# Książeczka o danych osobowych

Paweł Litwiński

# Książeczka o danych osobowych

Paweł Litwiński

Kraków 2024

Skład: JustLuk Łukasz Drzewiecki
Korekta: Literalnie Justyna Szumieł
Projekt okładki: Katarzyna Dulińska



Wydanie I
www.bartalitwinski.pl

# Spis treści

# Wstęp

Po co powstała ta książeczka? Żeby podzielić się z Czytelniczkami i Czytelnikami pewnymi praktycznymi przemyśleniami związanymi ze stosowaniem przepisów o ochronie danych osobowych. Czyli mówiąc jasnym i prostym językiem: żeby dać kilka praktycznych rad. Nie opisuję wszystkich problematycznych kwestii – skupiam się na tych, które moim zdaniem budzą najwięcej wątpliwości. Nie aspiruję do tego, żeby tą książeczką zastąpić opasłe tomy komentarzy i monografii – chcę w sposób zrozumiały opowiedzieć o tym, co w ochronie danych osobowych trudne.

A co do tytułu: nie ukrywam, że inspiracją w tym zakresie była „Jak pisać pisma procesowe i prowadzić komunikację w sporze. Czyli książeczka o pisaniu pism" autorstwa Piotra Biernatowskiego i Macieja Gawrońskiego (Warszawa 2022). Powstała więc „Książeczka o danych osobowych", którą niniejszym przekazuję w Państwa ręce.

Paweł Litwiński

# Po co nam ochrona danych osobowych?

Pytanie postawione w tytule stawia sobie nadal – po ponad 50 latach od przyjęcia pierwszych w Europie przepisów o ochronie danych osobowych – wiele osób. Spróbujmy więc na nie odpowiedzieć.

Pamiętamy, skąd wzięła się ochrona danych osobowych w znaczeniu, jakie temu pojęciu przypisujemy dzisiaj – wzięła się z chęci ochrony jednostki, jej prywatności i, mówiąc bardziej ogólnie, sfery informacyjnej. Historycznie rzecz biorąc, były dwa konkretne impulsy do powstania tej gałęzi prawa:

1) gwałtowny wzrost apetytu państw i podmiotów prywatnych na informacje o nas wszystkich,
2) skokowy rozwój technologii komputerowych ułatwiających przetwarzanie tych informacji.

Więcej danych połączone z łatwością ich przetwarzania to nowe, nieznane zagrożenia – pomyślano więc o tym, żeby z góry określić, jak te dane trzeba chronić i jak je można wykorzystywać. Pomysł zakładał przy tym, że to „określenie" nastąpi przy wykorzystaniu instrumentów prawa publicznego, a więc poprzez konkretne nakazy i zakazy, które będzie egzekwował specjalnie do tego powołany organ władzy publicznej. Powstało współczesne europejskie prawo ochrony danych osobowych.

Gdy więc ktoś pyta, po co nam prawo ochrony danych osobowych, odpowiadamy przy użyciu trzech słów: żeby nas chronić. I to nie są czcze deklaracje – popatrzmy tylko na ostatnie lata:

1) władze publiczne gromadzą coraz więcej informacji na nasz temat, powstają nowe rejestry publiczne (nie tylko słynny „rejestr ciąż", ale choćby rejestr sprawności fizycznej uczniów, centralny rejestr wyborców, rejestr emisyjności budynków, zbieranie odcisków palców w związku z wydawaniem dowodów osobistych itd.), a dane z nich pochodzące bywają wykorzystywane nie do końca zgodnie z ich

przeznaczeniem, że wspomnę tylko pewnego ministra i to, co opublikował na pewnym portalu społecznościowym;
2) podmioty prywatne prześcigają się w wykorzystywaniu informacji, które na nasz temat zbierają i które najczęściej sami im podajemy – profilowanie w mediach społecznościowych to tylko wierzchołek góry lodowej;
3) powstają nowe, coraz bardziej inwazyjne, metody przetwarzania informacji, w większości pod hasłem większego bezpieczeństwa, jak choćby biometryczna identyfikacja klientów.

Prawo ochrony danych osobowych jest po to, żeby nas chronić przed niekontrolowanym wykorzystaniem naszych danych osobowych – to jedna wielka procedura mająca zapewnić poszanowanie naszego podstawowego prawa do ochrony danych osobowych. Ale, jak każda procedura, prawo ochrony danych osobowych jest o tyle tylko efektywne, o ile jest w odpowiedni sposób stosowane – a z tym akurat w Polsce mamy tradycyjnie pewne problemy: można odnieść wrażenie, że czasem sens ochrony danych osobowych gubimy w zalewie procedur, klauzul, oświadczeń i innych nikomu niepotrzebnych dokumentów. Stąd też, być może, powracające głosy podające w wątpliwość sens istnienia przepisów o ochronie danych osobowych – i stąd też pomysł na tę książeczkę.

# Dane osobowe, czyli właściwie co?

Jedną z typowych praktyk telemarketerów jest rozpoczynanie rozmowy od tego, że nasz „numer telefonu został wylosowany", a marketer nie dysponuje żadnymi naszymi danymi osobowymi – ma przecież tylko ten zestaw 9 cyfr wybrany przez algorytm na podstawie Planu Numeracji Krajowej. To nic, że zaraz po tym informuje nas, że ma ofertę dla mieszkańców naszej miejscowości, a dzwoni na naszą komórkę, która przecież może znajdować się gdziekolwiek, a jej numer nic nie mówi o naszej lokalizacji; to nic, że kieruje ofertę do osób akurat w naszym wieku, a tego wieku przecież nie mógł odczytać z tego wylosowanego numeru – nie ma danych i już. Jak to więc jest z tymi danymi osobowymi – czym one są?

Dane osobowe to informacje dotyczące osoby fizycznej, która to osoba jest osobą zidentyfikowaną albo którą można zidentyfikować. Informacja – czyli potencjalnie wszystko; wszystko może mieć charakter danych osobowych: imię, nazwisko, numer telefonu, adres zamieszkania, adres IP, kod DNA, numer rejestracyjny pojazdu itd. Wszystko może mieć charakter danych osobowych, jeżeli dotyczy osoby fizycznej zidentyfikowanej lub możliwej do zidentyfikowania – „osoby fizycznej", a więc osoby prawne nie mają danych osobowych, a informacja w rodzaju „XYZ sp. z o. o." nie jest daną osobową tej spółki. Ale uwaga: dane osobowe mogą mieć członkowie organów osób prawnych („Paweł Litwiński, członek zarządu …. sp. z o. o.") lub ich pracownicy. Trzeba też pamiętać, że osoba fizyczna to osoba żyjąca, osoby zmarłe nie mają więc danych osobowych. Ale znów: z jednej strony informacja o osobie zmarłej może identyfikować np. jej dzieci, a z drugiej strony – nieograniczone wykorzystanie informacji o osobach zmarłych może naruszać dobra osobiste osób żyjących. Dane osobowe mają także dzieci i to niezależnie od wieku; ba, nawet dziecko nienarodzone, o ile urodzi się żywe, ma dane osobowe – danymi osobowymi będą więc np. wyniki badań tegoż nienarodzonego dziecka i to danymi osobowymi dwóch (a może i trzech) osób: dziecka, matki, a być może i ojca.

Żeby informacja dotycząca osoby fizycznej miała charakter danych osobowych, osoba ta musi być zidentyfikowana albo możliwa do zidentyfikowania. To, czy informacja spełnia ten warunek, zawsze oceniamy z perspektywy tego, kto identyfikuje, np.: numer telefonu dla operatora sieci, w której ten numer działa, ma charakter danych osobowych; tak samo będzie w przypadku pracodawcy, jeżeli numer podał mu pracownik – ale już dla przypadkowej osoby niekoniecznie. Numer rachunku bankowego ma charakter osobowy dla banku, który ten rachunek prowadzi, i dla pracodawcy, który przelewa na niego wynagrodzenie, ale dla osoby postronnej już nie. To zjawisko, które w Polsce określamy jako relatywizacja pojęcia danych osobowych, a które zawdzięczamy nieodżałowanej pamięci Wacławowi Zimnemu, w nauce prawa określa się jako subiektywne rozumienie przesłanki identyfikowalności – po prostu każdy, kto ma informację, ocenia, czy dla niego ma ona charakter danych osobowych. Ale znów uwaga: ocenia nie tylko na podstawie tej informacji, której status ma określić, ale na podstawie wszystkich tych informacji, do których ma lub może mieć legalny dostęp – poza takimi, które co prawda teoretycznie są dostępne, ale których pozyskanie wymagałoby poświęcenia niewspółmiernie dużo czasu lub poniesienia ogromnych kosztów.

Jak to więc wygląda w praktyce? W ogromnej większości przypadków pewne zestawy informacji z prawdopodobieństwem graniczącym z pewnością można uznać za dane osobowe: imię, nazwisko i adres lub imię, nazwisko i numer telefonu. W przypadku pojedynczych informacji charakter danych osobowych ma np. numer NIP osoby, która prowadzi działalność gospodarczą – bo każdy, w kilka sekund, może ustalić, czyj to numer NIP, korzystając z wyszukiwarki na stronie CEIDG; podobnie będzie np. z numerem KRS w sytuacji, gdy w danym podmiocie występuje np. jednoosobowy zarząd. Adres poczty elektronicznej może, ale nie musi, mieć charakter danych osobowych: adres e-mail uznamy za dane osobowe, jeżeli identyfikacja osoby będzie możliwa na podstawie jego samego (typowy służbowy adres to imię, nazwisko i informacja o miejscu pracy) albo na podstawie innych informacji (w sklepie internetowym podajemy imię, nazwisko, adres zamieszkania i adres e-mail w rodzaju „misio234@coś tam.pl" – wtedy taki adres to dane osobowe); ale ten sam „misiowy" adres, występujący samodzielnie i bez żadnych dodatkowych informacji, daną osobową nie jest. Adres IP z kolei, występujący samodzielnie, jeżeli kogoś identyfikuje, to wyłącznie osobę będącą stroną umowy o świadczenie usług telekomunikacyjnych, a nie osobę, która znajduje się na drugim końcu łącza.

Może się to wydawać trudne do przyjęcia, ale nawet numer PESEL nie będzie miał zawsze i dla każdego charakteru danych osobowych mimo tego, że każdy z nas ma od urodzenia unikatowy numer PESEL. Dlaczego? Dlatego, że pomijając przypadki, w których numery PESEL są jawne, np. w KRS, nie możemy ot tak, po prostu, ustalić, kto jest posiadaczem określonego numeru PESEL; poza szczególnymi przypadkami, warunkiem udostępnienia informacji z bazy PESEL jest wykazanie interesu prawnego.

Wysiłek, jaki musimy włożyć w identyfikację osoby, to tzw. próg identyfikowalności. Jest on relatywnie niżej usytuowany w przypadku podmiotów publicznych – ponieważ co do zasady dysponują szerszym dostępem do rejestrów publicznych niż podmioty z sektora prywatnego, łatwiej jest im zidentyfikować przysłowiowego Kowalskiego. Ten próg w ostatnich latach znacznie się obniżył, głównie dzięki naszej aktywności i pewnej wyszukiwarce internetowej – ale nadal nie każda informacja ma charakter danych osobowych. Może więc być tak, że marketer ma tylko nasz numer telefonu, który wytypował algorytm – ale jeżeli zaczyna rozmowę od „dzień dobry Panie Pawle, Pana numer został wylosowany przez komputer…" to wiedzmy, że nie mówi całej prawdy.

# Dane osobowe dzieci

Dane osobowe mamy od narodzin aż do śmierci. Wie o tym doskonale biznes, coraz częściej sięgając po dane osobowe dzieci i młodzieży, najczęściej w kontekście oferowanych im usług: portali społecznościowych, gier, konkursów i loterii promocyjnych lub po prostu w związku z usługami edukacyjnymi. Ale jak takie dane przetwarzać, żeby zapewnić poszanowanie prawa do ochrony danych osobowych, a jednocześnie dbać o bezpieczeństwo prawne naszej firmy?

Zacznijmy od tego, że dzieci zasługują na szczególną ochronę w kontekście przetwarzania danych osobowych, co kilkukrotnie akcentuje preambuła do RODO. W efekcie do danych osobowych dzieci – rozumiem przez to osoby, które nie ukończyły 18. roku życia – stosuje się takie same zasady przetwarzania, jak do danych osobowych osób dorosłych, pamiętając o tym, że w pewnych przypadkach szczególne przepisy przyznają dzieciom większą ochronę. Co to w praktyce oznacza? W pierwszej kolejności to, że przetwarzając dane osobowe dziecka, trzeba wobec niego wykonać te same obowiązki, które wykonuje się w stosunku do osoby dorosłej: przekazać dziecku informacje przy gromadzeniu danych (art. 13 i 14 RODO), poinformować o naruszeniu ochrony danych osobowych (art. 34 RODO), zapewnić możliwość korzystania z tych samych praw (art. 15–22 RODO) itd. Ale wykonując te obowiązki pamiętajmy o tym, że wykonuje się je wobec dziecka, które zasługuje na szczególną ochronę, a więc każda komunikacja z dzieckiem musi być dostosowana do jego zdolności poznawczych i stopnia percepcji. Przykłady – bardzo proszę:

1) zamiast pisać, że mały pacjent ma prawo dostępu do swoich danych osobowych, napiszmy, że może zobaczyć, co lekarz zapisał na jego temat;
2) zamiast informować w przypadku wycieku danych, że ktoś może zagłosować za niego w budżecie obywatelskim, napiszmy, że ktoś może podszyć się pod niego w grze komputerowej lub na portalu społecznościowym.

Tak działa zasada przejrzystości, która rządzi wszelką komunikacją wynikającą z przepisów RODO. W efekcie np. zbierając dane osobowe dzieci, powinniśmy przy-

gotować dwie wersje informacji wymaganych przez art. 13 RODO: dla rodzica w – powiedzmy – standardowej formie i dla dziecka, w formie dostosowanej do niego.

Po drugie, w stosunku do danych osobowych dzieci istnieją pewne ograniczenia, nieistniejące w przypadku przetwarzania danych osób dorosłych. Przywołać tu trzeba w pierwszej kolejności motyw 71 preambuły do RODO, zgodnie z którym profilowanie wywołujące skutki prawne (tzw. profilowanie kwalifikowane) nie powinno dotyczyć dzieci. W opinii większości ekspertów, w tym Europejskiej Rady Ochrony Danych, nie oznacza to całkowitego zakazu takiego profilowania, ale nakaz traktowania go w sposób wyjątkowy i obudowania dodatkowymi zabezpieczeniami tak, by możliwie najlepiej chronić prawa dzieci. Inny przykład modyfikacji ogólnych zasad przetwarzania danych w kontekście danych dzieci dotyczy możliwości powołania się na tzw. uzasadniony interes administratora danych jako podstawę przetwarzania danych osobowych. Sam przepis RODO (art. 6 ust. 1 lit. f) jest w tym kontekście dość niejasny, stąd w literaturze można spotkać głosy opowiadające się albo za całkowitym zakazem wykorzystania tej podstawy przetwarzania w stosunku do dzieci, albo za koniecznością stosowania jej z daleko idącymi ograniczeniami. Z perspektywy czasu wydaje się, że całkowity zakaz byłby trudny do uzasadnienia (np. monitoring wizyjny zawierający zapis kradzieży dokonanej przez dziecko byłby w tym kontekście zakazany), tym niemniej przetwarzając dane osobowe dzieci na podstawie art. 6 ust. 1 lit. f RODO, w każdym przypadku trzeba wdrożyć dalej idące zabezpieczenia niż gdyby przetwarzanie obejmowało wyłącznie dane osób dorosłych.

I wreszcie trzecia kwestia, najbardziej praktycznie doniosła: zgoda na przetwarzanie danych udzielana przez dziecko. W kontekście polskich przepisów prawa cywilnego trzeba mieć pełną zdolność do czynności prawnych, żeby skutecznie wyrazić zgodę na przetwarzanie swoich danych – czyli co do zasady trzeba mieć ukończony 18. rok życia. Jeżeli jednak zgoda jest udzielana w kontekście oferowania usług społeczeństwa informacyjnego bezpośrednio dziecku, taka granica wynosi 16 lat (art. 8 ust. 1 RODO). Podążając za Europejską Radą Ochrony Danych (EROD), wypada uznać, że przepis ten dotyczy takich serwisów, których treść przeznaczona jest dla dzieci. Jeżeli więc w kontekście takich serwisów przeznaczonych dla dzieci zbierane są zgody dzieci na przetwarzanie ich danych osobowych, granica wieku wynosi 16 lat. Co to oznacza w praktyce? Jeżeli np. serwis edukacyjny dla uczniów szkół średnich w związku ze swoją działalnością zbiera zgody na przetwarzanie danych, zgody może udzielić użytkownik lub użytkowniczka, którzy ukończyli 16. rok życia. Ale jeżeli zgody są zbierane bez kontekstu tego rodzaju serwisów, stosuje się granicę 18 lat. Pamiętać

też trzeba o tym, że dziecko powinno być zawsze włączane w proces wyrażania zgody dotyczącej jego danych osobowych – nawet więc, gdy formalnie rzecz biorąc zgody udziela przedstawiciel ustawowy, w tym procesie powinno uczestniczyć dziecko i winno się uwzględniać jego proces rozwoju i osiągania dojrzałości.

I na koniec najważniejsze: jak weryfikować wiek dziecka, a jeżeli wymagana jest zgoda przedstawiciela ustawowego – jak weryfikować, że osoba udzielająca zgody jest tym przedstawicielem? Tu znów pomaga nam EROD, sugerując, by dostosować ten proces do ciężaru gatunkowego sprawy. Nie odsyłajmy więc rodzica do notariusza i nie wymagajmy kwalifikowanego podpisu elektronicznego wówczas, gdy zbieramy zgodę na marketing w serwisie edukacyjnym dla 13-latków; ale już zgoda na przetwarzanie danych dotyczących zdrowia dziecka w celu prowadzenia badań naukowych powinna zakładać weryfikację tożsamości opiekuna prawnego.

# Usuwanie danych, anonimizacja i pseudonimizacja

Warto przybliżyć jedną z podstawowych zasad przetwarzania danych osobowych, jaką jest zasada ograniczenia przechowywania, zgodnie z którą danych nie wolno przechowywać bez żadnego ograniczenia czasowego, czyli w nieskończoność. W praktyce znaczy to tyle, że dane trzeba usuwać – ale jak to zrobić?

Mówiąc o usunięciu danych, mamy na myśli prostą wydawałoby się sytuację: dane osobowe są i nagle ich nie ma, bo zostały usunięte. W tym sensie usuwanie danych osobowych to ostatni etap ich istnienia – proces przetwarzania danych rozpoczyna się wraz z ich zebraniem, potem następują inne operacje ich przetwarzania, a na samym końcu dane powinny zostać usunięte. Samo usunięcie może przy tym przybrać jedną z dwóch postaci:

1) usunięcie danych przy pozostawieniu ich nośnika,
2) zniszczenie nośnika prowadzące do usunięcia danych.

Pierwsza sytuacja ma miejsce zazwyczaj wtedy, gdy dane są przetwarzane w systemach informatycznych – usuwany jest odpowiedni zapis lub rekord w bazie danych, podczas gdy sama baza i maszyna, w której pamięci ta baza się znajduje, istnieją nadal. Druga sytuacja z kolei będzie występowała przede wszystkim wtedy, gdy niszczymy wydruki zawierające dane osobowe, co najczęściej następuje przy użyciu niszczarki (ale nie tylko – wyjątkowo skutecznym sposobem niszczenia wydruków jest ich spalenie w odpowiednim piecu). Niszczarka niszczarce nie równa – to, w jaki sposób niszczarka niszczy dokumenty, a mówiąc precyzyjnie, jakie jest prawdopodobieństwo tego, że te dokumenty będzie się dało odtworzyć, określa norma DIN 66399. Aktualnie obowiązująca norma definiuje 7 poziomów bezpieczeństwa, gdzie na poziomie 7 odtworzenie dokumentu powinno być wykluczone nawet przy zastosowaniu najbardziej wyrafinowanych metod jego odzyskania. Oczywiście w typowej organizacji nie ma potrzeby stosowania niszczarek najwyższego poziomu

– ale dobrze jest zwrócić uwagę na to, jakiej niszczarki używamy, aby w przyszłości uniknąć przykrych niespodzianek.

Ale zniszczenie nośnika to nie tylko zniszczenie wydruku. Przykładowo dyski twarde niszczy się w specjalnych niszczarkach-kruszarkach albo poddaje działaniu silnego pola magnetycznego. Uwaga: proste usunięcie pliku z danymi z dysku twardego nie prowadzi do trwałego usunięcia danych!

Prawidłowo skonfigurowany system informatyczny powinien obejmować efektywne procedury wykonywania kopii zapasowych – i tu pojawia się fundamentalne pytanie: czy usunięcie danych osobowych z systemu informatycznego oznacza także konieczność usunięcia ich z backupu? Przed koniecznością udzielenia odpowiedzi na to pytanie stanął w 2007 r. Generalny Inspektor Ochrony Danych Osobowych, a następnie Wojewódzki Sąd Administracyjny w Warszawie, który w wyroku z 16 stycznia 2008 r. (II SA/Wa 1801/07), wydanym na podstawie ustawy o ochronie danych osobowych z 1997 r., stwierdził bardzo jednoznacznie: „Jeżeli zatem dane osobowe Pana A. J. zostały usunięte ze zbiorów danych osobowych prowadzonych przez Bank, wobec braku podstaw prawnych do ich przetwarzania, to nie ma żadnych podstaw prawnych, by dane te były przetwarzane w kopii zapasowej. […] Kopia zapasowa powinna odzwierciedlać stan rzeczywisty zbioru, faktyczną jego zawartość". Pytanie tylko, jak to zrobić – jak usunąć konkretne dane osobowe z backupu? Ja nie znam odpowiedzi na to pytanie i odnoszę wrażenie, że nie zna jej także rynek produktów przeznaczonych do wykonywania kopii zapasowych. Przywołany wyrok zalicza się więc do tych, co do których można zaryzykować twierdzenie, że w praktyce nie przyjęły się do stosowania, a stan ten nie wynika ze złej woli administratorów danych.

Mówiąc o usunięciu danych osobowych, nie można zapominać o tym, że istnieje jeszcze jedno rozwiązanie pozwalające na przyjęcie, iż danych osobowych już nie ma: anonimizacja danych. Anonimizacja to, mówiąc najogólniej, takie przekształcenie informacji, żeby nie można jej już było połączyć z osobą fizyczną, której ta informacja dotyczy – i to przekształcenie nieodwracalne. Przykładowo sklep internetowy usuwa konto klienta; może to zrobić albo usuwając całość danych z systemu informatycznego, albo usuwając tylko niektóre z nich, a pozostawiając np. historię zakupów, kod pocztowy i miejscowość. W ten sposób pozostawione informacje nie będą już pozwalały na identyfikację klienta, lecz mogą się przydać np. przy planowaniu działań marketingowych. Ale uwaga: anonimizacja musi być skuteczna, a to znaczy, że identyfikacja osoby, której te dane dotyczyły, po prostu musi być niewykonalna.

Na ten problem zwraca uwagę Grupa Robocza art. 29 w opinii 4/2007 w sprawie pojęcia danych osobowych, pisząc o anonimizacji adresu IP. Otóż zdaniem Grupy nawet usunięcie ostatnich 3 cyfr adresu IP nie może przesądzać o jego anonimizacji, gdyż pozostawia to 254 potencjalne adresy IP, które mogą bez wielkich komplikacji zostać odtworzone.

I wreszcie pseudonimizacja – pseudonimizacja to także przekształcenie danych osobowych, ale takie, które pozwala przywrócić ich osobowy charakter. Pseudonimizacja zazwyczaj odbywa się w ten sposób, że zamiast danych osobowych – których nie usuwamy – posługujemy się „pseudonimem", którym jest np. numer identyfikacyjny nadany osobie fizycznej. Dane osobowe i pseudonim przechowujemy oddzielnie, co istotnie zwiększa bezpieczeństwo spseudonimizowanych danych, ale nie uniemożliwia połączenia pseudonimu z pozostałymi danymi. Pseudonimizacja nie prowadzi więc do usunięcia danych, a jako proces odwracalny nie jest też równoznaczna z anonimizacją danych. Co nie znaczy, że pseudonimizacja nie jest zalecana w praktyce – wręcz przeciwnie, to jeden z klasycznych sposób zabezpieczenia danych osobowych.

# Kiedy stosujemy RODO?

Bezpieczna firma to taka, która wie, jakim przepisom podlega i w związku z tym, jakie obowiązki powinna wykonywać – także w kontekście ochrony danych osobowych. Zastanówmy się więc, kiedy polscy przedsiębiorcy stosują przepisy RODO.

Z punktu widzenia tego, co i jak przedsiębiorca robi, zasada wynikająca z art. 2 ust. 1 RODO jest prosta – stosujemy RODO wtedy, gdy przetwarzamy dane w sposób choćby częściowo zautomatyzowany albo gdy dane stanowią lub mają stanowić część zbioru danych osobowych. Częściowe choćby zautomatyzowanie procesu przetwarzania oznacza tyle, że wystarczy jedna operacja przetwarzania odbywająca się automatycznie, aby proces uznać za częściowo zautomatyzowany, a więc podpadający pod przepisy RODO. Przykład? Bardzo proszę – automatycznie wykonujący się backup wystarczy. To sprawia, że w zasadzie każdy proces przetwarzania danych, który odbywa się przy wykorzystaniu systemów teleinformatycznych, jest z definicji objęty RODO. A co, jeżeli przetwarzanie od początku do końca odbywa się ręcznie? Mam dane zapisane na kartkach papieru, te kartki ręcznie porządkuję, a następnie ręcznie niszczę? Wówczas RODO stosujemy wtedy, gdy takie dane stanowią lub mają stanowić część zbioru danych osobowych. „Stanowią" wtedy, gdy są częścią zbioru danych; „mają stanowić", gdy co prawda jeszcze nie stanowią, ale administrator ma zamiar je do zbioru wprowadzić (np. porządkuje dokumenty, które następnie wepnie do akt, które już są zbiorem danych). A czym jest zbiór danych? To zestaw danych, które spełniają dwie cechy: są uporządkowane i dostępne wg określonych kryteriów (wbrew dosłownemu brzmieniu przepisu, wystarczy jedno kryterium, aby powstał zbiór danych). W efekcie wystarczy, że te kartki uporządkuję chronologicznie – przecież mówimy o dowolnym kryterium – i mam zbiór danych, a więc stosuję RODO.

Czy więc można sobie wyobrazić przypadki, w których przetwarzam dane osobowe, ale na gruncie art. 2 ust. 1 RODO nie stosuję? Tak, ale w zasadzie tylko teoretycznie, ponieważ – po pierwsze – przypadki, w których w ogóle można by mówić o ręcznym przetwarzaniu danych, które nie mają stać się częścią zbioru danych, będą występowały bardzo rzadko. Po drugie, przepisy o ochronie danych osobowych nie mogą być

interpretowane w ten sposób, aby w wyniku tej interpretacji obniżać poziom ochrony danych – nie taki jest ich cel, na co w przeszłości zwracano uwagę w orzecznictwie sądowym (zob. wyrok Naczelnego Sądu Administracyjnego [NSA] z 10 grudnia 2015 r., I OSK 3053/14).

A jak wygląda sytuacja z punktu widzenia tego, kto przetwarza dane osobowe, czyli na gruncie art. 3 RODO? RODO stosujemy do przetwarzania danych osobowych w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego w Unii Europejskiej, niezależnie od tego, czy przetwarzanie odbywa się w Unii. Jest to niezwykle szerokie ujęcie zakresu zastosowania przepisów o ochronie danych osobowych, bo nie ma znaczenia, gdzie są przetwarzane dane, i wystarczy, by przesłankę zastosowania RODO spełniał przetwarzający. Patrząc z tej perspektywy, odwieczne pytanie o to, gdzie jest serwer z danymi, staje się bezprzedmiotowe. Znaczenie ma wyłącznie to, czy przetwarzanie następuje w związku z działalnością prowadzoną w Unii przez jednostkę organizacyjną administratora lub przetwarzającego. Weźmy prosty przykład: administrator danych ma siedzibę w USA, a więc poza Unią, i decyduje się skorzystać z usług podwykonawcy przetwarzającego dane w Polsce, a więc w Unii – w efekcie ten administrator danych z USA zostaje objęty przepisami RODO. Albo inna sytuacja: administrator danych ma siedzibę w USA i decyduje się skorzystać z usług podwykonawcy mającego siedzibę w Polsce, który przetwarza dane osobowe w Ukrainie – znów podmiot amerykański staje się objęty przepisami RODO. Nie wspomnę już o tym, że podmiot mający siedzibę w Polsce i będący administratorem danych stosuje RODO zawsze, niezależnie od tego, kto i gdzie przetwarza te dane osobowe. Rozwiązania outsourcingowe nie dość, że nie spowodują wyjścia przez podmioty mające jednostki organizacyjne w Unii spod zakresu stosowania RODO, to jeszcze mogą spowodować w przypadku podmiotów niemających jednostek organizacyjnych w Unii, a outsourcujących się do Unii, wejście przez nie w zakres stosowania RODO.

I teraz najważniejsze – jednostka organizacyjna. To autonomiczne pojęcie prawa wspólnotowego, więc nie możemy go rozumieć tak, jak rozumiemy pojęcie jednostki organizacyjnej na gruncie polskich przepisów o prowadzeniu działalności gospodarczej. Zresztą z tym pojęciem wiąże w sumie zabawna historia: pojęcie jednostki organizacyjnej w RODO wywodzi się z angielskiego słowa *establishment*, które używane jest w tym kontekście niezmiennie od czasów dyrektywy 95/46/WE. Problem w tym, że w polskiej wersji dyrektywy przetłumaczono go jako „prowadzenie działalności gospodarczej", ale w wyroku TS (Wielka Izba) z 13 maja 2014 r. (C-131/12,

*Google Spain and Google*) już jako „zakład". Z kolei w polskim tekście RODO mamy jednostkę organizacyjną – jedno słowo angielskie, trzy różne polskie tłumaczenia, zamieszanie gotowe. Wszystko to nie zmienia jednego: jednostkę organizacyjną rozumiemy w sposób elastyczny, nie wymagamy istnienia filii ani oddziału, a czasem wystarczy, że na terenie państwa działa nasz przedstawiciel i w tym państwie mamy rachunek bankowy i adres do doręczeń, aby przyjąć, że istnieje tam nasza jednostka organizacyjna.

W rezultacie także z tej perspektywy zakres zastosowania RODO jawi się jako ogromny – obrazu całości dopełniają już tylko wyłączenia spod niego, ale o tym w kolejnym rozdziale.

# Kiedy nie stosujemy RODO?

Aby w pełni określić zakres zastosowania RODO, oprócz jego strony pozytywnej, musimy przeanalizować także jego stronę negatywną, a więc uwzględnić wyjątki od zastosowania RODO, czyli sytuacje, w których świadomie i celowo wyłączone zostało stosowanie przepisów RODO.

Zacznę – dość przewrotnie – od wyjątku, którego w RODO nie ma: w dyrektywie tej nie znajdziemy odpowiednika wyjątku przewidzianego w ustawie o ochronie danych osobowych z 1997 r., zgodnie z którym przepisów o ochronie danych w zasadzie nie stosowało się do zbiorów danych osobowych tworzonych doraźnie; pomijając już to, że RODO odeszło od myślenia w kategoriach zbiorów danych. Dla stosowania (lub nie) RODO nie ma znaczenia to, że mamy te dane tylko przez chwilę, a później je usuniemy – czynność przetwarzania już nastąpiła i choćby trwała tylko przez moment, nie ma to znaczenia.

A zatem wyjątki: pierwszy, moim zdaniem najważniejszy, to ten przewidziany w art. 2 ust. 2 lit. a RODO; zgodnie z nim RODO nie stosujemy do takiego przetwarzania danych, które odbywa się w ramach działalności nieobjętej prawem Unii. Podstawowy problem polega jednak na tym, że istnieją bardzo istotne wątpliwości co do tego, czy zakresem prawa Unii Europejskiej objęty jest cały obszar ochrony danych osobowych, czy też może zakres zastosowania RODO zależy od tego, czy dana dziedzina prawa, w ramach której pojawia się kwestia ochrony danych osobowych, należy do zakresu prawa Unii. Mówiąc prościej, czy RODO stosuje się do ochrony danych osobowych w ogóle, jak ustawę z 1997 r., czy może tylko do ochrony danych osobowych tam, gdzie prawo Unii jest właściwe? A nie jest właściwe w każdym przypadku.

Przykładem sytuacji, w której prawo Unii nie jest właściwe, jest „bezpieczeństwo narodowe". Mówi o tym wprost samo RODO w motywie 16 preambuły. Ale czym jest „bezpieczeństwo narodowe"? Nie wiadomo – jednak np. w ustawie o obronie ojczyzny można znaleźć przepis, zgodnie z którym do przetwarzania danych przez organy wojskowe nie stosuje się RODO właśnie na podstawie art. 2 ust. 2 lit. a RODO.

Pomijając już to, że to tak nie działa (albo coś jest objęte zakresem prawa Unii, albo nie i nie można tego zadekretować w prawie krajowym), warto zauważyć, że także orzecznictwo sądowe uznaje, że wojsku z RODO nie po drodze – np. Wojewódzki Sąd Administracyjny (WSA) w Warszawie (wyrok z 6 sierpnia 2020 r., II SA/Wa 2222/19) przyjął, że RODO nie znajduje zastosowania do przetwarzania danych zawartych w ewidencji poborowych. Ale z drugiej strony coś tak nieunijnego i *par excellence* narodowego jak Instytut Pamięci Narodowej już RODO podlega, przynajmniej w ocenie NSA (wyrok z 25 sierpnia 2020 r., I OSK 3325/19). Gdzie tu logika? Nie wiem, przyznam szczerze, i zapewne jeszcze kilka lat przyjdzie nam poczekać na wyklarowanie tej sytuacji w orzecznictwie, ostatecznie prawdopodobnie w wykonaniu Trybunału Sprawiedliwości UE.

Drugi bardzo ważny przypadek niestosowania RODO, to przetwarzanie danych w ramach czynności o czysto osobistym lub domowym charakterze (art. 2 ust. 2 lit. c RODO). Przykłady takich czynności? Bardzo proszę: dane w prywatnym telefonie lub na prywatnym komputerze (motyw 18 preambuły do RODO). Istota tego wyłączenia to przetwarzanie danych w kontekście życia osobistego lub rodzinnego: planujemy ślub i tworzymy listę gości, wysyłamy kartki świąteczne, nagrywamy ważne wydarzenia rodzinne itp. Jeżeli natomiast celem przetwarzania danych jest udostępnienie ich nieograniczonemu kręgowi odbiorców albo gdy kontekst życia osobistego lub domowego wkracza do przestrzeni publicznej, wówczas takie przetwarzanie nie może zostać uznane za wyłączone spod zakresu zastosowania RODO – tak przynajmniej wynika z orzecznictwa TS UE, m.in.:

1) w sprawie C-101/01, *Lindqvist*, gdzie przyjęto, że wyjątek dla celów osobistych kończy się tam, gdzie zaczyna się rozpowszechnianie danych;
2) w sprawie C-345/17, *Buivids*, gdzie uznano, że zakresem zastosowania przepisów o ochronie danych osobowych jest objęte nagranie na wideo policjantów na komisariacie policji w chwili przyjmowania przez nich zeznań oraz opublikowanie tak nagranego wideo na stronie internetowej;
3) w sprawie C-212/13, *Ryneš,* gdzie uznano, że wykracza poza zakres wyjątku dla celów osobistych lub domowych stosowanie monitoringu przez osobę fizyczną na jej domu rodzinnym w celu ochrony własności, zdrowia i życia właścicieli domu, który to system monitoruje również przestrzeń publiczną.

Co ważne, na ten wyjątek mogą się powołać wyłącznie osoby fizyczne, a więc nie osoby prawne. Potencjalnie więc jednoosobowy przedsiębiorca może z tego wyjątku

skorzystać, ale musi rozgraniczyć to, co osobiste, od tego, co związane z prowadzoną działalnością.

I wreszcie ostatni wyjątek, o którym chciałbym napisać: przetwarzanie danych osobowych przez właściwe służby w celu zapobiegania i zwalczania przestępczości. Takie przetwarzanie danych podlega nie RODO, lecz szczególnej ustawie z 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. Gdy przedsiębiorca spotyka się więc z przetwarzaniem danych osobowych przez Policję, Straż Graniczną lub CBA w celu realizacji ich ustawowych zadań, może być pewny, że takie przetwarzanie nie jest regulowane przepisami RODO.

Co się dzieje tam, gdzie RODO nie sięga? Jako podstawa ewentualnych roszczeń pozostają przepisy o dobrach osobistych, z prywatnością na czele. W większości przypadków będą one skuteczne, choć niewątpliwie brak możliwości zaangażowania organu nadzorczego, czyli Prezesa Urzędu Ochrony Danych Osobowych (UODO), może czasami utrudniać dochodzenie ochrony swoich praw.

# Jak poprawnie komunikować się z klientami w sprawach ochrony danych osobowych?

Lubicie Państwo czytać przeróżne formułki i informacje dotyczące ochrony danych osobowych? „Wyrażam niniejszym dobrowolną zgodę na przetwarzanie...", „Pana dane osobowe stały się przedmiotem naruszenia poufności..." lub moje ulubione: „podanie danych jest dobrowolne, ale niezbędne". Lubicie? Bo ja nie lubię – ale czytam; czytam i nieraz włosy z głowy rwę, gdy myślę sobie, jak to miało wyglądać, a wyszło, jak zwykle. Ale po kolei.

Całą komunikacją wychodzącą od administratora danych do osoby, której dane dotyczą, wszelkie przekazywane informacje, polityki i komunikaty obejmuje tzw. zasada przejrzystości. Jej główne elementy to:

1) nakaz formułowania przekazu w sposób zwięzły, przejrzysty, zrozumiały i łatwo dostępny;
2) obowiązek posługiwania się jasnym i prostym językiem.

Zacznijmy od zwięzłości – w myśl zasady przejrzystości w sprawach dotyczących ochrony danych osobowych trzeba komunikować się w sposób efektywny i zwięzły, tak aby nie przytłoczyć odbiorcy informacjami. Nie jest więc tak, że im tzw. obowiązek informacyjny dłuższy, tym lepiej – wręcz przeciwnie. Zamiast tego zaleca się przekazywanie informacji w sposób warstwowy, tzn. przekazując tylko najważniejsze informacje, a do pozostałych odsyłając. Jak to działa? Zamiast pod umową pisać kilkadziesiąt linijek informacji dotyczących ochrony danych osobowych, napiszmy: kto te dane zbiera, po co i jakie prawa ma osoba, której dane są zbierane, a pozostałe informacje umieśćmy np. na odwrocie umowy, tak żeby można się było z nimi zapoznać. Zamiast na stronie internetowej umieszczać kilkadziesiąt linijek tekstu do przewijania, powiedzmy: kto i po co przetwarza dane osobowe i poinformujmy o prawach przysługujących osobie, której dane dotyczą, a w pozostałym za-

kresie odeślijmy np. do podlinkowanej polityki prywatności. To naprawdę lepiej wygląda, lepiej się to czyta i lepiej to działa – bo nie odrzuca zainteresowanego przy pierwszym spojrzeniu. Stosowanie podejścia warstwowego jest przy tym nie tylko akceptowane, ale i zalecane przez EROD i krajowe organy regulacyjne, w tym przez naszego Prezesa UODO.

Zrozumiałość przekazu wiąże się z używanym językiem – piszmy tak, żeby zrozumiał nas przeciętny odbiorca naszych towarów lub usług. Inaczej piszmy więc do dzieci, inaczej do profesjonalistów, inaczej do osób starszych. Naprawdę, Urząd Ochrony Danych Osobowych nie przyznaje punktów za stosowanie zdań wielokrotnie złożonych lub obco brzmiących zwrotów. Zamiast więc pisać do osoby dotkniętej wyciekiem danych, że może utracić kontrolę nad własnymi danymi, napiszmy, że ktoś może zaciągnąć kredyt na jej szkodę albo podszyć się pod nią w jej banku. Unikajmy nieostrych pojęć i piszmy precyzyjnie, bez używania sformułowań w rodzaju „możemy", „niektóre" lub „czasem". Konkretne przykłady? Bardzo proszę:

1) „Możemy wykorzystywać Twoje dane osobowe do celów badawczych" – źle; „Będziemy przechowywać i badać informacje na temat Twoich ostatnich wizyt na naszej stronie i sposobu, w jaki poruszasz się po różnych sekcjach naszej strony, do celów analitycznych, aby dowiedzieć się, w jaki sposób użytkownicy korzystają z naszej strony i uczynić ją bardziej intuicyjną" – dobrze;
2) „Możemy wykorzystywać Twoje dane osobowe do opracowywania nowych usług" – źle; „Będziemy przechowywać historię Twoich zakupów i wykorzystywać szczegółowe informacje na temat produktów, które kupiłeś w przeszłości, aby proponować Ci inne produkty, którymi naszym zdaniem możesz być zainteresowany" – dobrze;
3) „Możemy wykorzystywać Twoje dane osobowe do oferowania spersonalizowanych usług" – źle; „Będziemy rejestrować, na które artykuły na naszej stronie kliknąłeś, i wykorzystamy te informacje do tworzenia na tej stronie reklam przeznaczonych dla Ciebie, które będą dopasowane do Twoich zainteresowań, zidentyfikowanych przez nas na podstawie przeczytanych przez Ciebie artykułów" – dobrze.

Używajmy też takiego języka, jakim posługują się osoby, do których kierujemy nasz przekaz – jeżeli np. prowadzimy rekrutację i kierujemy ją także do osób pochodzenia ukraińskiego, przygotujmy po ukraińsku nie tylko samo ogłoszenie, ale też informację dotyczącą ochrony danych osobowych.

Przejrzystość komunikacji oznacza, że informacje dotyczące ochrony danych osobowych nie mogą być poukrywane gdzieś między wierszami, wrzucone do któregoś tam paragrafu umowy lub zaszyte w gęstwinie regulaminu. Ta komunikacja musi być wyraźnie oznaczona jako dotycząca danych osobowych, najlepiej gdy będzie wyodrębniona, np. ramką albo czcionką tak, by już na pierwszy rzut oka było jasne, że jest to coś ważnego, co warto przeczytać.

Wreszcie łatwa dostępność – niech zainteresowany nie będzie zmuszony do gorączkowego poszukiwania informacji. Zamiast tego miejsce i sposób dostępu do informacji powinny być oczywiste, a informacje dotyczące ochrony danych osobowych – być stale dostępne, np. na stronie internetowej przedsiębiorcy.

Przejrzystość komunikacji w sprawach dotyczących ochrony danych osobowych wpisuje się w szerszy tręd upraszczania języka stosowanego w korespondencji z naszymi klientami. To nie moda, ale wymóg czasów – w zalewie wszelkiego rodzaju informacji, na jaki jesteśmy codziennie narażeni, starajmy się postępować tak, żeby ułatwiać naszym klientom dotarcie do istotnych dla nich informacji i ich zrozumienie. A temu właśnie służy zasada przejrzystości.

# Im więcej danych, tym (nie zawsze) lepiej

Z perspektywy biznesu zazwyczaj im więcej zebranych danych osobowych, tym lepiej – na zasadzie, że a nuż się kiedyś przydadzą. Im więcej danych o kliencie, tym lepiej możemy go sprofilować; im więcej danych o kandydacie do pracy, tym lepiej, bo rekrutacja będzie bardziej efektywna; im więcej danych w programie lojalnościowym, tym lepiej, bo zbudujemy dokładniejszy profil uczestnika – i tak dalej. Myliłby się jednak ten, kto by na takie praktyki bezrefleksyjnie zezwalał – prawo ochrony danych osobowych widzi problem zakresu danych osobowych nieco inaczej.

Zakres danych, czyli kategorie danych osobowych, jakie zbieramy w konkretnym procesie przetwarzania: imię, nazwisko, adres zamieszkania, numer telefonu, historia zakupów, ulubione marki, wykształcenie i doświadczenie zawodowe – to tylko ułamek potencjalnych kategorii danych osobowych, które możemy sobie wyobrazić. To, jakie dane o osobie fizycznej możemy zbierać, zależy od celu, w jakim będziemy je przetwarzać. Inaczej mówiąc, z tego, po co nam są dane, wynika, jakie dane możemy zbierać. Przykładowo, gdy prowadzimy księgarnię internetową i ktoś kupuje u nas książkę, musimy wiedzieć, kto jest stroną umowy sprzedaży (co najmniej imię i nazwisko), co kupił (tytuł książki), gdzie ją wysłać (adres, może numer automatu do paczek, a wtedy i numer telefonu, a być może i adres poczty elektronicznej) i jak klient za nią zapłaci (tu zazwyczaj sprzedawca dostaje po prostu informację, że zapłacił). Jeżeli sklep wysyła potwierdzenie zakupu, co jest standardem, dodatkowo powinno się zbierać adres poczty elektronicznej – i tyle. Gdy dodatkowo chcemy wiedzieć, jakich autorów i autorki lubi czytać i jakie gatunki literatury go interesują, musimy te informacje przetwarzać dla innego celu, niż wykonanie umowy sprzedaży – tym celem w typowej sytuacji będzie nasz własny marketing i do tak określonego celu znów dobieramy zakres danych osobowych: adres poczty elektronicznej, może numer telefonu komórkowego, a także informacje potrzebne do personalizacji mailingu, jak wspomniane już wyżej zainteresowania czytelnicze.

Jak dowiadujemy się z art. 4 ust. 1 lit. c RODO, dane osobowe muszą być „adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane". To właśnie zasada minimalizacji danych osobowych, którą w poprzednim akapicie analizowaliśmy: zakres przetwarzanych danych zawsze wynika z celu ich przetwarzania. Takie, a nie inne, sformułowanie jest nieco mylące: adekwatne to jednak co innego niż niezbędne, a to, co jest adekwatne, nie zawsze musi być jednocześnie niezbędne. Z upływem czasu, jak się wydaje, wykładnia opowiedziała się za rozumieniem zasady minimalizacji jako bliższej adekwatności niż niezbędności. Taka właśnie myśl wyłania się z wyroku WSA w Warszawie z 7 sierpnia 2023 r. (II SA/Wa 809/20), w którym sąd przyjął, że „użyte w przepisie art. 5 ust. 1 lit. c RODO określenie «adekwatne» oznacza «odpowiednie, zgodne, proporcjonalne, nienadmierne» i może być traktowane jako synonim słowa «stosowne»".

Zatem „adekwatne" oznacza „stosowne" (w domyśle: w stosunku do celu przetwarzania). A kto decyduje, czy określone dane są „stosowne" do celu przetwarzania? Administrator danych, a przynajmniej tak się właśnie dzieje w większości przypadków. Określenie zakresu danych to jeden z kluczowych elementów projektowania procesu przetwarzania danych osobowych: gdy już wiemy, po co (w jakim celu) będziemy przetwarzać dane, kolejnym etapem powinno być ustalenie, jakie kategorie danych będziemy zbierać i przetwarzać. Co do zasady więc to decyzja – i odpowiedzialność – administratora; zwłaszcza tę odpowiedzialność trzeba tutaj podkreślić, gdyż jeżeli Prezes UODO uzna, że administrator zbiera zbyt dużo danych, może mu nakazać ograniczenie zakresu zbieranych danych na przyszłość oraz usunięcie danych już zebranych z naruszeniem zasady minimalizacji. I jedno, i drugie może administratora drogo kosztować: trzeba przebudować bazę danych, zmienić stosowane formularze oraz usunąć zebrane dane, co oznacza tylko jedno: koszty. A że zakres zbieranych danych jest zazwyczaj bardzo prosto ustalić, to i ryzyko w przypadku zbierania danych nadmiarowych materializuje się stosunkowo łatwo.

Problem odpowiedzialności za nadmiarowe dane nie występuje wtedy, gdy zakres przetwarzanych danych został z góry określony przez ustawodawcę, co w polskich realiach występuje stosunkowo często. Ba, każdy pracodawca spotyka się z tą praktyką na gruncie przepisów Kodeksu pracy, który w art. $22^1$ określa w formie katalogu dane, które pracodawca może zbierać od kandydata do pracy i od pracownika. Na podobny zabieg zdecydowano się także w przepisach Prawa telekomunikacyjnego, ustawy o świadczeniu usług drogą elektroniczną oraz w wielu regulacjach z zakresu prawa administracyjnego.

Określenie w przepisach prawa katalogu przetwarzanych danych ma też negatywne konsekwencje: usztywnia proces przetwarzania danych osobowych w tym sensie, że uniemożliwia zbieranie innych danych niż wskazane w przepisie. O ile w sektorze publicznym ma to głęboki sens w kontekście art. 51 Konstytucji RP, o tyle w sektorze prywatnym sprawia, że nie istnieje możliwość dostosowania takiego procesu przetwarzania danych do zmiennych realiów. Dlatego zazwyczaj katalogowi danych towarzyszy możliwość jego rozszerzenia, typowo za zgodą osoby, której dane dotyczą. Ale uwaga – jeżeli administrator danych na takie rozszerzenie się zdecyduje, wówczas to on określa zakres danych, które chce zbierać ponad katalog ustawowy, a więc to on ponosi odpowiedzialność za zgodność tego zakresu danych z zasadą minimalizacji. W zakresie dodatkowych danych mamy więc sytuację analogiczną do opisanej wyżej, a więc i potencjalnie analogiczne problemy w przypadku naruszenia zasady minimalizacji.

# Kopiować czy nie kopiować dokumenty tożsamości?

Wśród praktycznych problemów związanych z ochroną danych osobowych w organizacjach regularnie wraca jedno konkretne pytanie: kopiować dokumenty tożsamości czy ich nie kopiować? Mam na myśli dokumenty kandydatów do pracy, pracowników, współpracowników, klientów; dowody osobiste, paszporty, legitymacje. A jeżeli kopiować, to może także inne dokumenty, nie tylko dokumenty tożsamości: umowy, zaświadczenia, protokoły – słowem wszystko to, co zawiera informacje potrzebne tym organizacjom.

Problem kopiowania dokumentów najlepiej przedstawić na przykładach: rekrutujemy nowego pracownika, a więc zbieramy jego dane osobowe – i prosimy go o kopię lub skan dowodu osobistego, kopię dyplomu ukończenia studiów, kopię dokumentów poświadczających jego kwalifikacje; zawieramy umowę z konsumentem – prosimy go więc o kopię dowodu osobistego; wynajmujemy mieszkanie – do umowy załączamy kopię dowodu osobistego najemcy; przyjmujemy wniosek o pożyczkę z kasy zapomogowo-pożyczkowej z przeznaczeniem na remont mieszkania – prosimy o kopię umowy najmu tego mieszkania. I tak dalej, praktyki kopiowania dokumentów zdają się nie mieć końca.

Zacznijmy od tego, czym jest kopiowanie dokumentów – z punktu widzenia prawa ochrony danych osobowych to nic więcej, jak po prostu zbieranie danych osobowych (tak to przynajmniej widziały polskie sądy administracyjne – zob. wyrok NSA z 13 lipca 2004 r., OSK 420/04, oraz wyrok NSA z 19 grudnia 2001 r., II SA 2869/00). Kopiowanie dokumentów zawierających dane osobowe to technika zbierania danych, ale taka, która niesie ze sobą bardzo konkretne zagrożenia wpisane w nią samą, które przekładają się na ryzyka zarówno dla organizacji, która decyduje się na kopiowanie dokumentów, jak i dla osób, których dokumenty zostały skopiowane.

Pierwsze ryzyko wiąże się z gromadzeniem zbyt dużej ilości danych. Jedną z podstawowych reguł prawa ochrony danych osobowych jest gromadzenie tylko takich danych, które są odpowiednie do celu, w jakim te dane są przetwarzane. I patrząc z tej perspektywy na kopiowanie dokumentów, warto się zastanowić, po co pracodawcy np. informacja o wzroście pracownika, która znajduje się jeszcze w niektórych dowodach osobistych? A taką informację zbierze, jeżeli skopiuje dowód osobisty wydany przed 31 grudnia 2014 r. Po co kasie zapomogowo-pożyczkowej informacja o tym, kto jest wynajmującym mieszkanie pracownikowi? A taką informację zbierze, gdy skopiuje umowę najmu mieszkania w związku z wnioskiem o pożyczkę na cele remontowe. Tego rodzaju przykłady można mnożyć w nieskończoność i zawsze będą prowadziły do jednego wniosku: kopiowanie dokumentów, w tym dokumentów tożsamości, zazwyczaj powoduje zbieranie nadmiarowych danych osobowych.

Drugi problem, znów dla organizacji, która wdrożyła kopiowanie dokumentów jako technikę zbierania danych, to problem przydatności danych zebranych w ten sposób. Co wynika z tego, że ktoś pokaże nam wypis z aktu notarialnego obejmującego umowę, na podstawie której ten ktoś kupił dom lub mieszkanie? Wynika tylko to, że ten ktoś zawarł taką właśnie umowę – ale wcale nie wynika, że jest właścicielem tego domu lub mieszkania! Przecież jeszcze w tym samym dniu mógł je sprzedać innej osobie. Co wynika z tego, że poprosimy osobę, która się z nami kontaktuje listownie i prosi np. o wydanie zaświadczenia, o przesłanie przez nią kopii jej dowodu osobistego? Czy będziemy mieli pewność, że osoba, z którą korespondujemy, jest tą samą, za którą się ona podaje? Nie, będziemy tylko pewni tego, że druga strona ma dostęp do kopii dowodu osobistego, który nam przesłała – ale nadal nie będziemy wiedzieć, kto jest po drugiej stronie.

Trzeci problem, który wiąże się z kopiowaniem dokumentów, zwłaszcza dokumentów tożsamości, pojawia się wtedy, gdy dojdzie do wycieku takich kopii. Jak pokazują dane, wyciek skanów dowodów osobistych rodzi istotnie większe ryzyko kradzieży tożsamości osób dotkniętych wyciekiem. Decydując się na kopiowanie dokumentów tożsamości, trzeba więc uwzględnić ryzyko z tym związane i zastosować odpowiednio większe środki zabezpieczenia zebranych w ten sposób danych.

Kopiować więc czy nie kopiować? Gdybym miał odpowiedzieć jednym słowem, odpowiedziałbym „nie”: zbyt duże ryzyko, zbyt mało korzyści, zbyt wiele niekoniecznie przydatnych danych. Nie bez znaczenia pozostaje też to, że konsekwentnie przeciwko praktykom kopiowania dokumentów zawierających dane osobowe wypowiada się

Prezes UODO. Choć jego stanowisko jest w tym kontekście nieco dyskusyjne (twierdzi, że „[s]porządzenie kopii dowodów tożsamości jest legalne jedynie wtedy, kiedy wynika to wprost z przepisów rangi ustawy", zob. pismo do Prezesa Związku Banków Polskich, https://archiwum.uodo.gov.pl/pl/138/1182), to w swym ogólnym wydźwięku stwierdza wyraźnie: nie kopiować, chyba że konieczność kopiowania wynika z przepisów ustawy. Tak będzie w szczególności w dwóch przypadkach:

1) gdy pracodawca zatrudniający cudzoziemca ma prawny obowiązek przechowywania kopii dokumentu pobytowego cudzoziemca przez cały okres wykonywania przez niego pracy,
2) jeżeli podmiot stosujący przepisy ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu w pewnych przypadkach może zastosować środki bezpieczeństwa finansowego polegające na sporządzeniu kopii dokumentów tożsamości klienta.

Poza przypadkami, w których obowiązek kopiowania dokumentów wynika z przepisów ustawy, rekomendowanym rozwiązaniem jest okazanie dokumentu i zebranie (spisanie) tylko tych danych, które są organizacji przydatne, bez kopiowania całego dokumentu.

# Kiedy usuwamy dane osobowe?

Jeden z moich klientów otrzymał niedawno od jednego ze swoich klientów wniosek o kopię swoich danych osobowych. Kopia została sporządzona – składała się z zestawu kilkudziesięciu faktur, klient uznał, że najprościej mu będzie te faktury po prostu zeskanować i wysłać – i przesłana klientowi. I jakież było zdziwienie mojego klienta, gdy niedługo po tym dotarła do niego informacja z Urzędu Ochrony Danych Osobowych, że oto została na niego złożona skarga przez tego samego klienta, który otrzymał kopię swoich danych osobowych. Skarga, dodajmy, związana ze zbyt długim przechowywaniem danych osobowych – bo oto okazało się, że mój klient miał w swych zasobach faktury od początku swojej działalności (bagatela, ponad 20 lat) i kopie tych faktur bezrefleksyjnie udostępnił swojemu klientowi.

Zacznijmy od początku – danych osobowych nie wolno przechowywać bez żadnego ograniczenia czasowego, czyli w nieskończoność. Jest to jedna z fundamentalnych zasad prawa ochrony danych osobowych, zwana zasadą ograniczenia przechowywania danych. Zasada ta dosłownie brzmi tak: „[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". Mamy więc konstrukcję, w której czas przechowywania danych osobowych jest wyznaczany przez cel przetwarzania tych danych: dane przechowujemy tak długo, jak jest to niezbędne do osiągnięcia celu przetwarzania. Nawiasem mówiąc, cel przetwarzania danych to podstawowa zmienna, która definiuje cały proces przetwarzania danych (na gruncie RODO zwany dla niepoznaki czynnością przetwarzania): cel wyznacza to, jakie dane zbieramy; cel ma wpływ na podstawę przetwarzania danych; cel – a precyzyjnie: jego zrealizowanie – wyznacza chwilę usunięcia danych.

Jak działa zasada ograniczenia przechowywania danych? Działa co najmniej na dwóch płaszczyznach:

1) w celu zapewnienia rozliczalności, czyli jako element dokumentacji ochrony danych osobowych;

2) w celu zapewnienia rzeczywistej zgodności z prawem, czyli uruchamiając proces usuwania danych.

Zasada ograniczenia przechowywania danych na poziomie dokumentacji ochrony danych osobowych to po prostu zapisanie w rejestrze czynności przetwarzania danych planowanych terminów usunięcia poszczególnych kategorii danych osobowych w ramach określonego procesu. Tylko skąd administrator danych ma wiedzieć, po jakim terminie powinien usunąć dane? Mamy w tym zakresie dwie możliwości:

1) okres przechowywania danych może zostać zapisany w powszechnie obowiązujących przepisach prawa;
2) okres przechowywania danych może zostać samodzielnie określony przez administratora danych.

Ta pierwsza sytuacja to po prostu przepis prawa, który mówi, jak długo przechowujemy dane w określonym celu. Przykładem takiego rozwiązania mogą być choćby nieszczęsne faktury, które dały początek tym rozważaniom – otóż oryginały i kopie faktur VAT przechowujemy przez 5 lat od końca roku, w którym upłynął termin płatności podatku. Inny przykład to dane pracownicze – tu z kolei zasada jest taka, że dokumentację pracowniczą należy przechowywać przez okres zatrudnienia pracownika, a także przez okres 10 lat, licząc od końca roku kalendarzowego, w którym stosunek pracy uległ rozwiązaniu lub wygasł.

Jeżeli żaden przepis prawa nie określa, jak długo należy przechowywać określone kategorie danych osobowych, wówczas to administrator danych powinien ten okres zdefiniować samodzielnie. Zasadą jest, że dane przechowujemy przez cały czas istnienia celu ich przetwarzania – czyli jeżeli tym celem jest np. wykonywanie umowy najmu, wynajmujący przechowuje dane najemcy przez cały czas trwania umowy najmu; jeżeli dane są przetwarzane w celu marketingowym na podstawie zgody – są przechowywane tak długo, jak długo ta zgoda nie zostanie odwołana. Jeżeli ten cel ustanie, bo np. rozwiązano umowę najmu albo odwołano zgodę, oczywiście nie usuwamy danych od razu: jeżeli wystawiono fakturę, dane przechowujemy przez 5 lat itd. (patrz wyżej). Jeżeli natomiast faktury nie wystawiono i nie istnieją żadne przepisy, które nakazywałyby przechowywać dane przez określony czas, pozostaje kwestia roszczeń: otóż zawsze może się zdarzyć tak, że najemca po zakończeniu umowy postanowi nas pozwać, twierdząc np., że nadpłacił czynsz; może się zdarzyć tak, że po odwołaniu zgody ktoś, komu wysyłaliśmy przez lata treści marketingowe, „przypomni sobie", że jednak tej zgody nigdy nie wyraził i też postanowi nas pozwać.

A jak się bronić, nie mając danych? Dlatego podejmując decyzję o tym, kiedy usunąć dane, wypada uwzględnić jeszcze okres przedawnienia roszczeń, które mogą zostać podniesione wobec nas (albo które my możemy podnieść) w związku z takim przetwarzaniem.

Gdy już zdefiniujemy okres przetwarzania danych, pozostaje nam przejść do drugiej płaszczyzny działania zasady ograniczenia przechowywania danych, czyli do faktycznego usuwania danych po wymaganym czasie. W małej organizacji można to robić ręcznie, choć na pewno preferowane będą rozwiązania automatyczne, bo tylko takie zapewniają powtarzalność i względną pewność, że dane zostaną rzeczywiście usunięte.

Bezpieczna firma musi więc wdrożyć rozwiązania zapewniające, że nie będzie przetwarzała danych osobowych w nieskończoność, bez żadnego ograniczenia czasowego. A niezależnie od tego, przesyłając klientowi kopię jego danych osobowych, radzę dwa razy się zastanowić nad tym, co w tej kopii się znajduje.

# Dokumentacja ochrony danych osobowych

Przed kilkoma laty zameldowaliśmy się z Żoną na izbie przyjęć pewnego szpitala, celem przyjęcia na planowany zabieg; siedzieliśmy i czekaliśmy na swoją kolej, a tymczasem przyjmowane były pacjentki, które zgłosiły się na tąż izbę przyjęć z bólami porodowymi i rozpoczętą akcją porodową. I każda z tych pacjentek, zanim została przyjęta, otrzymywała plik „dokumentów RODO" z prośbą o podpisanie na każdej stronie. Podpisanie, żeby szpital mógł wykazać, że im te dokumenty przekazał. A treścią tych dokumentów było nic innego, jak informacja – słynne klauzule – dotycząca przetwarzania danych.

Co szpital osiągnął w ten sposób, prócz dozgonnej nienawiści pod adresem przepisów o ochronie danych osobowych? Niewiele albo prawie nic. A na pewno postąpił wbrew jednej z podstawowych zasad ochrony danych osobowych, jaką jest zasada rozliczalności.

Czym jest rozliczalność w znaczeniu, jakie nadaje temu pojęciu art. 5 ust. 2 RODO? Jak tłumaczy Grupa Robocza art. 29, na rozliczalność składają się dwa elementy. Po pierwsze, każdy administrator danych ma obowiązek wdrożenia odpowiednich środków, w tym wewnętrznych procedur, gwarantujących przestrzeganie przepisów o ochronie danych w związku z operacjami ich przetwarzania. Po drugie, rozliczalność oznacza konieczność sporządzenia dokumentacji wskazującej osobom, których dane dotyczą, oraz organom nadzorczym, jakie środki podjęto, aby zapewnić przestrzeganie przepisów o ochronie danych osobowych (Opinia 3/2010 w sprawie zasady rozliczalności, WP 173, str. 9). Mówiąc prościej, rozliczalność oznacza, że trzeba zrobić tak, żeby było zgodnie z prawem i żeby móc to wykazać.

Jak to zrobić, żeby było zgodnie z prawem? – wypełniać obowiązki wynikające z RODO. Dobrze, ale jak tą zgodność wykazać? Poległo na tym wielu, że przywołam przykład pewnego polskiego administratora danych, który uznał, że jedynym

sposobem wykazania tego, że przekazał osobom, których dane dotyczą, informację o przetwarzaniu ich danych, jest wysłanie jej… listem poleconym – no bo jak inaczej mógłby wykazać, że ją przekazał? Inny przykład opacznego rozumienia rozliczalności to postępowanie szpitala, o którym wspominałem wyżej: przekazał, co według niego można wykazać tylko własnoręcznym podpisem. Tymczasem takie podejście, zakładające udowadnianie zgodności z prawem każdego pojedynczego przypadku, pozostaje w jawnej sprzeczności z istotą rozliczalności, która polega na wykazywaniu zgodności w odniesieniu do całego procesu przetwarzania danych osobowych.

I w tym miejscu właśnie pojawia się tytułowa dokumentacja ochrony danych osobowych. Bo założenie jest jasne od początku: konsekwencją zasady rozliczalności jest to, że w razie sporu z osobą, której dane dotyczą, albo z organem nadzorczym administrator danych powinien być w stanie przedstawić dowody na to, iż przestrzega przepisów o ochronie danych osobowych. Ale dowodami takimi mogą być przede wszystkim dokumenty opisujące zasady przetwarzania i ochrony danych osobowych, czyli właśnie dokumentacja. Pomimo braku wyraźnego wymogu wynikającego z przepisów RODO – zasadne i rekomendowane jest prowadzenie dokumentacji przetwarzania danych osobowych, czyli „polityk ochrony danych", o których mowa w art. 24 ust. 2 RODO.

Jak takie polityki działają? Są narzędziem wykazywania zgodności, czego przykładem może być owa sprawa, w której pojawił się pomysł wysyłania informacji o ochronie danych osobowych pocztą poleconą. Co na to Prezes UODO? W decyzji z 15 marca 2019 r. (ZSPR.421.3.2018) stwierdził wprost, że z przepisów RODO nie wynika, „żeby prawodawca nałożył na administratora obowiązek wysyłania takiej informacji np. przesyłką poleconą, byleby tylko administrator mógł stosownymi dowodami wykazać, że ów obowiązek informacyjny został przez niego spełniony wobec podmiotów, których dane osobowe przetwarza". Jak więc wykazać, że ten obowiązek się spełniło? Na przykład umową na wysyłkę wiadomości SMS lub e-mail zawierających informację; umową na wysyłkę listów, ale zwykłych, nie poleconych; odpowiednimi postanowieniami polityki ochrony danych, opisującymi cały proces. Przekładając to na przykład szpitala i podpisywania dokumentów, wystarczyło informację dotyczącą ochrony danych osobowych wystawić w widocznym miejscu na ladzie recepcyjnej, a cały proces opisać w dokumentacji ochrony danych. Inny przykład to skrypt rozmowy prowadzonej przez telemarketera: to właśnie skrypt jest podstawowym narzędziem wykazywania treści rozmowy, czyli np. tego, czy w jej trakcie przekazano informacje wymagane przez RODO.

Choć RODO nie zawiera praktycznie żadnych wytycznych odnoszących się do sposobu prowadzenia dokumentacji przetwarzania danych osobowych ani jej zawartości, w praktyce można wskazać trzy grupy dokumentów składających się na dokumentację ochrony danych:

1) polityka ochrony danych jako samodzielny środek mający zapewnić, by przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać;
2) dokumenty wymagane przez RODO, jak np. rejestr czynności przetwarzania danych lub raport z analizy ryzyka;
3) dokumenty związane z wykonywaniem obowiązków wynikających z RODO, jak np. dokumenty dotyczące naruszeń ochrony danych.

Spośród nich zdecydowanie najistotniejsza na co dzień jest polityka ochrony danych, która będzie stanowiła dowód na wdrożenie rozwiązań zapewniających zgodność z RODO i może być doskonałym narzędziem umożliwiającym szkolenie pracowników.

Przy pomocy dokumentacji ochrony danych nie możemy wykazywać tylko jednego: zgody na przetwarzanie danych osobowych, co wynika wprost z art. 7 ust. 1 RODO (i co może był kolejnym argumentem przeciwko „zgodozie"). W pozostałym zakresie dokumentacja to doskonały środek służący wykazywaniu zgodności z RODO, do której opracowania i wdrożenia nieodmiennie zachęcam.

# „Zgodoza", czyli dlaczego tak lubimy zgodę na przetwarzanie danych?

Zgody na przetwarzanie danych osobowych są wszędzie: w kontaktach z urzędami, w aplikacjach, które instalujemy na telefonie, na stronach internetowych, które odwiedzamy. Wymaga się od nas „zgody na nagrywanie rozmów telefonicznych", „na monitoring w sklepie" i wielu, wielu innych jeszcze zgód. Ale czy słusznie? Czy rzeczywiście zgoda jest najlepszą z podstaw przetwarzania danych osobowych?

Żeby odpowiedzieć na to pytanie, trzeba przypomnieć, po co nam jest właściwie ochrona danych osobowych – po to, żeby z góry określić w przepisach prawa, kiedy można te dane przetwarzać. Europejski pomysł na ochronę danych zakłada istnienie tzw. podstaw prawnych przetwarzania danych osobowych, czyli sytuacji wskazanych w przepisach prawa, kiedy te dane można zbierać i dalej przetwarzać. I wśród tych podstaw przetwarzania danych mamy także zgodę, zazwyczaj wymienianą na pierwszym miejscu (tak też jest w art. 6 ust. 1 i art. 9 ust. 2 RODO). Ale czy to znaczy, że zgoda jest rzeczywiście podstawą pierwszego wyboru, jeśli chodzi o przetwarzanie danych? Nie, nie jest – to wymienienie zgody na początku wyliczenia podstaw przetwarzania danych to nic innego, jak ukłon w stronę zasady autonomii informacyjnej, która odcisnęła ogromne piętno na tym, jak dzisiaj podchodzimy do prawa do ochrony danych osobowych.

Zacznijmy od administracji publicznej, która w zasadzie w ogóle nie powinna opierać przetwarzania danych osobowych na zgodzie osób, których dane dotyczą. Jeżeli bowiem organ władzy publicznej przetwarza dane w celu wykonania swoich władczych kompetencji, np. w postępowaniu administracyjnym, wówczas zwyczajnie nie wolno mu przetwarzać danych osobowych na podstawie zgody osoby, której dane dotyczą, ani na żadnej innej podstawie, poza podstawą wynikającą z przepisów prawa. Jest to naturalna konsekwencja zasady legalizmu działania administracji, której wolno tyle,

ile wynika z przepisów prawa. Gdyby takie przetwarzanie oprzeć na zgodzie, można by doprowadzić do powstania mylnego wrażenia, że podanie danych jest dobrowolne, przez co osoba, której dane dotyczą, mogłaby zostać wprowadzona w błąd. Z kolei jeżeli podmioty publiczne wykonują działania niewładcze, np. informują, edukują, promują, wówczas naturalnym wyborem powinno być przetwarzanie danych na podstawie art. 6 ust. 1 lit. e RODO jako niezbędne do wykonania zadania w interesie publicznym. Oczywiście te zadania muszą wynikać z przepisów prawa – przykładem może być zadanie własne gminy, o którym mowa w art. 7 ust. 1 pkt 18 ustawy o samorządzie gminnym, jakim jest promocja gminy. Jeżeli w wykonaniu tego zadania gmina będzie organizowała np. konkurs na hasło promujące gminę, wówczas przetwarzanie danych na potrzeby tego konkursu będzie się odbywało właśnie jako przetwarzanie niezbędne do wykonania zadania realizowanego w interesie publicznym. Inne przykłady zadań realizowanych w interesie publicznym, w ramach których przetwarzanie danych osobowych będzie następowało na zasadzie wynikającej z art. 6 ust. 1 lit. e RODO, to konsultacje z mieszkańcami gminy czy budżet obywatelski.

W praktyce wygląda to różnie – pierwszy z brzegu przykład to Portal Podatkowy, który przy założeniu konta wymaga... tak, zgody na przetwarzanie danych. Znam przypadek gminy, która oczekiwała zgody na przetwarzanie danych przy zameldowaniu. To w oczywisty sposób błędne praktyki, z którymi trzeba walczyć.

A sektor prywatny? Ten oczywiście nie jest dotknięty takimi samymi ograniczeniami, jak administracja publiczna, ale także zdarza mu się pozyskiwać zgody na przetwarzanie danych, które są zwyczajnie bez sensu. Przykładem może być zawieranie umów z konsumentami i praktyka oczekiwania zgody „na przetwarzanie danych w celu wykonania umowy". Taka praktyka jest błędna, ponieważ jeżeli przedsiębiorca zawiera umowę z osobą fizyczną, wówczas już sam ten fakt zawarcia umowy wystarczy w świetle art. 6 ust. 1 lit. b RODO do przetwarzania danych w zakresie niezbędnym do wykonania umowy. Zbierając zgody, po pierwsze, wprowadzalibyśmy w błąd co do rzeczywistej podstawy przetwarzania danych, co prowadziłoby do naruszenia zasady przejrzystości. Po drugie, mogłoby dojść do trudnych do rozwikłania skutków – bo zgodę można zawsze odwołać, jak więc zinterpretować oświadczenie o odwołaniu takiej zgody udzielonej w kontekście umowy? Wypowiedział umowę? Chyba tak, skoro nie chce już przetwarzania danych na potrzeby tej umowy... Inna typowa sytuacja to oczekiwanie zgody na przetwarzanie danych „w celu rekrutacyjnym" – otóż taka zgoda jest potrzebna tylko wtedy, gdy tworzymy bazę danych po-

tencjalnych kandydatów do pracy, z którymi chcemy się kontaktować w przyszłości. Jeżeli kandydat przesyła ofertę w odpowiedzi na konkretne ogłoszenie i nie chcemy budować bazy danych kandydatów, zgoda na przetwarzanie danych jest zbędna, a dane przetwarzamy na podstawie art. 6 ust. 1 lit. b RODO. Zgoda na przetwarzanie danych na potrzeby monitoringu nie jest potrzebna, bo stosowanie monitoringu w celu ochrony mienia, np. w sklepie, to typowy przykład realizacji tzw. uzasadnionego interesu administratora danych, a więc podstawa z art. 6 ust. 1 lit. f RODO. Nie ma również potrzeby prosić o zgodę na nagrywanie rozmowy – o nagrywaniu trzeba poinformować, bo głos to po prostu nowa kategoria danych osobowych.

Czym jest więc tytułowa „zgodoza”? To schorzenie trapiące naszą polską praktykę stosowania prawa ochrony danych osobowych, polegające na przywiązywaniu nadmiernej wagi do zgody na przetwarzanie danych i na stosowaniu jej tam, gdzie przetwarzanie danych można oprzeć na innej podstawie. Oczywiście nie unikniemy sytuacji, w których zebranie zgody na przetwarzanie danych będzie niezbędne – ale starajmy się takie sytuacje ograniczać do minimum, a w sektorach takich, jak sektor publiczny, zgód w ogóle unikajmy.

# Prawo do uzyskania kopii danych osobowych

Prawo do uzyskania kopii danych osobowych jest jednym z tych praw, które po raz pierwszy zostały nam przyznane dopiero w przepisach RODO. Od rozpoczęcia stosowania ogólnego rozporządzenia minęło już ponad 5 lat, więc stopniowo zaczynają się pojawiać rozstrzygnięcia TS UE dotyczące pierwszych spraw powstałych na kanwie przepisów RODO. Tak też się stało w odniesieniu do prawa do uzyskania kopii danych osobowych – wyrokiem w sprawie C-487/21, *Österreichische Datenschutzbehörde*, TS UE rozstrzygnął chyba najbardziej istotną kwestię związaną z wykonywaniem tego prawa. Ale nie uprzedzajmy faktów.

Dostęp każdego z nas do informacji na nasz temat to fundament ustroju informacyjnego naszego państwa, gwarantowany także przez art. 8 Karty praw podstawowych Unii Europejskiej. Historycznie rzecz biorąc, przyjmował on postać prawa wglądu do danych, które rozumiano jako prawo dostępu do treści danych osobowych, bez wglądu do nośników danych – taka wykładnia była powszechnie akceptowana w Polsce i innych krajach Unii na gruncie dyrektywy 95/46/EW, czyli poprzedniczki RODO. Nieco upraszczając: korzystając z tego prawa, można było otrzymać raport z bazy danych zawierającej nasze dane z treścią tych danych, ale zajrzeć do tej bazy już nie; można było otrzymać treść danych, jakie na nasz temat zebrał administrator, ale kopii dokumentów, przy pomocy których to zrobił, już nie. A takie kopie dokumentów czasem okazują się przydatne, np. w kontekście toczonych przez nas sporów.

Problem z takim rozumieniem prawa dostępu do danych jest jednak tego rodzaju, że obecnie w art. 15 RODO akcentowane jest słowo „kopia" – powstało więc pytanie, czy być może „przepis ten ustanawia ogólne prawo osoby, której dane dotyczą, do otrzymania kopii – również – całych dokumentów, w których przetwarzane są dane osobowe tej osoby", które legło u podstaw wyroku w sprawie C-487/21. Czy więc musimy przekazać kopie dokumentów, czy wystarczy raport z bazy danych?

Zasadniczy wniosek wypływający z wyroku TS UE w sprawie C-487/21 można sprowadzić do stwierdzenia, że osobom, których dane dotyczą, co do zasady nie przysługuje prawo do żądania kopii fragmentów dokumentów lub całych dokumentów. „Co do zasady", bo kopie dokumentów jednak trzeba przekazać, jeżeli spełnione są dwa warunki:

1) przekazanie dokumentów jest niezbędne do umożliwienia wykonywania praw,
2) które zostały przyznane przez RODO.

Jak więc postępować w przypadku otrzymania wniosku o kopię danych osobowych? W ogromnej większości przypadków prawidłowe będzie postępowanie, do którego zdążyliśmy się już przyzwyczaić, czyli przekazanie wnioskodawcy treści jego (jej) danych osobowych w postaci wyciągu, zestawienia, wydruku z bazy danych itp. Będą jednak takie przypadki, w których takie standardowe podejście nie wystarczy – będzie tak wtedy, gdy od przekazania kopii nośnika uzależniona jest możliwość korzystania z praw osoby, której dane dotyczą, przyznanych jej przez RODO. Konieczność przekazania kopii nośnika nie będzie więc występowała wtedy, gdy jest to niezbędne do umożliwienia wykonywania jakichkolwiek praw przysługujących osobie, np. prawa do sądu, a wyłącznie w odniesieniu do takich praw, które zostały jej przyznane przez przepisy RODO.

Trybunał Sprawiedliwości UE wskazuje dwa przypadki, w których przekazanie kopii nośnika będzie konieczne: „gdy dane osobowe są generowane z innych danych lub gdy dane te wynikają z wolnych pól, a mianowicie z braku informacji ujawniających informację o osobie, której dane dotyczą". Pierwszy przypadek to sytuacja, gdy administrator danych na podstawie danych osoby, której dane dotyczą, samodzielnie tworzy nowe kategorie danych odnoszące się do tej osoby. Przykładowo instytucja finansowa ocenia zdolność kredytową swojego klienta na podstawie danych uzyskanych z innych źródeł; jeżeli osoba, której dane dotyczą, twierdzi, że ocena została dokonana nieprawidłowo, wówczas, aby umożliwić wykonanie prawa do sprostowania danych, musi uzyskać dostęp do dokumentów źródłowych. Drugi przypadek to sytuacja, gdy „dane te [dane osobowe] wynikają z wolnych pól", a więc kiedy osoba, której dane dotyczą, nie podała swoich danych osobowych, a informacja ta została wykorzystana w procesie przetwarzania jej danych. Przykładowo osoba, której dane dotyczą, pozostawiła w ankiecie wolne (puste) pole oznaczone jako „zainteresowania". Następnie osoba ta – w jej mniemaniu – jest traktowana jak osoba, która udzieliła na to pytanie odpowiedzi, bo np. otrzymuje korespondencję przeznaczoną – w jej ocenie – dla osób mających konkretne zainteresowania. Aby umożliwić ta-

kiej osobie wykonanie prawa do sprostowania danych, musi ona uzyskać dostęp do dokumentów źródłowych.

Obydwa przypadki odnoszą się do prawa do sprostowania danych osobowych, przyznanego przez art. 16 RODO. Aby dane sprostować, trzeba je najpierw zrozumieć. I taki też będzie najczęstszy przypadek, w którym żądanie udostępnienia kopii nośników będzie żądaniem zasadnym: przypadek, w którym jest to niezbędne dla zrozumienia treści danych osobowych. A jak postępować, żeby minimalizować problemy związane ze zrozumieniem treści danych? Korzystać z możliwości, o której mowa w motywie 63 preambuły do RODO, odnoszącym się do możliwości zapewniania dostępu do danych osobowych poprzez zdalny dostęp „do bezpiecznego systemu, który zapewni osobie, której dane dotyczą, bezpośredni dostęp do jej danych osobowych". Prezentowanie w takim systemie dokumentów źródłowych eliminuje ten problem w całości, a prezentowanie w nim danych osobowych przetwarzanych przez administratora pozwala na jego ograniczenie, ale nie wyeliminuje go w całości.

# Sprzeciw, czyli kontrola nad wykorzystaniem własnych danych

Po co nam prawo ochrony danych osobowych? Między innymi po to, żeby umożliwić nam kontrolę nad tym, jak nasze dane są wykorzystywane. Ta kontrola przybiera wiele praktycznych form: musimy być informowani o tym, kto i po co przetwarza nasze dane, bo jeśli tego nie wiemy, to nie możemy tego kontrolować; czasem to wyłącznie od nas zależy, czy zgodzimy się na korzystanie z naszych danych, bo możemy (albo nie) wyrazić zgodę na ich przetwarzanie; czasem możemy zażądać usunięcia danych. Ale chyba najbardziej charakterystyczną instytucją prawa ochrony danych osobowych stanowiącą przejaw decydowania o tym, co się dzieje z naszymi danymi, jest instytucja sprzeciwu.

Sprzeciwy w RODO mamy dwa:

1) bezwzględnie wiążący administratora danych, do którego został skierowany;
2) pozostawiający administratorowi danych możliwość oceny, czy sprzeciw jest zasadny, czy nie.

Sprzeciw wiążący administratora danych jest związany z przetwarzaniem danych dla celów marketingu bezpośredniego: jeżeli nasze dane są przetwarzane dla celów marketingu bezpośredniego, możemy w każdej chwili powiedzieć „stop", a administrator danych powinien takiego przetwarzania zaprzestać. Ale czym jest ów „marketing bezpośredni"? Definicji ustawowej brak, ale ponieważ to pojęcie jest już z nami wiele lat, można pokusić się o próbę jego przybliżenia: otóż marketing bezpośredni to kierowanie komunikatów marketingowych do konkretnych osób, w oparciu o ich dane osobowe. To listy zwykłe, telefony, e-maile, marketing SMS-owy, a przy wykorzystaniu systemów obsługi klienta, np. w banku: przekaz marketingowy, który jest kierowany bezpośrednio do konkretnego odbiorcy.

Wniesienie sprzeciwu powoduje, że po stronie adresata takiego sprzeciwu – administratora danych – powstaje zakaz dalszego przetwarzania danych w celu marketingu bezpośredniego: nie można dzwonić, wysyłać maili czy nawet dokładać ulotek reklamowych do faktury wysyłanej pocztą zwykłą. Ten zakaz ma bezwzględny charakter, administrator nie może oceniać, czy sprzeciw jest zasadny, czy nie – oczywiście jeżeli nie przetwarza on danych dla celów marketingu bezpośredniego, to sprzeciw nie wpłynie na jego sytuację w danym momencie, ale za to zadziała na przyszłość, blokując mu możliwość skorzystania z tej formy marketingu. Wniesienie sprzeciwu działa też od razu, od momentu otrzymania oświadczenia o sprzeciwie – komunikaty w rodzaju „dziękuję za kontakt, potrzebujemy X dni na dostosowanie naszych systemów" są prawnie bezskuteczne.

Z kolej sprzeciw pozostawiający administratorowi danych możliwość oceny, czy jest on zasadny, czy nie, można wnieść wtedy, gdy:

1) podstawą przetwarzania danych osobowych jest art. 6 ust. 1 lit. e lub lit. f RODO, a więc gdy przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi lub gdy następuje w warunkach tzw. uzasadnionego interesu oraz
2) po stronie wnioskodawcy zachodzi szczególna sytuacja, która uzasadnia wniesienie sprzeciwu.

Takie ujęcie tej postaci sprzeciwu powoduje, że nie ma znaczenia cel przetwarzania danych; dane mogą być przetwarzane w celach np.: prowadzenia konsultacji z mieszkańcami przez organ samorządu, aby umożliwić głosowanie w budżecie obywatelskim; marketingowym; udostępniania danych o zadłużeniu przez biuro informacji kredytowej, ale także w celu związanym z dochodzeniem roszczeń – to wszystko są przypadki przetwarzania danych wynikające z art. 6 ust. 1 lit. e lub lit. f RODO. Czy dłużnik może więc skutecznie sprzeciwić się przetwarzaniu przez wierzyciela swoich danych osobowych w celu dochodzenia zapłaty długu? Co do zasady nie, ponieważ sprzeciw będzie tylko wtedy skuteczny, gdy osoba go zgłaszająca wykaże istnienie szczególnej sytuacji związanej z nią i przetwarzaniem jej danych. A czym ta szczególna sytuacja jest? Znów nie wiemy tego po lekturze przepisów RODO, brak jest też wyjaśnień naszego organu nadzorczego w tym zakresie. Przyjmuje się więc, że szczególna sytuacja osoby, której dane dotyczą, powinna wpływać na przetwarzanie jej danych osobowych w ten sposób, że dojdzie do zachwiania równowagi interesów tej osoby oraz administratora danych – w wyniku tego interes osoby, której dane doty-

czą, będzie przeważać nad interesem administratora danych. Innymi słowy, potrzeba ochrony danych osobowych powinna przeważyć nad potrzebą przetwarzania tych danych przez administratora. Administrator danych, który taki sprzeciw otrzyma, nie ma więc innego wyjścia i musi przeprowadzić test nadrzędności interesów, jak przy ocenie istnienia uzasadnionego interesu w przetwarzaniu danych. Oczywiście nie sposób przewidzieć rezultatu takiego testu w każdej sytuacji, ale z prawdopodobieństwem graniczącym z pewnością można założyć, że dłużnik zgłaszający sprzeciw związany ze swoją szczególną sytuacją nie uniknie konieczności zapłaty długu, a osoba, której dane przetwarza BIK, z biura nie zniknie.

I jeszcze jedna niezwykle istotna kwestia: sprzeciw to instytucja odrębna od możliwości odwołania zgody na przetwarzanie danych. Odrębna w tym sensie, że odwołać zgodę można tylko wtedy, gdy to właśnie na zgodzie opierało się przetwarzanie, a sprzeciw można wnieść tylko w opisanych wyżej przypadkach. I dobrze, ale jeżeli klient udzielił zgody na przetwarzane swoich danych w celach marketingowych, a po jakimś czasie pisze do nas wiadomość w stylu: „dajcie mi spokój, nic mi już nie przysyłajcie", to odwołuje zgodę czy wnosi sprzeciw związany z marketingiem bezpośrednim? Moim zdaniem raczej wnosi sprzeciw, ale oczywiście inne interpretacje są jak najbardziej możliwe. Aby więc w praktyce zminimalizować odsetek takich przypadków, stwórzmy – jasnym, prostym językiem – formularze do kontaktu, dzięki którym z góry będzie wiadomo, czy mamy do czynienia ze sprzeciwem, czy z odwołaniem zgody. Tak będzie po prostu łatwiej.

# Gdy klient chce, by o nim zapomnieć

Prawo do bycia zapomnianym przez wiele lat funkcjonowało jako jedna z medialnych twarzy RODO, wówczas dopiero nadchodzącej reformy prawa ochrony danych osobowych. Było wykorzystywane, by przekonać nas do tego, że RODO rzeczywiście odda nam na powrót kontrolę nad naszymi danymi. Czy oddało? Można z tym dyskutować – ale na pewno prawo do usunięcia danych weszło nam mocno w świadomość; do tego stopnia, że po maju 2018 r. zaczęły pojawiać się żądania usunięcia danych osobowych z bazy PESEL czy ZUS, właśnie z powołaniem się na prawo do bycia zapomnianym.

Z rejestru PESEL nie można zniknąć, „bo RODO", to pewne. Zamiast tego w ostatnim czasie prawo do bycia zapomnianym zaczęło zmierzać w dość niespodziewanym kierunku, który może okazać niebezpieczny dla całej gospodarki.

Punktem wyjścia do opisania problemu powinno być założenie, na którym opiera się europejski pomysł na ochronę danych osobowych – otóż przepisy o ochronie danych osobowych to tak naprawdę jedna wielka procedura ochrony danych. Oczywiście nie „procedura" w znaczeniu języka prawniczego, ale „procedura" w znaczeniu języka potocznego: RODO to zbiór przepisów, które mają zapewnić ochronę naszego prawa podstawowego do ochrony danych osobowych. RODO nie ma w założeniu kreować rzeczywistości gospodarczej, RODO ma chronić dane osobowe w rzeczywistości istniejącej. Z tego założenia wyszli także twórcy prawa do bycia zapomnianym, przyjmując, że jeżeli np. nasze dane nie są już potrzebne do celu, w jakim zostały zebrane, wówczas powinny zostać na nasze żądanie usunięte. I teraz wyobraźmy sobie następującą sytuację: mamy kontrahenta, któremu dostarczyliśmy towar, płatność mamy otrzymać w ciągu 30 dni od doręczenia faktury. Wystawiamy fakturę, mija 10 dni i co się dzieje? Otrzymujemy od kontrahenta żądanie usunięcia jego danych osobowych, bo umowa została wykonana, nie ma więc potrzeby, byśmy jego dane przetwarzali. Cóż, gdyby podejść do problemu dosłownie, to rzeczywiście cel przetwarzania danych osobowych

po stronie dostawcy w postaci wykonania umowy został osiągnięty, ale czy to oznacza, że dane powinny zostać usunięte? A gdzie płatność?

Żeby wykluczyć w praktyce takie sytuacje, prawo do bycia zapomnianym nie zostało ukształtowane jako prawo nieograniczone. Przeciwnie, RODO przewidziało od niego aż pięć wyjątków, a jeden z nich to niezbędność przetwarzania danych „do ustalenia, dochodzenia lub obrony roszczeń". Czyli jeżeli usunięcie danych spowodowałoby, że nie możemy dochodzić przysługującego nam roszczenia albo bronić się przed roszczeniem drugiej strony, danych nie usuwamy. Słusznie, zapewne pomyśli większość z nas – gdyby było inaczej, prawo ochrony danych osobowych kształtowałoby rzeczywistość gospodarczą, pozbawiając nas prawa dochodzenia niektórych roszczeń albo obrony przed innymi, naruszając w ten sposób nasze konstytucyjne prawo do sądu.

Zakładamy, że prawo ochrony danych osobowych nie może kształtować rzeczywistości gospodarczej: przychodzi więc do banku klient i chce otrzymać kredyt. Kredytu nie dostaje, a po kilku dniach żąda usunięcia swoich danych osobowych z powołaniem się na prawo do bycia zapomnianym i to, że po stronie banku nie istnieje żaden cel, dla którego jego dane mogłyby być przetwarzane. Usunąć dane czy nie? A co zrobi bank, gdy dane usunie, a po kilku miesiącach otrzyma pozew, w którym niedoszły klient będzie twierdził, że nieudzielenie mu kredytu było wynikiem dyskryminacji ze względu na płeć, narodowość lub np. stan zdrowia? Z tym samym założeniem podchodzimy do sytuacji, w której kandydat do pracy nie zostaje wybrany w procesie rekrutacji, po czym żąda usunięcia swoich danych osobowych, bo przecież nie został wybrany, więc dane nie są potrzebne. Usunąć czy nie? A co zrobi niedoszły pracodawca, jeżeli usunął dane, a następnie otrzyma pozew z argumentacją jak wyżej? Jak będzie się bronił, gdy nie ma danych?

Choć może wydawać się to dziwne, Prezes UODO w tego rodzaju sytuacjach nakazuje… usuwać dane osobowe. Argumentacja jest prosta: skoro żadne roszczenie nie jest dochodzone, to nie można odmówić usunięcia danych z powołaniem na niezbędność przetwarzania danych „do ustalenia, dochodzenia lub obrony roszczeń". To nic, że czym innym jest istnienie roszczenia, a czym innym jego dochodzenie przed sądem; to nic, że można dochodzić nawet roszczeń przedawnionych i także przed takimi powództwami trzeba się bronić, wykazując fakt przedawnienia – Prezes UODO tego nie widzi. W sprawach związanych z kandydatami do pracy doczekaliśmy się na szczęście wyroku WSA w Warszawie, który przyznaje rację tym, którzy potrzeby

przetwarzania danych upatrują w ochronie przed roszczeniami dotyczącymi dyskryminacji (wyrok z 4 sierpnia 2022 r., II SA/Wa 542/22). Ale w sprawach bankowych także orzecznictwo sądowe w większości opowiada się za usuwaniem danych osobowych. Pojawia się pytanie, skąd ten dualizm, skoro oba przytaczane przypadki są niemal identyczne i w obu tych przypadkach obowiązuje to samo RODO.

Sprawy pracownicze i bankowe to wyłącznie przykłady problemu, który ma wręcz fundamentalne znaczenie dla gospodarki: czy muszę usunąć dane osobowe, które przetwarzam, jeżeli żąda tego mój klient, któremu przysługują wobec mnie roszczenia (a mnie wobec niego), ale te roszczenia nie są dochodzone? Zamiast banku możemy tu podstawić dowolnego sprzedawcę, który sprzeda np. książkę, usunie dane na żądanie, a następnie nie będzie mógł bronić się przed zarzutami dotyczącymi nienależytego wykonania umowy sprzedaży; ba, ten sprzedawca nawet nie będzie mógł wykazać, że tę książkę rzeczywiście dostarczył! Jeżeli na wyżej postawione pytanie odpowiemy twierdząco, wówczas musimy się przygotować na bardzo daleko idące skutki ekonomiczne, a prawo ochrony danych osobowych – wbrew jego konstrukcyjnemu założeniu – ukształtuje nam rzeczywistość gospodarczą, eliminując z niej prawo do sądu przysługujące przedsiębiorcom.

# Powierzenie a udostępnienie danych

Pamiętacie Państwo Inżyniera Mamonia z „Rejsu" i jego słynne „mnie się podobają melodie, które już raz słyszałem"? Mnie ta postać zawsze przychodzi do głowy, gdy mierzę się z tematem umów dotyczących danych osobowych. Tylko co ma wspólnego Inżynier Mamoń i RODO? Zaraz postaram się wszystko wyjaśnić.

Gdy myślimy o umowach dotyczących danych osobowych, pierwsze – i bardzo często jedyne – skojarzenie to umowa powierzenia danych osobowych do przetwarzania. Dlaczego? Bo ten typ umowy (z góry przepraszam cywilistów za użycie tutaj pojęcia typu umowy) znamy od lat, bo został on dokładnie opisany w przepisach RODO, bo zawsze zawieraliśmy właśnie umowę powierzenia, bo... Tak, lubimy te umowy, które znamy. A tymczasem to błąd, który czasem może nas drogo kosztować.

W kontekście danych osobowych możemy mówić o trzech rodzajach umów: powierzenia, udostępnienia danych oraz uzgodnienia współadministratorów danych. O ile kwestie współadministrowania to zupełnie odrębny temat, o tyle powierzenie i udostępnienie danych lubią się w praktyce mieszać, z nieustanną tendencją do traktowania przypadków udostępnienia jako powierzenia. Z jakiego powodu? Z takiego, że powierzenie mamy szczegółowo uregulowane w RODO, a o udostępnieniu nie znajdziemy tam ani słowa (lubimy te umowy, które znamy). Czym więc jest powierzenie, a czym udostępnienie?

I powierzenie, i udostępnienie to rodzaj operacji przetwarzania danych osobowych, która charakteryzuje się tym, że dane osobowe wychodzą z pierwotnej organizacji, w której były przetwarzane. Mówiąc inaczej, administrator danych decyduje się na to, żeby dane były przetwarzane poza jego organizacją. Ale o tym, czy mamy do czynienia z powierzeniem, czy udostępnieniem, nie decydują strony zaangażowane w ten proces, lecz decyduje wyłącznie stan faktyczny, w szczególności cel przetwarzania danych przez ich odbiorcę. W przypadku powierzenia przetwarzanie odbywa

się w celu przyjętym przez pierwotnego administratora i w jego imieniu, podczas gdy udostępnienie oznacza tyle, że odbiorca danych staje się ich nowym administratorem, a więc będzie te dane wykorzystywał we własnym celu. Dobrze ujmuje to Prezes UODO, pisząc na swojej stronie, że powierzenie przetwarzania powinno mieć miejsce w przypadkach, gdy administrator prowadzący działalność w określonej dziedzinie ma potrzebę skorzystać z pomocy zewnętrznych specjalistów, których usługi będą miały charakter pomocniczy, nierzadko techniczny, wspierający działalność główną administratora. Będzie więc powierzeniem przetwarzania sytuacja, w której pracodawca korzysta z usług zewnętrznej firmy zajmującej się naliczaniem płac; będzie powierzeniem skorzystanie z usługi zniszczenia danych osobowych; powierzenie to usługi zewnętrznego call center, outsourcing administrowania stroną internetową lub przechowywanie przez zewnętrzny podmiot kopii bezpieczeństwa danych. Ale nie będzie już powierzeniem przetwarzania danych sytuacja, gdy podmiot A przekazuje podmiotowi B bazę danych osobowych po to, żeby podmiot B przesłał do osób, których dane dotyczą, własną ofertę; przetwarzanie będzie się odbywało we własnym celu podmiotu B, będzie to więc klasyczne udostępnienie danych osobowych. Z udostępnieniem danych będziemy mieli do czynienia m.in. wtedy, gdy w umowie umieścimy dane osobowe osób „do kontaktu" w związku z tą umową lub jeśli w ofercie zamieścimy dane osobowe osób, które w ramach tej oferty będą świadczyć usługi.

Wokół powierzenia i udostępnienia narosło przez lata wiele mitów – bo jak nazwać sytuację, w której oddając do czyszczenia stroje robocze z nadrukowanym imieniem i nazwiskiem pracownika, uznajemy to za powierzenie przetwarzania danych? W tej sytuacji nie ma powierzenia, bo przedmiotem usługi jest czyszczenie strojów, a nie wykonywanie operacji na danych osobowych w imieniu zleceniodawcy. Przekazując Poczcie Polskiej lub operatorowi pocztowemu dane osobowe w zamkniętej kopercie, też nie powierzamy tych danych do przetwarzania, bo na tych danych nie są wykonywane żadne operacje, po prostu przemieszczany jest nośnik z danymi. Poczta Polska i operator pocztowy nie przetwarzają także na zlecenie nadawcy danych osobowych tegoż nadawcy i adresata – te dane są przetwarzane przez te podmioty w imieniu własnym, w celu świadczenia przez nie usługi, a nie w imieniu nadawcy, są więc one administratorami danych nadawcy i odbiorcy przesyłki. W pułapkę powierzenia wpadł też Urząd Ochrony Danych Osobowych, wyjaśniając na swojej stronie, że „przekazanie do odkażania (fumigacji) pudeł zawierających dokumenty w sytuacji, gdy pudła są zamknięte, zapieczętowane i nie są na żadnym etapie odkażania otwierane przez pracowników zleceniobiorcy należy uznać za przypadek powierzenia

przetwarzania danych" – nie ma tutaj żadnego powierzenia, bo przedmiotem zlecenia nie jest przetwarzanie danych, ale odkażanie nośników z danymi.

Prawidłowe rozróżnienie między powierzeniem a udostępnieniem danych jest kluczowe nie tylko z punktu widzenia dogmatycznej poprawności. Jest to istotne także dlatego, że niezawarcie umowy powierzenia w sytuacji, gdy przekazanie danych osobowych na zewnątrz jest powierzeniem, może skutkować nałożeniem kary finansowej na administratora danych, o czym przekonał się niedawno Sułkowicki Ośrodek Kultury ukarany przez Prezesa UODO (https://uodo.gov.pl/decyzje/DKN.5131.29.2022). Z kolei potraktowanie udostępnienia danych osobowych jak powierzenia będzie skutkowało tym, że w takim procesie przetwarzania danych osobowych może zwyczajnie nie istnieć podstawa prawna dla udostępnienia danych, a przez brnięcie w kierunku powierzenia pozostanie to niezauważone. W każdym przypadku, gdy dane osobowe wychodzą z naszej organizacji na zewnątrz, badajmy więc w pierwszej kolejności cel, w jakim będą one przetwarzane przez ten zewnętrzny podmiot, bo od tego zależy, czy te dane powierzamy, czy udostępniamy.

# Wybieramy przetwarzającego, czyli jak sprawdzić podwykonawcę?

Nie ma chyba organizacji w naszym kraju, która nie korzystałaby z zewnętrznych usług specjalistycznych, wspomagających tę organizację w jej codziennym funkcjonowaniu: dostawca usług poczty elektronicznej, firma księgowa, specjalista BHP, prowadzenie dokumentacji kadrowej, usługi ochrony czy wsparcie informatyczne – to tylko niektóre typowe przykłady. Bardzo często tego rodzaju usługi wiążą się z dostępem do danych osobowych i z ich przetwarzaniem, a taki outsourcer odgrywa rolę podmiotu przetwarzającego dane. I tu pojawia się zasadnicze pytanie: jak wybrać taką zewnętrzną firmę, żeby zapewnić odpowiednią ochronę danych osobowych, do których dajemy jej dostęp?

Zacznijmy od początku: administrator danych może albo sam przetwarzać dane osobowe, albo ten proces przetwarzania outsourcować. Jeżeli przetwarza dane samodzielnie, np. dane swoich pracowników lub klientów, to sam za to przetwarzanie odpowiada. Ale jeżeli zdecyduje się na outsourcing i przykładowo zamiast prowadzić dokumentację kadrowo-płacową samodzielnie, skorzysta z usług specjalisty, ta odpowiedzialność za bezpieczeństwo danych rozkłada się na dwa podmioty uczestniczące w przetwarzaniu. Mówiąc obrazowo, jeżeli dane wycieką z zewnętrznej firmy, wówczas to ta firma za to odpowiada. Kusząca perspektywa, prawda? Tniemy koszty, korzystając z outsourcingu, i jeszcze rozwiązujemy problem odpowiedzialności za dane – ale mamy tu jeden haczyk: możemy korzystać z usług tylko takich zewnętrznych podmiotów, które „zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi [RODO] i chroniło prawa osób, których dane dotyczą" (art. 28 ust. 1 RODO). Tylko jak te podmioty sprawdzić?

Najprościej będzie opisać najpierw to, jak takiego sprawdzenia nie przeprowadzać. Właśnie, „sprawdzenia" – administrator danych, zanim wybierze przetwarzającego, musi go sprawdzić. Nie może więc polegać na jego oświadczeniach, zapewnieniach i nie wiadomo, czym jeszcze, zwłaszcza jeżeli te oświadczenia znajdą się w umowie między administratorem a przetwarzającym. Dlaczego? Dlatego, że to ma być sprawdzenie przed zawarciem umowy, na etapie umowy jest więc za późno. Sprawdzamy i jeśli jakiś podmiot daje gwarancje, możemy z nim kontraktować; jeżeli nie daje – nie możemy.

Dobrze, ale jak dokonujemy sprawdzenia? Tak naprawdę odpowiedź na to pytanie może być tylko jedna: to zależy. Zależy od tego, jakie dane powierzamy do przetwarzania, komu je powierzamy i jakie mamy faktycznie możliwości sprawdzenia podwykonawcy. Innymi słowy, mierzymy zamiary podłóg sił i ryzyka, jakie to powierzenie może stwarzać. Możemy – jeżeli mamy na to środki i jeśli sytuacja to uzasadnia – przyjechać i przeprowadzić na miejscu pełny audyt takiego potencjalnego przetwarzającego; ale możemy też bazować na analizie dokumentów, które ten potencjalny podwykonawca udostępnia i na tej podstawie podjąć decyzję o tym, czy dopuszczamy go do kontraktowania z nami, czy nie. Jest też trzecie rozwiązanie, bardzo szeroko stosowane w praktyce, które polega na skierowaniu do kandydata na przetwarzającego listy pytań, najczęściej w formie ankiety, i podjęciu decyzji po otrzymaniu na nie odpowiedzi. To też forma audytu, ale korespondencyjnego, bazującego na informacjach przekazywanych przez drugą stronę.

W typowej sytuacji korzystania z usług tzw. dużych graczy na rynku o jakiejkolwiek ankiecie dla przetwarzającego możemy zapomnieć. Wtedy pozostaje wyłącznie analiza dokumentów, które te podmioty udostępniają publicznie, takich jak ich polityki ochrony danych lub informacje o stosowanych zabezpieczeniach. Można ich szukać na stronach internetowych tych podmiotów – ale można też pójść na skróty i powołać się na stanowisko wyrażone przez WSA w Warszawie w wyroku z 19 kwietnia 2022 r. (II SA/Wa 2259/21). Istotę tego poglądu można sprowadzić do jednego zdania: wybór usługi świadczonej „przez profesjonalny podmiot, jakim jest renomowana Microsoft Corporation, z całą pewnością gwarantuje stosowanie przez podmiot przetwarzający środków organizacyjnych i technicznych, o których mowa w art. 28 ust. 1 RODO". Renoma jako podstawa wyboru przetwarzającego? Dlaczego nie, przecież już EROD pisała w wytycznych 7/2020, że reputacja rynkowa przetwarzającego jest jednym z istotnych czynników, jakie należy uwzględnić przy ocenie, czy ten

podmiot daje gwarancje odpowiedniej ochrony danych. Cóż, duzi mają łatwiej, ale mali przy okazji też.

Jakikolwiek sposób sprawdzenia przetwarzającego wybierze administrator danych, o jednym nie może zapominać: to, co zrobi, musi udokumentować. Jest to konsekwencja jednej z podstawowych zasad ochrony danych osobowych, jaką jest rozliczalność, czyli możliwość wykazania, że działało się zgodnie z prawem. Przekonał się o tym niedawno Sułkowicki Ośrodek Kultury, który został ukarany przez Prezesa UODO właśnie za naruszenie obowiązku sprawdzenia przetwarzającego. Jak podkreślił Prezes UODO w uzasadnieniu decyzji o nałożeniu kary, w toku sprawy organ nadzorczy ustalił, że administrator nie posiadał żadnych dokumentów potwierdzających weryfikację warunków współpracy z podmiotem przetwarzającym. A tymczasem brak weryfikacji podmiotu przetwarzającego oraz jego gwarancji dla przetwarzania zgodnie z przepisami o ochronie danych osobowych może wiązać się z konsekwencjami dla osób fizycznych, których dane osobowe zostały powierzone podmiotowi przetwarzającemu, np. w postaci utraty danych osobowych. Decyzja, komu administrator ma powierzyć przetwarzanie danych osobowych, powinna być zatem podejmowana dopiero po zbadaniu kompetencji i adekwatności wybranego podmiotu przetwarzającego – wtedy administrator może przystąpić do zawarcia stosownej umowy powierzenia. Tylko tyle i aż tyle: najpierw sprawdzajmy, a później decydujmy.

# Bazę danych osobowych kupię

Co się stanie, gdy do najpopularniejszej wyszukiwarki internetowej wpiszemy frazę „kupię bazę danych”? Dostaniemy ok. kilkaset wyników. A co zrobić, by nie kupić w ten sposób kota w worku w pakiecie z karą od Prezesa UODO lub Prezesa Urzędu Ochrony Konkurencji i Konsumentów (UOKiK)? Postaram się wyjaśnić.

Zacznijmy może od tego: po co w ogóle kupować bazę danych osobowych? Cóż, zazwyczaj po to, żeby zaoferować coś osobom, których dane się w tej bazie znajdują. To nadal podstawowy powód, dla którego biznes „bazodanowy” kwitnie: generowanie leadów, czyli w pewnym uproszczeniu pozyskiwanie nowych klientów. Zazwyczaj też mamy dwie podstawowe możliwości pozyskania danych potencjalnych klientów: albo kupimy gotową bazę danych, albo ktoś te leady dla nas wygeneruje, czyli kupimy bazę tworzoną specjalnie dla naszych potrzeb.

Z perspektywy prawa ochrony danych osobowych zakup bazy danych to nic innego, jak zbieranie danych osobowych – ten, kto bazę kupuje, zbiera w ten sposób dane osobowe. Co istotne, o ile nabywca bazy kupuje ją dla siebie, żeby przy jej pomocy promować własne towary i usługi, staje się w ten sposób administratorem danych osobowych zawartych w tej bazie. A administrator, jak wiadomo, odpowiada za spełnienie wszystkich obowiązków związanych z przetwarzaniem danych osobowych.

Mit założycielski biznesu związanego z handlem bazami danych można sprowadzić do jednego zdania, które nadal możemy jeszcze zobaczyć w stopkach trafiających do nas maili reklamowych: „dane osobowe zostały pozyskane z powszechnie dostępnych źródeł” – i co z tego? Nie ma znaczenia, skąd pochodzą dane zawarte w bazie, którą kupiliśmy; czy z jakiegoś powszechnie dostępnego rejestru, czy z rozmów telefonicznych z klientami, czy z formularzy internetowych, nie ma to znaczenia – żeby móc te dane legalnie wykorzystać do kontaktu i przedstawienia oferty, nabywca bazy musi mieć możliwość powołania się na jakąś podstawę przetwarzania tych danych. W praktyce w grę wchodzą dwie:

1) zgoda na przetwarzanie danych,

2) uzasadniony interes.

Żeby nabywca bazy mógł się powołać na zgodę jako swoją podstawę przetwarzania danych, zbywca bazy, czyli ten, kto te dane zebrał, musiałby zebrać zgodę na ich przetwarzanie przez tego konkretnego nabywcę, wymienionego z nazwy. Mało prawdopodobne, prawda? Wręcz niemożliwe, bo niby skąd taki podmiot miałby wiedzieć, kto kupi od niego dane? Stąd jedyną realną podstawą przetwarzania danych osobowych przez nabywcę bazy jest niezbędność takiego przetwarzania do realizacji jego uzasadnionego interesu. Oczywiście taki uzasadniony interes trzeba sprawdzić, wykonując tzw. test nadrzędności interesu, ale jako zasadę możemy przyjąć, że wynik tego testu będzie pozytywny. Ale to jeszcze nie wszystko – gdyby na tym poprzestać, do osób z bazy można by jedynie wysłać tradycyjny, papierowy list. A co, gdy chcemy zadzwonić albo np. wysłać maila? Wówczas potrzebujemy jeszcze zgód na komunikację elektroniczną, czyli zgód, o których mowa w art. 172 Prawa telekomunikacyjnego oraz w art. 10 ustawy o świadczeniu usług drogą elektroniczną i od konieczności posiadania tych zgód odwrotu już nie ma.

Zgody na komunikację elektroniczną może oczywiście zebrać ten, kto handluje bazami danych – problem polega jednak na tym, że w stosunku do tego rodzaju zgód mamy do czynienia z coraz bardziej wyśrubowanymi standardami określanymi dla odmiany przez Prezesa UOKiK; najistotniejsze z nich to:

1) konieczność wskazania z nazwy, jakie podmioty mogą powoływać się na zgodę;
2) zakaz używania środków komunikacji elektronicznej w celu zapytania o zgodę.

I znów, wypada zapytać, czy zajmując się handlem bazami danych i zbierając zgody, można przewidzieć, kto będzie naszym klientem? Nie ma takiej możliwości, jak się wydaje. A to prowadzi do jednoznacznego wniosku: zakup na rynku gotowej bazy danych wiąże się z dość istotnym ryzykiem dla tego, kto taką bazę kupi. Ryzyko to polega na tym, że prawie na pewno taka baza nie będzie spełniała wymogów dotyczących zgód na komunikację elektroniczną prowadzoną przy pomocy rekordów z niej pochodzących. Oczywiście sprzedawcy baz danych zazwyczaj zapewniają nabywców o tym, że oferowane przez nich bazy spełniają wszelkie możliwe do wyobrażenia wymogi prawne, ale tutaj też ukryta jest pułapka: otóż spełnienie wymagań związanych ze zgodami dotyczącymi komunikacji elektronicznej to efekt realizacji obowiązków publicznoprawnych, a te są albo wykonane, albo nie, zgoda albo została zebrana, albo nie. Nie ma znaczenia, że zbywca zapewniał o tym, że zgodę zebrał, jeżeli w rzeczywistości tak nie było. Oznacza to, że zapewnienia kontraktowe o tym,

że zgoda jest, nie chronią przed nałożeniem kary, gdy tej zgody nie ma – można co najwyżej dochodzić odszkodowania od zbywcy takiej wadliwej bazy, ale to zazwyczaj marne pocieszenie.

Co więc robić? Moja rekomendacja to unikanie zakupu gotowych baz danych, oferowanych masowo każdemu chętnemu klientowi, bo zazwyczaj użycie takich baz w zamierzonym celu nie doprowadzi do niczego dobrego. Zamiast tego preferowanym rozwiązaniem powinno być korzystanie z baz danych tworzonych specjalnie dla naszych potrzeb. Pozwoli to – po pierwsze – zebrać wszelkie wymagane przez prawo zgody. Po drugie, już na etapie zbierania danych można przekazać osobom, których dane znajdą się w bazie, informacje wymagane przez art. 14 RODO, a to oznacza, że nabywca takiej bazy nie musi się z tymi osobami dodatkowo kontaktować i wykonywać wobec nich tzw. obowiązku informacyjnego. Po trzecie wreszcie, taką bazę tworzoną dla nas można w praktyce dostosować do naszych potrzeb: nie zbierać niepotrzebnych danych lub np. właściwie określić cel przetwarzania. A stare bazy danych, pamiętające czasy akcji „Przygarnij Kropka" czy „Paszport" pewnego znanego nadawcy, pozostawmy historii.

# Przydatne (i darmowe) wzory

Oferowanie wzorów dokumentów związanych ze stosowaniem przepisów o ochronie danych osobowych wydaje się nadal stosunkowo intratną gałęzią biznesu: z jednej strony raz a dobrze przygotowany wzór ma to do siebie, że potrafi żyć latami, z drugiej jednak strony istnieje pewien zbiór przedsiębiorców, którzy właśnie w ten sposób chcą wdrażać w swojej organizacji przepisy o ochronie danych osobowych: posługując się gotowymi wzorami procedur, polityk lub umów. Koło się więc zamyka i popyt spotyka się z podażą. Problem w tym, że zapewnianie zgodności z RODO przy pomocy wzorów dokumentów nie jest tym, co tą zgodność gwarantuje. Owszem, wzory można nabyć relatywnie tanio, ale nawet najlepszy wzór nie zastąpi wdrożenia – nie spisania, wdrożenia – wymaganych przez prawo rozwiązań na miarę potrzeb konkretnej organizacji. Istnieją jednak dwa przypadki, w których korzystanie ze wzorów jest nie tylko merytorycznie uzasadnione, ale wręcz zalecane – a do tego darmowe. Mam na myśli wzory przygotowane przez Komisję Europejską w wykonaniu postanowień RODO.

Pierwszy wg kolejności przepisów RODO przypadek, w którym możemy wykorzystać oficjalny wzór dokumentu, to umowa powierzenia przetwarzania danych osobowych. Jest to umowa zawierana masowo i z pewnością spotkał się z nią każdy przedsiębiorca – stąd właśnie ten wzór uważam za niezwykle ważny. Możliwość określenia przez Komisję tzw. standardowych klauzul powierzenia wynika z art. 28 ust. 7 RODO i Komisja skorzystała z niej, przyjmując decyzję wykonawczą 2021/915 z dnia 4 czerwca 2021 r. Sama decyzja jest niezwykle krótka – ma cztery artykuły – bo najważniejszy jest załącznik do niej, czyli standardowe klauzule umowne, które są niczym innym, jak właśnie umową powierzenia. Umową, której nie wolno zmieniać – trzeba za to uzupełnić cztery załączniki, w których wskazuje się te elementy powierzenia, które charakteryzują konkretny proces przetwarzania danych: od administratora i przetwarzającego, przez kategorie przetwarzanych danych i czas trwania przetwarzania, a na środkach zabezpieczenia danych kończąc. W efekcie uzupełniając załączniki, otrzymujemy umowę powierzenia przetwarzania zgodną z wymaganiami stawianymi przez art. 28 RODO; otrzymujemy ją za darmo i w praktyce z gwarancją tego,

że organ nadzorczy nie zarzuci nam naruszenia wymagań co do treści umowy powierzenia. Oczywiście umowę powierzenia przygotowaną z wykorzystaniem decyzji wykonawczej 2021/915 możemy traktować jako samodzielną umowę, możemy ją też włączyć w treść innej umowy – to już zależy od przyjętej konstrukcji.

Drugi przypadek, w którym możemy posłużyć się oficjalnym wzorem dokumentu dotyczącym przetwarzania danych osobowych, to standardowe klauzule ochrony danych związane z przekazywaniem danych osobowych do krajów trzecich. W tym przypadku możliwość przyjęcia takich klauzul przez Komisję wynika z art. 46 ust. 2 RODO i, powołując się na ten przepis, Komisja przyjęła – także 4 czerwca 2021 r. – decyzję wykonawczą 2021/914.

Standardowe klauzule związane z transferami danych to także wzór umowy, którą zawiera się w przypadku przekazywania danych osobowych poza Europejski Obszar Gospodarczy: jest to jeden ze sposobów zalegalizowania takiego transferu danych. Dzielą się one na trzy grupy postanowień:

1) klauzule ogólne, które znajdują zastosowanie do wszystkich przypadków transferów;
2) klauzule szczegółowe, które dodatkowo podzielone zostały na różne moduły w zależności od konkretnego scenariusza przekazywania danych do państwa trzeciego;
3) załączniki: załącznik nr 1 zawierający wykaz stron, opis transferów, właściwy organ nadzorczy; załącznik nr 2 opisujący środki techniczne i organizacyjne, w tym środki techniczne i organizacyjne zapewniające bezpieczeństwo danych; załącznik nr 3 zawierający wykaz tzw. podprocesorów.

Standardowe klauzule dotyczące transferów nie mogą być również zmieniane przez strony. Trzeba za to, jak w przypadku klauzul dotyczących powierzenia, uzupełnić brakujące informacje, ale także – co może stanowić pewną trudność – wybrać odpowiedni moduł w treści klauzul szczegółowych. Przykładowo, jeżeli przekazanie danych do kraju trzeciego wiąże się z powierzeniem danych do przetwarzania (odbiorca danych jest podmiotem przetwarzającym), wybieramy moduł drugi; jeżeli natomiast dane są przekazywane między dwoma administratorami – należy wybrać moduł pierwszy.

Obowiązujące obecnie standardowe klauzule dotyczące transferów danych zastąpiły klauzule obowiązujące poprzednio i przyjęte jeszcze na podstawie dyrektywy

95/46/WE, która została uchylona przez przepisy RODO. Przyjęcie nowych klauzul oznaczało uporządkowanie systemu, jako że poprzednio obowiązywały trzy zestawy klauzul stanowiące załączniki do trzech różnych decyzji Komisji, a także dostosowanie treści klauzul do wymagań rynkowych, np. poprzez uregulowanie przypadku przekazywania danych pomiędzy podmiotami przetwarzającymi. Nowe klauzule wymusiły także zmianę umów zawartych w oparciu o poprzednio obowiązujące wzory, co powinno było nastąpić do 27 grudnia 2022 r.

Dwa opisane przeze mnie przypadki wzorów przyjętych na podstawie przepisów RODO to nie jedyne sytuacje, w których RODO przewiduje taką możliwość – ale jedyne, z których w praktyce skorzystano. Do dzisiaj np. nie doczekaliśmy się tzw. ikonek prywatności, do których stosowania RODO zachęca, dając Komisji możliwość przyjęcia aktów delegowanych, określających informacje przedstawiane za pomocą standardowych znaków graficznych oraz procedury ustanawiania takich znaków. Tym bardziej więc trzeba korzystać z tych wzorów, które zostały przyjęte.

# Podejście oparte na ryzyku

„Ryzyko" – to słowo, odmieniane przez wszystkie przypadki, pada w tekście RODO 76 razy. To świadomy i celowy zabieg, bo tzw. podejście oparte na ryzyku to jedna z podstawowych zasad ochrony danych osobowych.

Dane osobowe, zwłaszcza we współczesnych czasach, trzeba odpowiednio zabezpieczać. Stąd wśród zasad przetwarzania danych wymienionych w art. 5 RODO znalazła się zasada integralności i poufności danych. W jej myśl każdy, kto przetwarza dane osobowe, winien to czynić w taki sposób, aby zapewnić odpowiednie bezpieczeństwo danych osobowych, w tym ich ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem. To zapewnienie winno następować za pomocą odpowiednich środków technicznych lub organizacyjnych. Mówiąc inaczej, jeżeli przetwarzamy dane, musimy je odpowiednio zabezpieczyć; „odpowiednio" – czyli jak?

W RODO na próżno szukać konkretnych wymagań dotyczących zabezpieczenia danych osobowych: nie znajdziemy minimalnych parametrów, jakie musi spełniać hasło, nie dowiemy się, jak często trzeba wykonywać kopie bezpieczeństwa danych ani też którego oprogramowania użyć, żeby te dane zabezpieczyć przed nieautoryzowanym dostępem. I choć stosujemy RODO już prawie 6 lat, to ciągle trzeba o tym przypominać, bo w epoce przed RODO przywykliśmy do zgoła odmiennych rozwiązań prawnych: obowiązujące poprzednio przepisy określały konkretnie, jakie środki trzeba zastosować w celu zabezpieczenia danych. Dlatego rozpoczęcie stosowania RODO to była prawdziwa rewolucja w myśleniu o zabezpieczeniu danych – zamiast odhaczania na liście kontrolnej (niezmienianej od 15 lat) kolejnych wymaganych środków zabezpieczania danych, pojawiła się konieczność oceny ryzyka i samodzielnego doboru odpowiednich środków zabezpieczenia.

Patrząc nieco z boku, wydaje się, że taki zabieg ma głęboki sens: nie da się z góry określić, jak zabezpieczać dane osobowe we wszystkich możliwych konfiguracjach; albo inaczej: da się, ale to bez sensu, bo istnieje tyle różnych możliwych sytuacji

przetwarzania danych, a zagrożenia zmieniają się tak często, że żaden ustawodawca nie jest w stanie przyjąć efektywnych przepisów przed nimi chroniących. RODO nie mówi więc, jak trzeba postępować; mówi, jaki efekt trzeba osiągnąć, a to podejście to właśnie podejście oparte na ryzyku.

Zasada jest bardzo prosta: ten, kto przetwarza dane, powinien określić i wdrożyć środki techniczne i organizacyjne odpowiednie do ryzyka generowanego przez to przetwarzanie danych, a środki te mają gwarantować bezpieczeństwo przetwarzania. Zanim przystąpimy do przetwarzania danych, trzeba więc oszacować ryzyko związane z tym przetwarzaniem. Szacowanie ryzyka to proces, w ramach którego ustala się dwie zmienne: zagrożenia dla bezpieczeństwa danych osobowych i prawdopodobieństwo tego, że te zagrożenia się ziszczą. Motyw 83 preambuły do RODO dostarcza nam pewnych wskazówek co do tego, jak taka ocena ryzyka powinna być dokonywana – należy wziąć pod uwagę ryzyko związane z przetwarzaniem danych osobowych, takie jak przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych, i mogące w szczególności prowadzić do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych. Unaocznieniu, jak skomplikowany jest to proces, niech posłuży następujący przykład: zalanie serwerowni, które następuje w wyniku gaszenia – wodą – pożaru w lokalu znajdującym się bezpośrednio nad serwerownią to ryzyko, które zmaterializowało się pewnemu dostawcy usług telekomunikacyjnych; czy uwzględnił to ryzyko w toku szacowania ryzyka? Jeżeli tak, to z pewnością przyjął, że prawdopodobieństwo ziszczenia się tego ryzyka jest na tyle niewielkie, że można je zaakceptować. A tymczasem ryzyko się ziściło, serwerownia została zalana. Albo inny przykład: wojna w Ukrainie. Wiele polskich podmiotów korzystało z usług ukraińskich podwykonawców świadczących usługi związane z przetwarzaniem danych osobowych. Wojna to klasyczna siła wyższa, a więc okoliczność, za którą, przynajmniej w prawie cywilnym, nie ponosi się odpowiedzialności – ale RODO to nie prawo cywilne. Ilu więc z tych dostawców uwzględniło wojnę w swojej analizie ryzyka i podjęło działania celem minimalizacji tego ryzyka?

Prawidłowo wykonana analiza ryzyka daje podstawę do wdrożenia środków, które mają zapewnić bezpieczeństwo danych osobowych. Weźmy jako przykład ryzyko, które występuje u każdego podmiotu: ryzyko nieuprawnionego dostępu do danych w wyniku złamania hasła. Jak temu ryzyku zapobiec? Jednym ze sposobów jest nakaz stosowania skomplikowanych i odpowiednio długich haseł; a czy częsta zmiana

hasła może być jakimś rozwiązaniem? Nie, bo – jak wskazują badania, choćby przeprowadzone przez Microsoft – wymuszanie częstej zmiany haseł prowadzi do tego, że hasła stają się powtarzalne (Marzec2023!, Kwiecień2023@ itd.), albo zwyczajnie są zapisywane na jakichś karteluszkach. Albo ryzyko ujawnienia danych w związku z przesyłaniem danych pocztą elektroniczną – jak mu zapobiec? Przez szyfrowanie danych.

Analizy ryzyka nie wykonuje się raz na całe życie – o nie! Zagrożenia dla bezpieczeństwa danych stale ewoluują, więc i analizę ryzyka trzeba powtarzać: co pewien, zdefiniowany, czas, kiedy pojawią się nowe zagrożenie, np. zostanie ujawniona nowa podatność, albo gdy wdrażane są nowe rozwiązania dotyczące przetwarzania danych, np. migrujemy do nowego dostawcy. Analiza ryzyka jest też tym dokumentem, który niejednokrotnie ratuje skórę administratora lub przetwarzającego: gdy np. zdarzy się wyciek danych, właśnie analizą ryzyka możemy wykazać, że doszło do niego mimo odpowiedniej ochrony danych. Wreszcie analiza ryzyka jest tym dokumentem, o który standardowo, w pierwszym dniu kontroli, proszą nas inspektorzy UODO.

# Upoważniać czy nie upoważniać?

Jednym z elementów składających się na bezpieczeństwo danych osobowych w organizacji jest zapewnienie kontroli nad tym, kto ma do tych danych dostęp, co może z nimi zrobić i co tak właściwie zrobił. W epoce przed RODO tak właśnie rozumiano rozliczalność: jako właściwość systemu pozwalającą przypisać określone działanie w systemie do osoby fizycznej lub procesu oraz umiejscowić je w czasie i wiązano ją najczęściej z obowiązkiem nadawania upoważnień do przetwarzania danych osobowych. Ale czasy się zmieniły, zmieniło się znaczenie pojęcia rozliczalności, a problem upoważnień pozostał. Nadawać więc upoważnienia czy nie nadawać upoważnień do przetwarzania danych? A jeżeli tak, to jak to robić?

Wypada zacząć od tego, że ustawa o ochronie danych osobowych z 1997 r. przewidywała obowiązek dopuszczenia do przetwarzania danych wyłącznie osób posiadających upoważnienie nadane przez administratora danych oraz obowiązek prowadzenia przez administratora danych ewidencji osób upoważnionych. Takiego obowiązku w RODO nie ma – zamiast tego mamy art. 29 RODO o treści następującej: „[p]odmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie administratora, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego". Jak rozumieć słowo „upoważnienie" padające w tym przepisie? Na pewno nie można go rozumieć tak, jak to miało miejsce na gruncie starych przepisów – z przepisów RODO nie wynika obowiązek prawny nadawania upoważnień w formie odrębnych dokumentów wręczanych przed rozpoczęciem przetwarzania danych. Jednak skoro określona osoba ma działać „z upoważnienia", a obowiązkiem administratora lub podmiotu przetwarzającego jest zapewnienie, aby każda osoba działająca z ich upoważnienia przetwarzała dane wyłącznie na ich polecenie (art. 32 ust. 4 RODO), to jakoś trzeba ustalić zakres tego upoważnienia (polecenia). Samo „upoważnienie" jawi się więc bardziej jako sposób określenia tego, co

konkretna osoba może robić z danymi osobowymi, niż jako odrębny dokument – co nie zmienia tego, że gdzieś ten zakres upoważnienia trzeba wskazać.

Upoważnienie do przetwarzania danych osobowych to obecnie nie wymóg czysto biurokratyczny, lecz element systemu zabezpieczenia danych osobowych, którego istotę można sprowadzić do jednego: każdy, kto przetwarza dane, może to robić wyłącznie na polecenie administratora lub przetwarzającego, a wdrożenie systemu upoważnień ma to zapewnić. Gdy patrzy się z tej perspektywy, zmienia się też sposób nadawania upoważnień: co do zasady nie musi to być odrębny dokument wręczany osobie fizycznej; może to być np. system kontroli dostępu i uprawnień na poziomie oprogramowania wykorzystywanego do przetwarzania danych, który będzie zapewniał to, że konkretny pracownik będzie miał dostęp tylko do takich danych i będzie mógł wykonać na nich tylko takie operacje, które wynikają z decyzji administratora lub przetwarzającego. A nawet jeżeli będzie to upoważnienie w postaci odrębnego dokumentu, nie musi już ono zostać sporządzone w formie pisemnej lub elektronicznej. Będzie więc zgodne z art. 29 RODO nadawanie upoważnień przez przyznanie uprawnień w aplikacji do przetwarzania danych – pod warunkiem, że administrator lub podmiot przetwarzający będą w stanie wykazać, komu i jakie upoważnienia nadali, a więc iż oprogramowanie będzie zapewniało eksport odpowiedniego zestawienia. Można też nadać upoważnienia, przesyłając je pocztą elektroniczną, niekoniecznie opatrując wiadomości podpisem kwalifikowanym. Jednak i tu pozostaje małe „ale": czasem wręczenie odrębnego pisemnego dokumentu zawierającego upoważnienie do przetwarzania może być zalecane dlatego, że przyczynia się do budowania świadomości potrzeby ochrony danych osobowych wśród pracowników. Mówiąc wprost, otrzymanie do ręki kartki papieru, której kopia ląduje w aktach pracowniczych, może spowodować, iż pracownik baczniej zwróci uwagę na swoje obowiązki związane z ochroną danych osobowych. Do rozważenia więc pozostaje w konkretnych sytuacjach, czy jednak pozostanie przy upoważnieniu jako odrębnym dokumencie nie będzie uzasadnione. Podkreślić jednak trzeba, że nawet taki odrębny „dokument" może mieć formę pisemną, formę elektroniczną lub po prostu formę dokumentową.

Tu można by skończyć, gdyby nie polski ustawodawca, który w art. $22^{1b}$ § 3 Kodeksu pracy zawarł następującą zasadę: do przetwarzania danych osobowych szczególnych kategorii mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie do przetwarzania takich danych wydane przez pracodawcę. I mamy kłopot, do tego podwójny: w każdym dziale kadr, z definicji, mamy dane szczególnych kategorii, a „posiadanie pisemnego upoważnienia" to regres nawet w stosunku do stanu praw-

nego, jaki znamy z ustawy o ochronie danych osobowych z 1997 r. Pewnym rozwiązaniem mogłoby się okazać nadawanie upoważnień w formie elektronicznej, czyli z kwalifikowanym podpisem – ale i tym nie każdy dysponuje. Tu natomiast z pomocą przychodzi nie kto inny, jak Prezes UODO, który uznał, że „[n]adawanie upoważnień w postaci elektronicznej [nie w formie elektronicznej – dopisek P.L.] należy uznać za wykonanie obowiązku nadania upoważnień w formie pisemnej" (niestety, ze względu na zmianę strony internetowej Prezesa UODO, to stanowisko – jak i wiele innych cennych opinii – jest obecnie niedostępne). Także więc w przypadku upoważnień nadawanych na podstawie przepisów Kodeksu pracy upoważnienie może zostać nadane w postaci elektronicznej, bez konieczności posługiwania się podpisem kwalifikowanym. Od jednego tylko nie uciekniemy: powinien istnieć dokument potwierdzający fakt nadania upoważnienia.

# Inspektor Ochrony Danych, czyli lekarz pierwszego kontaktu

Inspektor Ochrony Danych (IOD) – trzeba go wyznaczyć czy nie? Zatrudnić czy zlecić pełnienie jego funkcji zewnętrznej firmie? Jak ułożyć relacje z IOD w organizacji? To tylko niektóre z pytań, przed którymi stajemy w związku z organizacją procesów przetwarzania danych osobowych. Ale w gruncie rzeczy najważniejsze pytanie brzmi jeszcze inaczej: czy w ogóle warto wyznaczać Inspektora?

Zacznijmy od początku – kim jest IOD? Mówiąc nieco obrazowo, IOD zapewnia pierwszą linię wsparcia w organizacji w kwestiach ochrony danych osobowych. To taki lekarz pierwszego kontaktu, czyli ktoś, kto monitoruje przestrzeganie przepisów o ochronie danych osobowych, w razie potrzeby doradza i rekomenduje rozwiązania, a także szkoli pracowników i współpracuje z organem nadzorczym. Inspektor Ochrony Danych nie podejmie decyzji za administratora danych, zresztą nie wolno mu tego robić – IOD ma za zadanie pomóc administratorowi w podjęciu właściwej decyzji.

Czasem nasza organizacja musi wyznaczyć IOD – będzie tak w sektorze publicznym, a także wtedy, gdy:

1) główna działalność organizacji polega na przetwarzaniu danych wymagającym regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę lub
2) główna działalność organizacji polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych albo danych dotyczących skazań.

Podmioty, które zajmują się np. obsługą systemów monitoringu wizyjnego, przeciwdziałaniem praniu brudnych pieniędzy, oceną wiarygodności kredytowej lub outsourcingiem prowadzenia dokumentacji medycznej, mają więc prawny obowiązek wyznaczenia IOD. Ale jak zachować się w pozostałych przypadkach – wyznaczać

go czy nie? Moim zdaniem zdecydowanie tak – po prostu z Inspektorem powinno być łatwiej przedzierać się przez gąszcz regulacji. Ale żeby osiągnąć taki efekt, IOD musi być rzeczywiście częścią naszej organizacji. Wynika to wprost z przepisów RODO, które stanowią, że Inspektor powinien być „włączany we wszystkie sprawy dotyczące ochrony danych osobowych". Bazując więc na tym założeniu i wieloletnim doświadczeniu w sprawach ochrony danych osobowych, wyrażę być może niepopularny pogląd, ale do takiego właśnie wniosku skłaniam się od lat: efektywne wykonywanie funkcji IOD zazwyczaj wymaga stałej obecności Inspektora na miejscu, głębokiego poznania procesów przetwarzania danych i integracji z organizacją. A to z kolei sprawia, że nie jestem zwolennikiem korzystania z usług tzw. zewnętrznych Inspektorów, pełniących tę funkcję jednocześnie w wielu organizacjach. I tak, mam świadomość tego, że żadne przepisy nie zabraniają outsourcingu funkcji IOD; ba, taką możliwość przewiduje też samo RODO. Nie mam więc nic przeciwko Inspektorowi współpracującemu na podstawie umowy B2B, który formalnie rzecz biorąc prowadzi własną działalność gospodarczą. Ale przypadki, w których Inspektorzy – zwłaszcza w sektorze publicznym – obejmują swoją funkcją dziesiątki podmiotów jednocześnie, będąc obecnymi w nich przez kilka godzin w miesiącu, zwyczajnie nie dają możliwości efektywnego wypełniania obowiązków IOD.

Właśnie, obowiązki IOD – te nigdy nie mogą obejmować działań, które powodowałyby, że Inspektor staje się jednocześnie administratorem danych osobowych. Mówiąc inaczej, IOD doradza, monitoruje i wspiera, ale nie podejmuje decyzji w zakresie celów i sposobów przetwarzania danych, czyli nie wykonuje czynności zarządczych. Przykładowo IOD powinien uczestniczyć w postępowaniu zakupowym dotyczącym dostawcy oprogramowania kadrowo-płacowego, ale nie może podejmować decyzji o wyborze konkretnego dostawcy; IOD powinien uczestniczyć w obsłudze naruszeń ochrony danych osobowych i rekomendować konkretne rozwiązania, ale decyzja o tym, czy naruszenie zgłaszać, czy nie, powinna być decyzją administratora danych. Ten nakaz unikania konfliktu interesów powoduje, że nie można łączyć niektórych funkcji zarządczych z wykonywaniem obowiązków IOD – co warte podkreślenia, odpowiedzialność za naruszenie tego zakazu ponosi administrator danych, który do takiej sytuacji dopuści. I choć w Polsce nie doczekaliśmy się jeszcze nałożenia takiej kary, w innych krajach UE takie przypadki się zdarzają: przykładowo można tutaj wymienić przypadek belgijski, w którym bank został ukarany kwotą 75 000 euro za powierzenie funkcji IOD osobie, która jednocześnie pełniła w organizacji funkcję szefa działu *compliance*, zarządzania ryzykiem i audytu.

Wśród zadań IOD znajdziemy także obowiązek pełnienia funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych osobowych. Uwzględniając pewne historyczne zaszłości, czyli tzw. sprawdzenia na zlecenie Generalnego Inspektora Ochrony Danych Osobowych (GIODO), istniejące w polskim porządku prawnym przed majem 2018 r., niektórzy administratorzy zwyczajnie obawiają się tego, że wyznaczając Inspektora, wprowadzą sobie do organizacji swoistą piątą kolumnę, czyli osobę, która bez ich wiedzy i zgody będzie współpracować z Prezesem UODO. Nic bardziej mylnego – punkt kontaktowy to nie pełnomocnik, a każdorazowe umocowanie do reprezentowania administratora danych w konkretnym postępowaniu musi wynikać z decyzji tegoż administratora i udzielonego przez niego pełnomocnictwa. Punkt kontaktowy to po prostu osoba, do której pracownicy UODO mogą się zwracać w związku z prowadzonymi postępowaniami, czego najlepszym przykładem mogą być postępowania dotyczące naruszeń – pracownicy Urzędu czasem zwyczajnie dzwonią lub mailują do IOD, co znacznie przyspiesza przekazywanie informacji.

Warto więc czy nie warto inwestować w Inspektora Ochrony Danych? Zdecydowanie warto, pod warunkiem że za wyznaczeniem IOD pójdą także inne działania, zapewniające mu efektywne wykonywanie swojej funkcji. Ale jeżeli wyznaczenie IOD ma być czystą formalnością, czymś, co ma dobrze wyglądać na zewnątrz, to może lepiej te środki przeznaczyć na coś innego.

# Naruszenia ochrony danych – dobre praktyki

W 2021 r. w ciągu jednego dnia do Prezesa UODO zgłaszano średnio 35 przypadków naruszeń ochrony danych osobowych. To na tyle dużo, że przedsiębiorców można podzielić na tych, którzy naruszenie już zgłaszali, i na tych, którzy nie zgłaszali, a powinni byli – bo zwyczajnie nie mają świadomości tego, że do naruszenia doszło. Taka liczba naruszeń sprawia też, że możemy wskazać kilka najważniejszych problemów i dobrych praktyk z nimi związanych.

Po pierwsze, nie ulegajmy medialnej narracji i nie utożsamiajmy naruszenia ochrony danych osobowych wyłącznie z tzw. wyciekiem danych. Oczywiście wyciek, czyli ujawnienie danych osobie nieupoważnionej, to też naruszenie; ale naruszeniem będzie też brak dostępu do danych, które wykorzystujemy w organizacji (np. lekarz traci dostęp do danych pacjentów) lub zniszczenie danych, które nie powinny zostać zniszczone (np. sklep internetowy przez pomyłkę usuwa konta aktywnych klientów).

Drugi problem to często jeszcze pokutujące wśród przedsiębiorców podejście zakładające, że im ciszej o naruszeniu, tym lepiej. Cóż, informacja o tym, że ktoś nie chroni należycie danych klientów lub pracowników, nie buduje reputacji; ale jeszcze gorzej na tę reputację wpływa informacja, że przedsiębiorca próbował naruszenie zatuszować. A jak uczy życie, prędzej czy później informacja o naruszeniu przedostanie się do opinii publicznej: albo przeczytamy o niej na specjalistycznym portalu internetowym, albo w prasie lokalnej, albo ktoś zwyczajnie poskarży się do Prezesa UODO. Co więcej, jeżeli tak się stanie, reakcja ze strony organu nadzorczego będzie zapewne dużo ostrzejsza niż jeżeli naruszenie zgłosi organizacja, w której to naruszenie wystąpiło. Nie próbujmy więc zamiatać naruszeń pod dywan – zazwyczaj będzie to przeciwskuteczne.

Właśnie, zgłoszenie naruszenia – przepisy o ochronie danych osobowych wymagają, aby naruszenie, gdy już się o nim dowiemy, zgłosić Prezesowi UODO. Zasadą jest, że

każde naruszenie podlega zgłoszeniu, chyba że jest mało prawdopodobne, by stwarzało ono ryzyko dla praw i wolności osób, których dane dotyka. Mówiąc obrazowo, inaczej wygląda sytuacja, gdy lekarz zgubi zaszyfrowany *pendrive* z danymi pacjentów, a inna, gdy na śmietniku wylądują pełne kartoteki z zapisem historii choroby. Ale jak ocenić to ryzyko? Istnieje wiele sposobów oceny, ale zawsze będą one miały jedną cechę wspólną: rezultat oceny będzie tylko tak dobry, jak prawidłowe będą dane, które podamy. Jeżeli więc np. przez pomyłkę wysłaliśmy dane osobowe ubezpieczonego nie do niego, ale do przypadkowej osoby, to oceniając ryzyko, nie zakładajmy, że ktoś te dane usunie, jak tylko je zobaczy, albo że ich w ogóle nie przeczyta.

A jakie metody oceny ryzyka stosować? Najpewniejsze rezultaty daje metoda opracowana przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa, tzw. ENISĘ. Metoda ta jest dostępna za darmo na stronach ENISY, była wielokrotnie zalecana przez Prezesa UODO i na jej podstawie opracowano wiele dostępnych w Internecie kalkulatorów. Pamiętajmy tylko o tym, że każdy kalkulator da na tyle tylko prawidłowy wynik, na ile prawidłowe będą dane, które do niego wpiszemy.

Czasem o naruszeniu trzeba też poinformować osoby dotknięte naruszeniem. Po co? Żeby mogły zapobiegać skutkom, jakie to naruszenie może dla nich wywołać. Oczywiście nie jest prawdą, że każde naruszenie – nawet to, gdy wyciekną numery PESEL klientów – będzie prowadziło do masowego wyłudzania kredytów „na dane osobowe"; ale też nie można takiego ryzyka wykluczyć. Trzeba też pamiętać o tym, że co trzecia Polka i co trzeci Polak boją się naruszeń ochrony ich danych osobowych. Dlatego jeżeli przedsiębiorca oceni ryzyko, jakie wiąże się z naruszeniem, i okaże się, że jest ono wysokie, trzeba o naruszeniu poinformować osoby będące jego ofiarami. Jak to zrobić? W możliwie zrozumiały dla nich sposób. Urzędowy, zbyt formalny język niczemu dobremu nie służy. Nie bójmy się też poinformowania o naruszeniu np. w prasie lokalnej, zwłaszcza jeżeli ta sama prasa już wcześniej o nim napisała. Gdy nasi klienci to np. osoby starsze, z większym prawdopodobieństwem przeczytają informację prasową niż ostrzeżenie wysłane im na pocztę elektroniczną, o ile w ogóle mają konto pocztowe i z niego korzystają.

I na koniec ostatnia kwestia – w mediach najczęściej można przeczytać o naruszeniach ochrony danych osobowych w kontekście kar nałożonych przez Prezesa UODO. W 2021 r. tych kar nałożono 18, z czego rzeczywiście najwięcej, bo aż 10, w związku z naruszeniami ochrony danych osobowych. Ale w tym samym 2021 r. tych naruszeń zgłoszono Prezesowi UODO prawie 13 000! O czym to świadczy? Na pewno nie

o tym, że zgłoszenie naruszenia wiąże się z ryzykiem nałożenia kary – wręcz przeciwnie, analiza tych kar prowadzi do wniosku, że największe ryzyko kary powstaje wówczas, gdy przedsiębiorcy sztucznie zaniżają ryzyko, jakie związane jest z naruszeniem, albo w ogóle starają się to naruszenie ukryć. Jeżeli więc do naruszenia już dojdzie, starajmy się przede wszystkim myśleć o bezpieczeństwie osób dotkniętych naruszeniem, bo tylko wtedy możemy odbudować zaufanie do naszej organizacji – a to bezpieczeństwo można osiągnąć tylko przez rzetelne informowanie o naruszeniu.

# Gdy zdarzy się atak ransomware

W mediach branżowych coraz częściej możemy przeczytać o przypadkach tzw. ataków *ransomware*. Ich ofiarami padają podmioty tak prywatne, z branży usługowej, zajmujące się ochroną zdrowia, z sektora transportowego, jak i w zasadzie każde inne. Specjaliści z zakresu *cybersec* i bezpieczeństwa informacji podpowiedzą, jak starać się uniknąć ataku – ale co zrobić, gdy on już się przydarzy?

Zacznijmy od tego, czym jest *ransomware*: jest to rodzaj złośliwego oprogramowania, które blokuje dostęp do systemu komputerowego lub uniemożliwia odczyt zapisanych w nim danych, często wykorzystując do tego techniki szyfrujące, a następnie żąda od ofiary okupu za przywrócenie stanu pierwotnego, czyli za udostępnienie danych. Najbardziej widocznym dla użytkownika systemu efektem działania *ransomware* jest zablokowanie mu dostępu do danych przechowywanych w tym systemie; u jednego z klientów dotkniętych tego rodzaju atakiem wyglądało to dosłownie tak, że gdy rankiem pracownicy stawili się do pracy, na wszystkich stacjach roboczych zobaczyli ten sam komunikat wyświetlony przez *ransomware*.

Z perspektywy prawa ochrony danych osobowych skuteczny atak typu *ransomware* oznacza naruszenie ochrony danych osobowych przyjmujące postać naruszenia dostępności danych. Jak bowiem wyjaśnia UODO, naruszenie dostępności to takie naruszenie, w wyniku którego dochodzi do czasowej bądź trwałej utraty danych osobowych lub zniszczenia tychże danych. Inaczej mówiąc, albo dane gdzieś są, ale administrator danych nie ma do nich dostępu, albo danych nie ma, bo zostały zniszczone – czyli dokładnie to, co dzieje się w wyniku ataku *ransomware*. Ale to nie wszystko – jak podkreśla EROD, w wyniku tego rodzaju ataku często może też dojść do naruszenia dotyczącego poufności, a więc do ujawnienia danych osobowych osobie do tego nieuprawnionej. Podstawowe pytanie, na które musi więc odpowiedzieć administrator danych dotknięty atakiem *ransomware*, dotyczy tego, co tak naprawdę się stało: czy dane są u niego, ale zaszyfrowane, a on nie ma do nich dostępu (naru-

szenie dostępności), czy może komunikat o zaszyfrowaniu danych miał na celu przykrycie tego, że doszło do tzw. eksfiltracji danych, czyli uzyskania dostępu do danych przez osobę nieuprawnioną (naruszenie poufności danych). Ale jak to zrobić? Czasem wystarczy analiza transferów danych na łączu internetowym, która pozwoli wyłapać przypadki nieuzasadnionego wzrostu ilości transferowanych danych z organizacji, co niechybnie będzie znakiem tego, że doszło do eksfiltracji danych. W mniej jednoznacznych przypadkach trzeba będzie skorzystać z usług specjalistycznego podmiotu zajmującego się informatyką śledczą, który w większości przypadków ustali, czy doszło „tylko" do naruszenia dostępności, czy także do naruszenia poufności danych.

Kiedy już wiemy, co się stało, pora przystąpić do standardowej procedury oceny prawdopodobieństwa ryzyka naruszenia praw i wolności osób fizycznych w wyniku zaistniałego naruszenia ochrony danych. Podkreślam przy tym i apeluję: nie traktujmy naruszeń dostępności danych osobowych w jakiś przedziwnie uprzywilejowany sposób – a takie zachowania można w praktyce zaobserwować, gdy z ust klienta słyszy się, że przecież nie doszło do wycieku danych, a „tylko" zaszyfrowało mu dane w jego systemie, które to dane on sobie odtworzy z backupu. Świetnie, że sobie odtworzy – to będzie miało wpływ na wynik oceny prawdopodobieństwa ryzyka, czyli – inaczej mówiąc – na to, czy naruszenie podlega zgłoszeniu Prezesowi UODO, czy może trzeba też poinformować osoby dotknięte naruszeniem o tym fakcie; ale naruszenie dostępności danych to takie samo naruszenie, jak inne postaci naruszenia ochrony danych. Co więcej, można sobie wyobrazić takie sektory gospodarki, jak np. sektor ochrony zdrowia, w których brak dostępu do danych zapisanych np. w dokumentacji medycznej będzie rodził wprost ryzyko utraty zdrowia lub życia pacjenta. Nawet więc, jeśli doszło „tylko" do zaszyfrowania danych, a nie do ich eksfiltracji, administrator danych powinien takie zdarzenie traktować tak, jak każde inne naruszenie. Aha, jeszcze jedno: nawet jeżeli zostanie zapłacony okup i tak się złoży, że dostęp do danych zostanie przywrócony, to i tak nie ma to wpływu na zaistniałe wcześniej naruszenie dostępności danych.

W zależności od rezultatu oceny ryzyka, czasem naruszenie będące efektem ataku *ransomware* trzeba będzie zgłosić Prezesowi UODO, a czasem też poinformować osoby dotknięte naruszeniem. Od razu też uprzedzam: przygotujmy się na dodatkowe pytania ze strony UODO: a to o konkretną podatność wykorzystaną do przeprowadzenia ataku, a to o analizę ryzyka dla procesów dotkniętych atakiem, a to o testowanie skuteczności stosowanych zabezpieczeń itd. Innymi słowy, Urząd z dużym prawdopodobieństwem będzie chciał ustalić, czy organizacja, stosując odpowiednie

środki zabezpieczenia danych, powinna się była przed atakiem obronić, czy też stosując podejście oparte na ryzyku, powiedzielibyśmy, że przed tym konkretnym atakiem obronić się nie dało. Dlatego z doświadczenia w tego rodzaju sprawach mogę poradzić jedno, konkretne rozwiązanie: przygotujmy własną, możliwie szczegółową dokumentację naruszenia i opiszmy w niej to, co się stało, ale także to, jak się przed tym atakiem broniliśmy. Taka dokumentacja, po pierwsze, pokaże, że naruszenie zostało potraktowane przez organizację poważnie; po drugie, pozwoli odtworzyć tok rozumowania administratora dotkniętego atakiem i wyjaśnić Urzędowi, dlaczego np. przyjęto taką, a nie inną wartość prawdopodobieństwa ryzyka naruszenia praw i wolności osób fizycznych; po trzecie wreszcie, taka dokumentacja zwyczajnie ułatwia odpowiadanie na pytania zadawane przez Urząd.

A na koniec, życzmy sobie wszyscy aktualnych backupów.

# Jak to jest z tymi transferami danych?

Są takie tematy związane z ochroną danych osobowych, które nie schodzą z pierwszych stron mediów branżowych od lat; są też takie tematy, które można sprowadzić do wyłącznie jednego słowa. W przypadku przekazywania danych osobowych do innych krajów, ta data graniczna to 2015 r., a to słowo – a w zasadzie nazwisko – to Schrems. Max Schrems.

Mało kto wywarł tak ogromny wpływ na prawo dotyczące nas wszystkich, jak właśnie ten austriacki prawnik, od lat toczący boje najpierw z Facebookiem (obecnie Meta), a obecnie chyba z całym światem, począwszy od biznesu, na niektórych organach nadzorczych kończąc. O co więc chodzi z tymi transferami danych?

Gdy ponad 30 lat temu Unia Europejska zastanawiała się nad tym, jak uregulować ochronę danych osobowych w Unii, przyjęła zasadę, w myśl której dane mogą być swobodnie przekazywane między państwami Unii (a w zasadzie Unii i Europejskiego Obszaru Gospodarczego – EOG), a jednocześnie nie powinny tego obszaru opuszczać. Wszelkie przypadki, w których mogłoby dochodzić do przekazania danych poza EOG, czyli do transferu właśnie, zostały zapisane w ówcześnie przygotowywanej dyrektywie jako precyzyjne wyjątki od zasady, jaką był zakaz transferowy.

Unia, regulując transfery, nie zdefiniowała jednak czegoś tak podstawowego, jak samo pojęcie transferu. Zrobił to TS UE w wyroku w sprawie C-101/01, *Bodil Lindqvist*, przyjmując, że transfer zachodzi wtedy, gdy dane osobowe opuszczają obszar EOG. W pewnym uproszczeniu, jeżeli serwer stoi w Warszawie, ale dostęp do danych jest z całego świata, to transferu nie ma, ale jeżeli ten sam serwer stoi już we Lwowie, to choćby dostęp do danych był wyłącznie z Warszawy i to po VPN, to transfer jest. Tak rozumieliśmy transfery danych do czasu, gdy niejaki Edward Snowden ujawnił programy masowej inwigilacji prowadzone przez amerykańskie służby specjalne. I okazało się wtedy, że tak naprawdę nie ma znaczenia, gdzie ten serwer z danymi jest – ważne, kto

ma dostęp do danych. Dzisiaj transfer danych (w ślad za wyrokiem TS UE w sprawie C-311/18, *Schrems II*) rozumiemy więc jako sytuację, w której ktoś, kto jest objęty przepisami RODO, ujawnia lub umożliwia dostęp do danych komuś, kto tymi regulacjami objęty nie jest. Innymi słowy, gdy dane wychodzą z europejskiej przestrzeni prawnej.

Z transferami danych ma do czynienia chyba każdy przedsiębiorca – wystarczy, że korzysta z najpopularniejszego pakietu biurowego lub telefonu z jednym z dwóch najpopularniejszych systemów operacyjnych. Nawet jeżeli w ramach tego pakietu wybiera przechowywanie swoich danych w EOG, transferu (do USA) nie uniknie – amerykańskie służby mogą mieć do nich dostęp na podstawie CLOUD Act. Co więc zrobić?

Transfery danych są zakazane, chyba że zachodzi jedna z sytuacji opisanych w art. 45–49 RODO. Z punktu widzenia statystycznego polskiego przedsiębiorcy i biorąc pod uwagę usługi, z których zapewne korzysta, najważniejsze znaczenie mają transfery do jednego kraju: do USA. I wokół nich też najwięcej się dzieje. Dość powiedzieć, że:

1) do 2015 r. istniał system zwany *Safe Harbor*, umożliwiający podmiotom amerykańskim dobrowolne przestrzeganie zasad ochrony danych osobowych zbliżonych do tych europejskich, który przestał istnieć w wyniku wyroku TS w sprawie C-362/14, *Schrems I*;
2) dość szybko wprowadzono kolejne rozwiązane, *Privacy Shield*, które jednak w 2020 r. podzieliło losy poprzedniego w wyniku wyroku *Schrems II*;
3) od 10 lipca 2023 r. obowiązuje trzecie już z kolei rozwiązanie, tzw. *Privacy Framework*, legalizujące transatlantyckie przekazywanie danych.

Jak to rozwiązanie działa? Tak, jak poprzednie dwa, bo w zasadzie jest ich kopią, z niewielkimi zmianami: konkretne podmioty z USA deklarują, że będą przestrzegać zasad ochrony danych osobowych opartych na RODO, co sprawia, że transfer danych do tych konkretnych firm jest dopuszczalny. Wykaz tych podmiotów można sprawdzić na stronie https://www.dataprivacyframework.gov/s/participant-search – jest już wśród nich podmiot prowadzący największą wyszukiwarkę na świecie, a niedługo zapewne dołączą kolejni wielcy gracze. Tym, co różni *Privacy Framework* od jego poprzedników, to poprzedzające go zmiany w prawie federalnym USA, wynikające z Executive Order 14086 podpisanego przez prezydenta J. Bidena w 2022 r. Celem tych zmian było ograniczenie programów masowej inwigilacji oraz zapewnienie Europejczykom realnej ochrony prawnej na terenie USA. Wiele wskazuje więc na to, że

transfery danych do USA związane z najpopularniejszymi usługami zostały – przynajmniej na pewien czas – zalegalizowane.

A co, gdy chcemy przetransferować dane do USA poza *Privacy Framework* albo w ogóle nie do USA, tylko np. do Chin, Wielkiej Brytanii, Rosji lub Brazylii? Bo mimo tego, że Unia ma jakiś fundamentalny problem z transferami danych do USA, to transfery danych do USA to nie koniec problemu, nie początek końca, a być może dopiero koniec początku.

Każdy przypadek transferu trzeba oceniać indywidualnie i dobierać odpowiednie rozwiązanie spośród tych wskazanych w przepisach RODO. Czasem będzie to stosunkowo łatwe, bo np. odnośnie do Wielkiej Brytanii została wydana decyzja Komisji Europejskiej uznająca, że cały ten kraj daje gwarancje odpowiedniej ochrony danych, a więc można przekazywać dane do każdego podmiotu z terenu UK. Czasem z kolei będzie to bardzo trudne, bo nie dość, że z podmiotem z kraju trzeciego trzeba będzie zawrzeć odpowiednią umowę wg wzoru określonego przez Komisję Europejską, to jeszcze trzeba będzie ocenić, czy prawo i praktyka w tym kraju zapewniają odpowiednią ochronę dla przekazywanych danych. Zwłaszcza z tym drugim elementem może być czasami bardzo trudno, bo skoro mamy problem ze służbami specjalnymi z USA, to nie sposób uznać, że służby rosyjskie lub chińskie działają jakoś diametralnie inaczej. Czasem wreszcie nie będzie wyjścia, tylko trzeba będzie przyjąć, że do transferu danych nie może dojść, bo nie zachodzi żaden wyjątek uchylający zakaz transferowy.

# Kontrole UODO

Czy przetwarzamy dane przy wykorzystaniu aplikacji mobilnych, czy nie, zawsze możemy zostać skontrolowani przez pracowników UODO. I choć w ostatnich latach – ze względu na pandemię COVID-19 – liczba kontroli znacznie spadła (z 98 w 2019 r. do 12 w 2020 oraz 22 w 2021 r.), to obecnie możemy spodziewać się powrotu tych wartości od przedpandemicznych wielkości. Jak więc zachować się w sytuacji, gdy znajdziemy się wśród kontrolowanych?

Podstawową zasadą kontrolowanego jest współpraca z kontrolującymi. Dlaczego? Z prostego powodu – brak współpracy stanowi samoistną podstawę do nałożenia kary finansowej, a jednocześnie jest przestępstwem zagrożonym karą pozbawienia wolności do lat 2. Poza tym, nie współpracując, pozbawiamy się możliwości przekonania Prezesa UODO do tego, że jednak nie naruszyliśmy prawa. Mimo tego, co dla mnie niezrozumiałe, kary za brak współpracy to nadal czołówka nakładanych w Polsce kar (w 2021 r. na 14 kar 3 zostały nałożone za brak współpracy z organem). Warto też pamiętać o tym, że obowiązek współpracy z organem nadzorczym nie dotyczy wyłącznie kontroli rozumianej jako wizyta kontrolujących, których w ostatnich latach było stosunkowo niewiele – dotyczy też udzielania odpowiedzi na pytania, które organ kieruje w związku z otrzymaną skargą. A że takich skarg wpływa do UODO rocznie dużo (w 2021 r. do UODO wpłynęło 8318 skarg), to i prawdopodobieństwo tego, że będziemy musieli współpracować z organem, nie jest już takie niewielkie, jak w przypadku kontroli.

Kontrolujący zazwyczaj informują kontrolowanego z pewnym wyprzedzeniem o planowanej kontroli i o jej przedmiocie – kontrolowany ma więc czas, żeby się do kontroli przygotować: uporządkować dokumentację ochrony danych osobowych, sprawdzić jeszcze raz procesy przetwarzania danych, zorganizować miejsce pracy dla kontrolerów. A ci, gdy już się pojawią, zazwyczaj zaczynają właśnie od prośby o dokumenty: o dokumentację ochrony danych osobowych i o dokumenty kontrolowanego (statut, umowa spółki, regulaminy itp.). Z niezrozumiałych dla mnie powodów polska ustawa o ochronie danych osobowych z 2018 r. wymaga, aby kopie lub wydruki dokumentów

przekazywane kontrolującym były „potwierdzone za zgodność z oryginałem" – przed kontrolowanym nieraz więc długie godziny parafowania i podbijania „za zgodność". Trzeba też pamiętać o tym, że kontrolujący mogą zażądać przedstawienia tłumaczenia – przysięgłego – na język polski dokumentów sporządzonych w języku obcym. Nie dość, że drukujemy, parafujemy i podbijamy, to czasem jeszcze tłumaczymy (i to na własny koszt).

Przekazując dokumenty, kontrolowany może zastrzec ich poufność ze względu na swoją tajemnicę przedsiębiorstwa. W takim przypadku dostarcza się dwie wersje dokumentacji: wersję jawną, pozbawioną informacji poufnych, i wersję niejawną, tylko dla Prezesa UODO. Gorąco zachęcam do korzystania z tej możliwości, bo przecież akta kontroli stanowią informację publiczną.

To, co i jak będą sprawdzać kontrolujący, zależy od przedmiotu kontroli. Dość typowymi działaniami są np. sprawdzenie zabezpieczeń systemów służących do przetwarzania danych osobowych, sprawdzenie fizycznych zabezpieczeń obszaru przetwarzania danych, sprawdzenie zasad współpracy z podwykonawcami lub sposobu realizacji praw osób, których dane dotyczą. Wszystko oczywiście zaczyna się od poziomu dokumentacji, która jest podstawowym narzędziem wykazywania zgodności, ale to, jaką przybierze ostatecznie formę, zależy już tylko od inwencji kontrolujących; pamiętam np. sytuację, gdy kontrolowany był przedsiębiorca świadczący usługi kurierskie, a kontrolujący poprosili o towarzyszenie przesyłce od nadania do doręczenia.

Kontrolę kończy protokół kontroli. Co może wydawać się zaskakujące, protokół nie zawiera opisu stwierdzonych uchybień – zawiera opis ustalonego stanu faktycznego, ale bez wskazania, co było nie tak. Jest tak dlatego, że protokół wędruje do UODO i dopiero tam jest analizowany i jeżeli urzędnicy dojdą do wniosku, iż doszło do uchybień w procesie przetwarzania danych, wszczynane jest postępowanie. Taka konstrukcja protokołu znacznie utrudnia skorzystanie przez kontrolowanego z prawa do zgłaszania zastrzeżeń do protokołu: bo co kwestionować, skoro w protokole nie ma żadnych ocen? Z drugiej strony to właśnie zastrzeżenia do protokołu stanowią najlepszy, a często niedoceniany, sposób na istotne polepszenie sytuacji kontrolowanego. Trzeba bowiem zawsze liczyć się z tym, że w wyniku kontroli jednak zostanie wszczęte postępowanie, które doprowadzi do niekorzystnego dla nas rozstrzygnięcia. A wtedy pozostaje tylko skarga do sądu administracyjnego. Ale sąd orzeka na podstawie akt postępowania przed Prezesem UODO, sam nowych dowodów nie bę-

dzie zbierał. Co więc ma zrobić kontrolowany, który np. twierdzi, że przecież przeprowadził analizę ryzyka i proszę, o tutaj ona jest, a kontrolujący na to, że to nie o to chodzi i w protokole pojawia się wzmianka o braku takiej analizy? Odpowiedź jest prosta: zgłosić zastrzeżenie do protokołu i załączyć do niego tę właśnie ocenę. Wtedy nawet, jeżeli kontrolujący nie uwzględni takiego zastrzeżenia, będzie ono stanowiło część akt sprawy i będzie mogło zostać wykorzystane w postępowaniu sądowym.

I na koniec mała prośba: nie traktujmy kontrolujących jak naszych wrogów. Bo choć zdaniem Sądu Najwyższego nieprzychylne, niekulturalne czy nawet niegrzeczne traktowanie kontrolujących nie stanowi jeszcze utrudniania kontroli (wyrok z 19 czerwca 2002 r., V KKN 454/00), to z pewnością jej też nie ułatwia.

# Cookies – między prawem, praktyką a zdrowym rozsądkiem

Każdy, kto korzystał z Internetu 15 czy 20 lat temu, pamięta, jak to wtedy wyglądało – wpisywało się adres strony, wchodziło na nią i korzystało. A dzisiaj? Zanim doszukamy się treści, na których nam zależy, musimy przeklikać się przez niezliczoną liczbę wyskakujących okienek, zgód, informacji i bannerów. Gdy pominąć reklamy, na które przeglądarki mają swoje sposoby, za najbardziej irytujące uznaje się powszechnie informacje i zgody dotyczące tzw. ciasteczek.

Z technicznego punktu widzenia *cookies* to informacje zapisywane po stronie przeglądarki użytkownika na żądanie serwera lub skryptu stosowanego na stronie internetowej. To tekst, który ma jedno zadanie: odróżnienie osób odwiedzających dany serwis internetowy. A że nie zawsze wiadomo, kto siedzi po drugiej stronie komputera, tak naprawdę odróżniamy przeglądarkę internetową, przy pomocy której korzystamy z Internetu – stąd właśnie anegdotyczne sytuacje, gdy partner poszukuje w sieci pierścionka zaręczynowego, a jego partnerka, korzystająca z tej samej przeglądarki na tym samym komputerze, widzi następnie… reklamy pierścionków zaręczynowych.

*Cookies* zasadniczo pełną dwie funkcje:

1) umożliwiają korzystanie z konkretnej strony;
2) służą celom reklamowym, także podmiotów trzecich innych niż dostawca strony, która zapisuje ciastka.

Ciasteczka mogą, ale nie muszą, mieć charakter danych osobowych. Przekonał się o tym niedawno Prezes UODO, gdy WSA w Warszawie (wyrokiem z 11 lipca 2022 r., II SA/Wa 3993/21) m.in. z tego powodu uchylił wydaną przez niego decyzję w sprawie spółki iSecure, w której uznano, że *cookies* mają charakter danych osobowych. Nie zmienia to jednak tego, że z używaniem technologii *cookies* wiążą się konkret-

ne wymagania prawne, które wynikają w pierwszej kolejności z art. 173 Prawa telekomunikacyjnego.

Podstawowy wymóg, jaki prawo stawia ciasteczkom, to transparentność – trzeba poinformować osoby wchodzące na stronę o tym, że *cookies* są stosowane, w jakim celu to się odbywa oraz o tym, że osoba taka może nie zgodzić się na zapisywanie ciasteczek poprzez wyłączenie takiej możliwości w ustawieniach swojej przeglądarki. Co ciekawe, wyrażenie zgody na stosowanie ciasteczek powinno nastąpić po otrzymaniu tych informacji. A dlaczego to jest ciekawe? Ano dlatego, że zgodnie z polskimi przepisami zgodę na stosowanie ciasteczek można wyrazić na jeden z dwóch sposobów:

1) klikając „zgadzam się" lub podobny banner,
2) „poprzez ustawienia przeglądarki".

Co to znaczy „poprzez ustawienia przeglądarki"? Każda przeglądarka internetowa daje możliwość wyboru, czy użytkownik zgadza się na instalowanie ciastek, czy nie. „Poprzez ustawienia przeglądarki" znaczy więc tyle, że zgodę na *cookies* możemy wyrazić w ten sposób, że z poziomu przeglądarki internetowej, już za pomocą jej ustawień, możemy zezwolić na ich zapisywanie.

Zaraz, zaraz – ale jak mamy wyrazić zgodę przez ustawienia przeglądarki, jeżeli przed wyrażeniem tej zgody musimy być poinformowani o tym, w jakim celu te ciasteczka będą stosowane? Przecież informuje… konkretny usługodawca, na konkretnej stronie. Tego się w ten sposób nie da zrobić. Gdyby więc zestawić wymóg informowania o ciasteczkach z koniecznością wyrażenia na nie zgody, zostanie tylko jedna możliwość – zgoda przez kliknięcie. W tym kierunku od lat podąża też praktyka organów Unii Europejskiej: wyrok TS UE (C-673/17, Planet49), który nakazuje zbieranie zgód w sposób aktywny, to 2019 r., odpowiednie wytyczne EROD to 2020 r. W ślad za nimi poszły też niektóre europejskiej organy nadzorcze, wydając rekomendacje, w których:

1) zakazano zbierania zgód przez ustawienia przeglądarki oraz przyjęto, że kontynuowanie przeglądania strony po otrzymaniu informacji o ciasteczkach nie może być uznane za zgodę (Commission nationale de l'informatique et des libertés, CNIL);
2) nakazano informować raczej o typach stosowanych ciasteczek i ich funkcjach, zamiast automatycznie wypisywać wszystkie ciastka, jakie strona zapisuje (Information Commissioner's Office, ICO).

Powszechna zgoda, przynajmniej w Europie Zachodniej, panuje co do jednego: nie wolno stosować tzw. *cookie wall*. O co chodzi? O uzależnianie dostępu do strony od wyrażenia zgody na ciasteczka, które nie są niezbędne do korzystania z tej strony. Najczęściej dotyczy to ciasteczek wykorzystywanych w celach reklamowych także – a może przede wszystkich – podmiotów trzecich.

Polska na tym tle wypada blado: mamy częściowo niewykonalne przepisy, brak jest jakichkolwiek wytycznych organu nadzorczego, mamy jedną decyzję, i tak uchyloną przez sąd, a praktyka administratorów stron jest niespójna: nadal można znaleźć wiele przykładów *cookie wall*, wciąż kontynuowanie przeglądania strony uznawane jest za zgodę na zapisywanie wszelkich możliwych ciasteczek. Myliłby się jednak ten, kto by przypuszczał, że w temacie *cookies* nic się w Polsce nie dzieje – do Prezesa UODO wpłynęły dziesiątki, jeżeli nie setki, skarg pochodzących od aktywistów zajmujących się ochroną prywatności w Internecie i, chcąc nie chcąc, Urząd te skargi będzie musiał rozpatrzyć i wydać jakieś decyzje – z dużym prawdopodobieństwem będą one zgodne z tendencjami europejskimi.

Jak więc rozwiązać dzisiaj problem zgód na *cookies*? To muszą być zgody aktywne, przez kliknięcie; zgodzie musi towarzyszyć informacja o tym, jakie ciasteczka i po co są instalowane; nie można uzależniać wejścia na stronę od zgody na stosowanie ciasteczek. Te węzłowe kwestie z pewnością trzeba wdrożyć już dzisiaj, nie czekając na decyzje Prezesa UODO.

# Usługi i treści w zamian za dane – przykład Meta

Nie zawsze warto kurczowo trzymać się zgód na przetwarzanie danych osobowych jako panaceum na wszystkie problemy administratorów danych – to już wiemy. Ale problemy możemy mieć także wtedy, gdy wahadło zbytnio wychyla się w drugą stronę, o czym przekonał się niedawno Meta, podmiot prowadzący serwisy społecznościowe Facebook i Instagram.

Żeby zrozumieć problem, z którym w pewnym sensie mamy do czynienia wszyscy, trzeba cofnąć się w czasie o jakieś 20–25 lat. Internet, jaki zna moje pokolenie, to Internet „darmowych" treści. „Darmowych", bo za nic nie płaciliśmy w pieniądzu – ale płaciliśmy w danych. Oczywiście nie było wtedy przepisów o ochronie danych osobowych, nie było bannerów *cookies* i zgód. Nie było też tak agresywnych metod personalizacji reklam i budowania profili, jakie są dostępne dzisiaj. Jednym słowem, nic nie było – więc i świadomość tego, jak to działa, była ogólnie niewielka. Ale z czasem świadomość zaczęła rosnąć, a wraz z nią towarzyszące regulacje. Zdaliśmy sobie sprawę z tego, że nie ma darmowych lunchów, a za treści, które czytamy, płacimy własnymi danymi.

Zmiana, jaka nastąpiła w nas mniej więcej przed 10 laty, wiąże się z tym, że zaczęliśmy bardziej dbać o naszą prywatność i źródło finansujące treści zaczęło zwyczajnie wysychać. Zaczęliśmy np. korzystać ze specjalistycznego oprogramowania blokującego śledzenie i reklamy (kojarzycie Państwo te bannery blokujące dostęp do strony i proszące o wyłączenie oprogramowania X?). Naturalne stało się też to, że niektórzy dostawcy zaczęli przechodzić na płatność za treści w pieniądzu, np. w modelu subskrypcji. Ale Meta nie chciała ani wprowadzić odpłatności w pieniądzu za korzystanie ze swoich platform, ani zbierać naszych zgód na korzystanie z naszych danych. Meta uważała, że personalizowanie pokazywanych nam reklam na podstawie naszych danych osobowych to element naszej umowy z Meta. Inaczej mówiąc, korzystamy z platform Meta m.in. po to, żeby dostawać personalizowane reklamy.

A to wszystko oczywiście na zasadach opisanych w regulaminie, który określa jednostronnie Meta.

Taka praktyka spotkała się ze sprzeciwem ze strony europejskich organów nadzorczych zajmujących się ochroną danych osobowych i doprowadziła do wydania przez irlandzki organ nadzorczy decyzji zakazującej Meta stosowania tego rozwiązania. Co jednak jeszcze bardziej istotne, TS UE w wyroku w sprawie C-252/21, Meta Platforms and Others, przyjął, że możliwość powołania się na konieczność przetwarzania danych w celu wykonania umowy istnieje wyłącznie wtedy, gdy przetwarzanie to jest obiektywnie niezbędne do osiągnięcia celu, który stanowi integralną część świadczenia umownego na rzecz tych samych użytkowników, skutkiem czego główny cel umowy nie mógłby zostać osiągnięty bez tego przetwarzania – taka sytuacja nie zachodzi w przypadku Meta i personalizowania reklam rzekomo jako elementu umowy z Meta o korzystanie z serwisów Facebook i Instagram. Czy takie podejście może mieć wpływ na całość Internetu? Tak, ale nie do końca takie, jakich spodziewają się niektórzy. Bo trzeba to powiedzieć jasno – model „treści za dane" nie został tą decyzją pogrzebany. Wręcz przeciwnie, model płatności za usługi naszymi danymi dzięki tej decyzji ma szasnę towarzyszyć nam jeszcze wiele, wiele lat.

Aby to wyjaśnić, zacznijmy od wskazania, gdzie Meta popełniła błąd – polegał on mianowicie na tym, że przyjęto, iż elementem usług świadczonych nam przez Meta jest personalizowanie reklam. Tymczasem tak nie jest – korzystamy z mediów społecznościowych w wielu różnych celach, ale nie po to, żeby otrzymywać reklamy dobrane do naszych zainteresowań. Dlatego przetwarzanie danych w celu reklamowym miało się nijak do zasadniczego celu, w jakim Meta przetwarza dane użytkowników swoich platform. A skoro tak, to nie mógł to być element niezbędny do wykonania umowy o korzystanie z platformy. Co więc pozostaje? Pozostaje zbieranie zgód na przetwarzanie danych w celu personalizowania reklam – ale uwaga: taka zgoda musi być dobrowolna, a więc nikogo nie można przymuszać do jej wyrażenia. Stąd konieczność pozostawienia niezmienionych usług także dla tych, którzy zgody nie wyrażą.

„Gdzie tu płatność danymi?" – można zapytać, skoro nawet jak ktoś nie zapłaci, ma dostęp do usług. I tu właśnie dochodzimy do sedna – płatność w danych musi być dobrowolna. Żeby tak było, użytkownik musi mieć jakąś alternatywę, którą – realnie oceniając – może być tylko płatność w pieniądzu. Dlatego popularne polskie portale oferują dzisiaj dwa główne warianty poczty elektronicznej: „darmowy", bo

płatny danymi, i niedarmowy, bo płatny w pieniądzu. Oczywiście żaden z nich nie jest darmowy, ale taka konstrukcja daje wybór w postaci płacenia albo danymi, albo pieniędzmi. A to powoduje, że decyzja o zapłacie w danych jest dobrowolna, bo przecież była realnie dostępna inna możliwość.

Kropla drąży skałę i oto doczekaliśmy się chwili, w której i Meta wprowadziła możliwość zapłaty w pieniądzu za jej usługi. Dlaczego trwało to tak długo? Nie mnie to oceniać. Czy zaproponowana kwota nie jest „odrobinę" za wysoka, przez co ma zachęcać do pozostania przy dotychczasowym modelu? Być może. Wiem za to na pewno, że wszędzie tam, gdzie chcemy udostępniać treści lub świadczyć usługi w zamian za dane, musimy tak ten proces skonstruować, żeby dać wybór: jeżeli ktoś nie chce wyrażać zgody, musi mieć inną możliwość skorzystania z naszych usług. W takim przypadku zebrane zgody – których zapewne będzie ogromna większość – będą w pełni dobrowolne, a więc ten, kto je zbiera, nie narazi się na zarzut wymuszania zgód.

# Aplikacje mobilne

Aplikacje mobilne: czasem stanowią tylko narzędzie reklamy, czasem są elementem skomplikowanych procesów sprzedażowych lub obsługowych, na równi z innymi kanałami kontaktu z klientem, a czasem wręcz cały biznes można sprowadzić do aplikacji, przy pomocy której jest on realizowany.

Aplikacje mobilne od lat tradycyjnie pozostają w orbicie zainteresowania UODO. Spróbujmy więc zastanowić się nad tym, jak podejść do projektowania i stosowania aplikacji mobilnych z perspektywy RODO.

Założenie wstępne ma charakter fundamentalny: ochronę danych osobowych należy uwzględniać przez cały cykl życia aplikacji, od etapu projektowania począwszy. To zasada *privacy by design*, czyli uwzględniania ochrony danych osobowych już na etapie projektowania procesu przetwarzania danych (tu: przy pomocy aplikacji). Jest to obowiązek prawny, a nie postulat kierunkowy – projektując nowe aplikacji i używając aplikacji mobilnych, od początku musimy więc podchodzić do ochrony danych osobowych w sposób proaktywny i starać się przewidywać zagrożenia, które mogą wystąpić w toku korzystania z aplikacji, a nie wyłącznie reagować na to, co będzie się działo. I oczywiście, w myśl zasady rozliczalności, musimy to podejście proaktywne dokumentować.

Zakładając, że chronimy dane osobowe przez cały cykl ich życia, pierwsze pytanie, które przed nami staje, jest o to, czy nasza aplikacja w ogóle powinna przetwarzać jakiekolwiek dane osobowe. Bo przysłowiowa aplikacja latarka z logo naszej firmy nie potrzebuje żadnych danych osobowych do prawidłowego działania. Oczywiście aplikacje stanowiące element procesów sprzedażowych lub obsługowych z definicji służą do przetwarzania danych – wtedy z kolei przechodzimy do pytania drugiego: jak wiele danych aplikacja powinna przetwarzać? Czy np. aplikacja bankowa musi mieć dostęp do zdjęć w smartfonie? A dostęp do lokalizacji? Odpowiedź na każde z takich pytań wymaga przeanalizowania funkcjonalności aplikacji i ustalenia, czy taki dostęp jest niezbędny z perspektywy funkcjonalności aplikacji.

Kolejna kwestia to sposób zabezpieczenia danych przetwarzanych za pomocą aplikacji – na to szczególną uwagę będzie zwracał Urząd w toku kontroli. W każdym przypadku należy przeprowadzić analizę ryzyka, które dla praw i wolności osób, których dane będą przetwarzane w aplikacji, wiąże się z takim przetwarzaniem. Jest to standardowa procedura umożliwiająca dobór odpowiednich środków zabezpieczenia danych osobowych, obecna z nami od początku stosowania RODO – ale nadal bywa, że traktowana po macoszemu. A tymczasem aplikacje mobilne to takie przetwarzanie danych, w przypadku którego ta analiza jest szczególnie potrzebna. Bo zastanówmy się nad pierwszym z brzegu pytaniem: gdzie dane będą przechowywane i przetwarzane? Zapewne, jak wskazuje doświadczenie, u jednego z najpopularniejszych zewnętrznych dostawców usług hostingowych. A czy wiemy, gdzie ten dostawca ma swoje *data center*? Czy wiemy, kto będzie miał dostęp do tych danych? Czy dane są bezpieczne przed zapędami służb tego kraju? Zapewne w ogólnym rozrachunku taki zewnętrzny dostawca będzie zapewniał większe bezpieczeństwo niż przysłowiowy serwer w piwnicy, ale choćby nieodległy w czasie przypadek pożaru u jednego z takich dostawców nie pozwala przyjąć z automatu, że duży dostawca daje większe bezpieczeństwo.

Właśnie – kto będzie miał dostęp do danych? Urząd w czasie kontroli oprócz zabezpieczenia danych, szczególną uwagę będzie zwracał na udostępnianie danych osobowych przetwarzanych w związku z użytkowaniem aplikacji. Zapewne chodzi tu o przeróżne przypadki dostępu zewnętrznych podmiotów do naszych danych – a te dane mogą mieć ogromną wartość. Preferencje zakupowe w aplikacji do przechowywania paragonów, stan zdrowia w aplikacji treningowej lub aptecznej, poglądy polityczne w aplikacji do analizy preferencji wyborczych – to tylko niektóre przykłady. Reklamowana niedawno aplikacja służąca do obsługi termometru elektronicznego to kopalnia wiedzy np. dotyczącej płodności, którą to wiedzę można bardzo efektywnie przełożyć na targetowanie reklamy. Każdy taki dostęp do danych, jeżeli miałby się odbywać dla własnych celów tego, kto je uzyskuje, powinien się odbywać na podstawie zgody osoby, której dane dotyczą.

Zgody to osobny temat, który już zresztą na tych łamach poruszałem; a aplikacje zazwyczaj umożliwiają zbieranie zgód. Samo w sobie to nic złego, o ile oczywiście twórcy aplikacji pamiętają, że zgody powinny być świadome, dobrowolne, jednoznaczne i konkretne. W szczególności bywają problemy z dobrowolnością: nie jest dobrowolną zgoda np. na dostęp do lokalizacji i wiadomości, jeżeli ta zgoda jest niezbędna do tego, by korzystać z aplikacji służącej do edycji zdjęć.

I na koniec kwestia z pozoru oczywista, czyli informowanie użytkowników aplikacji. Począwszy od tego, kto jest administratorem danych, poprzez informacje umożliwiające kontakt z nim celem korzystania z praw przysługujących osobom, których dane dotyczą, a na polityce ochrony danych osobowych kończąc – to wszystko trzeba uwzględnić przy tworzeniu aplikacji mobilnej.

Choć w praktyce Urząd skontroluje może promil polskich aplikacji mobilnych, to ujęcie aplikacji w planie kontroli bez wątpienia wpłynie pozytywnie na poziom ochrony danych osobowych aplikacji dostępnych na rynku. Nie czekajmy więc na bycie skontrolowanym, a już teraz spróbujmy wdrożyć choćby te podstawowe zasady, które przywołałem wyżej.

# Procesowe podejście do ochrony danych osobowych

Na koniec tego krótkiego zbioru przemyśleń dotyczących stosowania przepisów o ochronie danych osobowych chyba kwestia najważniejsza: gdy już wiemy, czym są dane osobowe i jakie są zasady ich przetwarzania, spróbujmy wznieść się nieco wyżej ponad te szczegółowe kwestie i zastanówmy nad tym, w jaki sposób RODO podchodzi do przetwarzania danych osobowych w ogóle i jak to powinno się przekładać na nasze myślenie o procesach przetwarzania danych.

Ci z Państwa, którzy pamiętają jeszcze ustawę o ochronie danych osobowych z 1997 r., pamiętają też zapewne pojęcie zbioru danych osobowych, na którym opierało się ówczesne podejście do ochrony danych osobowych: zbiory danych się nazywało, opisywało się przepływy danych między nimi, rejestrowało się zbiory w ówczesnym GIODO. To zbiorocentryczne podejście skończyło się wraz z rozpoczęciem stosowania RODO w 2018 r. – RODO już nie myśli w kategoriach zbiorów, RODO podchodzi do ochrony danych osobowych w sposób procesowy.

Procesowe podejście do ochrony danych osobowych wywodzi się z zasady uwzględniania ochrony danych w fazie projektowania, czyli *privacy by design*. *Privacy by design* zakłada ochronę informacji od początku do końca jej cyklu życia, od zebrania do usunięcia. Co więcej, *privacy by design* to także podejście proaktywne do ochrony danych osobowych, zakładające włączenie ochrony danych osobowych w projekt od samego początku i dążenie do tego, by ewentualne problemy przewidywać i starać się ich uniknąć, a nie reagować na te, które dopiero wystąpią.

Obowiązek uwzględniania ochrony danych w fazie projektowania wymusza na administratorach danych patrzenie na przetwarzanie danych jako na proces, rozpoczynający się od zebrania danych, a kończący się na ich usunięciu – ale wymusza także odpowiednie zaprojektowanie tego procesu. A narzędziem, które ma to umożliwić, są obowiązki skupione wokół pojęcia czynności przetwarzania danych osobowych.

Czynność przetwarzania danych to – w ślad za stanowiskiem Prezesa UODO – „zespół powiązanych ze sobą operacji na danych, wykonywanych przez jedną lub kilka osób, które można określić w sposób zbiorczy, w związku z celem, w jakim te czynności są podejmowane" („Wskazówki i wyjaśnienia dotyczące obowiązku rejestrowania czynności i kategorii czynności przetwarzania określonego w art. 30 ust. 1 i 2 RODO", https://uodo.gov.pl/data/filemanager_pl/708.pdf). „Zespół powiązanych ze sobą operacji", to nic innego, jak czynności przetwarzania danych składające się na cykl życia danych osobowych – od ich zebrania, po usunięcie. Czynnością będzie np. rekrutacja pracowników, którą zaczyna zebranie danych, a kończy usunięcie ich po zakończeniu procesu i upływie terminów przedawnienia roszczeń; czynnością będzie obsługa zamówień w sklepie internetowym, którą rozpoczyna złożenie zamówienia, a kończy usunięcie danych osobowych po wykonaniu zamówienia, upływie terminów przedawnienia i usunięciu dokumentów finansowo-księgowych; czynnością będzie przyjmowanie wniosków o świadczenie z zakresu pomocy społecznej, którą rozpoczyna przyjęcie wniosku, a kończy usunięcie danych lub przekazanie ich do archiwum – i tak dalej.

Procesowe podejście do ochrony danych osobowych rozpoczyna się od zaprojektowania czynności przetwarzania danych. W pewnym uproszczeniu, ale jednak oddającym istotę problemu, całe zagadnienie można sprowadzić do sześciu pytań:

1) po co mi są dane?
2) jakie dane będę zbierał?
3) dlaczego mogę je przetwarzać?
4) jak zapewnię poprawność danych?
5) jak je zabezpieczę?
6) jak długo będę je przechowywał?

Te pytania to nic innego, jak refleks zasad ochrony danych osobowych z art. 5 ust. 1 RODO. A jak działają w praktyce? Wyobraźmy sobie, że projektujemy czynność przetwarzania danych osobowych dla celów rekrutacji. Mamy więc cel przetwarzania danych: rekrutacja. Zakres danych wyznaczają nam przepisy prawa, konkretnie Kodeksu pracy. Nie musimy zbierać zgody na przetwarzanie danych, o ile prowadzimy rekrutację na konkretne stanowisko – ale jeżeli chcemy zachować dane dla przyszłych rekrutacji, musimy zebrać zgody. Poprawność danych zapewniamy, stosując np. w formularzach internetowych słownikowanie nazw ulic lub kodów pocztowych, a środki zabezpieczenia danych dobieramy na podstawie analizy ryzyka. Dane przechowujemy do zakończenia procesu rekrutacji i upływu terminów przedawnienia

roszczeń, chyba że kandydata zatrudniamy lub wyraził on zgodę na przetwarzanie danych dla celów przyszłych rekrutacji.

Oczywiście w odniesieniu do innych czynności przetwarzania swoboda decyzyjna po stronie administratora projektującego czynność może być znacznie większa – w szczególności w typowych sytuacjach powstanie potrzeba samodzielnego określenia zakresu przetwarzanych danych osobowych. Tym niemniej istota projektowania czynności pozostanie taka sama.

Ponieważ w przepisach RODO zrezygnowano z rejestracji zbiorów danych osobowych przez organ nadzorczy, w zamian zdecydowano się nałożyć pewne obowiązki rejestracyjne bezpośrednio na administratorów danych. W efekcie administrator danych powinien samodzielnie opisywać czynności przetwarzania danych w swojej organizacji w prowadzonym przez siebie rejestrze czynności przetwarzania danych. W rejestrze umieszcza się informacje o czynnościach przetwarzania, takie jak dane administratora, cel przetwarzania, opis kategorii osób, których dane dotyczą, opis kategorii przetwarzanych danych osobowych, kategorie odbiorców danych, informacje o ew. transferach danych do krajów trzecich, planowane terminy usunięcia danych i ogólne informacje o stosowanych środkach zabezpieczenia danych. Jest to więc podstawowe narzędzie zapewnienia zgodności z przepisami o ochronie danych osobowych, bo opisujące każdą czynność przetwarzania, ale też podstawowe źródło informacji dla audytora lub inspektorów Urzędu Ochrony Danych Osobowych.

Procesowe podejście do ochrony danych osobowych to dzisiaj obowiązek prawny. Nie powinniśmy go jednak traktować wyłącznie jako ciężaru nałożonego na administratorów danych – to doskonały sposób na to, by przetwarzanie danych w organizacji spełniało wymogi stawiane przez obowiązujące prawo.

BARTA LITWIŃSKI
KANCELARIA
RADCÓW PRAWNYCH
I ADWOKATÓW
SPÓŁKA PARTNERSKA

www.bartalitwinski.pl
www.linkedin.com/in/paweł-litwiński