 maja 2018 r. W przypadku jednego z operatorów sięga ok. 10 000 rocznie.

Prawo do usunięcia danych

Najczęściej osoby, których dane dotyczą oczekiwały usunięcia ich danych wraz z rozwiązaniem umowy łączącej je z operatorami telekomunikacyjnymi.

W prawie wszystkich przypadkach usunięcie danych nie było możliwe ze względu na konieczność ich dalszego przetwarzania niezbędną dla wykonywania obowiązków nałożonych na administratorów (jak obowiązek przechowywania faktur za wykonane usługi) lub dla realizacji przez nich ich usprawiedliwionych interesów (jak dochodzenie roszczeń). Zdarzały się nieliczne przypadki wniosków składanych przez dłużników, które oczywiście nie mogły być uwzględnianie.

Prawo do ograniczenia przetwarzania

Prawo to budziło najwięcej kontrowersji, administratorzy nie mieli dotychczas żadnych doświadczeń w stosowaniu ograniczenia przetwarzania. Jednocześnie ponieśli znaczne nakłady finansowe, aby zapewnić odznaczenie ograniczenia przetwarzania w systemach teleinformatycznych. Wbrew wcześniejszym przypuszczeniom niewielu Klientów domagało się ograniczenia przetwarzania ich danych osobowych. W roku 2018 wpłynęło od 14 do 67 wniosków (z wyłączeniem większości tych administratorów, do których nie wpłynął żaden wniosek). Do kwietnia 2019 r. wpłynęły po 1 lub 2 wnioski.

Osoby, których dane są przetwarzane żądając ograniczenia ich przetwarzania mylą je często z prawem do sprzeciwu wobec przetwarzania danych. Po uzyskaniu od nich dodatkowych informacji, często okazuje się, że faktycznie oczekują uwzględnienia sprzeciwu wobec przetwarzania ich danych.

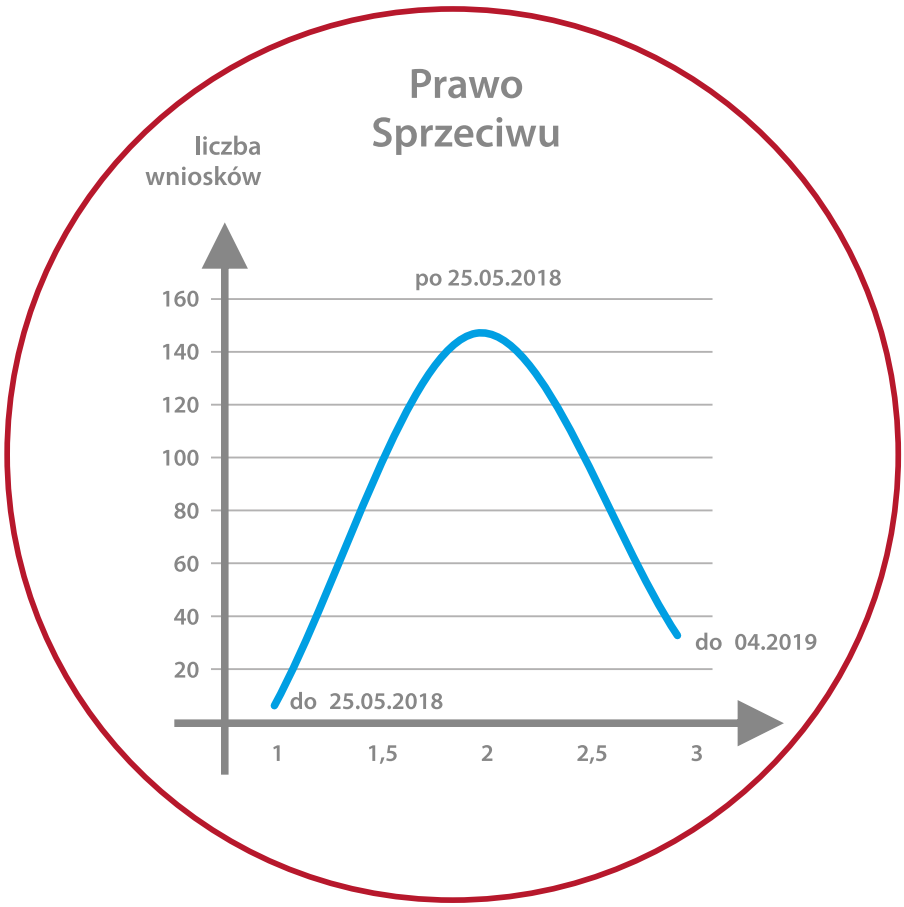
Prawo do przenoszenia danych

W trakcie rozmów prowadzonych w gronie przedsiębiorstw sektora telekomunikacyjnego i IT w okresie przed 25 maja 2018 r. pojawiało się wiele wątpliwości odnoszących się do sposobów wykonywania tego prawa. Zgodnie z motywem 68 Rozporządzenia: *Przysługujące osobie, której dane dotyczą, prawo do przesłania lub otrzymania swoich danych osobowych nie powinno nakładać na administratorów obowiązku prowadzenia lub wprowadzenia kompatybilnych technicznie systemów przetwarzania.* Niemniej operatorzy telekomunikacyjni i przedsiębiorcy sektora IT podjęli rozmowy o skutecznych sposobach umożliwienia Klientom przenoszenia na ich prośbę danych pomiędzy administratorami.

W praktyce podmioty danych w bardzo nielicznych przypadkach występowały z wnioskiem o przeniesienie danych, najczęściej myląc do z wnioskiem o przeniesienie numeru telefonu do innego operatora. W kilku przypadkach Klienci wnioskowali o przeniesienie numeru telefonu przed zakończeniem obowiązywania łączącej ich z operatorem telekomunikacyjnym umowy, powołując się na prawo do przenoszenia danych. Oczywiście ich żądania w tym zakresie nie mogły zostać spełnione.

Prawo do sprzeciwu wobec przetwarzania danych

Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych opartego na art. 6 ust. 1 lit. e) lub f), w tym profilowania na podstawie tych przepisów. Administratorowi nie wolno już przetwarzać tych danych osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.



Do większości administratorów takich wniosków nie złożono. Składano je do operatorów telekomunikacyjnych. W roku 2018 wpłynęło od 14 do prawie 300 wniosków. W roku 2019 złożono od 5 do 61 wniosków – z wyłączeniem tych administratorów, do których nie wpłynął żaden wniosek. Ponieważ Klienci zostali poinformowani o prawie sprzeciwu wobec przetwarzania ich danych w celu marketingu bezpośredniego, większość żądań stanowiła sprzeciwy wobec przetwarzania danych w celach marketingowych.

Kontakt z Inspektorem Ochrony Danych

Uprawnienie do uzyskania danych kontaktowych Inspektora Ochrony Danych znacznie poprawiło kontakt podmiotów danych z administratorami. W większości przypadków administratorzy wskazują adres e-mail jako sposób nawiązania kontaktu z Inspektorami.

Osoby, których dane są przetwarzane bardzo chętnie korzystają z tej możliwości. Jeden z administratorów, którzy odpowiedzieli na ankietę otrzymuje od 1120 (2018 r.) do 1155 (2019 r.) e-maili miesięcznie. Inny administrator w roku 2018 r. otrzymał ok. 1300 e-maili. Większość z nich niestety nie dotyczy przetwarzania danych osobowych. W przypadku operatorów telekomunikacyjnych zdecydowana większość korespondencji kierowanej do IOD dotyczy kwestii związanych z obsługą Klienta i reklamacjami.

Pytania odnoszące się do przetwarzania danych osobowych, pokazują znaczny wzrost świadomości podmiotów danych, co do przysługujących im praw.

Ocena skutków dla ochrony danych

Rozporządzenie w odróżnieniu do dotychczasowych przepisów, które wyraźnie wskazywały sposób zabezpieczenia danych[4] pozostawiło administratorom decyzję o zastosowaniu środków niezbędnych dla zapewnienia bezpieczeństwa danym osobowym przetwarzanym w związku z nowymi usługami, produktami. Zabezpieczenie danych zgodnie z Rozporządzeniem zostało oparte na zasadzie *risk based approach* tj. podejściu opartym na analizie ryzyka. Na administratorów nałożono obowiązek przeprowadzenia uprzedniej wobec operacji przetwarzania oceny skutków dla ochrony danych.

Administratorzy sektora telekomunikacyjnego i IT poszukiwali właściwej metody przeprowadzania oceny skutków dla ochrony danych.

Niektóre podmioty wprowadziły sformalizowane zasady przeprowadzania analizy wpływu na prywatność.

Najczęściej administratorzy posługują się zasadami przeprowadzania analizy ryzyka wynikającymi z normy zarządzania bezpieczeństwem informacji ISO 27001. Oczywiście oparto się na Wytycznych Prezesa Urzędu Ochrony Danych Osobowych z 17 sierpnia 2018 r. Jeden z administratorów wykorzystał także wytyczne francuskiego organu nadzorczego[5]. Niektórzy skorzystali z wytycznych przygotowanych przez Agencję Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA)[6]. Uwzględniono także Wytyczne Grupy Art. 29 *dotyczące skutków dla ochrony danych (DPIA) oraz ustalenia czy przetwarzanie „z dużym* prawdopodobieństwem może powodować wysokie ryzyko" do celów Rozporządzenia 2016/679 przyjęte 4 kwietnia 2017 r. Jeden z administratorów uwzględnił także normę ISO/IEC 29134 „Information technology – Security techniques – Guidelines for privacy impact assessment".

Celem wprowadzenia sformalizowanych zasad było ustalenie kryteriów identyfikowania przypadków wymagających przeprowadzenia oceny wpływu na prywatność, określenie sposobu jej dokonywania, zdefiniowanie zakresu działań związanych z identyfikacją Ryzyka, wskazanie metody oceny Ryzyka związanego z naruszeniem praw i wolności Podmiotów danych w procesie Przetwarzania Danych osobowych i postępowania z Ryzykiem.

Większość administratorów, którzy odpowiedzieli na ankietę zaimplementowało narzędzia informatyczne, ankiety mające na celu wsparcie organizacji przy przeprowadzaniu analizy wpływu na prywatność.

Umowy powierzenia danych osobowych zawierane przez administratorów sektora telekomunikacyjnego i IT uwzględniają zapisy zobowiązujące podmioty przetwarzające do udzielenia wsparcia przy przeprowadzaniu analizy wpływu na prywatność, zgodnie z art. 28 ust. 3 lit. f. W praktyce do udzielania wsparcia w tym zakresie, przez podmioty przetwarzające dochodzi niezwykle rzadko. Administratorzy samodzielnie przeprowadzają ocenę skutków dla ochrony danych, również dla procesów przetwarzania, które wymagają powierzenia danych osobowych innym podmiotom. Przedstawiciele sektora telekomunikacyjnego i IT występujący na rynku jako podmioty przetwarzające również prawie nigdy nie spotykają się z oczekiwaniami administratorów w zakresie udzielania wsparcia przy przeprowadzeniu analizy wpływu na prywatność.

4 ROZPORZĄDZENIE MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. 2004 nr 100 poz. 1024 ze zm.)

5 Źródło CNIL – Commission Nationale de l'Informatique et des Libertés – https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment

6 Źródłó European Data Protection Supervisor, Data Protection Impact Assessment (DPIA) – https://edps.europa.eu/data-protection/notre-rôle-en-tant-que-contrôleur/data-protection-impact-assessment-dpia_en

Rozporządzenie przewiduje możliwość przeprowadzenia uprzednich konsultacji z organem nadzorczym, gdy przeprowadzona ocena wpływu na prywatność wskaże na wysoki poziom ryzyka dla prywatności osób, których dane mają być przetwarzane. Żaden z administratorów nie zdecydował się na wszczęcie uprzednich konsultacji z organem nadzorczym. Występują dwa rodzaje przyczyn. Jedni z administratorów nie napotkali dotychczas w swoich analizach na wysokie ryzyko przetwarzania danych. Drudzy nie dopuszczają możliwość wdrażania produktów, usług obarczonych wysokim ryzykiem dla prywatności, bez jego uprzedniego obniżenia do poziomów akceptowalnych tj. co najmniej średnich.

Implementacja Rozporządzenia w dużych organizacjach jakimi są najczęściej podmioty sektora telekomunikacyjnego oraz IT stanowiła ogromne wyzwanie prawne, organizacyjne i finansowe. W większości spółek powołano Programy, Projekty odpowiedzialne za doprowadzenie do stosowania nowych przepisów zapewniających bezpieczeństwo danych osobowych. Wszystkie podmioty zastosowały rozwiązania zapewniające, że prawa osób, których dane przetwarzają są odpowiednio chronione.

Po roku pojawiają się pomysły na doskonalenie wprowadzonych rozwiązań. Mają one na celu z jednej strony usprawnienie wywiązywania się przez administratorów z ich obowiązków, z drugiej ułatwienie podmiotom, których dane dotyczą korzystania z ich praw.

Administratorzy wyczekują stanowisk, wytycznych Prezesa Urzędu Ochrony Danych Osobowych. Są one szczególnie cenne w pierwszych latach obowiązywania Rozporządzenia, gdy stosowaniu go towarzyszy brak pewności niezbędnej do prowadzenia działalności gospodarczej, a wprowadzanie zmian oznacza poniesienie znacznych nakładów finansowych.

Powierzenie przetwarzania danych, weryfikacja processorów, zarządzanie wzajemnymi relacjami

Autorzy: Bartosz Marcinkowski, Robert Brodzik, Domański Zakrzewski Palinka

Istota powierzenia przetwarzania danych

Administrator danych może posłużyć się w przetwarzaniu danych osobowych innym podmiotem działającym w jego imieniu. Skorzystanie ze wsparcia takiego podmiotu (zwanego processorem) stosowane bywa zwłaszcza w przypadku potrzeby outsourcingu określonych funkcji gospodarczych administratora (aspekt profesjonalnego przetwarzania danych przez profesjonalny podmiot bywa czynnikiem decydującym, choć nie jedynym przy podjęciu decyzji w tym zakresie).

Niemniej administrator dokonując operacji outsourcingu i powierzenia przetwarzania danych osobowych innemu (często wysoce wyspecjalizowanemu) podmiotowi nie wyłącza odpowiedzialności administratora z tytułu dysponowana danymi osobowymi – stąd doniosłość nie tylko należytej selekcji processorów świadczących usługi, ale też odpowiednich sformułowań umowy o powierzenie przetwarzania danych (często stanowiącej część większej umowy, tj. o świadczenie określonych usług, np. księgowych czy z zakresu IT), w tym m.in. w odniesieniu do dalszego powierzenia (podpowierzenia) przetwarzania danych. O tych kwestiach mowa jest w dalszej części Raportu.

Centralnym punktem instytucji powierzenia jest umowa powierzenia przetwarzania danych. Stanowi ona obligatoryjny element powierzenia, wiążący administratora i processora. Z jednej strony umowy powierzenia są ściśle regulowane co do treści przez przepisy, z drugiej mogą być modyfikowane i dostosowywane – zgodnie z kodeksową zasadą swobody umów – do potrzeb danego przypadku. Nie mogą jednak stać w sprzeczności z wymogami wynikającymi z RODO.

Umowa powierzenia zgodna z art. 28 RODO powinna zawierać co najmniej:

1) Określenie przedmiotu przetwarzania.
2) Wskazanie czasu trwania przetwarzania.
3) Określenie celu przetwarzania.
4) Określenie charakteru przetwarzania.
5) Wskazanie rodzaju powierzanych danych osobowych.
6) Wskazanie kategorii osób, których dane dotyczą w związku z powierzeniem.
7) Polecenie przetwarzania danych kierowane do processora wydane przez administratora.
8) Zapewnienie processora, aby osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy.
9) Zobowiązania do podjęcia środków bezpieczeństwa przetwarzania.
10) Określenie warunków podpowierzenia przetwarzania danych.
11) Zobowiązanie processora do wsparcia administratora w realizacji żądań praw osób, których dane dotyczą oraz innych obowiązków wskazanych w art. 32-36 RODO, odnoszących się do zapewnienia odpowiedniego poziomu bezpieczeństwa danych.
12) Zawarcie uprawnienia administratora do podjęcia decyzji usunięciu lub zwróceniu wszelkich danych osobowych w związku z powierzeniem.
13) Umożliwienie administratorowi dostępu do informacji do wykazania spełnienia wymogów umowy.
14) Postanowienia dotyczące umożliwienia administratorowi lub audytorowi, przeprowadzania audytów i inspekcji, i przycinania się do nich.

Nie istnieją oczywiste wytyczne odnośnie wskazania, w jakich sytuacjach powinna zostać zawarta umowa powierzenia, a w jakich udostępnienie danych osobowych następuje bez takiej umowy. Prawidłowa kwalifikacja zależy zwykle od wielu czynników, wykształconej praktyki oraz charakteru relacji łączącej processora i administratora. Zasadniczo umowa powierzenia jest zawierana, gdy przetwarzanie danych będzie się odbywało przez inny podmiot niż administrator. Dzieje się to wyłącznie dla celów administratora, a przy tym nie istnieją podstawy do „pełnego" (całkowitego) udostępnienia danych osobowych (art. 6 ust. 1 lit. a-f RODO).

Poniżej zestawienie* branż i sektorów, w których najczęściej jest stosowana instytucja powierzenia, a w których w praktyce dochodzi do odrębnego administrowania i umowa powierzenia nie jest stosowana:

Najczęściej bez powierzenia:	Najczęściej z powierzeniem:
1) Usługi telekomunikacyjne**	1) Support IT (np. zdalna konserwacja)
2) Ubezpieczenia	2) Usługi hostingu
3) Usługi kurierskie	3) Payroll
4) Szkolenia	4) Scentralizowane centrum usług wspólnych w grupie przedsiębiorstw
5) Taxi	5) Niszczenie dokumentów
6) Hotele	6) Archiwizacja
7) Biura podróży	7) Prywatna opieka medyczna
8) Usługi pocztowe	8) Tłumaczenia
9) Medycyna pracy	9) Usługi księgowe
10) Kancelarie prawne	10) Pośrednictwo handlowe

* Tabela przedstawia najczęstsze praktyki rynkowe wg obserwacji poczynionych w praktyce doradztwa prawnego – każda relacja powinna jednak zostać zakwalifikowana indywidualnie.

** Nie dot. usług towarzyszących, np. archiwizacja telefonów służbowych, usuwanie danych z chmury itp.

Przedmiotem powierzenia nie są w istocie same dane osobowe, a operacje wykonywane na danych osobowych, czyli ich przetwarzanie. W stosunku powierzenia przetwarzania, podmiot przetwarzający na zlecenie administratora zobowiązuje się do wykonywania określonych czynności, zobowiązując się zarówno do starannego działania (w tym zwłaszcza zapewnienia danym bezpieczeństwa), ale też do osiągnięcia określonego rezultatu (realizacji „celu przetwarzania danych").

Cel przetwarzania

Podmiotem przetwarzającym (processorem) jest ten, kto przetwarza dane wyłącznie w imieniu administratora, a więc w granicach wyznaczanych przez administratora. W przypadku wykroczenia przez processora poza zakreślony w umowie powierzenia cel przetwarzania danych osobowych, processor staje się administratorem danych w stosunku do tego przetwarzania. Dlatego tak istotne jest, aby określenie celów przetwarzania przez strony umowy powierzenia było możliwie konkretne i precyzyjne.

Oczywiście pierwotne cele przetwarzania, realizowane w sposób uprawniony przez administratora danych wyznaczają nieprzekraczalne granice powierzenia danych. Jednocześnie w praktyce zdarza się, że pierwotny cel przetwarzania na przestrzeni czasu ulega zmianom i zachodzi konieczność jego modyfikacji. Należy zatem zwrócić uwagę, iż na gruncie zasady ograniczenia celu dane nie mogą być przetwarzane niezgodnie z pierwotnymi celami, a ich zmiana wymaga między innymi przeprowadzenia testu zgodności celu (*purpose compatibility test*) i zważania:

a) związków między celami pierwotnymi a celami zamierzonego dalszego przetwarzania,
b) kontekstu (w tym relacji między osobami, których dane dotyczą a administratorem),
c) charakteru danych osobowych (czy nie są to np. tzw. „dane wrażliwe"),
d) ewentualnych konsekwencji lub skutków dalszego przetwarzania,
e) istnienia odpowiednich zabezpieczeń, w tym np. szyfrowania lub pseudonimizacji.

Zmiana celu oraz przeprowadzenie testu zgodności obciążą administratora. Z kolei w przypadku wydania przez administratora processorowi polecenia wykraczającego poza pierwotny cel, processor winien poinformować administratora o tym, iż w jego ocenie polecenie stanowi naruszenie przepisów i zasady związania celem przetwarzania, żądając przedstawienia wyników testu zgodności.

Dobór processora

Konsekwencją zasady rozliczalności oraz charakteru zobowiązania, rezultatu stanowiącego cechę, umowy powierzenia jest nałożona na administratora odpowiedzialność za dobór podmiotu przetwarzającego.

Processor powinien zapewniać w szczególności wdrożenie środków technicznych i organizacyjnych, które gwarantują spełnienie wymogów RODO oraz chronią prawa podmiotów danych.

W związku z tym, że administrator odpowiada za dobór processora, konieczne staje się wypracowanie możliwie zobiektywizowanych narzędzi i środków ocennych. Praktyka rynkowa wypracowała ankiety wypełniane przez processorów (kandydatów na processorów), zapewniające porównywalność kryteriów i wyników ocen. Uproszczona ankieta służąca weryfikacji processora z komentarzami może obejmować przykładowo poniżej wskazane obszary i elementy:

ANKIETA WERYFIKACJI PROCESSORA (przykład)	
Treść pytania	**Odpowiedź processora**
Aspekty organizacyjne	
Czy processor wyznaczył Inspektora Ochrony Danych?	[tak albo nie]
Czy processor posiada politykę bezpieczeństwa informacji lub inne dokumenty opisujące zabezpieczenia stosowanych systemów, w tym dostęp do systemów IT?	[tak / nie; jeśli tak, tekst może podlegać dalszej ocenie]
Czy processor korzysta z dalszych processorów w procesie przetwarzania danych osobowych na zlecenie administratora danych osobowych? Jakich i ilu?	[wyszczególnienie podprocessorów]
Jeżeli processor korzysta z dalszych processorów, to czy są oni zlokalizowani w ramach EOG?	[podprocessorzy spoza EOG nie dyskwalifikują processora, jednak powinny zostać powzięte dodatkowe działania]
Jeżeli transfer danych odbywa się poza EOG to na jakiej podstawie prawnej?	[przywołanie podstawy]
Czy processor prowadzi rejestr czynności dla powierzonych operacji przetwarzania danych osobowych?	[wymóg z art. 30 ust. 2 RODO]
Jak często organizowane są szkolenia obejmujące tematykę bezpieczeństwa informacji (w tym szkolenia z obowiązujących przepisów dot. danych osobowych)?	[wykaz]
Czy processor wdrożył procedury dotyczące zarzadzania incydentami bezpieczeństwa?	[tak / nie]
Środki techniczne	
Czy processor posiada zabezpieczenia ograniczające ryzyko ataku hackerskiego, np. poprzez użycie oprogramowania antywirusowego?	[opis stosowanego oprogramowania antywirusowego]
Czy wszystkie przenośne urządzenia IT wykorzystywane do przechowywania danych osobowych lub informacji są szyfrowane?	[tak / nie; opis zastosowanych rozwiązań]
Czy processor przechodzi regularne audyty z zakresu bezpieczeństwa danych? Jeśli tak, to czy może udostępnić raporty?	[audyt przez firmy zewnętrzne stanowi jeden ze standardowych sposobów regularnego mierzenia i testowania skuteczności środków technicznych]

Ankieta weryfikująca processora może okazać się zbędna, jeśli processor posiada zatwierdzony przez organ nadzorczy kodeks postępowania lub mechanizm certyfikacji (zob. art. 28 ust. 5 RODO).

Zarządzanie relacjami z podprocessorami w kontekście zachowania rozliczalności

Processor może, w celu wykonania powierzenia, powierzyć kolejnemu podmiotowi przetwarzanie danych. Mówimy wówczas o podpprzetwarzaniu czy podpowierzeniu. Na takiego podprocessora, na mocy umowy łączącej go z processorem, nałożone zostają przynajmniej te same obowiązki, które ciążą na processorze na podstawie umowy z administratorem (swoista transpozycja uzgodnień umownych). Dlatego w praktyce celowe jest wypracowanie możliwie jednolitych wzorów umów (klauzul umownych) tak, by nie zachodziły rozbieżności pomiędzy zakresami obowiązków wynikających z umów. Co więcej, umowa podpowierzenia nie może skutecznie przenieść na podprocessora odpowiedzialności za naruszenie obowiązków ochrony danych wobec administratora – spoczywa ona niezależnie od postanowień umownych na pierwotnym podmiocie przetwarzającym.

Processor w celu skorzystania z usługi podprocessora, zobowiązany jest do pozyskania zgody administratora. Zgodnie z art. 28 ust. 2 RODO wyróżnić można dwa rodzaje zgody na podpowierzenie:

Zgoda ogólna – wybrane implikacje	Zgoda szczegółowa – wybrane implikacje
– Obowiązek informowania administratora o zamiarze dodania lub zastąpienia podprocessora – możliwość wyrażenia sprzeciwu przez administratora	– brak możliwości dodania lub zastąpienia podprocessora bez zmiany treści umowy – zgoda wyrażona na czas obowiązywania umowy powierzenia (brak możliwości wyrażenia sprzeciwu)

W stosunku powierzenia, modele zgody ogólnej i szczególnej mogą być łączone, np. co do części podprocessorów wskazanych konkretnie, może zostać wyrażona zgoda szczegółowa, a równocześnie umowa może udzielać zgody ogólnej. W modelu zgody ogólnej processor musi mieć zapewnioną możliwość wyrażenia sprzeciwu wobec zmiany podprocessorów. W praktyce najczęściej wskazuje się okres liczony od chwili poinformowania administratora o zamierzonej zmianie podprocessorów z zastrzeżeniem możliwości wyrażenia sprzeciwu. Przed upływem wskazanego w umowie terminu nie powinno rzecz jasna dojść do podpowierzenia przetwarzania danych.

W przypadku modelu zgody szczegółowej zmiana podprocessorów wymaga zmiany umowy lub zawarcia nowej. Jednak w przypadku modelu zgody ogólnej, w praktyce pojawiają się problemy w sytuacjach częstych zmian podprocessorów oraz informowania o tym administratora.

Jednym z rozwiązań problemu dynamiki zmian podprocessorów jest prowadzenie monitoringu przy pomocy dedykowanych platform elektronicznych. Główną funkcjonalnością tego typu platform jest interaktywne wspomaganie procesów zarządzania powierzeniami, aktualizacja zmian podprocessorów oraz powiadamianie o nich. Kluczowym elementem takich platform jest zapewnienie komunikacji między administratorem a processorem, w tym umożliwienie administratorowi zgłoszenia sprzeciwu wobec zmian podprocessorów. Choć taki model zarządzania procesami nie jest jeszcze rozpowszechniony, zyskuje on na popularności z uwagi na wysokie walory funkcjonalne po uzyskaniu zgody wyrażonej w omówionym wcześniej modelu zgody ogólnej.

Transfer danych osobowych

Autor: Bartosz Marcinkowski

Według regulacji art. 44 RODO przekazanie danych osobowych do państwa trzeciego (lub organizacji międzynarodowej) zasadniczo może następować tylko wówczas, gdy administrator i podmiot przetwarzający spełnią szczegółowe warunki określone na taką okoliczność w RODO. Sprawa komplikuje się dodatkowo, jeśli dane osobowe miałyby być przekazywane jeszcze dalej, z określonego państwa trzeciego do kolejnego państwa trzeciego (lub innej organizacji międzynarodowej). Zasadniczą dyrektywą postępowania pozostaje przy tym podstawowa zasada RODO zakładająca konieczność zapewnienia nienaruszalności stopnia ochrony praw i wolności osób fizycznych zagwarantowanego w RODO

Zasadnicze pojęcia

Pojęcie przekazywania danych do państwa trzeciego zasadniczo należy rozumieć w sposób szeroki, zaliczając do niego przypadki przetwarzania danych osobowych w taki sposób, iż są one dostępne (widoczne, możliwe do ściągnięcia, mogą podlegać zmianom) w państwie trzecim.

Występują jednak sytuacje, w których oczywiste *udostępnienie* danych nie zostało uznane przez sąd za ich przekazania do państwa trzeciego[7]. Stąd kierując się względami ostrożnościowymi należy przyjmować, że każda sytuacja, w której dane mogą być dostępne w państwie trzecim, wymaga analizy pod kątem konieczności spełnienia wymogów przekazywania danych do państwa trzeciego opisanych w RODO.

Opisane ujęcie wynika z tradycyjnego, przyjętego przez prawodawcę unijnego dychotomicznego podziału państw świata na takie, które należycie spełniają wyznaczony unijnymi przepisami standard ochrony danych osobowych oraz na takie, które owego standardu nie spełniają. Obecnie owe standardy wytyczone są przez regulację RODO, do maja 2018 roku standardów wyznaczała Dyrektywa 95/46/WE i implementujące ją normy państw członkowskich. Najkrócej zatem ujmując, państwo trzecie to państwo, które nie jest ani członkiem Unii Europejskiej, ani też Europejskiego Obszaru Gospodarczego. Zatem z perspektywy prawa unijnego państwa nienależące do powyższych struktur zasadniczo – z pewnymi wyjątkami, o których mowa poniżej – chronią dane osobowej słabiej niż Polska czy innej kraje członkowskie. Takie ujęcie wymusza na podmiotach przekazujących dane osobowe do państwa trzeciego zapewnienie spełnienia szczególnych przesłanek, które gwarantują danym osobowym wysyłanym do państwa trzeciego należyty poziom bezpieczeństwa. Wynika to z zasady odpowiedzialności podmiotu przekazującego (eksportera danych) za transferowane dane osobowe, a fakt utraty bezpośredniej („fizycznej") pieczy nad danymi w żądnym razie nie uwalnia go od odpowiedzialności i rozliczalności.

Warto odnotować, iż taka sama reguła dotyczy przekazywania danych w granicach Unii Europejskiej – każdorazowo bowiem odpowiedzi wymaga pytanie, na jakiej podstawie i dla jakich celów dane są przez administratora czy podmiot przetwarzający przekazywane innemu podmiotowi. Fakt przekazania danych poza obszar UE czy EOG siłą rzeczy zwiększa doniosłość pytań o zabezpieczenie danych, gdyż administrator (czy processor) nie tylko tracą nad danymi bezpośrednią pieczę, ale także trafiają one na terytorium, które zgodnie z unijnym zapatrywaniem nie spełnia wymogów określonych w RODO.

7 Zob. Wyrok Trybunału Sprawiedliwości Unii Europejskiej z dn. 6 listopada 2003r. – http://curia.europa.eu/juris/document/document.jsf?docid=48382&doclang=en

Biała lista Komisji Europejskiej

Jak zostało to już zasygnalizowane, istnieją „państwa trzecie" które w ocenie Komisji Europejskiej zapewniają odpowiedni z perspektywy regulacji unijnej poziom ochrony danych osobowych. W konsekwencji, w pewnych, nielicznych przypadkach Komisja Europejska oficjalnie stwierdza, iż konkretne państwo trzecie spełnia unijny standard ochrony danych.

Obecnie tzw. „biała lista" Komisji obejmuje Andorę, Argentynę, Izrael, Japonię, Kanadę (w ograniczonym zakresie), Nową Zelandię, Szwajcarię, Urugwaj, Wyspy Faraona, Wyspy: Guernsey, Jersey i Man. Na liście tej próżno szukać takich państwa jak Chiny, Indie czy Rosja.

Unijne materiały informacyjne wskazują ponadto, że prowadzone są rozmowy mające skutkować wydaniem decyzji o odpowiedniości stopnia ochrony danych w Korei Południowej oraz, że w pewnym zakresie Stany Zjednoczone spełniają należyty poziom ochrony danych osobowych[8]. W przypadku tego ostatniego państwa odpowiada stwierdzenie takie zdaje się odpowiadać rzeczywistości jedynie w sensie formalnym – w relacjach pomiędzy UE a USA znajduje zastosowanie porozumienie *Privacy Shield*, niemniej jego znaczenie pozostaje istotnie ograniczone, a przyszłość zdaje się, zwłaszcza z perspektywy orzeczenia w sprawie Maximillian Schrems v. Data Protection Commissioner – niepewna[9].

Obecnie firmy z siedzibą w USA, które zostały objęte programem Privacy Shield traktowane są pod względem zapewnienia bezpieczeństwa danym osobowym tak, jakby znajdowały się w jednym z państw członkowskich UE[10].

Oceniając, czy stopień ochrony danych osobowych w państwie jest odpowiedni, Komisja Europejska uwzględnia w czasochłonnym postępowaniu między innymi takie czynniki i elementy, jak praworządność, poszanowanie praw człowieka i podstawowych wolności, ustawodawstwo (ogólne, jak i sektorowe), zasady ochrony danych, zasady dotyczące wykonywania zawodu, środki bezpieczeństwa (w tym dot. dalszego przekazywania danych osobowych do kolejnego państwa trzeciego), orzecznictwo, a przede wszystkim „istnienie skutecznych i egzekwowalnych praw osób, których dane dotyczą, oraz prawa osób, których dane dotyczą, których dane osobowe są przekazywane, do skutecznych administracyjnych i sądowych środków zaskarżenia", oraz istnienie i skuteczne działanie niezależnego organu nadzorczego, zapewniającego i egzekwującego przestrzeganie przepisów o ochronie danych (art. 45 RODO). Jak zatem widać, przeprowadzenie takiej oceny wymaga bardzo wielowątkowych prac, co skutkuje stopniem komplikacji i czasochłonnością przedsięwzięcia.

Z perspektywy praktycznej, krokiem poprzedzającym przekazanie danych poza obszar Unii Europejskiej (i EOG) powinno być sprawdzenie, czy konkretne państwo (bądź odpowiednio: część jego terytorium, organizacja międzynarodowa, a nawet sektor lub sektory gospodarki w państwie trzecim) zostały uznane w drodze decyzji Komisji Europejskiej za zapewniające odpowiedni poziom ochrony danych osobowych. Taka decyzja – w połączeniu ze specyfiką konkretnej sprawy – zasadniczo może przesądzić o legalności przekazania danych osobowych do państwa trzeciego (choć nie eliminuje innych zagadnień, jak na przykład ustalenia podstawy przekazania danych przez administratora bądź processora innemu podmiotowi).

8 Źródło: Komisja Europejska, International Dimension of Data Protection-https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

9 Zob. Orzeczenie ws Maximillian Schrems v. Data Protection Commissioner: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_pl oraz https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362

10 Źródło: Privacy Shield Framework, International Trade Association, U.S. https://www.privacyshield.gov/Program-Overview

„Alternatywne" podstawy transferu danych

Naturalnie, brak wpisania państwa importera danych na „białą listę" Komisji Europejskiej nie blokuje w sposób całkowity przekazywania danych osobowych do takiego państwa trzeciego. W przeciwnym razie zamarłby obrót międzynarodowy, w tym z takimi partnerami jak USA, Chiny czy Indie. Stąd, zgodnie z art. 46 RODO, w braku stosownej decyzji Komisji Europejskiej administrator lub podmiot przetwarzający mogą przekazać dane osobowe do państwa trzeciego (organizacji międzynarodowej), gdy zapewnią odpowiednie zabezpieczenia „alternatywne", i pod warunkiem, że obowiązują egzekwowalne prawa osób, których dane dotyczą, i skuteczne środki ochrony prawnej. Owe „alternatywne" odpowiednie zabezpieczenia można zapewnić między innymi za pomocą:

- wiążących reguł korporacyjnych (*Binding Corporate Rules; BCR*), zachowujących moc pomiędzy podmiotami należącymi do grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą. Zgodnie z art. 47 RODO, wskazane tu BCR muszą być prawnie wiążące oraz mieć zastosowanie do każdego z członków grupy, w tym ich pracowników, i są przez każdego z tych członków egzekwowane, a także muszą wyraźnie przyznawać osobom, których dane dotyczą, egzekwowalne prawa w związku z przetwarzaniem ich danych osobowych,
- standardowych klauzul ochrony danych, czyli przyjętych przez Komisję Europejską klauzul kontraktowych mających zapewnić należyty poziom ochrony danych transferowanych między podmiotami związanymi postanowieniami tych klauzul,
- standardowych klauzul ochrony danych przyjętych przez krajowy organ nadzorczy i zatwierdzonych przez Komisję Europejską,
- klauzul umownych wynegocjowanych pomiędzy administratorem lub podmiotem przetwarzającym a administratorem, podmiotem przetwarzającym lub odbiorcą danych osobowych w państwie trzecim (lub organizacji międzynarodowej),
- zatwierdzonego kodeksu postępowania bądź – rodzajowo odmiennego – zatwierdzonego mechanizmu certyfikacji, w obu przypadkach wraz z wiążącymi i egzekwowalnymi zobowiązaniami administratora (lub podmiotu przetwarzającego) w państwie trzecim do stosowania odpowiednich zabezpieczeń, w tym w odniesieniu do praw osób, których dane dotyczą.

Cechą wspólną wskazanych rozwiązań jest wymóg ich urzędowej akceptacji, warunkującej legalność przekazywana na ich podstawie danych do państwa trzeciego. W każdym zatem wypadku wymagają one uprzedniego zaangażowania organu, aczkolwiek odbywa się to w różnym momencie (standardowe klauzule ochrony korzystają z przymiotu oficjalnego wzorca, podczas gdy np. wiążące reguły korporacyjne czy klauzule umowne *ad hoc* wymagają każdorazowej oceny organu nadzorczego).

Prawodawca przyjął kaskadową koncepcję podstaw przekazania danych do państwa trzeciego: „biała lista" Komisji Europejskiej – inne przesłanki natury formalnej oraz (o czym jest mowa w dalszej części) – wyjątkowe rozwiązania szczególne.

Co ważne, do momentu wydania nowego zestawu standardowych klauzul ochrony danych, dotychczasowe standardowe klauzule umowę (*Standard Contractual Clauses*) opracowane i opublikowane przez Komisję Europejską zachowują swoją moc i mogą być skutecznie stosowane[11].

Co ważne, przedsiębiorcy mogą wprowadzać zmiany i dokonywać modyfikacji zatwierdzonych standardowych klauzul umownych, niemniej zakres i treść modyfikacji nie mogą zmieniać zasady i istoty odpowiedzialności podmiotów-sygnatariuszy. Tego rodzaju daleko idące odstępstwa od przyjętego oficjalnie wzorca winny być uznane za zmianę istotną, wymagającą odrębnej, uprzedniej oceny urzędowej.

11 Rzeczone klauzule dostępne są na stronie Bazy aktów Prawnych Unii Europejskiej w dokumencie 32010D0087 (decyzja Komisji z dnia 5 luteo 2010r. – https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex%3A32010D0087

Pozostałe sytuacje transferu danych

Ocena taka może być przeprowadzona w szczególności w trybie i na podstawie art. 49 RODO, zgodnie z którym w braku decyzji Komisji Europejskiej stwierdzającej odpowiedni stopień ochrony danych osobowych w państwie trzecim lub braku odpowiednich zabezpieczeń „alternatywnych", o których była mowa powyżej, jednorazowe lub wielokrotne przekazanie danych osobowych do państwa trzeciego (lub organizacji międzynarodowej) mogą nastąpić wyłącznie pod warunkiem, że:

a) podmiot danych poinformowany o ryzyku udzielił wyraźnej zgody,
b) przekazanie danych jest niezbędne do wykonania umowy między podmiotem danych a administratorem lub do wprowadzenia w życie środków przedumownych na żądanie podmiotu danych,
c) przekazanie danych jest niezbędne do zawarcia lub wykonania umowy zawartej w interesie podmiotu danych między administratorem a inną osobą fizyczną lub prawną,
d) przekazanie danych jest niezbędne do zawarcia lub wykonania umowy zawartej w interesie podmiotu danych, między administratorem a inną osobą,
e) przekazanie jest niezbędne ze względu na ważne względy interesu publicznego,
f) przekazanie jest niezbędne do ustalenia, dochodzenia lub ochrony roszczeń,
g) przekazanie jest niezbędne do ochrony żywotnych interesów podmiotu danych lub innych osób, jeżeli podmiot danych jest fizycznie lub prawnie niezdolny do wyrażenia zgody, lub też, gdy
h) przekazanie następuje z rejestru, który zgodnie z prawem Unii Europejskiej lub prawem państwa członkowskiego ma służyć za źródło informacji dla ogółu obywateli i który jest dostępny dla ogółu obywateli lub dla każdej osoby mogącej wykazać prawnie uzasadniony interes – ale wyłącznie w zakresie, w jakim w danym przypadku spełnione zostały warunki takiego dostępu określone w prawie UE lub w prawie państwa członkowskiego[12]

Jeżeli jednak przekazanie nie może się opierać na żadnej z powyższych przesłanek, w tym na żadnym z wyjątków z katalogu z art. 49 RODO, przekazanie do państwa trzeciego (lub organizacji międzynarodowej) może nastąpić wyłącznie, gdy przekazanie danych do państwa trzeciego:

- nie jest powtarzalne,
- dotyczy ograniczonej liczby podmiotów danych,
- jest niezbędne ze względu na ważne prawnie uzasadnione interesy realizowane przez administratora, wobec których charakteru nadrzędnego nie mają interesy ani prawa i wolności podmiotu danych, a administrator ocenił wszystkie okoliczności przekazania danych i na podstawie tej oceny zapewnił odpowiednie zabezpieczenia w zakresie ochrony danych osobowych.

W takiej sytuacji administrator informuje organ nadzorczy o przekazaniu, a także podaje podmiotowi danych – poza standardowym zakresem informacji z klauzuli informacyjnej –informacje o przekazaniu i o realizowanych ważnych prawnie uzasadnionych interesach (zob. art. 49 RODO in fine).

Przekazanie danych osobowych do państwa trzeciego na podstawie przytoczonej podstawy ekstraordynaryjnej wymaga ważenia: (i) prawnie uzasadnionych interesów realizowanych przez administratora danych oraz (ii) interesów i praw oraz wolności podmiotu danych, a to wszystko w kontekście okoliczności przekazania danych („balancing test"[13]).

12 Zob. art. 49 RODO „Wyjątki w szczególnych sytuacjach".
13 Przykład rodzajowo zbliżonego 'balancing test' można znaleźć np. na stronie Information Commissioner's Office w UK – https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/

Zautomatyzowane podejmowanie decyzji

Autorzy: Daniel Szmurło i Karol Warzecki, T-mobile

Zgodnie z art. 4 pkt. 4 RODO definicja profilowania obejmuje dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się. Dowolna forma zautomatyzowanego przetwarzania, nie oznacza „wyłącznie" zautomatyzowanego przetwarzania (o którym mowa w art. 22 RODO). Profilowanie musi obejmować pewną formę zautomatyzowanego przetwarzania – interwencja ludzka nie musi jednak powodować, że dane działanie wykracza poza definicję profilowania.

Profilowanie składa się z trzech elementów: profilowanie musi stanowić zautomatyzowaną formę przetwarzania, profilowaniu muszą podlegać dane osobowe oraz celem profilowania musi być ocena czynników osobowych osób fizycznych. Profilowanie obejmuje gromadzenie informacji o osobie (lub grupie osób), analizę ich charakterystyk lub wzorców zachowań, umieszczenie ich w określonej kategorii/grupie lub przewidywanie/ocenę obecnych lub przyszłych zachowań podmiotów, których dane dotyczą.

Zgodnie z wytycznymi Grupy Roboczej Art. 29 z 3.10.2017 r., RODO nie odnosi się wyłącznie do podejmowania decyzji na podstawie zautomatyzowanego przetwarzania (art. 22 RODO), ale ma też zastosowanie do gromadzenia danych w celu tworzenia profili i przypisywania ich do konkretnych osób. W związku z tym sama ocena lub klasyfikacja osób na podstawie określonych charakterystyk (takich jak np. wiek, płeć, często odwiedzane miejsca (lokalizacja), ruch na stronie internetowej) może być zakwalifikowana jako profilowanie niezależnie od dokonywania jakichkolwiek predykcji.

Każde profilowanie w rozumieniu RODO jest formą przetwarzania danych osobowych i podlega ogólnym przepisom RODO dotyczącym przetwarzania danych osobowych, takim jak przepisy określające podstawy prawne przetwarzania lub zasady ochrony danych (art. 5 RODO). Administrator jest odpowiedzialny za przestrzeganie tych zasad i musi być w stanie wykazać – zgodnie z zasadą rozliczalności – ich przestrzeganie.

Dla każdego profilowania danych osobowych musi więc istnieć podstawa. W zależności od podstawy prawnej profilowania zakres uprawnień osób fizycznych w odniesieniu do przetwarzania ich danych, i w konsekwencji zakres obowiązków administratora, będzie się różnił. Należy wskazać, że jeżeli profilowanie odbywa się na podstawie zgody, to podmiotowi danych przysługuje np. prawo do wycofania zgody. Jeśli profilowanie odbywa się bez zgody, np. w ramach przetwarzania mającego za podstawę uzasadniony cel administratora, to wtedy podmiot danych ma prawo do wyrażenia sprzeciwu. Dodatkowo, jeśli profilowanie prowadzi do podejmowania decyzji mających wpływ na prawa i obowiązki/lub wywiera inny znaczący skutek, to podmiot danych ma prawo do niepodlegania takiej decyzji. Tak więc w zależności od podstawy prawnej przetwarzania danych osobowych, które odbywa się z udziałem profilowania, osoby fizyczne mogą realizować różne prawa w związku z takim przetwarzanie.

Decyzja

Podejmowanie decyzji polega na wystosowaniu odpowiednich działań w stosunku do osoby w związku z przypisaniem jej profilu, np. decyzja o wysłaniu konkretnego materiału marketingowego, czy też złożeniu oferty o konkretnych parametrach.

W przypadku gdy dochodzi do zautomatyzowanego podejmowania decyzji, zawsze pociągać będzie to za sobą obowiązek informacyjny. Natomiast, gdy takie zautomatyzowane podejmowanie decyzji dodatkowo wywołuje wobec osoby, której dane dotyczą, skutki prawne lub w podobny sposób istotnie na nią wpływa, tzn. że efekt przetwarzania nie jest błahy i musi być na tyle istotny, by zasługiwać na uwagę ze strony administratora.

Zgodnie z wytycznymi Grupy Roboczej Art. 29: *„Aby operacja przetwarzania w sposób istotny wpływała na jednostkę, efekt przetwarzania nie może być błahy i musi być istotnie większy, by zasługiwać na uwagę. Oznacza to, że decyzja musi mieć potencjalnie istotny wpływ na okoliczności, zachowanie lub wybory dokonywane przez zainteresowane jednostki. W ekstremalnych przypadkach, decyzja taka może prowadzić do wykluczenia lub dyskryminacji jednostki"*.

Grupa Robocza nie wskazuje definicji „istotnego wpływu" czy też „błahości". Wskazuje jednak, że zautomatyzowane podejmowanie decyzji w celach marketingowych zazwyczaj nie będzie miało istotnego wpływu na jednostkę. Wynika stąd jednak, że pewne działania w tym zakresie mogą być objęte koniecznością pozyskania zgody, a do oceny takich sytuacji służyć powinny kryteria wskazane przez Grupę Roboczą Art. 29. Zgodnie z wytycznymi Grupy Roboczej Art. 29 zastanawiając się nad tym czy podejmowana – w oparciu o zautomatyzowane przetwarzanie, w tym profilowanie – decyzja istotnie wpływa na osobę, której dane dotyczą, należy wziąć pod uwagę w szczególności: inwazyjność procesu profilowania; oczekiwania zainteresowanych jednostek, sposób prezentacji i dostarczenia treści marketingowej, lub szczególną sytuację (wrażliwość, podatność) targetowanego podmiotu.

Zautomatyzowane podejmowanie decyzji w tym profilowanie

Zautomatyzowane podejmowanie decyzji obejmuje inny zakres niż profilowanie, może jednak częściowo pokrywać się z profilowaniem lub z niego wynikać. Podejmowanie decyzji wyłącznie w sposób zautomatyzowany to zdolność do podejmowania decyzji z wykorzystaniem rozwiązań technicznych bez interwencji ludzkiej. Zautomatyzowane decyzje mogą być podejmowane w oparciu o wszelkiego rodzaju dane, w tym na przykład:

- dane przekazane bezpośrednio przez zainteresowane osoby fizyczne (np. respondentów wypełniających kwestionariusz na stronie www);
- dane zaobserwowane na temat osób fizycznych (np. dane o lokalizacji zbierane za pośrednictwem aplikacji);
- dane pochodne lub wywnioskowane, na przykład profil osoby fizycznej, który został już utworzony (np. punktowa ocena kredytowa).

Zależność między zautomatyzowanym podejmowaniem decyzji a profilowaniem jest taka, że zautomatyzowane podejmowanie decyzji może, ale nie musi obejmować profilowania, z kolei profilowanie może zachodzić bez podejmowania zautomatyzowanych decyzji. Nie muszą one jednak stanowić odrębnych działań. Czasami zdarza się tak, że działanie, które początkowo stanowi zwykły proces zautomatyzowanego podejmowania decyzji, może przekształcić się w działania oparte na profilowaniu, co będzie zależało od wykorzystania danych.

Dobrym przykładem, ilustrującym to działanie może być nakładanie mandatów za przekroczenie dozwolonej prędkości na podstawie zdjęć z fotoradarów. Jest to proces zautomatyzowanego podejmowania decyzji, który nie musi obejmować profilowania. Decyzja ta jednak stałaby się decyzją opartą na profilowaniu, jeżeli przez pewien czas monitorowano by zachowania danej osoby fizycznej jako kierowcy a wysokość mandatu uzależniona byłaby od oceny innych czynników, jak a przykład czy wcześniej dany kierowca przekraczał już prędkość albo naruszał przepisy ruchu drogowego. Decyzje, które nie opierają się wyłącznie na zautomatyzowanym przetwarzaniu, również mogą obejmować profilowanie. Przykładowo przed udzieleniem kredytu hipotecznego bank może analizować punktową ocenę kredytową kredytobiorcy, co może obejmować dodatkową znaczącą interwencję ludzką przed wydaniem decyzji wobec danej osoby fizycznej.

Przed rozpoczęciem przetwarzania danych osobowych należy podjąć odpowiednie czynności. Aby można było zidentyfikować proces profilowania, należy najpierw stwierdzić, czy dochodzi w ogóle do przetwarzania danych osobowych, czy oceniane są czynniki osobowe osób fizycznych, takie jak m.in. sytuacja ekonomiczna, zdrowie, osobiste preferencje, zachowania, przemieszczanie się, zadłużenie, styl życia oraz czy przetwarzanie odbywa się w sposób zautomatyzowany, tj. w procesie nie występuje znaczący czynnik ludzki dokonujący dalszej oceny i mający na nią wpływ?

Informacja do osoby, której dane dotyczą o fakcie profilowania oraz jego konsekwencjach

Obowiązek informowania spoczywa na administratorze niezależnie od tego, czy celem profilowania jest wyłącznie analiza, prognoza czy też przypisanie prawdopodobieństwa wystąpienia jakiejś cechy. Wymagają tego zasady rzetelnego i przejrzystego przetwarzania danych osobowych. Osobę, której dane dotyczą należy poinformować – zgodnie z motywem 60 RODO – o fakcie profilowania oraz jego konsekwencjach. Obowiązki te należy spełnić niezależnie od podstawy prawnej przetwarzania.

W zakresie profilowania w oparciu o dane wrażliwe, przed rozpoczęciem przetwarzania danych, administrator powinien zweryfikować, czy do profilowania wykorzystywane są dane wrażliwe, tj. ujawniające np. pochodzenie rasowe czy dane biometryczne. W przypadku profilowania w celach marketingowych z wykorzystaniem danych wrażliwych, konieczne wydaje się pozyskanie zgody na taki proces, niezależnie czy wynikiem profilowania jest podjęcie decyzji mającej istotny wpływ na osobę.

Jeżeli dane wrażliwe są przetwarzane, w szczególności może istnieć konieczność pozyskania wyraźnej zgody na takie przetwarzanie.

W zakresie istotnego wpływu na osobę fizyczną, jeżeli administrator, podejmuje decyzję w wyniku zautomatyzowanego przetwarzania danych, w tym profilowania, powinien sprawdzić czy taka decyzja wywołuje wobec osoby, której dane dotyczą, skutki prawne lub w istotny sposób na nią wpływa. Oznacza to, że decyzja musi mieć potencjalnie istotny wpływ na okoliczności, zachowanie lub wybory dokonywane przez zainteresowane jednostki. W ekstremalnych przypadkach, decyzja taka może prowadzić do wykluczenia lub dyskryminacji osoby, której dane dotyczą. Administrator musi mieć na względzie, że osoba, której dane dotyczą, ma prawo do tego, by nie podlegać takim decyzjom.

W zakresie prawa do interwencji ludzkiej i innych praw, należy wskazać, że RODO wyposaża podmiot, którego dane dotyczą w prawo do uzyskania interwencji ludzkiej ze strony administratora, do wyrażenia własnego stanowiska i do zakwestionowania podjętej decyzji (art. 22 ust. 3 RODO) wywołuje istotne skutki dla osób fizycznych. TMPL ma obowiązek zapewnić podmiotowi danych łatwy sposób realizacji tych praw, np. podjęcie działań w wyniku skierowania skargi przez klienta/potencjalnego klienta, kontaktu z infolinią.

Sprzeciw wobec przetwarzania dotyczących jej danych osobowych, w tym profilowania

Niezależnie od prawa niepodlegania decyzji na podstawie zautomatyzowanego przetwarzania danych, która istotnie wpływa na osobę, podmiot danych, którego dane dotyczą ma też prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jego szczególną sytuacją – wobec przetwarzania dotyczących go danych osobowych, w tym profilowania, jeżeli podstawą takiego przetwarzania jest: niezbędność do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

lub niezbędność do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią (np. marketing). Osobę, której dane dotyczą, należy wyraźnie poinformować o przysługującym jej prawie do sprzeciwu, o którym mowa w art. 21 ust. 1 i 2 RODO, przedstawiając te informacje w jasny sposób i odrębnie od wszelkich innych informacji (art. 21 ust. 4 RODO). Administratorzy muszą zapewnić, by informacje o tym prawie były zamieszczone w widocznym miejscu na ich stronach internetowych i/lub w każdej innej istotnej dokumentacji oraz by nie zostały one ukryta wśród innych warunków

Jeżeli dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo wnieść sprzeciw w dowolnym momencie wobec takiego przetwarzania, w tym wobec profilowania, w zakresie, w jakim związane jest z marketingiem bezpośrednim. Jeżeli osoba, której dane dotyczą, wniesie sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, danych osobowych nie wolno już przetwarzać do takich celów. (art. 21 ust. 2 RODO).

W zakresie obowiązków informacyjnych związanych z przypadkami zautomatyzowanego podejmowania decyzji w tym profilowania, administrator jest zobowiązany poinformować osobę, której dane dotyczą, zgodnie z art. 13 – 15 RODO, o:

a) Fakcie zautomatyzowanego podejmowania decyzji, w tym o profilowaniu,
b) Istotnych informacjach o zasadach ich podejmowania, które powinny obejmować, informacje wykorzystane w procesie zautomatyzowanego podejmowania decyzji, w tym kategorie danych użytych do profilowania,
c) Źródło tych informacji, wskazanie w jaki sposób profil użyty w procesie zautomatyzowanego podejmowania decyzji został zbudowany,
d) Wskazanie dlaczego dany profil jest istotny dla zautomatyzowanego podejmowania decyzji, wskazanie w jaki sposób dany profil jest używany do podejmowania decyzji dotyczących podmiotu, o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Dodatkowe obowiązki związane ze zautomatyzowanym przetwarzaniem danych

Niezbędne jest zapewnienie rzetelności i przejrzystości zautomatyzowanego podejmowania decyzji wobec osoby, której dane dotyczą. Należy stosować odpowiednie matematyczne i/lub statystyczne procedury profilowania, wdrożyć środki techniczne i organizacyjne zapewniające w szczególności korektę nieprawidłowości w zakresie przetwarzania danych osobowych i maksymalne zmniejszenie ryzyka błędów, zabezpieczyć dane osobowe w sposób uwzględniający potencjalne ryzyko dla interesów i praw osoby, której dane dotyczą, oraz w sposób zapobiegający m.in. skutkom w postaci dyskryminacji lub skutkujący środkami mającymi taki efekt.

W przypadku systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną, istnieje obowiązek przeprowadzenia procesu oceny skutków przetwarzania dla ochrony danych (PIA). (art. 35 ust. 3 lit a) RODO).

Monitoring danych osobowych pracowników

Autorzy: Bartosz Marcinkowski, Robert Brodzik

Uwagi wprowadzające

Zagadnienie monitorowania pracowników i ich danych stanowi od wielu lat istotny punkt regulacji i praktyki stosowania przepisów z dziedziny prawa pracy na styku z zagadnieniami z zakresu ochrony danych osobowych.

Problematyka prawnopracownicza w tym ujęciu ma, z uwagi na nierówność stron stosunku pracy, znaczenie wyjątkowe. Stąd przepisy regulujące stosunki pomiędzy pracodawcą a pracownikiem mają w pierwszym rzędzie niwelować ów brak równowagi.

Na tle tych uwag wprowadzających na szczególna uwagę zasługują ostatnie zmiany w kodeksie pracy, mające na celu ułatwienie stosowania RODO, w tym dotyczące monitoringu, podstaw jego prowadzenia oraz związanych z nim obowiązków[14].

Monitoring i jego odmiany

W ujęciu normatywnym monitoring występuje najczęściej w kontekście regularnej i systematycznej obserwacji (w tym kontroli), prowadzonej w sposób metodyczny przy zastosowaniu określonych urządzeń technicznych.

Ani przepisy RODO, ani przepisy kodeksu pracy nie zawierają definicji monitoringu ani zamkniętego katalogu form monitoringu.

Kodeks pracy wsk azuje przykładowe rodzaje (formy) monitoringu, tj.:

a) monitoring w znaczeniu wąskim (monitoring wizyjny – art. 22^2 kodeksu pracy),
b) monitoring poczty elektronicznej (art. 23^3 kodeksu pracy),
c) inne formy monitoringu (art. 23 §4 kodeksu pracy).

Owe inne formy monitoringu – np. monitoring GPS, monitoring aktywności w systemie komputerowym, monitoring wejść/wyjść) są prawnie dopuszczalne, o ile są „niezbędne do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwe użytkowanie udostępnionych pracownikowi narzędzi pracy" (art. 23^3 §4 kodeksu pracy). Tym sposobem można uznać, że o dopuszczalności stosowania monitoringu przesądza cel jego prowadzenia[15].

Podstawy monitorowania

Polski ustawodawca zdecydował się skorzystać z możliwości dopuszczonej art. 88 RODO, wprowadzając szczegółowe przepisy krajowe dotyczące sfery zatrudnienia.

14 Ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 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. 2019 poz. 730).

15 Jak orzekł Europejski Trybunał Praw Człowieka w wyroku nr 62617/00 z dnia 3 kwietnia 2007 r. w sprawie Lynette Copland przeciwko Wielkiej Brytanii, stosowane środki powinny być adekwatne i proporcjonalne do zamierzonego celu, co podlega kontroli w przypadku ewentualnych sporów z pracownikami (*Lynette Copland* vs. UK, 62617/00).

RODO zastrzega, iż przepisy wewnętrzne winny zapewniać poszanowanie godności pracownika, jego prawnie uzasadnionych interesów i praw podstawowych, w szczególności poprzez zapewnienie przejrzystości przetwarzania.

Szczególną pozycję w regulacjach prawnopracowniczych w dziedzinie ochrony danych osobowych zajmują przepisy dotyczące monitoringu pracowników, co wynika zarówno ze specyfiki stosunków zatrudnienia (brak równowagi stron), jak i z powszechności wszelkiego rodzajów monitoringów.

Na gruncie art. 22^2 kodeksu pracy, monitoring w znaczeniu wąskim (monitoring wizyjny) może być prowadzony przez pracodawcę w zakresie, w jakim jest to niezbędne do:

a) zapewnienia bezpieczeństwa pracowników
b) ochrony mienia,
c) kontroli produkcji,
d) zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę.

Z kolei monitoring poczty elektronicznej i inne formy monitoringu można stosować, gdy jest to niezbędne do zapewnienia:

a) organizacji czasu pracy umożliwiającej pełne wykorzystanie czasu pracy,
b) właściwego użytkowania udostępnionych pracownikowi narzędzi pracy.

Jak się wydaje, niezbędność stosowania monitoringu dla realizacji wskazanych celów (a nie np. przydatność) będzie w praktyce kwalifikowała daną formę monitoringu jako dopuszczalną.

Transparentność

Nowelizacja kodeksu pracy nie tylko określiła podstawy prowadzenia monitoringu, ale nałożyła na pracodawców szereg dodatkowych obowiązków, mających na celu zapewnienie przejrzystości przetwarzania danych osobowych pracowników.

Pracodawca rozpoczynając monitoring lub zmieniając jego cel, zakres lub sposób prowadzenia, dokonuje tego w układzie zbiorowym pracy lub w regulaminie pracy, alternatywnie – w obwieszczeniu (jeżeli pracodawca nie jest objęty układem zbiorowym pracy, ani nie jest obowiązany do wprowadzenia regulaminu pracy). W tym wewnątrz zakładowym akcie pracodawca określa cele, zakres oraz sposób stosowania monitoringu.

Ponadto, pracodawca informuje pracowników o zastosowaniu danej formy monitoringu nie później niż na 2 tygodnie przed uruchomieniem monitoringu, w sposób przyjęty w zakładzie pracy, np. poprzez informację zamieszczoną w intranecie lub zakładowej tablicy ogłoszeń. Ponadto, każdorazowo przed dopuszczeniem pracownika do pracy, pracodawca podaje mu na piśmie informacje o celach, zakresie i sposobie prowadzenia monitoringu.

Oprócz tego, pracodawca obowiązany jest oznaczyć monitorowane pomieszczenia i teren w sposób widoczny i czytelny, za pomocą odpowiednich znaków (np. piktogramów) lub ogłoszeń dźwiękowych. Winno to nastąpić nie później niż jeden dzień przed uruchomieniem monitoringu.

Wyłączenia i retencja

Spod monitoringu, co do zasady, wyłączone są pomieszczenia sanitarne, szatnie, stołówki, palarnie. W przypadku tych pomieszczeń można zastosować monitoring wizyjny pod warunkiem, że nie naruszy on godności, praw lub innych dóbr osobistych pracownika, co w szczególności można osiągnąć przez zastosowanie technik uniemożliwiających rozpoznanie osób (pseudonimizacja). W przypadku pomieszczeń sanitarnych (np. łazienek) wymagana jest uprzednia zgoda zakładowej organizacji związkowej, a w przypadku jej braku –przedstawicielstwa pracowników. Z możliwości zastosowania monitoringu wizyjnego całkowicie są wyłączone pomieszczenia udostępnione zakładowej organizacji związkowej.

Nagrania obrazu uzyskane poprzez monitoring pracodawca może przechowywać przez okres nieprzekraczający 3 miesięcy od dnia nagrania. Wydłużenie tego okresu możliwe jest w przypadku, w którym nagrania stanowią przedmiot postępowania lub pracodawca powziął wiadomość, że mogą taki przedmiot stanowić (zatem wszczęcie postępowania nie jest warunkiem koniecznym). W takiej sytuacji zapisy z monitoringu wizyjnego są przechowywane do prawomocnego zakończenia postępowania, np. w sprawie o kradzież mienia pracodawcy.

Poczta elektroniczna i inne formy monitoringu

Pracodawca jest uprawniony do tego, aby prowadzić monitoring poczty elektronicznej. Nie może on jednak naruszać tajemnicy korespondencji ani innych dóbr osobistych pracownika. Wobec powyższego w praktyce spotykane bywa ograniczenie do korzystania z poczty służbowej wyłącznie do celów służbowych.

> **Należy pamiętać, że ocena dopuszczalności prowadzenia danej formy monitoringu wymaga odniesienia do konkretnego przypadku oraz kontekstu, w którym ważony jest cel monitoringu oraz jego niezbędność.**

Przy przeprowadzaniu oceny dopuszczalności monitoringu należy wziąć pod uwagę m.in. charakter prowadzonej działalności pracodawcy, zakres monitorowanych danych oraz stanowisko pracy pracownika objętego monitoringiem. Jednocześnie ocenie podlega niezbędność danej formy monitoringu, tj. czy cel (np. użytkowanie udostępnionych pracownikowi narzędzi pracy) może zostać zrealizowany przy użyciu alternatywnych, mniej inwazyjnych środków.

Przetwarzanie danych osobowych pracowników na rynku ICT

Autorzy: Monika Wieczorek, radca prawny i adw. Michał Kibil, Kibil i Wspólnicy

Na przestrzeni ostatnich lat jesteśmy świadkami trwającej rewolucji cyfrowej. Największymi jej beneficjentami są firmy z sektora IT/ICT wytwarzające i wykorzystujące rozwiązania oparte na nowych technologiach, pozwalające im osiągać dotąd niedostępny wykładniczy wzrost rozwoju (nierzadko korelowany z prawem Moore'a). Co można zaobserwować na rynku, wzrost zapotrzebowania na technologię, pomimo stosowanych automatyzacji i robotyzacji skutkuje systematycznym wzrostem zapotrzebowania na wykwalifikowanych pracowników z obszaru IT, których liczba nie wzrasta już wykładniczo. Między innymi z tego względu, w ostatnich latach w sektorze IT/ICT zauważalna jest coraz większa konkurencja w walce o wykwalifikowanego pracownika, co jednocześnie sprzyja zwiększaniu konkurencji w oferowanych warunkach pracy. Wszystkie te czynniki prowadzą do dynamicznych zmian w obszarze HR, gdzie obok pracowników, z którymi zawierane są umowy o pracę nie tylko coraz częściej wykorzystuje się alternatywne formy zatrudnienia (takie jak podejmowanie współpracy w modelu B2B, pozwalającym zaproponować wyższe wynagrodzenie netto przy tym samym koszcie brutto dla firmy), ale też korzysta się z zewnętrznych firm dostarczających wykwalifikowanej siły roboczej, pod dany kontrakt, bądź do bieżącego wsparcia.

Z raportu z badania branży IT w 2019 r. przygotowanego przez portal Bulldogjob[16] wynika, że aż 44% osób „zatrudnionych" w IT podejmuje współpracę z firmą na innej podstawie niż na umowie o pracę. Z kolei z raportu „Rynek usług IT w Polsce 2015" przygotowanego przez ABSL[17] wynika, że udział kontraktorów w całkowitym zatrudnieniu w firmach świadczących usługi IT (z uwzględnieniem personelu zewnętrznego dostarczanego przez agencje HR i partnerów outsourcingowych) wynosi aż 58%.

Wskazane zmiany w formach podejmowania współpracy z personelem, mają niebagatelne znaczenie dla wielu szczegółów, które powinny być uwzględniane przy zatrudnianiu (niejako wpisanych w stosunek pracy, a przy umowach cywilnoprawnych wymagających doprecyzowani) – w tym m.in. kwestii przekazywania praw autorskich, zasad zachowania poufności, ograniczania działalności konkurencyjnej, czy też właśnie zasad przetwarzania danych osobowych zarówno kontraktora przez organizację, jak i tych którymi organizacja administruje przez kontraktora. Przyjrzyjmy się czemu należy poświęcić największą uwagę w tym obszarze, z uwzględnieniem doświadczeń wdrożeniowych po roku obowiązywania RODO.

Kto jest administratorem a kto processorem w relacjach pracowniczych?

Co zostało wskazane powyżej, przy współpracy tak z pracownikami, jak i z kontraktorami (tak z tymi z którymi podejmujemy współpracę bezpośrednio jak i z tymi, z którymi współpracujemy za pośrednictwem zewnętrznego podmiotu) niezwykle istotną kwestią jest prawidłowe ukształtowanie zasad przetwarzania danych osobowych tak poszczególnych członków personelu, jak i danych osobowych, które powierzono danej organizacji do przetwarzania przez jej klientów.

Na gruncie art. 4 RODO administratorem danych osobowych (dalej jako **Administrator**) będzie każdy podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. W praktyce Administratorem będzie ten kto zbiera i przetwarza wedle własnego uznania (w granicach tego do czego jest uprawniony) dane osobowe osób trzecich. Administratorem z kolei nie będzie podmiot którego dane dotyczą, podmiot przetwarzający (processor) czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe.

16 Źródło: Raport z Badania Branży IT, Bulldogjob, 2019 – https://bulldogjob.pl/it_report_2019, dostęp 6.05.2019 r.
17 Źródło: Raport Rynek Usług IT w Polsce 2015, ABSL – https://absl.pl/wp-content/uploads/2016/10/raport_it_2015_PLv151210.pdf, dostęp: 30.04.2019 r.

W relacjach pracowniczych, to kto jest Administratorem nie będzie budzić wątpliwości. Administratorem danych pracownika oraz (w zdecydowanej większości przypadków) danych, do których pracownik ma dostęp, będzie pracodawca. Dla zachowania wszystkich wymogów poprawności przetwarzania danych pracownika i tych do których pracownik będzie miał dostęp (o czym będzie mowa w dalszej części raportu) konieczne będzie jedynie przygotowanie stosownych upoważnień wewnątrz organizacji, bądź umów powierzenia, gdy dane pracownika będziemy przekazywali podmiotom zewnętrznym (np. biuru księgowemu). Pozostałe zasady przetwarzania danych pracownika wynikać będą wprost z poszczególnych przepisów Kodeksu pracy. Sytuacja nieco się komplikuje przy współpracy z kontraktorem prowadzącym jednoosobową działalność gospodarczą, gdzie będziemy mieli do czynienia z inną podstawą przetwarzania danych (co będzie wymagać szczegółowego dookreślenia zasad przetwarzania danych osobowych w umowie B2B). Odrębną i najbardziej skomplikowaną na gruncie przetwarzania danych osobowych, relacją będzie przypadek korzystania przez firmę z personelu dostarczanego przez podmioty trzecie.

W ostatnim ze wskazywanych powyżej przypadków, firma outsourcingowa bezsprzecznie funkcjonuje w roli Administratora dla danych osobowych jej personelu. To czy firma korzystająca z jej usług (do której personel de facto jest delegowany) będzie funkcjonowała w roli drugiego Administratora (czego nie należy mylić ze współadministrowaniem danymi osobowymi), czy też processora będzie uzależnione od konkretnych zapisów w umowie pomiędzy stronami.

Jako, że to Administrator jest tym podmiotem, który nie tylko ponosi odpowiedzialność za przetwarzanie danych, ale także ma prawo podejmować wszelkie decyzje w obszarze przetwarzania danych (w tym nadawać i cofać upoważnienia), w interesie organizacji jest takie ukształtowanie relacji z firmą delegującą pracowników, aby to faktycznie organizacja funkcjonowała jako Administrator (chociażby po to, żeby nie mogła być pozbawiona prawa przetwarzania danych części personelu).

Jakie dane można zbierać od kandydata, pracownika i kontraktora?

Bezsprzecznie dane osobowe pracownika, zleceniobiorcy, wykonawcy dzieła, a także jak wskazuje Prezes Urzędu Ochrony Danych Osobowych, dane kontraktora (pomimo ich wpisu w CEIDG) stanowią dane osobowe przetwarzane przez organizację zatrudniającą daną osobę.

Chociaż najczęściej pracownicy nie różnią się w swoich obowiązkach od kontraktorów (za wyjątkiem innych zasad rozliczania czasu pracy/usług oraz nadzoru), to w zakresie ochrony danych osobowych pojawiają się wyraźne różnice w sposobie zarządzania danymi tych grup personelu.

W przypadku pracowników zatrudnionych w pracowniczych formach zatrudnienia, zasady przetwarzania danych osobowych wydają się być w pełni klarowne. Od 4 maja 2019 r., na skutek uchwalenia przepisów sektorowych, obowiązuje zmieniony art. 22^1 k.p., zgodnie z którym pracodawca żąda od kandydata do pracy podania następujących danych osobowych:

I) imię (imiona) i nazwisko;
II) datę urodzenia;
III) dane kontaktowe wskazane przez taką osobę
IV) wykształcenie;
V) kwalifikacje zawodowe;
VI) przebieg dotychczasowego zatrudnienia

przy czym informacji, o których mowa w pkt. 4-6 jedynie wtedy, gdy jest to niezbędne do wykonywania pracy określonego rodzaju lub na określonym stanowisku.

To nie wszystkie dane osobowe, jakie może przetwarzać pracodawca. Kolejnym etapem jest zbieranie danych już nie od kandydata, a od pracownika. Na mocy art. 22^1 § 3 k.p. katalog tych danych obejmuje:

I) adres zamieszkania;
II) numer PESEL, a w przypadku jego braku – rodzaj i numer dokumentu potwierdzającego tożsamość;
III) inne dane osobowe pracownika, a także dane osobowe dzieci pracownika i innych członków jego najbliższej rodziny, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy;
IV) wykształcenie i przebieg dotychczasowego zatrudnienia, jeżeli nie istniała podstawa do ich żądania od osoby ubiegającej się o zatrudnienie;
V) numer rachunku płatniczego, jeżeli pracownik nie złożył wniosku o wypłatę wynagrodzenia do rąk własnych.

Zbieranie innych danych od kandydata lub pracownika jest możliwe wyłącznie, gdy jest to niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa. Pracodawca jest zatem ograniczony nie tylko ogólną zasadą minimalizacji danych, ale także precyzyjnymi w tym względzie przepisami kodeksu pracy.

Przy planowaniu współpracy z kontraktorami realizacja zasady *privacy by design* będzie przebiegała inaczej niż w przypadku pracowników. Tu nie istnieją przepisy na poziomie ustawowym, a jedyną, chociaż obszerną wskazówkę stanowią przepisy RODO, a w szczególności art. 5 ust. 1 lit. c RODO, z którego wynika zasada minimalizacji danych przewidująca, że dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane. W praktyce przypadku kontraktorów w celu zawarcia i wykonywania umowy za adekwatne i celowe uznać należy przetwarzanie imienia, nazwiska, firmy pod jaką prowadzi działalność gospodarczą, adresu prowadzenia działalności gospodarczej oraz numeru NIP, jak również numeru telefonu lub adresu e-mail – tych ostatnich w celu zapewnienia prawidłowego wykonywania umowy przy założeniu komunikacji tymi kanałami.

Pracownicy i kontraktorzy – czy taki sam obowiązek informacyjny?

Nie ulega wątpliwości, że dane osobowe powinny być przetwarzane w sposób zapewniający im odpowiednie bezpieczeństwo i poufność, w tym ochronę przed nieuprawnionym dostępem do nich (tak motyw 39 RODO), bez względu na rodzaj stosunku prawnego łączącego administratora i podmiot danych. Dane pracowników i kontraktorów powinny zatem być chronione według jednolitych standardów. Różnice w realizacji przez pracodawcę wymogów wynikających z RODO pojawiają się natomiast na etapie wykonywania obowiązku informacyjnego, o którym mowa w art. 13 RODO. Realizacja tego obowiązku powinna polegać na poinformowaniu osoby, której dane dotyczą już podczas pozyskiwania danych o:

I) tożsamości i danych kontaktowych administratora oraz, gdy ma to zastosowanie, tożsamości i danych kontaktowych swojego przedstawiciela; a gdy ma to zastosowanie także danych kontaktowych inspektora ochrony danych;
II) celach przetwarzania danych osobowych oraz podstawie prawnej przetwarzania;
III) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) – o prawnie uzasadnionych interesach realizowanych przez administratora lub przez stronę trzecią;
IV) o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;

V) gdy ma to zastosowanie – o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony, a w określonych przypadkach o odpowiednich lub właściwych zabezpieczeniach oraz o sposobach uzyskania kopii tych zabezpieczeń lub o miejscu ich udostępnienia,

VI) okresie retencji danych,

VII) prawach przysługujących jednostce oraz prawie wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych,

VIII) o prawie cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem – jeżeli przetwarzanie odbywa się na podstawie zgody,

IX) tym, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;

X) o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu.

Ten szeroki katalog informacji, jakie należy podać już w momencie zbierania danych wymaga precyzyjnego określenia wszystkich etapów przetwarzania danych – począwszy od ustalenia celu i określenia podstawy prawnej, aż po wskazanie odbiorców danych, kończąc na sposobach określenia retencji danych. Inaczej jednak będzie wyglądała realizacja obowiązku informacyjnego w stosunku do pracowników i inaczej w stosunku do kontraktorów. Inny bowiem jest zakres informacji, jakimi dysponuje pracodawca. Różnice widać już na poziomie określenia celu przetwarzania danych – w stosunku do pracownika pracodawca będzie przetwarzał dane związane z rozliczeniem wynagrodzenia i obsługą ubezpieczeń społecznych w celu rozliczenia umowy i na podstawie realizacji obowiązku prawnego ciążącego na administratorze. W stosunku do kontraktora obowiązek ten nie istnieje, gdyż kontraktor samodzielnie obsługuje zobowiązania publicznoprawne wynikające z umowy B2B. I chociaż pracodawca, a ściślej zamawiający lub usługobiorca będzie przetwarzał jego dane również w celu rozliczenia umowy i na podstawie realizacji obowiązku prawnego, to zakres przetwarzanych danych będzie zupełnie inny – będą to, przy uwzględnieniu zasady minimalizacji danych, wyłącznie dane kontaktowe i identyfikacyjne, w tym numer NIP, adres prowadzenia działalności gospodarczej i numer rachunku bankowego. Kontraktorów nie obejmują przy tym przepisy o prowadzeniu dokumentacji pracowniczej, w tym okresy jej przechowywania.

Wbrew często stosowanej praktyce przygotowywania jednej klauzuli informacyjnej dla całego personelu oraz wprowadzania do rejestrów czynności przetwarzania danych jednej kategorii personelu, w organizacjach podejmujących współpracę ze swoim personelem na wielu odmiennych podstawach prawnych (takich jak te z sektora IT/ICT) niezbędne wydaje się wyodrębnienie różnych kategorii podmiotów oraz konsekwentnie przygotowanie dla nich odmiennych wersji informacji i uwzględnienie wskazanych kategorii personelu w prowadzonych rejestrach czynności przetwarzania danych, z uwzględnieniem różnic m.in. w zakresie kategorii danych osobowych, celu i podstawy prawnej przetwarzania, okresu przechowywania danych oraz odbiorców danych.

Wszelkie informacje związane z przetwarzaniem danych osobowych, w tym informacje kierowane do osoby w ramach realizacji obowiązku informacyjnego powinny być łatwo dostępne i zrozumiałe oraz formułowane jasnym i prostym językiem (motyw 39 do RODO, art. 12 RODO). Doświadczenia wdrożeniowe z ostatniego roku pokazują zupełnie odmienną praktykę na rynku, w tym w sektorze ICT. Bardzo wiele komunikatów formułowanych jest skomplikowanym językiem bliższym aktom prawnym niż codziennej komunikacji międzyludzkiej. Należy pamiętać, że to na Administratorze (zgodnie z zasadą rozliczalności) będzie spoczywał ciężar wykazania, że komunikat był sformułowany obiektywnie jasnym i prostym językiem. Jak wskazują komentatorzy, za dobrą praktykę można przyjąć weryfikowanie przygotowanych tekstów z osobami trzecimi (test przeciętnego odbiorcy, tzw. test Kowalskiego)

niestykającymi się z przepisami dotyczącymi ochrony danych osobowych i upraszczanie przekazu aż do czasu, gdy żaden z weryfikujących nie będzie miał wątpliwości, o co w komunikacie chodzi, lub gdy zejdziemy do poziomu wątpliwości, których nie da się uniknąć[18].

Na co warto zwrócić uwagę, w szeregu organizacji można się spotkać z praktyką polegającą na stosowaniu dwóch równoległych kanałów komunikacji – informacje do klientów o przetwarzaniu ich danych osobowych w przeważającej większości są – tam gdzie jest to możliwe – przekazywane im drogą elektroniczną, natomiast obowiązek informacyjny w stosunku do pracowników jest najczęściej spełniany w zwykłej formie pisemnej. Z uwagi na treść art. 12 RODO należy jednak dopuścić możliwość ujednolicenia kanałów komunikacji obowiązku informacyjnego. Z przepisu tego wynika bowiem możliwość komunikowania informacji o przetwarzaniu danych osobowych tak w sposób pisemny, jak i elektroniczny. Rekomendowanym rozwiązaniem jest zatem przekazywanie personelowi informacji o przetwarzaniu danych osobowych związanych z zatrudnieniem (lub kontraktem) w powszechnie przyjęty w danym miejscu pracy sposób, np. przy użyciu intranetu lub używanych w miejscu pracy komunikatorów lub systemów CRM z zaimplementowanymi modułami komunikacji.

Upoważnienie czy umowa powierzenia przetwarzania danych?

Administrator, zasadniczo ma pełną swobodę w zakresie powierzania przetwarzania danych osobowych osobom i podmiotom trzecim. W zależności od sytuacji może to następować tak na gruncie zawarcia umowy powierzenia przetwarzania danych osobowych (gdy upoważniamy do przetwarzania processora) jak i na gruncie upoważnienia konkretnej osoby do dostępu do określonych danych osobowych. Co jest niezwykle istotne, każdy podmiot i każda osoba mająca dostęp do danych osobowych zarządzanych przez Administratora upoważnienie lub umowę powierzenia przetwarzania musi mieć. W innym wypadku Administrator może się narazić na zarzut udzielenia dostępu do danych osobowych podmiotowi/osobie nieuprawnionej.

Jak pokazało blisko roczne doświadczenie ze stosowaniem RODO, w przypadku relacji pracowniczych, ze względu na wcześniej wskazywane różne formy współpracy, które łączą nas z personelem nie zawsze jest jasne, czy należy zastosować upoważnienie czy przytaczaną umowę powierzenia przetwarzania danych osobowych.

Na gruncie RODO wyraźnie wyróżnia się dwie kategorie podmiotów przetwarzających dane w sposób zależny względem Administratora. RODO przytacza podmioty przetwarzające (dalej jako **Processorzy)** oraz osoby, które – z upoważnienia administratora lub Processora – mogą przetwarzać dane osobowe (dalej jako **Personel**). Można uznać, że podstawowym kryterium, oprócz brzmienia przepisów stanowiących o upoważnieniu i umowie na przetwarzanie danych osobowych, jest realny wpływ i podległość wobec administratora danych osobowych czy też podmiotu przetwarzającego.

Processora w RODO (art. 4) definiuje się jako osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora. Może on przetwarzać dane osobowe sam lub z innym podmiotem (ale tylko na podstawie wyraźnej ogólnej lub szczegółowej zgody Administratora). W relacji do Administratora funkcjonuje on jako podwykonawca, a tym samym podejmując samodzielne decyzje co do przetwarzanych danych, w zakresie uprawnienia do przetwarzania otrzymanego od Administratora, ponosi on odpowiedzialność względem Administratora oraz osób trzecich za swoje działania.

Odmienny jest charakter personelu działającego na podstawie upoważnienia. W tym przypadku przetwarzanie następuje w ramach działania Administratora lub Processora (Processor powinien nadać upoważnienia wszystkim członkom swojego zespołu mającym dostęp do powierzonych danych), a rola personelu jest stricte techniczna.

18 Maciej Gawroński, Michał Kibi RODO przewodnik praktyczne z wzorami (wyd. Wolters Kluwer 2018 r.)

Za działania upoważnionego Personelu pełną odpowiedzialność względem osób trzecich ponosi podmiot udzielający upoważnienia (Administrator lub Processor), a ewentualna odpowiedzialność Personelu względem tego kto udzielił upoważnienia będzie regulowana charakterem umowy podstawowej (umowy o pracę, umowy zlecenia etc.).

Tak jak dla osób współpracujących z organizacją na podstawie umowy o pracę, a także umowy zlecenia, czy też umowy o dzieło z osobą fizyczną, możliwość nadawania upoważnień nie powinna budzić wątpliwości (choć w przypadku umów zlecenia upoważnienie powinno zostać zastąpione przez umowę powierzenia przetwarzania danych osobowych jeżeli zleceniobiorca faktycznie korzystałby z jakichkolwiek podwykonawców), tak w przypadku współpracy z personelem w modelu B2B, który definicyjnie zakłada że jest to *zorganizowana działalność zarobkowa wykonywana we własnym imieniu i w sposób ciągły*[19] należy zarekomendować zawieranie umów powierzenia przetwarzania danych osobowych. Co należy wyraźnie podkreślić, na gruncie samego RODO (co potwierdza UODO w swoich wyjaśnieniach), w przypadku gdyby współpraca w modelu B2B miała faktycznie wymiar samozatrudnienia (realizacji usług tylko dla jednego klienta na zasadzie wyłączności) nie ma przeszkód do uznania kontraktora za członka personelu oraz nadania mu upoważnienia. Przy wskazanym temacie pojawiły się jednak w praktyce wątpliwości, czy nadanie upoważnienia nie wzbudzi przypadkiem wątpliwości organów kontrolnych (ZUS i US) co do tego czy współpraca z kontraktorem spełnia wszystkie przesłanki charakterystyczne dla modelu B2B i czy nie będzie to argument służący zakwestionowaniu tej formy współpracy. Umowa powierzenia przetwarzania w takiej sytuacji, z pewnością będzie lepiej zabezpieczać organizację.

Przy współpracy z podmiotami delegującymi do organizacji swoich pracowników i współpracowników, należy zachować szczególną czujność. Jako, że naszym faktycznym zleceniobiorcą nie jest osoba realizująca pracę, a jego pracodawca/zleceniodawca, to właśnie ten podmiot powinien być stroną umowy powierzenia przetwarzania danych osobowych i w zależności od sytuacji (czy deleguje do nas swoich kontraktorów czy też swój personel) powinien być odpowiednio upoważniony do zawierania umów podpowierzenia przetwarzania danych osobowych.

O czym Administrator powinien pamiętać, jego odpowiedzialność za naruszenia danych osobowych roztacza się także na działania podwykonawców i swojego personelu mającego dostęp do danych osobowych. Przy przygotowywaniu umów należy więc zachować szczególną uwagę, aby zagwarantować sobie w nich możliwość kontroli działań podwykonawcy, czy też przeniesienia na sprawcę finansowej odpowiedzialności za jego działania.

O czym Administrator powinien pamiętać, jego odpowiedzialność za naruszenia danych osobowych roztacza się także na działania podwykonawców i swojego personelu mającego dostęp do danych osobowych. Przy przygotowywaniu umów należy więc zachować szczególną uwagę, aby zagwarantować sobie w nich możliwość kontroli działań podwykonawcy, czy też przeniesienia na sprawcę finansowej odpowiedzialności za jego działania.

Realizacja praw jednostek

Na gruncie RODO nie ma znaczenia podstawa formy zatrudnienia w zakresie realizacji praw jednostek. W każdym przypadku wszystkie prawa jednostek (w tym m.in. prawo do informacji, prawo do sprostowania danych, czy też prawo do zapomnienia) powinny być tak samo respektowane. Organizacje będąc przeważnie przygotowanymi do obsługi zgłoszeń swoich klientów bagatelizują zgłoszenia otrzymywane od personelu. O czym należy pamiętać, w przypadku, gdy dane osobowe są przekazywane do działu kadr/HR, niezależnie od tego na jakiej podstawie zatrudnienia dana osoba podejmuje współpracę z organizacją, zgłoszenie dotyczące realizacji praw jednostki może być zgłoszone tym samym kanałem komunikacji. Aby mieć pewność, że prawa naszego personelu są respektowane, należy zweryfikować, czy działy personalne są przygotowane do odbierania tego typu zgłoszeń, nadawania im biegu oraz ich rozpatrywania, zgodnie z zasadami wynikającymi z RODO.

19 Zgodnie z art. 3 ustawy z dnia 6 marca 2018 r. Prawo przedsiębiorców

Edukacja w obszarze RODO

Autorzy: Monika Wieczorek i Michał Kibil

Z doświadczeń w stosowaniu RODO na przestrzeni ostatniego roku wynika, że wokół RODO narósł szereg mitów i niedoprecyzowań. Pomimo szeregu informacji przekazywanych przez Ministerstwo Cyfryzacji oraz Urząd Ochrony Danych Osobowych, osoby których dane osobowe dotyczą, nadal uważają, że jedyną prawidłową formą przetwarzania danych jest ich zgoda (co nierzadko powielają sami administratorzy danych opierając na zgodach całe przetwarzanie danych osobowych), wciąż uważa się że prawo do zapomnienia oznacza całkowite usunięcie wszystkich danych z systemów Administratora (pomimo szeregu wyłączeń i ograniczeń wskazanego prawa) czy też wciąż uważa się, że przygotowanie początkowego zestawu dokumentów jest wystarczające, aby pozostawać zgodnym z wymogami RODO.

RODOmity	
RODOmit	**Wyjaśnienie**
„Żeby ktoś przetwarzał moje dane osobowe musi uzyskać moją zgodę”	RODO wyróżnia wiele różnych podstaw przetwarzania takich jak umowa, prawny obowiązek, czy też uzasadniony interes administratora. Zgodę powinniśmy stosować tam, gdzie nie istnieje inna podstawa przetwarzania danych osobowych, czy też np. w przypadku, gdy jesteśmy zainteresowani kierowaniem do danej osoby informacji marketingowych drogą elektroniczną.
„IT nie przetwarza danych, ponieważ ich nie pozyskuje”	Pozyskiwanie danych osobowych jest tylko jednym z rodzajów przetwarzania danych osobowych. Oprócz pozyskiwania RODO wymienia także inne operacje na danych, które będą kwalifikowały się jako przetwarzanie danych, takie 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. Jeżeli więc wykonujemy którąś, lub któreś ze wskazanych operacji na danych osobowych to dane przetwarzamy, czyli musimy stosować się do przepisów o ich ochronie.
„Adres e-mail jest zawsze daną osobową”	Adres e-mail nie zawsze będzie daną osobową. Zależy to od tego, czy administrator może na podstawie adresu e-mail zidentyfikować konkretną osobę czy też nie. Niemniej jednak, ponieważ wszystkie adresy e-mail przeważnie przechowywane są w jednej bazie, rekomendujemy każdorazowo wskazany adres e-mail traktować jako daną osobową. Ułatwi to wdrażanie wymogów RODO dla całego zbioru danych.
„Każdy incydent dotyczący danych osobowych powinien być zgłoszony do Prezesa Urzędu Ochrony Danych Osobowych”	Wbrew powszechnym twierdzeniom, zgodnie z RODO zgłoszeniu podlegają wyłącznie takie incydenty, które skutkują ryzykiem naruszenia praw i wolności osób fizycznych np. jeśli naruszenie może prowadzić do kradzieży lub fałszowania tożsamości, straty finansowej, naruszenia dobrego imienia, czy też naruszenia tajemnic prawnie chronionych. Gdy dany incydent nie będzie skutkował takim ryzykiem (np. gdy zostanie przypadkowo zniszczony dysk, na którym znajdują się dane osobowe, ale w zasobach administratora znajduje się kopia wskazanych danych) nie będzie konieczne zgłaszanie incydentu.

Część ze wskazanych RODOmitów rzutuje na niepotrzebne dyskusje prowadzone w szczególności pomiędzy Administratorami a osobami, których wskazane dane osobowe dotyczą. Wskazane dyskusje niepotrzebnie angażują czas pracy zespołów oraz angażują przekładające się na to środki finansowe.

To co można zrobić, aby nie doprowadzać do wskazanej sytuacji to podjęcie przez poszczególnych Administratorów edukacji w obszarze RODO tak dla własnego personelu, który odpowiedzialny jest za relacje z osobami, których dane osobowe są przetwarzane, jak i edukacji samych klientów. Będąc przyzwyczajonymi do tego, że misja edukacji prawnej winna obciążać organy administracji, a nie prywatny sektor, nie zauważa się, że edukacja może rzeczywiście rzutować na późniejszej redukcji liczby zapytań, czy też potencjalnych sporów.

Należy założyć, że Administratorzy są w stanie ze wskazaną informacją o tym jak prawidłowo rozumieć RODO, dotrzeć do osób których dane osobowe przetwarzają, skuteczniej niż organy administracji. Jeżeli więc edukacja miałaby ograniczyć liczbę przypadków bezzasadnych zgłoszeń naruszenia przepisów o ochronie danych osobowych oraz zwiększyć przejrzystość działań Administratorów (czyli de facto doprowadzić do poprawy komunikacji w obszarze RODO na linii Administrator – podmiot danych osobowych), należy zadać sobie pytanie czy nie jest to przypadkiem warte rozważenia.

Ponieważ podstawą edukacji, jest zdefiniowanie obszarów, w których wskazana edukacja powinna być prowadzona, za cenne należy przyjąć zebranie zestawu problemów w branży IT/ICT ze stosowaniem RODO oraz odnotowanie pojawiających się RODO-mitów. Wskazany katalog mógłby zostać rozpoczęty od następujących kwestii, które na gruncie roku stosowania RODO zdają się wyraźnie wybrzmiewać jako problemy:

I) które z danych przetwarzanych przez Administratora nie są danymi osobowymi;
II) kto może przetwarzać nasze dane osobowe;
III) komu można przekazać nasze dane osobowe;
IV) na jakich podstawach przetwarzane są dane osobowe;
V) czym tak naprawdę skutkuje realizacja praw jednostek (m.in. jak daleki jest skutek skorzystania z prawa do zapomnienia).

Z chwilą skatalogowania problemów oraz RODOmitów, podmioty zainteresowane edukacją swoich klientów oraz zespołów powinny w miarę swoich możliwości, działając w szczególności w izbach gospodarczych takich jak PIIT, przyjąć jednolitą metodykę edukacyjną, tak aby przekaz kierowany przez nie na zewnątrz pozostawał spójny i generował więcej odpowiedzi niż dalszych pytań. Z pewnością jednym z elementów metodyki mogłoby być sporządzenie wspólnego słownika branżowego, które poszczególne pojęcia RODO definiował z uwzględnieniem specyfiki IT/ICT.

Finalnym krokiem mogłoby być przygotowanie samych materiałów, które tak jak informacje przygotowywane na gruncie RODO powinny być przejrzyste oraz zrozumiałe dla każdego odbiorcy.

Przy kompleksowym podejściu do procesu edukacyjnego, z pewnością można osiągnąć zamierzony sukces w postaci bardziej świadomych pracowników oraz lepiej poinformowanych klientów, co paradoksalnie powinno skutkować niezwiększeniem liczby skarg, a zredukowaniem tych skarg i sporów, które na gruncie samego RODO nie znajdują żadnych podstaw.

Przetwarzanie danych osobowych w chmurze obliczeniowej

Autorzy: Sylwia Stefaniak, Halszka Suszek-Borowska

Żyjemy w świecie, w którym duża część naszego życia toczy się w Internecie. Dotyczy to zarówno strefy prywatnej, jak i zawodowej. Wirtualna rzeczywistość sprzyja naszej pracy, robieniu zakupów czy załatwianiu spraw urzędowych. Trudno sobie wyobrazić powrót do czasów, w których nie mieliśmy takiej możliwości. Ilość danych które przetwarzamy stale rośnie, dlatego czasem potrzebujemy pomocy podwykonawców, którzy pomogą nam w realizacji celu, do którego zbieramy dane. Przykładem takiego działania może być chmura obliczeniowa. Dla niektórych może być to trudne do zrozumienia, ale warto wiedzieć, że chmura to poczta elektroniczna, aplikacje biurowe, bankowe, portale społecznościowe oraz inne platformy w Internecie począwszy od pracy, a na rozrywce kończąc. Krótko mówiąc wszelkie dane i pliki, które przetrzymujemy poza własną infrastrukturą (np. komputer, serwer) znajdują się w chmurze.

Dla przypomnienia warto w prostych słowach opisać trzy podstawowe modele. Osobie zajmującej się zagadnieniami związanymi z bezpieczeństwem i przetwarzaniem danych, pozwoli to lepiej zrozumieć zagadnienie i w adekwatny sposób wprowadzić odpowiednie wymagania co do stosowania tego modelu technologicznego – w tym określenia wymagań do zapisania w umowach z podwykonawcami. Chmura obliczeniowa jest świadczona w trzech wariantach:

I) Infrastruktura jako usługa (ang. Infrastructure as a Service – IaaS);
II) Platforma jako usługi (ang. Platform as a Service – PaaS);
III) Oprogramowanie jako usługi (Software as a Service – SaaS).

W modelu IaaS dostawca chmury udostępnia jedynie infrastrukturę, obsługuje ją, serwisuje oraz zabezpiecza. PaaS z kolei rozszerzony jest o odpowiednią platformę informatyczną, którą może być system operacyjny lub inne narzędzia, które pozwolą nam utworzyć własne oprogramowanie. Najpopularniejszym modelem jest SaaS, czyli kompletne gotowe do użycia rozwiązanie (to wymieniona wyżej platforma, ale z oprogramowaniem utworzonym przez dostawcę).

Wszystkie te warianty w obrazowy sposób można przedstawić na przykładzie klasycznego dziennika szkolnego. I tak na przykład IaaS to czysty nieuzupełniony zeszyt z pustymi kartkami, które możemy potem odpowiednio „oprogramować" w tabele. PaaS to ten sam zeszyt z gotowymi już tabelami. Ale w tym modelu to użytkownik decyduje, do jakiego celu będą one wykorzystane – bo przecież finalnie nie muszą być dziennikiem. SaaS to gotowy dziennik ze zdefiniowanymi tabelami. Naszym zadaniem jest już tylko wpisywanie uczniom ocen.

Nie wszystkie chmury są takie same i nie każdy rodzaj chmury obliczeniowej jest odpowiedni dla każdego. Oprócz powyższego podziału, należałoby jeszcze wspomnieć o trzech typach wdrożeń chmury: w chmurze publicznej, w chmurze prywatnej i w chmurze hybrydowej.

I) Chmury publiczne należą do zewnętrznych dostawców usług w chmurze (podmiotów przetwarzających), którzy je obsługują i dostarczają zasoby obliczeniowe, takie jak serwery i magazyn, za pośrednictwem Internetu. W przypadku chmury publicznej cały sprzęt, oprogramowanie i pozostała infrastruktura pomocnicza należą do dostawcy chmury i to on nimi zarządza. Dostęp do usług i zarządzanie kontem odbywa się przy użyciu przeglądarki internetowej.

II) Chmura prywatna to zasoby chmury obliczeniowej używane wyłącznie przez jedno przedsiębiorstwo lub jedną organizację (administratora danych osobowych). Chmura prywatna może się fizycznie znajdować w lokalnym centrum danych przedsiębiorstwa. Niektóre firmy płacą zewnętrznym dostawcom usług za hostowanie ich chmury prywatnej.

III) Chmury hybrydowe łączą chmury publiczne i prywatne z wykorzystaniem technologii pozwalającej na udostępnianie danych i aplikacji między nimi. Zezwalając na przechodzenie danych oraz aplikacji między chmurami prywatnymi i publicznymi, chmura hybrydowa zapewnia większą elastyczność i więcej opcji wdrażania.

Podsumowując – w chmurze przechowujemy zarówno prywatne informacje, jak i – gdy chodzi o przedsiębiorców – dane o naszych klientach, oprócz danych osobowych, również dane finansowe czy medyczne. Dlatego tak bardzo istotne jest, by wiedzieć, jak działa chmura, kto nią administruje i jakie warunki bezpieczeństwa gwarantuje. Wszystko po to, by móc wykazać się należytą starannością przed organem nadzorczym czy osobą fizyczną, której dane dotyczą.

Punktem startu przy sprawdzaniu wdrożenia RODO jest stwierdzenie, że nie mamy do czynienia z problemem prawnym, ani z problemem informatycznym. Wdrożenie RODO to zadanie menedżerskie, problem organizacyjny, wyzwanie dla zarządzających procesami biznesowymi, ludźmi i w końcu całą firmą. Systemy wykorzystywane przez firmę do tworzenia, przechowywania, analizowania i zarządzania danymi obejmują szeroką gamę środowisk informatycznych – urządzenia osobiste, serwery lokalne (*on-premise*), usługi chmurowe czy nawet Internet Rzeczy. Oznacza to, że większość rozwiązań informatycznych w firmie może podlegać wymaganiom RODO.

Najlepiej rozpocząć od holistycznej analizy wymagań w kontekście wszystkich obowiązków regulacyjnych i prawnych w zakresie ochrony danych osobowych i warto tę część działania wykonać przy zgodnej współpracy informatyków i prawników. Przykładem na konieczność takiej współpracy techników, biznesu i prawa niech będzie fakt, że wiele spośród mechanizmów zabezpieczających, mających na celu zapobieganie, wykrywanie i reagowanie na luki w systemach zabezpieczeń i naruszenia ochrony danych osobowych wymaganych na mocy RODO, będzie podobnych do mechanizmów zabezpieczających wymaganych przez inne regulacje. Możemy wówczas zastanowić się czy korzystając z faktu posiadania certyfikatu ISO/IEC 27001 czy ISO/IEC 22301 bądź wymagając podobnych i dodatkowych certyfikatów od podmiotów przetwarzających (np. chmurowych ISO/IEC 27017 i 27018) uzyskamy właściwy poziomu ochrony.

Zamiast śledzenia mechanizmów zabezpieczających wymaganych przez poszczególne standardy lub regulacje osobno, najlepsza praktyka polega na zidentyfikowaniu całego zbioru mechanizmów i funkcji zabezpieczających zapewniających spełnienie tych wymagań. Dlatego, zamiast dokonywania oceny poszczególnych technologii i rozwiązań pod kątem spełnienia wymagań tak kompleksowej regulacji jak RODO, lepszym podejściem może być oparcie się na platformie – celem łatwiejszego zapewnienia zgodności nie tylko z RODO, ale również spełnienia innych ważnych wymagań.

Zalecamy rozpoczęcie drogi do zapewnienia zgodności z RODO od skoncentrowania się na **czterech** kluczowych krokach:

I) Inwentaryzacja danych – identyfikacja, jakie dane osobowe znajdują się w firmie i gdzie są przechowywane.
II) Zarządzanie – określenie, w jaki sposób dane osobowe są wykorzystywane i udostępniane.
III) Ochrona – wprowadzenie mechanizmów zabezpieczających mających na celu zapobieganie, wykrywanie i reagowanie na luki w systemach zabezpieczeń i naruszenia ochrony danych osobowych.
IV) Raportowanie – podejmowanie działań w odpowiedzi na wnioski o udostępnienie danych, raportowanie naruszeń ochrony danych osobowych oraz prowadzenie niezbędnej dokumentacji.

Cztery powyższe kroki są całkowicie niezależne od tego, jaka technologia informatyczna jest wykorzystywana w firmie. To tylko jeszcze raz wskazuje, że wdrożenie RODO nie jest problemem technologicznym. Ponieważ jednak chcemy w niniejszym artykule zwrócić uwagę na wykorzystanie chmury obliczeniowej, stąd jeszcze jedna uwaga związana z powyższym. Skoro RODO jest naszym obowiązkiem, jego wymagania są niezależne od technologii, zaś o skuteczności wdrożenia będzie decydowało wdrożenie w firmie odpowiednich procesów związanych z wymaganiami rozporządzenia, to warto zadać sobie pytanie, kto jest za to wszystko odpowiedzialny. A także, czy możemy się tą odpowiedzialnością z kimś podzielić lub ograniczyć ryzyko.

Odpowiedzialność spoczywa na administratorze – to jest jasne. Czy możemy od dostawców oprogramowania, które zainstalujemy w naszej serwerowni zażądać, aby ich produkty spełniały wymagania RODO? Oczywiście! Ale ich odpowiedzialność zależy od tego, jak w firmie będziemy korzystać z ich produktów. Co więcej, nawet jeśli zapewnią niektóre mechanizmy związane z RODO (np. przenoszenie danych, powiadamianie o naruszeniach) to od nas w firmie będzie zależało powiązanie wszystkich takich systemów w całość oraz utrzymywanie ich w należytym stanie (np. poprzez dokonywanie oceny skutków dla ochrony danych). Dlatego warto kierować się starą zasadą znaną wszystkim zajmującym się cyberbezpieczeństwem. Im prostsza jest infrastruktura, tym łatwiej uzyskać wyższy poziom. A to mówi, że lepiej jest decydować się na infrastrukturę bazującą na jednolitej platformie. Kolejnym krokiem jest wykorzystanie takiej platformy, ale platformy chmurowej. Ponieważ to chmura – niejako niezależnie od tego jakie zasoby mamy w firmie – będzie nieustająco zmieniać się w kierunku coraz większego bezpieczeństwa oraz zgodności z wymaganiami regulacyjnymi. Dostawcy platform i rozwiązań chmurowych będą oferowali również narzędzia pozwalające łatwo uzyskać zgodność z RODO i innymi aktami prawnymi. Całkowitej odpowiedzialności administrator nigdy nie przeniesie na dostawcę technologii, ale wykorzystanie chmury przenosi jej część na dostawcę usługi, a samemu administratorowi w znaczący sposób ułatwia życie.

Perspektywa administratora danych i jego współpracy z podmiotem przetwarzającym

Nikogo już chyba nie dziwi, szczególnie w kontekście rozwoju społeczeństwa informacyjnego i gospodarki cyfrowej, że dane i zasoby informacyjne mają konkretną wartość, a w kontekście RODO – jest to bardzo duża odpowiedzialność finansowa. Administrator danych, oprócz tego, że jest odpowiedzialny za spełnienie zgodności z RODO, powinien dokonać oceny skutków ochrony danych, którego efektem będzie oszacowanie ryzyka przetwarzania danych i wdrożenie środków minimalizujących to ryzyko. Według motywu 81 RODO:

„administrator powinien, powierzając podmiotowi przetwarzającemu czynności przetwarzania, korzystać z usług wyłącznie podmiotów przetwarzających, które zapewniają wystarczające gwarancje – w szczególności, jeżeli chodzi o wiedzę fachową, wiarygodność i zasoby – wdrożenia środków technicznych i organizacyjnych odpowiadających wymogom niniejszego rozporządzenia, w tym wymogom bezpieczeństwa przetwarzania."

Dlatego też administrator danych powinien przy wyborze dostawcy usług chmurowych zadać kilka podstawowych pytań:

Czy moje dane są odpowiednio chronione?

Ważne jest, czy dostawca chmury (przetwarzający) jest w stanie wykazać, że stosuje zatwierdzone kodeksy postępowania lub zatwierdzone mechanizmy międzynarodowych certyfikacji, np. ISO/IEC 27001, standaryzujące system zarządzania bezpieczeństwem informacji (SZBI), lub ISO/IEC 27017 i ISO/IEC 27018 mówiące o SZBI i bezpieczeństwie danych osobowych w przypadku dostarczania usług chmurowych. Renomowani dostawcy chmurowi powinni wykazać się również szeregiem zabezpieczeń fizycznych, takich jak monitoring fizyczny (24/7/365), mechanizmy szyfrowania, ograniczenia dostępu do danych personelu, mechanizmy zabezpieczania przed złośliwym oprogramowaniem, itp.

Czy dane przetwarzane w chmurze nadal należą do administratora i czy może on je kontrolować?

Administrator danych powinien wiedzieć i mieć wpływ na to, gdzie dane się znajdują. RODO ogranicza możliwość swobodnego przekazywania danych z Europejskiego Obszaru Gospodarczego do państw trzecich. Ważne jest zatem, aby każda strona wiedziała i miała wpływ na to, gdzie dane się znajdują i jakie wymogi prawa ich obejmują. Warto wspomnieć, że RODO wymaga szybkiego przywracania danych w razie awarii oraz odtworzenia ich w tym samym stanie, w którym były przed jej wystąpieniem. Oczywiście, nie ma systemów, które w 100% nie są narażone na awarie i ataki cybernetyczne, niemniej jednak korzystanie z renomowanych i sprawdzonych dostawców znacznie zwiększa pewność dobrego zabezpieczenia danych i tym samym przestrzegania prawa. Tutaj za dobrą praktykę można uznać spełnianie standardów normy ISO/IEC 22301, która potwierdza ciągłość działania danego systemu.

Jakie zapisy powinny wystąpić w umowie z dostawcą?

Korzystanie z usług chmurowych to typowe powierzenie przetwarzania danych. Niemniej jednak wymaga to zawarcia umowy pomiędzy administratorem danych a podmiotem przetwarzającym. Według art. 28 ust. 3 RODO umowa a powinna zawierać wiele zobowiązań ze strony podmiotu przetwarzającego. W szczególności należałoby zwrócić uwagę na:

a) Odpowiednie klauzule, które pozwalają na przetwarzanie danych i zobowiązanie przetwarzającego o tym, że cały proces będzie odbywał się tylko według instrukcji przekazanych przez administratora w określonym obszarze gospodarczym (najlepiej, gdyby miejsce przetwarzania można samodzielnie wybrać).

b) Informacje na temat środków organizacyjnych i technicznych, w tym bardziej szczegółowy opis zabezpieczeń danego systemu. Środki te powinny wspomóc wywiązywanie się administratora danych z narzuconych przez RODO obowiązków dotyczących żądań osób fizycznych, tj. prawa do dostępu do własnych danych, żądania sprostowania i usuwania, ograniczenia ich przetwarzania, przenoszenia, prawa do sprzeciwu wobec zautomatyzowanego przetwarzania, w tym profilowania. Dodatkowo informacja na temat stosowanych mechanizmów i zabezpieczeń wspomaga administratora w ocenie skutków przetwarzania przy wykorzystaniu określonej technologii.

c) Informacje na temat mechanizmów powiadomień i stosowanych procedur w przypadku wystąpienia naruszenia systemu, które może skutkować naruszeniem danych osobowych.

d) Zapisy dotyczące zachowania poufności przez osoby, które mają (ograniczony) dostęp do przekazywanych danych.

e) Informacje na temat ewentualnych podprzetwarzających oraz zobowiązanie o przestrzeganiu przez nich tych samych zasad, które obowiązują przetwarzającego.

f) Klauzule dotyczące wykonywanych czynności i procedur związanych z zakończeniem usługi, tj. usuwania lub zwracania wszelkich danych oraz ich ewentualnych kopii.

g) Informacje na temat przeprowadzanych audytów i certyfikacji oraz możliwość wglądu w treść dokumentów poaudytowych.

Wymagania, które niesie ze sobą RODO wydają się być obszerne, ale tym samym oddają wielowymiarowy wpływ cyfryzacji na rzeczywistość, w której funkcjonujemy, a świadomość ryzyk, jakie wiążą się z wykorzystywaniem technologii cały czas pobudza twórców regulacji do ustanawiania adekwatnych przepisów prawa. Jurysdykcja europejska wpływa na bezpieczeństwo osób fizycznych i wymaga od administratorów danych osobowych wyboru wiarygodnych podmiotów przetwarzających, którzy są w stanie wywiązać się z obowiązków nałożonych na nich przez prawo. Chmura zyskała nowe znaczenie i na stałe zagościła w terminologii związanej z technologią i jej wpływem na transformację przedsiębiorstw. Dziś nikt nie pyta, czy warto, ale w jakim stopniu korzystać z chmury, by przyniosła profity dla organizacji. Nie ulega wątpliwości, że chmura to konieczność.

Tytuł: Trendy technologiczne a ochrona danych osobowych

Autorzy: Sylwia Stefaniak, Halszka Suszek-Borowska

W dzisiejszym świecie ludzie przyzwyczajają się do wygody i nie zauważają, że rozwiązania z których korzystają bazują na zaawansowanej technologii. Najczęściej mamy do czynienia ze sztuczną inteligencją, Internetem rzeczy, a także dość popularną technologią blockchain. Jakie wyzwania przed nami one stawiają? Czy są bezpieczne, czy też stanowią zagrożenie? A przede wszystkim, jakie stawiają przed nami wyzwania etyczne oraz prawne, zwłaszcza w kontekście zapisów Rozporządzenia o Ochronie Danych Osobowych.

Jesteśmy tuż po rewolucji związanej z ochroną danych osobowych. Tym bardziej powinniśmy mieć świadomość, jak nieumiejętne interpretowanie przepisów prawa może blokować nowe technologie. Ich dynamiczny rozwój skutkuje nowymi wyzwaniami w wymiarze etycznym i prawnym. Zanim jednak przejdziemy do dalszych rozważań, warto zadać sobie pytanie, czy w ogóle istnieje potrzeba uchwalenia nowej legislacji? Brak szczegółowych ram prawnych nie musi oznaczać, że działamy w próżni. Nowe technologie opierają się na ciągłej wymianie ogromnych zasobów danych. W związku z tym wyzwaniem technologicznym, niezwykle ważne jest przygotowanie takich regulacji, które chronić będą prywatność i zapewniać bezpieczeństwo bez blokowania innowacyjności. Tylko w ten sposób stworzymy podstawę zaufania do technologii, która już dziś napędza światową gospodarkę.

Nie jesteśmy w tej opinii odosobnione, ponieważ nawet Parlament Europejski oraz Europejski Komitet Ekonomiczno-Społeczny wskazują potrzebę zdefiniowania sztucznej inteligencji. Jak dotąd nie została wypracowana żadna konkretna definicja, jednakże samo rozpoczęcie tych rozważań pokazuje, jak bardzo ta kwestia jest pilna, biorąc pod uwagę tempo rozwoju nowych technologii.

Razem ze wzrostem ilości, rodzaju oraz sposobu wykorzystywania danych, w tym w szczególności danych osobowych, firmy mają coraz większy problem z określeniem zakresu odpowiedzialności. Kto w kontekście sztucznej inteligencji ma odpowiadać za końcowy wynik działań na danych? Administrator danych, programista, twórca algorytmu czy też maszyna? Dlatego też oprócz szeregu praw, w tym RODO, należy stworzyć ramy, według których każdy twórca czy też właściciel oprogramowania, będzie umiał odpowiedzieć, czy przetwarzanie danych w oprogramowaniu, jest etyczne i według jakich zasad się odbywa. Zakres przetwarzania danych osobowych może być najtrudniejszy do zdefiniowania w przypadku sztucznej inteligencji. Dzieje się tak ze względu na skomplikowane działania algorytmu, który daje wyniki oparte o jego samonauczanie. Czyli to, co się dzieje od początku do końca podczas działania danego oprogramowania może być niekiedy niemożliwe do wyjaśnienia.

Zacznijmy od początku i odpowiedzmy sobie na pytanie, czym jest sztuczna inteligencja, czyli tak zwane "AI" (ang. *artificial intelligence*). Termin ten jest obszerny i niekiedy wydawałoby się, że dość rozmyty, ponieważ większość programów komputerowych, które wykonują czynności wymagające ludzkiej inteligencji, można by uznać za systemy AI. Problem z zakwalifikowaniem do tej definicji pojawia się jednak wtedy, kiedy nie wiemy, czy już mamy do czynienia ze sztuczną inteligencją, czy jest to tylko wykonywanie operacji, np. analiz i wnioskowania, na dużych bazach danych. Samo uczenie maszynowe to sytuacja, w której nasze oprogramowanie wykonuje określone działania przy użyciu danych. Ale jeśli nasze oprogramowanie na podstawie tej określonej ilości danych jest w stanie samoistnie wyciągać wnioski, kiedy jest w stanie myśleć podobnie (albo nawet w bardziej zaawansowany sposób) jak ludzie – wówczas możemy mówić o sztucznej inteligencji. Oczywiście daleko nam do momentu, w którym nie będziemy w stanie odróżnić „sposobu bycia" człowieka od maszyny, ponieważ maszyny jeszcze długo nie będą w stanie nauczyć się inteligencji emocjonalnej, ale nic nie stoi na przeszkodzie, aby już teraz zastanawiać się, w jaki sposób maszyny powinny postępować, jakich zasad się trzymać i do jakich praw się dostosowywać.

Błyskawiczna analiza zdjęć wraz z dodatkowymi danymi z Internetu pozwala sprawdzić po etykiecie rodzaj kupowanej kawy, wskazać gatunek sfotografowanej rośliny, określić kaloryczność pokarmu czy znaleźć podobne produkty i ich ceny w różnych sklepach. Firmy na całym świecie już teraz wprowadzają bazujące na sztucznej inteligencji usługi, korzystając z danych zebranych z wielu źródeł. Marzenia, które jeszcze niedawno oznaczylibyśmy etykietą „science fiction" stają się rzeczywistością, a w przyszłości możemy liczyć jedynie na jeszcze szybszy wzrost innowacji. Postęp techniczny i globalizacja wciąż przynoszą nowe wyzwania w dziedzinie ochrony danych osobowych. Skala zbierania i wymiany danych osobowych wzrasta. Dzięki technologii zarówno przedsiębiorstwa prywatne, jak i organy publiczne mogą na olbrzymią skalę wykorzystywać dane osobowe w swojej działalności. Z drugiej strony osoby fizyczne coraz częściej udostępniają informacje osobowe publicznie. Technologia zmieniła gospodarkę i życie społeczne i powinna nadal ułatwiać swobodny przepływ danych osobowych w Unii oraz ich przekazywanie do państw trzecich i organizacji międzynarodowych, równocześnie zaś, przy uwzględnieniu Motywu 6 RODO, powinna zapewniać wysoki stopień ochrony danych osobowych. Jak zatem pogodzić rozwój technologiczny z ochroną danych? W świecie zaawansowanych technologii informatycznych, w świecie chmury obliczeniowej oraz wielkich zbiorów danych, słowo „zaufanie" nabiera nowego znaczenia. Skoro pojęcie sztucznej inteligencji nie zostało do tej pory zdefiniowane w wymiarze ustawodawczym, jak mamy budować i wdrażać skomplikowane rozwiązania oparte o sztuczną inteligencję, aby mimo wszystko budować zaufanie ich odbiorcy? Zespoły opracowujące oraz wdrażające rozwiązania, które wykorzystują sztuczną inteligencję w Microsoft, kierują się sześcioma kluczowymi zasadami, które są tak uniwersalne, że mogą stanowić wyznacznik odpowiedzialnego tworzenia technologii, a tym samym wspierać ciągłe budowanie zaufania. Te zasady to **sprawiedliwość**, **niezawodność, prywatność i bezpieczeństwo, inkluzywność, transparentność i rozliczalność**.

Technologia powinna traktować wszystkich sprawiedliwie

Podstawową zasadą przetwarzania danych osobowych, w szczególności danych wrażliwych, jest zapewnienie, że działania, które wykonujemy są **sprawiedliwe**. Oczywiście, w tej kategorii znajdują się pytania dotyczące legalności i podstaw przetwarzania, ale oprócz tego musimy przejść do głębszej analizy. Dobrym przykładem mogą być systemy przetwarzające dane medyczne w celach ubezpieczeniowych – prawidłowo zaprogramowany system powinien pomóc podejmować decyzje w sposób pozbawiony emocji i uprzedzeń. Musimy mieć jednak pewność, że nasz algorytm jest sprawiedliwy i jest zaprogramowany tak, że uzyskane wyniki nie są oparte na czyichś uprzedzeniach i że końcowa decyzja nikogo nie dyskryminuje. Należy zauważyć i pamiętać o tym, jak stereotypowe myślenie, a nawet kulturowe widzenie świata, może wpływać na wyniki analiz. W przypadku przetwarzania danych osobowych wielokrotnie widzieliśmy dyskusje na temat sposobu postrzegania prawa przez Europę, tego, jak różni się ona z wizją obywateli amerykańskich czy azjatyckich. Dlatego też trzeba zapewnić, aby próba danych, na których opieramy wstępne testy algorytmu, była różnorodna, a przyjęte techniki były w stanie wykryć i wyeliminować ewentualne uprzedzenia, które mogą być i najczęściej są przez nas nieuświadomione. Pozwoli to nam zapewnić, że wynik działania systemu daje porównywalne decyzje i wyniki dla osób różnych nacji, kultur, płci czy poglądów. Jest to swego rodzaju zagadnienie nie tyle etyczne, co wręcz filozoficzne – należy tu bowiem połączyć nie tylko prawo, ale również nasze poglądy kulturowe. Efektem powinno być uniwersalne podejście oparte także na wiedzy eksperckiej, której w żadnym przypadku nie można pominąć chociażby z konieczności czasowej weryfikacji tego, czego nasz algorytm się nauczył. Niejednokrotnie słyszeliśmy o sytuacjach, kiedy algorytmy na podstawie danych internetowych uczyły się rasizmu czy seksizmu i na tym opierały swoje wyniki. Dlatego też powinno się wracać do założeń wejściowych i sprawdzać, czy nasz algorytm po okresie przyswajania informacji nadal opiera się na takich samych wartościach, do których został stworzony.

Kto ponosi odpowiedzialność za (nie)zawodność systemu?

Podejście do **niezawodności** nie polega jedynie na tym, żeby dany program komputerowy działał bezawaryjnie. W tym miejscu organizacja musi sobie odpowiedzieć na szereg pytań w przypadku, kiedy oprogramowanie przestanie działać lub co więcej – ktoś na tym ucierpi. Powinniśmy zacząć od ustalenia czy firmy mają legalne podstawy do zbierania i przetwarzania danych, następnie zdefiniować to, kto jest odpowiedzialny za dane przetwarzane w oprogramowaniu, jak są one zapisywane i przechowywane – być może odpowiedzią na te pytania jest blockchain? To pomoże nam odpowiedzieć na kolejne pytania: kto ponosi odpowiedzialność w przypadku, gdy nowoczesne technologie padną ofiarą działań hakerów i zaczną działać w niewłaściwy sposób? Będzie to producent oprogramowania, producent sprzętu, twórca algorytmu czy osoba ustalająca dany cel, który jest realizowany (na przykład administrator danych)? Czy powinno się brać pod uwagę kraj producenta czy kraj, w którym produkt jest wykorzystywany? W przypadku przetwarzania danych osobowych obywateli Unii Europejskiej odpowiedź jest dość prosta, ponieważ ani lokalizacja, ani technologia nie mają większego znaczenia. Jeśli bowiem organizacja przetwarza takie dane, jest zobligowana do przestrzegania zapisów RODO. Zapisy Rozporządzenia dają dużą elastyczność wobec stosowanej technologii i potencjalnych kierunków rozwoju cyfrowej rzeczywistości, co może być widziane jako zaleta lub jako wyzwanie. Ale na pewno wiemy, że ostateczną odpowiedzialność ponosi administrator danych wykorzystujący daną technologię lub przetwarzający, który działa na jego zlecenie.

W przypadku omawiania danych osobowych zagadnieniem, które zasługuje na moment zastanowienia, jest realizacja wymaganego przez RODO „prawa do bycia zapomnianym". To sytuacja, w której użytkownik nie chce, aby jego dane były dłużej przetwarzane, ale co się wydarzy, jeśli system AI stwierdzi, że żądanie użytkownika jest niewłaściwe i zdecyduje zachować dane? Lub idąc dalej – wykorzysta je w celu dalszego rozwoju systemu bez naszego udziału i świadomości? Prawo będzie stało po stronie użytkownika, a więc twórcy systemów AI powinni pamiętać, że wymagania regulacyjne mają ogromny wpływ na systemy, które projektują i to, w jaki sposób przetwarzają one dane. Dlatego też analiza nie tylko danych wejściowych, ale analiza danych wyjściowych i tego, co dzieje się z nimi w międzyczasie jest tak istotna. Dane takie powinny być monitorowane przez cały czas ich przetwarzania. Ważne jest ciągłe testowanie i zapewnianie, że algorytm funkcjonuje „w duchu" założeń wstępnych. Tu kluczowym elementem będzie jednak człowiek, który dokona subiektywnej oceny i walidacji działania oraz sprawdzenia, czy forma, w której działa sztuczna inteligencja nadal jest zgodna z pierwotnie założonymi celami. To pomoże zauważyć nieoczekiwane okoliczności i nietypowe scenariusze niezgodne ze wstępnymi założeniami. Zdecydowanie ułatwi to działanie i określenie końcowej odpowiedzialności za ewentualne niepowodzenia.

„Prawo do bycia zapomnianym" wydaje się jeszcze większym problemem w przypadku blockchain, którego głównym założeniem jest nieusuwalność i nieedytowalność poszczególnych bloków łańcucha. Przy tworzeniu tego typu oprogramowania należałoby zadać sobie pytanie, czy obecne założenia RODO, które mówią o braku obowiązku usunięcia danych, kiedy ich przetwarzanie jest niezbędne do „ustalenia, dochodzenia lub obrony roszczeń", są wystarczające.

Ciekawym przykładem nieprawidłowego działania sztucznej inteligencji pozbawionej „nadzoru" człowieka może być system wspomagający podjęcie decyzji o hospitalizacji ludzi z zapaleniem płuc. Na podstawie otrzymanych danych ów system „dowiedział się", że osoby z astmą mają niższy wskaźnik śmiertelności z powodu zapalenia płuc w stosunku do ogółu populacji. Jest to zaskakujący wniosek, ponieważ takie osoby są uważane za bardziej zagrożone śmiercią w tym przypadku. Chociaż korelacja ta była potwierdzona danymi i ich analizą, system nie wykrył, że głównym powodem tego niskiego wskaźnika jest fakt, że właśnie z powodu zwiększonego ryzyka pacjenci cierpiący na astmę otrzymują szybszą i bardziej kompleksową opiekę. Gdyby naukowcy nie zauważyli, że program komputerowy wyciągnął mylące wnioski, system mógł nie zlecić hospitalizacji tych osób. Podkreśla to kluczową rolę ludzi i wiedzy eksperckiej w trakcie obserwowania sztucznej inteligencji podczas jej opracowywania i wdrażania.

Po pierwsze prywatność i bezpieczeństwo

W dzisiejszych czasach nasze życie coraz bardziej przenosi się do świata cyfrowego, co powoduje, że zagadnienia na temat zasad **prywatności i bezpieczeństwa** są trudniejsze do zdefiniowania. Głównym założeniem sztucznej inteligencji jest to, że ma ona nam pomóc podejmować decyzje między innymi na podstawie danych dotyczących ludzi. A co za tym idzie – ludzie muszą chcieć, aby te dane były przetwarzane w systemach AI, a to się nie wydarzy bez ich wewnętrznego przeświadczenia, że ich dane są chronione. Założeniem blockchain jest z kolei zapewnienie bezpieczeństwa i nienaruszalności danych w utworzonych blokach. Na chwilę obecną to właśnie RODO jest traktowane przez wielu jako swego rodzaju remedium w temacie przetwarzania danych osobowych. Przepisy Rozporządzenia nakładają na organizacje większe obowiązki, przyznając jednocześnie większe prawa osobie, której dane są przetwarzane. Dodatkowo wprowadzają także ograniczenia w zakresie międzynarodowego przepływu informacji, ale błyskawiczny rozwój technologii sprawia, że realizacja tych założeń staje się coraz trudniejsza.

Organizacje muszą pamiętać, że aby być skutecznym i przede wszystkim wiarygodnym podmiotem, muszą rozumieć zakres zbieranych i przetwarzanych danych. Wprowadzenie odpowiednich polityk bezpieczeństwa oraz rozwiązań chroniących prywatne i wrażliwe informacje z pewnością pomoże uniknąć problemów, które mogą wynikać z niedostosowania się do nowych przepisów, a także do wymagań, do których dopiero będziemy się dostosowywać. Dlatego aspekty prywatności i bezpieczeństwa to nie tylko to, co dziś robimy z danymi, ale też to, do czego te dane będą wykorzystywane przez następne lata. Zaawansowane rozwiązania związane z bezpieczeństwem muszą zapewnić organizacjom pełen wgląd w infrastrukturę systemu, umożliwić wdrożenie i zarządzanie usługami po to, aby mogły one zaplanować ewentualny rozwój tych systemów i nadal zachować kontrolę i legalność przetwarzania danych.

RODO daje obywatelom szansę umocnienia fundamentalnych praw do prywatności. Jednak zarówno ustawodawcy, jak i organizacje powinny działać szybko i sprawnie, aby dostosowywać się do rozwoju technologicznego, a także być gotowym na związane z nim zagrożenia. Oczywiście, kluczowa wydaje się być współpraca ustawodawcy z różnego rodzaju organizacjami nad zapewnieniem użytkownikom bezpieczeństwa i prywatności w cyfrowym świecie. Ale należy pamiętać, że w tym przypadku to wiedza rynkowa firm prywatnych będzie dawała odpowiedź na większość zadawanych pytań.

Likwidowanie barier

Wiele firm przykłada ogromną wagę do wykorzystywania systemów informatycznych do **inkluzywności** i likwidowania barier społecznych, co jest niezwykle istotne w przypadku osób z niepełnosprawnością. Większość twórców oprogramowania zdaje sobie sprawę z potrzeby dostosowywania ostatecznego wyglądu i funkcjonalności systemu tak, aby eliminowały bariery, które mogą omyłkowo wykluczyć niektórych ludzi.

Technologia będzie miała największy wpływ w tym obszarze, ponieważ już dziś istnieją aplikacje, które opisują osobom niewidomym to, co znajduje się przed nimi, czy też czytają to, co wyświetla się na ekranie komputera. Niezależnie od typu niepełnosprawności, w przypadku każdego człowieka największą zaletą sztucznej inteligencji będzie przewidywanie ewentualnych chorób czy stanów mentalnych. Czeski startup MidPax rozwinął system do monitorowania naszej aktywności w opaskach, które nosimy na ręku. Na podstawie tych danych są oni w stanie przewidzieć nadchodzące ataki schizofrenii czy też choroby afektywnej dwubiegunowej, co dla osób chorych może okazać się głównym czynnikiem likwidującym ich niedopasowanie i wykluczenie z życia społecznego. Z kolei MIT Media Lab wykorzystuje przetwarzanie sygnału w czasie rzeczywistym do tego, żeby z naszego głosu wyczytać to, w jakim nastroju jesteśmy, czy też na co chorujemy. Całkiem niespodziewanie okazuje się, że ze sposobu wibracji

naszego głosu czy też jego nielinearności można stwierdzić wczesne stadium choroby Parkinsona, a z zadyszki można „wyczytać" ewentualne choroby serca czy nawet depresję. Jednak, żeby w taki sposób wykorzystywać technologię i to, co dobrego może nam dać, należy powrócić do bezpieczeństwa i prywatności, bo bez zapewnienia komfortu korzystania z danego oprogramowania i zbudowania zaufania, nie będziemy w stanie ani zgromadzić odpowiedniej próby danych, na której oprzemy działanie naszego oprogramowania, ani nie będziemy w stanie wykorzystać tego oprogramowania w celu, do którego zostało stworzone. Komfort taki może zostać utworzony na bazie wzajemnych interakcji pomiędzy człowiekiem a oprogramowaniem, z którego korzysta i tego, jakie korzyści nam jako ludziom to przyniesie i jak bardzo podniesie komfort naszego życia.

Transparentność działania algorytmu

Można stwierdzić, że opisane wyżej cztery aspekty są spełnione tylko wtedy, jeśli są one zrozumiałe na każdym etapie. Jeśli system AI podejmuje jakiekolwiek decyzje bazując na naszych danych i mając wpływ na nasze życie, musimy być w stanie zrozumieć, w jaki sposób te decyzje są podejmowane. Wydaje się być to problematyczne w szczególności w momencie, kiedy wiemy, że nasz algorytm sam się uczy. Powoduje to, że nie będziemy w stanie odtworzyć jego działania pomiędzy danymi wejściowymi i wstępnymi założeniami, a danymi wyjściowymi i wnioskami, które otrzymamy. Dlatego też twórca lub właściciel oprogramowania powinien być w stanie kontekstowo wyjaśnić, w jaki sposób system działa, jakie dane wykorzystuje, jakie założenia nim kierują, jak może wpłynąć na dane i jakie są wobec niego oczekiwania. Jeśli z kolei system korzysta z blockchain, to sam twórca powinien określić odpowiedzialności w łańcuchu – bo czy wiemy, kto w nim jest właścicielem i czy jest on jeden? Samo omówienie algorytmu działania systemu może nie mieć większego sensu, ponieważ nie będzie przejrzyście pokazywało, jak oprogramowanie funkcjonuje. Najnowsze oprogramowania oparte na sztucznej inteligencji dość często bazują na skomplikowanych systemach sieci neuronowych. Nie pozwalają one odtworzyć algorytmu, który pomógłby ludziom zrozumieć subtelne wzorce znalezione przez system. Dlatego powinno się określać kontekstowe podejście tworzenia systemu z wyjaśnieniem ewentualnych niuansów działania technologii.

Rozliczalność

Wylegitymowanie się ze wszystkiego w przypadku danych osobowych i dopełnienie „należytej staranności" jest dla każdego zaznajomionego z tematem czymś oczywistym. W kontekście nowoczesnych technologii nie chodzi jedynie o utworzenie dokumentacji, którą ewentualnie pokażemy jednostce nadzorującej, ale głównie o wyżej opisane aspekty w kontekście zbudowania zaufania i zapewnienia komfortu użytkownika. Tutaj akurat przepisy prawne, w szczególności dotyczące przetwarzania danych osobowych czy medycznych, dają nam bardzo dobre narzędzia do spełnienia tych warunków. Oprócz RODO przydatne będą również wytyczne Grupy Roboczej Art. 29 takie jak *Wytyczne w sprawie zautomatyzowanego podejmowania decyzji i profilowania w indywidualnych przypadkach.* Objaśniają one znaczenie zapisów RODO w tym zakresie i – choć ich tytuł może na to nie wskazywać – stanowią kolejny element ram prawnych dla rozwoju i wykorzystania nowoczesnych technologii. Według dokumentu zautomatyzowany jest nie tylko proces analityczny czy przygotowywanie rekomendacji, ale też faktyczne rozstrzyganie w określonych kwestiach. Najważniejszym wnioskiem z tego dokumentu jest to, że RODO nie tyle pozwala na wykorzystywanie sztucznej inteligencji, która jest oparta na starannym algorytmie, ile pozwala na wykorzystywanie danych do momentu, w którym osoba, której dane dotyczą uznaje, że z nim się zgadza. Prowadzi to zatem do utworzenia swego rodzaju klamry założeń opisanych wyżej, że na bazie RODO możemy stosować dowolne technologie, dopóki regulacje chroniące prawa osób fizycznych (między innymi prywatność) są uszanowane i respektowane. Bez względu na to, czy jest to blockchain, sztuczna inteligencja czy Internet rzeczy.

SŁOWNIK POJĘĆ

Administrator danych osobowych

Osoba lub organ, który samodzielnie lub wraz z innymi osobami lub organami określa cele i środki przetwarzania danych osobowych.

Blockchain

Rozproszona baza danych, która zawiera stale rosnącą ilość informacji (rekordów) pogrupowanych w bloki i powiązanych ze sobą w taki sposób, że każdy następny blok zawiera oznaczenie czasu (timestamp), kiedy został stworzony oraz link do poprzedniego bloku, będący zaszyfrowanym „streszczeniem" jego zawartości.

Chmura obliczeniowa

To dostarczanie usług obliczeniowych – w tym serwerów, magazynu, baz danych, sieci, oprogramowania, analizy i inteligencji – za pośrednictwem Internetu („chmura") w celu zaoferowania szybszych innowacji, elastycznych zasobów i ekonomii skali.

Dane osobowe

Wszelkie informacje odnoszące się do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej zwanej „osobą, której dane dotyczą". Osoba, której dane dotyczą to osoba fizyczna, którą można bezpośrednio lub pośrednio zidentyfikować.

Dane wrażliwe

Jest to rodzaj danych szczególnie sensytywnych dla podmiotów danych (np. dane o stanie zdrowia). Z przetwarzaniem tych danych wiążę się konieczność dochowania dodatkowych obowiązków w zakresie ich ochrony.

Dyrektywa w sprawie ochrony danych

Dyrektywa nr 95/46/WE, która regulowała dotąd kwestie przetwarzania danych osobowych na terytorium Unii Europejskiej i która zostanie zastąpiona przez RODO.

EOG

Europejski Obszar Gospodarczy obejmuje 28 państw członkowskich UE oraz Islandię, Liechtenstein i Norwegię. Nie obejmuje natomiast Szwajcarii.

Grupa Robocza Art. 29

W skład Grupy Roboczej Art. 29 („Grupy Roboczej") wchodzą przedstawiciele organów nadzorczych Państw członkowskich, Europejskiego Inspektora Ochrony Danych („EIOD") oraz Komisji Europejskiej. Grupa Robocza została przekształcona w Europejską Radę Ochrony Danych o podobnym składzie, jednakże z niezależnym sekretariatem (więcej informacji znajduje się w części poświęconej Europejskiej Radzie Ochrony Danych).

IMEI (International Mobile Equipment Identity)

Indywidualny numer identyfikacyjny telefonu komórkowego GSM lub UMTS.

IMSI (International Mobile Subscriber Identity)

Unikatowy numer przypisany do każdej karty SIM w sieci GSM lub UMTS, jednoznacznie ją identyfikujący

IaaS (Infrastructure as a Service)

Jest to natychmiastowa infrastruktura obliczeniowa, zarządzana i zarządzana przez Internet. Jest to jeden z trzech typów usług w chmurze, wraz z oprogramowaniem jako usługą (SaaS), platformą jako usługą (PaaS).

Inspektor ochrony danych

Inspektor ochrony danych, którego wyznaczenie jest obowiązkowe, gdy (i) przetwarzania dokonuje podmiot publiczny lub gdy (ii) „główna działalność" administratora danych lub podmiotu przetwarzającego wymaga (a) „regularnego i systematycznego monitorowania osób, których dane dotyczą na dużą skalę" lub (b) polega na przetwarzaniu"na dużą skalę" szczególnych kategorii danych lub danych dotyczących wyroków skazujących.

Internet Rzeczy/IoT (Internet of Things)

Koncepcja, wedle której jednoznacznie identyfikowalne przedmioty mogą pośrednio albo bezpośrednio gromadzić, przetwarzać lub wymieniać dane za pośrednictwem instalacji elektrycznej inteligentnej KNX lub sieci komputerowej.

Adres MAC

Jest to fizyczny adres karty sieciowej.

Ocena skutków dla ochrony danych

RODO nakłada na administratora danych i podmioty przetwarzające dane nowy obowiązek przeprowadzenia oceny skutków dla ochrony danych (zwanej również oceną skutków dla prywatności) przed podjęciem operacji przetwarzania danych, która – ze względu na swój charakter, zakres lub cele – może nieść za sobą wysokie ryzyko dla prywatności. Rozdział IV Sekcja 3 zawiera niewyczerpujące wyliczenie kategorii przetwarzania danych, objętych zakresem zastosowania tego przepisu.

Usługi OTT (over-the-top)

To usługa polegającą na dostarczaniu zawartości, usług lub aplikacji za pośrednictwem sieci Internet bez bezpośredniego zaangażowania dostawcy usługi dostępu do Internetu.

Organ nadzorczy/organ wiodący

Organy nadzorcze to krajowe organy właściwe w sprawach ochrony danych, do których kompetencji należy zapewnienie przestrzegania RODO w danym państwie członkowskim.
Jeśli przedsiębiorca ma jednostki organizacyjne w więcej niż jednym państwie członkowskim, „organ wiodący" wyznacza się ze względu na położenie jego głównej jednostki organizacyjnej w Unii. Pewne funkcje regulacyjne może wykonywać także organ nadzorczy niebędący organem wiodącym, np. w przypadku, gdy przetwarzanie oddziałuje na sytuację osób, których dane dotyczą, w państwie, w którym działa ten organ.

PaaS (Platform as a service)

Platforma jako usługa (PaaS) to kompletne środowisko deweloperskie i środowisko wdrażania w chmurze obejmujące zasoby umożliwiające dostarczanie dowolnego rozwiązania, od prostych aplikacji opartych na chmurze po złożone aplikacje dla przedsiębiorstw korzystające z chmury

Przetwarzanie

Przetwarzanie zostało zdefiniowane szeroko jako jakakolwiek operacja lub zespół operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany. Przykładami przetwarzania jest zbieranie, utrwalanie, organizowanie, przechowywanie, wykorzystywanie i niszczenie danych osobowych.

Pseudonimizacja

Technika polegająca na przetwarzaniu danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i zostały poddane zabezpieczeniom technicznymi i organizacyjnymi uniemożliwiającymi ich ponowne przypisanie tej osobie.

Prawo do usunięcia danych / prawo do bycia zapominanym

Dotychczasowe prawo do usunięcia danych osobowych, przyznane osobie, której dane dotyczą, zostało rozszerzone zgodnie z przepisami Rozdziału III Sekcji 3 RODO

Prawo dostępu

Jest to uprawnienie osoby, której dane dotyczą, do żądania od administratora udzielenia określonych informacji dotyczących przetwarzania jej danych osobowych zgodnie z przepisami Rozdziału III Sekcji 2 RODO.

Prawo do bycia zapomnianym

Prawo osoby, której dane są przetwarzane do żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, w tym danych upublicznionych przez administratora. Administrator zobowiązany jest – w przypadku upublicznienia danych – do poinformowania innych administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje.

Privacy by Design

Sposób projektowania aplikacji / systemów, który już w tej fazie bierze pod uwagę oraz wdraża metody i środki by chronić dane osobowe oraz prywatność osób, których te dane dotyczą. Ważne jest, by ochrona tych informacji była od samego początku.
Ochrona danych jest zaimplementowana w dany system i nie ma potrzeby użycia zewnętrznych dodatków czy modułów.

Privacy by Default

Mówi, że domyślnie prywatność użytkownika jest priorytetem. Systemy i aplikacje powinny mieć tak skonfigurowane ustawienia, by udostępniać ich tylko minimalną ilość.
Rozszerzenie zakresu udostępnianych danych, powinno nastąpić po zmianach dokonanych przez samego użytkownika. Dotyczyć to będzie zarówno aplikacji końcowych (np. sieci społecznościowe), jak i pośredniczących (np. przeglądarki internetowe)

Processor (Podmiot przetwarzający)

Podmiot, który przetwarza dane osobowe w imieniu administratora danych.

Przekazanie

Przekazanie danych osobowych do państw spoza EOG lub do organizacji międzynarodowych, poddane obostrzeniom przewidzianym w Rozdziale V RODO. Podobnie jak pod rządami dyrektywy w sprawie ochrony danych, przekazanie danych nie wymaga ich fizycznego przemieszczenia. Przekazaniem danych, dla celów RODO, jest już samo uzyskanie wglądu do danych przechowywanych w innej lokalizacji.

Przedsiębiorca

Pojęcie to pojawia się w RODO w rozmaitych kontekstach, najczęściej w odniesieniu do podmiotu prawnego prowadzącego „działalność gospodarczą". Pojęcie to ma szczególne znaczenie w kontekście przepisów RODO o karach finansowych. Przedsiębiorca podlega karom finansowym, obliczonym jako procent osiągniętego przezeń całkowitego rocznego światowego obrotu za poprzedni rok obrotowy. W tym kontekście pojęcie przedsiębiorcy nawiązuje do dorobku unijnego prawa ochrony konkurencji.

RODO

Rozporządzenie ogólne o ochronie danych osobowych uchwalone ostatecznie 27 kwietnia 2016 r. jako Rozporządzenie (UE) 2016/679. Niniejsze wydanie Przewodnika uwzględnia wytyczne opublikowane przez Grupę Roboczą w grudniu 2016 r.

Rozporządzenie o e-Prywatności

Ma to być komplementarny w stosunku do RODO akt prawny, regulujący wykorzystanie danych osobowych pozyskanych w związku ze świadczeniem usług łączności elektronicznej. Rozporządzenie to będzie miało charakter regulacji szczególnej wobec RODO, co ma istotne znaczenie dla dostawców usług łączności elektronicznej. W chwili obecnej na poziomie Unii Europejskiej trwają jeszcze prace nad ostateczną wersją Rozporządzenia o e-Prywatności.

SaaS (Software as a Service)

Oprogramowanie jako usługa (SaaS) zapewnia użytkownikom możliwość łączenia się z aplikacjami opartymi na chmurze za pośrednictwem Internetu i korzystania z nich

VOIP (Voice over Internet Protocol)

Technologia, dzięki której możliwe jest prowadzenie rozmów telefonicznych – przesyłanie dźwięków mowy – za pośrednictwem połączenia internetowego bądź sieci korzystającej z protokołu IP – tzw. telefonia internetowa.

7 Zasad RODO[20]

1. Zasada zgodności z prawem, przejrzystości i rzetelności. (art. 5 ust. 1 pkt a) RODO):

Dane osobowe muszą być:
przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość"). Zbieranie danych osobowych musi mieć określoną podstawę prawną (zgoda osoby, przepis prawa).
Prawidłowa realizacja obowiązków informacyjnych jest warunkiem niezbędnym dla osiągnięcia zgodności z zasadą rzetelności i przejrzystości.

2. Zasada ograniczenia celu przetwarzania (art. 5 ust. 1 lit. b) RODO):

Dane osobowe muszą być:
zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami („ograniczenie celu"); Cel zbierania danych musi być czytelnie zakomunikowany osobie, której dane dotyczą jeszcze przed faktycznym zebraniem od niej danych osobowych. Danych zebranych w określonym celu nie można przetwarzać w innym bez zgody osoby.

3. Zasada minimalizacji danych (art. 5 ust. 1 lit. c) RODO):

Dane osobowe muszą być: (...)
adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych");
Zakres przetwarzanych danych powinien być taki jaki jest niezbędny do osiągnięcia określonego celu przetwarzania danych.

4. Zasada prawidłowości danych (art. 5 ust. 1 lit. d) RODO):

Dane osobowe muszą być: (...)
prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość");
Przestrzeganie zasady prawidłowości danych sprowadza się do tego, aby stworzone zostały odpowiednie rozwiązania techniczne oraz organizacyjne umożliwiające korygowanie nieprawidłowych lub nieaktualnych danych.

5. Zasada ograniczenia przechowywania danych (art. 5 ust. 1 lit. e) RODO):

Dane osobowe muszą być:
przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań

20 Źródło: Analizy Deloitte, 2017
https://www2.deloitte.com/pl/pl/pages/doradztwo-prawne/articles/ochrona-danych-osobowych/RODO-zmiany-w-zasadach-przetwarzania-danych-osobowych.html

naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania");
Realizacja tej zasady jest możliwa poprzez wdrożenie odpowiednich procedur wyznaczających terminy przechowania danych lub procedur określających terminy okresowych przeglądów danych.

6. Zasada integralności i poufności (art. 5 ust. 1 lit. f) RODO):

Dane osobowe muszą być:
przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność").
Realizacja zasady integralności i poufności danych polega na wdrożeniu odpowiednich środków technicznych i organizacyjnych, które zapewnią bezpieczeństwo danych. „Odpowiednie środki" będą zawsze pojęciem niedookreślonym. Najprawdopodobniej zostaną w pewnym zakresie doprecyzowane w drodze dobrych praktyk, które ma wydać regulator – Prezes Urzędu Ochrony Danych Osobowych

7. Zasada rozliczalności (art. 5 ust. 2 RODO):

Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie („rozliczalność").

Autorzy

Robert Brodzik

Kancelaria Domański Zakrzewski Palinka

Sławomir Chmielewski

Orange Polska S.A.

Michał Kibil

Kancelaria Kibil i Wspólnicy

Xawery Konarski

Traple Konarski Podrecki i Wspólnicy

Bartosz Marcinkowski

Kancelaria Domański Zakrzewski Palinka

Barbara Sawina

Orange Polska S.A.

dr Grzegorz Sibiga

Traple Konarski Podrecki i Wspólnicy

Sylwia Stefaniak

Microsoft

Halszka Suszek-Borowska

Microsoft

Daniel Szmurło

T-mobile Polska S.A.

Karol Warzecki

T-mobile Polska S.A.

Monika Wieczorek

Kancelaria Kibil i Wspólnicy

Koordynator Projektu

Maciej Wnuk

Polska Izba Informatyki i Telekomunikacji