RODO

MASZ PRAWO I NIE WAHAJ SIĘ GO UŻYĆ

FUNDACJA PANOPTYKON

PROJEKT I SKŁAD: PIOTR CHUCHLA
KOREKTA: URSZULA DOBRZAŃSKA

ISBN: 978-83-938554-6-9

PANOPTYKON.ORG

FUNDACJA PANOPTYKON
WARSZAWA 2018

KAROLINA IWAŃSKA
WOJCIECH KLICKI
ANNA OBEM
MAŁGORZATA SZUMAŃSKA
KATARZYNA SZYMIELEWICZ

RODO

MASZ PRAWO I NIE WAHAJ SIĘ GO UŻYĆ

FUNDACJA PANOPTYKON

Burza medialna, zalew e-maili z informacjami i prośbami o zgodę na przetwarzanie danych, obawy przedsiębiorców straszonych karami, nerwowe ruchy publicznych instytucji, zamieszanie, bałagan i absurd goniący absurd – wdrożenie europejskiej reformy ochrony danych osobowych w Polsce sprawiło, że wielu osobom RODO kojarzy się jak najgorzej.

W tych okolicznościach z zasięgu wzroku łatwo stracić dwa kluczowe fakty. Po pierwsze, RODO to nie taka znowu rewolucja, a jedynie krok w wieloletnim procesie ewolucji prawa ochrony danych osobowych. Po drugie, zawiera ono kilka rozwiązań korzystnych z punktu widzenia konsumentów i obywateli: przyznaje nowe uprawnienia, np. do żądania kopii danych od podmiotów, które je przetwarzają, oraz nakłada na firmy spoza Unii obowiązek ochrony danych zgodnie z wysokim, europejskim standardem. A to w naszym zglobalizowanym świecie usług cyfrowych zmiana niebagatelna, zważywszy na to, jak wiele prywatnych informacji trafia na serwery firm z Krzemowej Doliny.

W Fundacji Panoptykon dążymy do tego, by każdy miał kontrolę nad tym, kto i w jaki sposób wykorzystuje jego dane. Jeszcze trochę czasu upłynie, zanim będzie można ocenić, czy RODO nas do tego przybliża – czy niesie realną zmianę w sposobie, w jaki różne podmioty podchodzą do przetwarzanych przez siebie danych. Zmiana zależy od tego, ile osób będzie rozumieć, o co chodzi w ochronie danych, i domagać się respektowania swoich praw. I tu widzimy rolę dla Panoptykonu.

W tej publikacji pokazujemy, co się zmieniło „po RODO" i jak ochrona danych funkcjonuje w różnych branżach (u lekarza, w szkole, w pracy, w sklepie czy w Kościele). Rozprawiamy się z mitami i absurdami oraz podpowiadamy, jak korzystać ze swoich praw.

Miłej lektury!

U LEKARZA

Batman, Skrzat i Muminek – między innymi takimi pseudonimami zostali obdarzeni pacjenci jednej z przychodni. Nie, to nie nowy wymóg prawny, a jedynie nadgorliwość albo zagubienie zarządzających tą placówką. RODO-absurdy w służbie zdrowia tylko utrudniają życie, podczas gdy prywatność pacjentów zasługuje na poważne traktowanie. Jakie wyzwania związane z ochroną danych osobowych ujawniły się podczas zmagań polskiej służby zdrowia z RODO?

Pacjenci jak numerki

W niektórych szpitalach i przychodniach podczas wywoływania do gabinetu chorzy zamiast swojego imienia i nazwiska słyszą przydzielony wcześniej numer, w innych personel posługuje się tylko imionami, niekiedy połączonymi np. z miesiącem urodzenia („Zapraszam do gabinetu Annę z września!"). Dyrekcje szpitali same dostrzegają, że część pacjentów nie rozumie, dlaczego są proszeni przez lekarza po numerze, a nie po nazwisku. Szczególnie ci starsi oburzają się na przedmiotowe traktowanie. W Internecie pojawiają się żarty, że zamiast nazwisk lekarze powinni używać nazw chorób („A teraz Wojciech z syfilisem!").

Jak takie praktyki mają się do RODO? Ochrona danych nie polega na ukrywaniu informacji za wszelką cenę, tylko na ich rozsądnym wykorzystywaniu – z zapewnieniem poufności. Jedną z kluczowych zasad jest minimalizacja: używanie tylko tych danych, które w konkretnej sytuacji są konieczne. W tym duchu przychodnie rzeczywiście mogłyby zrezygnować z wywoływania pacjentów do gabinetu po imieniu i nazwisku. Bo po co – skoro nie ma takiej potrzeby? Sensowny sposób na zgodne z RODO wywoływanie pacjenta to choćby użycie imienia w połączeniu z godziną, na którą pacjent był zapisany. Takie rozwiązania podpowiada przygotowany wspólnie przez Ministerstwo Cyfryzacji i Ministerstwo Zdrowia *Przewodnik po RODO w służbie zdrowia*.

Przychodnie i szpitale powinny też zadbać o prywatność rejestrujących się pacjentów. Najlepiej przenieść ten proces do osobnego pomieszczenia, a jeśli nie jest to możliwe – tak zaaranżować przestrzeń, by oczekujący w kolejce nie znajdowali się tuż obok osoby, która umawia się na wizytę lub odbiera wyniki badań.

Informowanie (rodziców) o stanie zdrowia

Kilka tygodni po wejściu w życie RODO na Zakopiance doszło do tragicznego wypadku autokaru wiozącego dzieci. Rodzice próbujący telefonicznie ustalić, do jakiego szpitala trafiło ich dziecko, odbijali się od ściany – nikt nie chciał udzielić im odpowiedzi, „bo RODO". Ta historia szybko stała się przykładem rzekomej absurdalności unijnych przepisów i bezsensowności ochrony danych osobowych wobec prawdziwych ludzkich dramatów.

OCHRONA DANYCH NIE POLEGA NA UKRYWANIU INFORMACJI ZA WSZELKĄ CENĘ, TYLKO NA ICH ROZSĄDNYM WYKORZYSTYWANIU – Z ZAPEWNIENIEM POUFNOŚCI.

Czy można zgodnie z RODO poinformować rodzica o tym, że dziecko przebywa w szpitalu i jak się czuje? Oczywiście. Szpital może przekazać rodzinie informacje o stanie zdrowia dziecka, szczególnie kiedy sytuacja jest nagła i odmowa kontaktu mogłaby zaszkodzić samemu pacjentowi. Brak komunikacji nie tylko naraża dziecko i rodziców na niepotrzebny stres, ale też odcina lekarzy od ważnych informacji, np. o uczuleniach, innych chorobach czy przyjmowanych lekach.

To jednak nie oznacza, że dyżurny lekarz czy pielęgniarka mają opowiadać każdemu dzwoniącemu o stanie pacjentów. Przed udzieleniem jakichkolwiek informacji powinni zweryfikować tożsamość rozmówcy i jego związek z pacjentem, np. prosząc o adres czy numer PESEL. Również w tej sytuacji znajdzie zastosowanie zasada minimalizacji: wystarczy, że szpital przez telefon potwierdzi, że dziecko zostało przyjęte i że jego życiu nie zagraża niebezpieczeństwo. Szczegółowe informacje lepiej przekazać osobiście, po weryfikacji tożsamości pytającego.

Cisza w szpitalu. O rozmowach lekarzy z pacjentami

Zgodnie z RODO dane dotyczące zdrowia podlegają szczególnej ochronie i bez zgody samego pacjenta nie powinny być udostępniane osobom trzecim. Dlatego RODO wprowadziło sporo zamieszania w rutynowe praktyki personelu, szczególnie podczas obchodów: czy można porozmawiać z pacjentem w obecności innych chorych i odwiedzających ich gości?

ZGODNIE Z RODO DANE DOTYCZĄCE ZDROWIA PODLEGAJĄ SZCZEGÓLNEJ OCHRONIE I BEZ ZGODY SAMEGO PACJENTA NIE POWINNY BYĆ UDOSTĘPNIANE OSOBOM TRZECIM.

Proste pytania o samopoczucie zazwyczaj nie ingerują głęboko w prywatność pacjentów, dlatego mogą padać na sali w obecności innych chorych (ale już odwiedzających warto w tej sytuacji na chwilę wyprosić). Natomiast szczegółowy wywiad prowadzony przy przyjęciu do szpitala oraz omówienie wyników badań czy wad i zalet proponowanej metody leczenia powinny odbywać się na osobności, w możliwie najbardziej komfortowych dla pacjenta warunkach, np. w gabinecie lekarskim.

Czasami zapewnienie takiego standardu oznacza konieczność wprowadzenia zmian organizacyjnych na oddziale. Wymaga też od personelu szpitala elastyczności i dostosowania się choćby do stanu zdrowia pacjenta. Wyzwaniem może być np. zadbanie o komfort osób, które nie mogą samodzielnie się poruszać.

Anonimowy lekarz

W dyskusji na temat RODO pojawiły się wątpliwości, czy w przychodniach i szpitalach gabinety mogą być oznaczone nazwiskami przyjmujących w nich lekarzy. Chowanie tabliczek z nazwiskiem to zdecydowanie nietrafiony pomysł, którego realizacja mogłaby utrudnić pacjentom znalezienie odpowiedniego gabinetu. Lekarz w pracy nie może być anonimowy. Z przepisów wynika, że pacjent ma prawo wyboru lekarza, a ten ma obowiązek w widocznym miejscu nosić identyfikator.

Wyzwania dla RODO

W przypadku większości RODO-absurdów, którymi żyją media i bulwersują się pacjenci, komuś najwyraźniej zabrakło zdrowego rozsądku i chwili zastanowienia nad tym, czy proponowana zmiana rzeczywiście przyczyni się do lepszej ochrony prywatności chorych.

A na tym polu jest wiele do zrobienia. Z jednej strony nowe wyzwania rodzi coraz szersze wykorzystanie nowych technologii do przetwarzania danych medycznych. Z drugiej – wciąż dochodzi do elementarnych naruszeń intymności i godności pacjentów w szpitalach, co pokazuje raport Najwyższej Izby Kontroli opublikowany raptem kilka dni przed wejściem w życie RODO. Łóżka na korytarzach i łazienki bez możliwości zamknięcia od wewnątrz to najbardziej jaskrawe przykłady naruszeń. Zdaniem kontrolerów NIK „bez radykalnej poprawy infrastruktury szpitali i uwrażliwienia personelu medycznego na potrzeby i uczucia hospitalizowanych osób prawo pacjenta do intymności i godności pozostanie tylko formalną deklaracją".

Poszanowanie prywatności i godności to nie tylko Twoje święte prawo jako pacjenta, ale też czynnik wpływający na samopoczucie, zaufanie do lekarzy i pielęgniarek, a w dłuższej perspektywie – szybkość i skuteczność całego procesu leczenia. W tym kontekście niewywoływanie chorych po nazwisku to tylko zmiana kosmetyczna. Najpoważniejsze problemy wymagają znacznie głębszych zmian.

W SZKOLE

Z początkiem roku szkolnego wybuchła RODO-panika. Nagle okazało się, że w szkole „nie wolno zawołać ucznia po nazwisku, bo RODO!". Co takiego się stało? Wielu dyrektorów zamiast dostosować istniejące procedury do nowych przepisów, zgodnie z własną misją i wartościami, na wszelki wypadek wprowadzało rozwiązania, na które rodzicom trudno było zareagować inaczej niż frustracją lub niedowierzaniem. Czy ochrona danych w szkolnej rzeczywistości naprawdę musi tak wyglądać?

Lista bez nazwisk

Szkoły i przedszkola nie powstały po to, żeby przetwarzać dane – mają przede wszystkim uczyć i wychowywać. Oczywiście, przy okazji gromadzą dużo informacji – o uczniach, ich rodzicach, nauczycielach oraz innych pracownikach. To prawda, nazwisko jest daną osobową i należy mu się ochrona, ale przecież nie bezwarunkowa. Dopóki takie dane są potrzebne szkołom do realizacji zadań, jakie nakłada na nie prawo, mogą je przetwarzać. Nauczyciele mogą legalnie odczytywać listę obecności, a dzieci – podpisywać zeszyty i sprawdziany. Więcej: na takie użycie danych nie potrzebują zgody rodziców.

Podobnie jest z organizowaniem konkursów: prawo oświatowe pozwala wyróżniać uczniów za ich osiągnięcia, a więc nagrodzone prace plastyczne mogą wisieć na szkolnych korytarzach z podpisami autorów. Warto się jednak zastanowić, czy podpisywanie prac zawsze stanowi najlepszą opcję: być może twórczość uczniów rozwijałaby się równie dobrze (a nawet lepiej), gdyby mogli tworzyć także pod pseudonimami?

A co z odczytywaniem na głos ocen: czy powinna to być reguła, czy też wyjątek? Kiedy możliwość porównania wyników jest dla uczniów ważna i pomaga im w nauce, a kiedy wręcz przeciwnie? Skoro mało kto lubi być oceniany na forum, może i dzieciom warto dać taki komfort? RODO nie zawiera sztywnych zakazów i nakazów, natomiast zmusza do myślenia i pytania o cel.

Zgoda na wszelki wypadek

Na pierwszym zebraniu rodzice otrzymali plik kartek z oświadczeniami. Na pewno znalazła się tam przynajmniej jedna zgoda na przetwarzanie danych: udział w programie profilaktyki zdrowotnej, wykorzystanie wizerunku dzieci, przekazanie danych ubezpieczycielowi. Zgody są też wymagane od osób, które mają odbierać dzieci z placówek (bo przecież szkoła będzie przetwarzać ich nazwisko i numer telefonu).

CZĘSTO SZKOŁY DMUCHAJĄ NA ZIMNE I ZBIERAJĄ ZGODY, KTÓRE WCALE NIE SĄ IM POTRZEBNE, BO MOGĄ SKORZYSTAĆ Z INNEJ PODSTAWY PRAWNEJ.

Często szkoły dmuchają na zimne i zbierają zgody, które wcale nie są im potrzebne, bo mogą skorzystać z innej podstawy prawnej (np. powołać się na przepis prawa lub niezbędność do realizacji zadań publicznych). Co gorsza, zdarza im się też zbieranie zgód, które są po prostu nieważne. Chodzi o sytuacje, kiedy podpisujący oświadczenie nie miał realnego wyboru (np. rodzice zostali poinformowani, że „muszą się zgodzić").

Najprostszy test na to, czy zbieranie zgody jest potrzebne, to pytanie: „Czy bez tych danych szkoła może działać normalnie i realizować swoje zadania?". Jeśli podanie danych rzeczywiście jest dobrowolne i można się bez nich obejść (uczyć, wychowywać, chronić), wtedy zgoda ma sens. W każdej innej sytuacji jest podejrzana.

Szkoły i przedszkola przyzwyczaiły się do wrzucania na swoje strony i profile w mediach społecznościowych zdjęć z uroczystości, zajęć świetlicowych i wycieczek. Takie wykorzystanie danych dzieci nie ma związku z edukacją – szkoła może sobie świetnie radzić bez Facebooka, a Facebook bez szkoły. Cele są inne: najczęściej chodzi o promocję placówki, czasem o lepszą komunikację z rodzicami.

W takich przypadkach zgoda na przetwarzanie danych zazwyczaj jest potrzebna. Warto jednak pamiętać, że zasady wykorzystania wizerunku reguluje nie tylko RODO, ale przede wszystkim prawo autorskie. Rodzic, który nie chce, by szkoła promowała się w Internecie zdjęciem jego uśmiechniętego dziecka, może po prostu odmówić wyrażenia zgody na takie działanie. Zgody nie można wymuszać ani uzależniać od niej np. przyjęcia do prywatnego liceum, może też być ona w każdej chwili wycofana.

Bardziej skomplikowana sytuacja pojawia się, gdy nauczyciel komunikuje się uczniami za pośrednictwem Facebooka i tylko z tego portalu można się dowiedzieć np. o odwołaniu klasówki. Uczeń, który nie korzysta z portalu społecznościowego, jest wtedy zmuszony, by oddać swoje dane Facebookowi. Ani konkretny nauczyciel, ani szkoła nie może od dzieci i rodziców wymagać korzystania z komercyjnego portalu. Dlatego dobrą praktyką jest komunikowanie się z uczniami za pośrednictwem innych kanałów (np. e-maila).

Teczka zgodna z RODO

W mediach społecznościowych roi się od anegdot o tym, jak nauczyciele mają teraz zabezpieczać dane osobowe. Pojawiają się absurdalne pomysły, takie jak zakaz przenoszenia dziennika między budynkami szkoły. Internet dobrze się bawi, ale nauczyciele naprawdę zaczynają mieć wątpliwości, czy ich teczka na sprawdziany i dziennik są „zgodne z RODO".

To prawda, na szkole i pracujących w niej nauczycielach spoczywa obowiązek zapewnienia bezpieczeństwa danych. Na szczęście tutaj przepisy RODO są bardzo elastyczne. Nie znajdziemy w nich ani jednego nakazu, do którego bezwzględnie trzeba się stosować. Dane można trzymać w papierze i w wersji elektronicznej, w ruchu i w spoczynku, w teczce i w szafie – tak długo, jak długo są bezpieczne. A konkretnie: dobrze zabezpieczone przed dostępem osób niepowołanych. Dlatego wprowadzenie zasad dostępu do zasobów szkolnych z prywatnych komputerów i ustalenie z nauczycielami tego, jak postępować z pracami klasowymi, które sprawdzają w domu, ma sens.

RODO nie wymaga procedur „na papierze": jeśli powstają, to po to, żeby działać. A więc jeśli szkoła ustala, że nauczyciel nie może korzystać z prywatnego komputera, powinna mu zapewnić służbowy. Jeśli ma nie pracować z domu, musi mieć dobre warunki do pracy w szkole. Jeśli ma szyfrować e-maile, trzeba go z tego przeszkolić i przekazać, które informacje przesyłane w e-mailach wymagają takiego standardu ochrony (bo przecież nie każda!).

Uczniowie pod okiem kamer

Mimo że zdaniem Rzecznika Praw Dziecka „nadzór sprawowany za pomocą kamer nie tylko nie sprzyja utożsamianiu się z określonymi wartościami, ale promuje konformizm i oportunizm", kamery są już zainstalowane w więk-

szości polskich szkół. Przez lata szkolny monitoring funkcjonował bez podstawy prawnej i bez zasad chroniących prawa osób monitorowanych. Dopiero RODO wymusiło zmianę prawa i zmieniło tę sytuację.

Zgodnie z obowiązującymi przepisami kamery w szkołach mogą być instalowane tylko w celu zapewnienia bezpieczeństwa uczniów i pracowników oraz w celu ochrony mienia. Dyrektor powinien skonsultować decyzję o instalacji kamer z radą pedagogiczną, radą rodziców i samorządem uczniowskim. Prezes Urzędu Ochrony Danych Osobowych podkreśla, że monitoring powinien być instalowany tylko tam, gdzie naprawdę ma sens.

PRZEZ LATA SZKOLNY MONITORING FUNKCJONOWAŁ BEZ PODSTAWY PRAWNEJ I BEZ ZASAD CHRONIĄCYCH PRAWA OSÓB MONITOROWANYCH. DOPIERO RODO WYMUSIŁO ZMIANY.

Pojawiło się też kilka twardych zakazów, których szkoła musi przestrzegać: monitoring nie może rejestrować dźwięku ani też być wykorzystywany jako narzędzie nadzoru nad pracownikami. Co do zasady kamery nie powinny obejmować sal lekcyjnych, gabinetów psychologicznych, szatni, przebieralni czy stołówki, chyba że stosowanie monitoringu w tych pomieszczeniach jest niezbędne i – jak mówią przepisy – nie naruszy godności ani innych dóbr osobistych uczniów (w szczególności jeśli zostaną zastosowane techniki uniemożliwiające rozpoznanie przebywających w pomieszczeniach osób).

Pomocna dłoń inspektora

Przez ostatnie miesiące RODO-panika zdążyła już wyhamować. Ale nie wszystkie wątpliwości zostały wyjaśnione. Warto pamiętać, że każda szkoła ma obowiązek wyznaczenia inspektora ochrony danych (IOD). Jego dane kontaktowe są przekazywane wraz ze standardową informacją o przetwarzaniu danych. W praktyce to on przygotowuje wszystkie klauzule, oświadczenia i polityki prywatności oraz odpowiada za bezpieczeństwo danych. Inspektor jest też osobą kontaktową, do której możesz – jako np. rodzic ucznia lub uczennicy – zwrócić się z prośbą o wyjaśnienia, a nawet skargą na naruszenie praw dziecka, zanim zdecydujesz się na dalsze kroki prawne.

W PRACY

Nie tak dawno media donosiły, że w 20 sklepach popularnej sieci handlowej pracownicy przez cały dzień nosili czujniki rejestrujące, jak pracują. Z kolei w szwedzkim biurze podróży zatrudnionym wszczepiono pod skórę chipy służące m.in. logowaniu do komputera i otwieraniu biurowych drzwi. Czy to wszystko jest legalne? Na co szefom pozwala kodeks pracy zmieniony w ramach dostosowywania polskich przepisów do RODO?

Praca pod kamerą

Monitoring to dziś norma w wielu miejscach pracy. Mimo że może ingerować w prywatność pracowników, przepisy do tej pory milczały na ten temat. Zgodnie z najnowszymi zmianami w prawie pracy, żeby móc zainstalować kamery, pracodawca powinien spełnić szereg warunków. Przede wszystkim monitoring musi być niezbędny do zrealizowania jednego z czterech wskazanych w przepisach celów:

- zapewnienia bezpieczeństwa pracowników,
- ochrony mienia,
- kontroli produkcji,
- zachowania tajemnicy pracodawcy.

Do tego pracodawcy nie powinni zbierać o pracownikach więcej informacji, niż to niezbędne (zgodnie ze wspominaną już zasadą minimalizacji). W praktyce oznacza to, że szef nie może zainstalować kamer, „bo to jego firma", a potem korzystać z nich wedle swego widzimisię. Wykluczone jest np. wykorzystanie nagrania podczas rozmowy okresowej. Kamery nie mogą też służyć do monitorowania wydajności pracowników ani weryfikowania godzin rozpoczęcia i zakończenia przez nich pracy.

Zanim pracodawca zainstaluje kamery, powinien o nich poinformować pracowników i czytelnie oznaczyć miejsca monitorowane. Zdaniem Prezesa Urzędu Ochrony Danych Osobowych wykluczona jest instalacja ukrytych kamer. We *Wskazówkach dotyczących wykorzysty-*

wania monitoringu wizyjnego pisze, że niejawny monitoring mogą prowadzić wyłącznie służby porządkowe i specjalne, a dla pracodawców taka praktyka oznacza ryzyko odpowiedzialności (nawet karnej!). Prezes Urzędu odradza także stosowanie atrap kamer, które wywołują poczucie ingerencji w prywatność, a jednocześnie nie spełniają swojej roli.

ZANIM PRACODAWCA ZAINSTALUJE KAMERY, POWINIEN O NICH POINFORMOWAĆ PRACOWNIKÓW I CZYTELNIE OZNACZYĆ MIEJSCA MONI-TOROWANE.

Kodeks pracy jednoznacznie wskazuje miejsca, w których monitoring jest niedopuszczalny. Chodzi nie tylko o toalety, ale także o palarnie, szatnie czy pomieszczenia udostępnione związkom zawodowym. Kamera nie może również zaglądać pracownikom do talerza – do miejsc zakazanych zaliczono bowiem stołówki.

Niestety, od zakazu instalacji kamer możliwe są wyjątki. Jeśli pracodawca uzna, że kamera jest niezbędna np. do ochrony mienia, a jednocześnie zastosuje urządzenie uniemożliwiające rozpoznanie nagranego, monitoring staje się legalny. Tyle że rozmazanie twarzy osoby korzystającej z WC to zdecydowanie za mało, żeby chronić jej tożsamość – zwłaszcza jeśli kamery na wiodącym do toalety korytarzu działają w wysokiej rozdzielczości i doskonale wiadomo, kto w danym momencie znajdował się w środku.

Mail (nie)prywatny

Od lat na rynku dostępne są programy automatycznie skanujące treści maili wysyłanych ze służbowych skrzynek. Jak twierdzi firma doradcza Deloitte, możliwe jest nawet określenie nastroju pracowników na podstawie pisanych przez nich wiadomości.

Nowe przepisy dopuszczają kontrolę służbowej poczty elektronicznej, o ile jest to niezbędne do:

- zapewnienia dobrej organizacji pracy (pełne wykorzystanie czasu pracy),
- właściwego użytkowania udostępnionego pracownikom sprzętu.

Kontrola poczty elektronicznej odbywa się na tych samych zasadach, co stosowanie monitoringu, pracownicy powinni więc zostać o niej poin-

formowani. Zasada minimalizacji każe np. rozważyć, czy w firmie, w której komunikacja mailowa jest rzadkością, kontrola korespondencji elektronicznej faktycznie jest niezbędna do zapewnienia dobrej organizacji pracy.

A co z prywatnymi e-mailami? Najlepiej nie wysyłać ich ze służbowej skrzynki. Jeśli jednak to się zdarzy (mimo bardzo często wprowadzanego przez pracodawców zakazu), to teoretycznie i tak szef – zorientowawszy się, że czyta o prywatnych sprawach – powinien natychmiast przerwać. Przepisy dopuszczają bowiem kontrolę skrzynki mailowej, ale w taki sposób, by nie naruszało to tajemnicy korespondencji.

PRZEPISY DOPUSZCZAJĄ KONTROLĘ SKRZYNKI MAILOWEJ, ALE W TAKI SPOSÓB, BY NIE NARUSZAŁO TO TAJEMNICY KORESPONDENCJI.

...i inne

Co zatem ze wszystkimi cyfrowymi szpiegami, których sprzedawcy pukają do drzwi pracodawców? Nowe przepisy wprowadzają furtkę do stosowania innych narzędzi niż kamery i monitoring poczty elektronicznej. Ale furtka ta nie jest zbyt szeroko otwarta: takie działania, jak monitoring GPS samochodów służbowych czy kontrola aktywności pracowników w Internecie, mogą być stosowane wyłącznie na tych samych zasadach co kontrola e-maili, a więc po wcześniejszym poinformowaniu pracowników i wyłącznie w dwóch celach: do zapewnienia dobrej organizacji pracy i właściwego użytkowania udostępnionego pracownikom sprzętu.

Kluczowe znaczenie ma znów zasada minimalizacji. Monitorowanie lokalizacji samochodów służbowych może być konieczne do zapewnienia ich właściwego użytkowania, trudno sobie natomiast wyobrazić firmę, w której dla dobrej organizacji pracy niezbędne jest śledzenie ruchu gałek ocznych pracowników.

Pracodawcy, zamiast ściśle monitorować aktywność pracowników, mogą stosować rozwiązania niewiążące się ze zbieraniem informacji na ich temat, np. blokować możliwość wejścia na konkretne strony internetowe ze służbowych komputerów – blokowanie portali społecznościowych jest dzisiaj powszechne. Jakkolwiek przepisy zostawiają tutaj pracodawcom pełną swobodę, to i te praktyki bywają kontrowersyjne (np. Ministerstwo

Finansów utrudniało pracownikom wejścia na strony internetowe związków zawodowych).

Nowe wyzwania

Jeśli pracujesz na podstawie umowy cywilnoprawnej (np. umowy o dzieło czy umowy zlecenia), nowe przepisy Kodeksu pracy Cię nie chronią. Nie oznacza to jednak, że jesteś bezradny/-a – skoro mówimy o zbieraniu danych osobowych, zastosowanie znajdzie RODO, które każdemu (bez względu na to, czy jest pracownikiem, czy nie) przyznaje m.in. prawo dostępu do zebranych na jego temat danych osobowych czy prawo do żądania usunięcia danych przetwarzanych nielegalnie. Z RODO wynika też obowiązek informowania o zbieraniu danych osobowych oraz ograniczenie, że strony umowy cywilnoprawnej mogą zbierać o sobie tylko tyle danych, ile jest niezbędne.

Nowe przepisy obowiązują od kilku miesięcy, więc dopiero okaże się, jak będą działały w praktyce i czy odpowiedzą na wyzwania związane będą ze stosowaniem nowych technologii w miejscu pracy. To zależy zarówno od postawy pracodawców, jak i gotowości pracowników do walki o swoje prawa. Jeśli podejrzewasz, że pracodawca je łamie, możesz zwrócić się do związków zawodowych, inspekcji pracy, ale przede wszystkim – do Urzędu Ochrony Danych Osobowych (w dalszej części tłumaczymy, jak to zrobić).

W SKLEPIE

Robiąc zakupy przez Internet, trudno uniknąć podawania swoich danych: buty zamawiasz pod konkretny adres, wpisujesz e-mail, aby dostać potwierdzenie, a płatność przelewem ujawnia Twój numer konta. To jest jasne. Dlaczego więc sklep prosi o wyrażenie pięciu zgód, a skrzynkę mailową regularnie zaśmiecają irytujące oferty? Co na to RODO?

Jakich danych potrzebuje sklep?

Sklepy stacjonarne są ze swojej istoty najmniej „danożerne": żeby kupić bułki, nie trzeba przecież podawać imienia i nazwiska. To jednak nie oznacza, że takie sklepy nigdy nie zbierają danych osobowych – wystarczy, że w środku zainstalowane są kamery, że zapłacisz kartą albo dołączysz do programu lojalnościowego.

W sklepach internetowych sytuacja wygląda inaczej. Kiedy przeglądasz stronę internetową, sklep za pomocą różnych technologii śledzących, np. ciasteczek, zbiera informacje o tym, jak niej korzystasz: np. które kategorie produktów najchętniej oglądasz, jak dużo czasu spędzasz na stronie, które produkty rzeczywiście kupujesz, a które wyrzucasz z koszyka w ostatnim momencie.

Normą jest też to, że sklep internetowy pyta o imię i nazwisko, adres oraz e-mail, na który wysyła potwierdzenie zamówienia. Podawanie tych wszystkich danych ma sens przy zamówieniach z dostawą do domu. Jednak w przypadku odbioru osobistego lub odbioru zamówienia w wybranym punkcie, np. paczkomacie, konieczność podania adresu zamieszkania może budzić wątpliwości. Dlaczego? Jedną z podstawowych zasad, którą powinny się kierować wszystkie firmy i instytucje, jest zasada minimalizacji. W przypadku sklepu oznacza ona, że powinien prosić tylko o takie dane, które są niezbędne do osiągnięcia konkretnego celu, w tym przypadku dostarczenia zamówionych produktów.

Uwaga na zgodę

Każdy podmiot, który przetwarza dane, musi mieć do tego odpowiednią podstawę prawną. W przypadku takich danych, jak imię i nazwisko, e-mail czy adres dostawy, sklep nie musi pytać o zgodę, bo są one konieczne do zawarcia umowy i realizacji zamówienia.

W praktyce zdarza się jednak, że niektóre sklepy do złożenia zamówienia wymagają zgody. Warto pamiętać, że zgoda, która „musi" być wyrażona, jest z gruntu podejrzana. Jeśli dotyczy danych, o których piszemy wyżej, najczęściej stanowi wyraz błędnej interpretacji prawa i jest zupełnie niepotrzebna. Ale możliwe jest też, że w ten sposób sklep próbuje wymusić zgodę np. na przekazywanie danych innym firmom.

SKLEPY STACJONARNE SĄ ZE SWOJEJ ISTOTY NAJMNIEJ „DANOŻERNE": ŻEBY KUPIĆ BUŁKI, NIE TRZEBA PRZECIEŻ PODAWAĆ IMIENIA I NAZWISKA. TO JEDNAK NIE OZNACZA, ŻE TAKIE SKLEPY NIGDY NIE ZBIERAJĄ DANYCH OSOBOWYCH.

W niektórych okolicznościach sklep powinien jednak o zgodę zapytać. Chodzi o przypadki, gdy chce skorzystać z danych osobowych do celów niezwiązanych z obsługą zamówienia. Nie musi pytać o zgodę na przekazanie danych kurierowi (dostawa jest elementem realizacji zamówienia), ale na wysyłanie ofert przez firmy trzecie: już tak. Taka zgoda musi być dobrowolna, jednoznaczna i świadoma. Domyślnie zaznaczone okienka-pułapki na osoby, które ich nie zauważą, jak i okienka, których w ogóle nie można odznaczyć, są nielegalne. Niezgodne z prawem jest także połączenie kilku zgód na różne cele wykorzystywania danych – np. na marketing firm trzecich i wzięcie udziału w konkursie.

Na gruncie RODO sklep nie musi pytać o zgodę na wykorzystywanie danych w celu przesyłania informacji o innych oferowanych produktach, bo może to robić w oparciu o tzw. uzasadniony interes. O co więc chodzi w zgodach na „przesyłanie informacji handlowych drogą elektroniczną" i na „wykorzystywanie urządzeń końcowych dla celów marketingu bezpośredniego"? Te zgody nie mają z RODO nic wspólnego, a obowiązek ich zebrania nakładają na sklep inne ustawy – o świadczeniu usług drogą elektroniczną i prawo telekomunikacyjne.

Newslettery i uporczywe oferty

Sklepy często zachęcają do zapisu na newsletter, w zamian oferując np. 10% zniżki na pierwsze zamówienie. Mogą też co jakiś czas rekomendować inne produkty na podstawie dotychczasowych zamówień. Bywa jednak tak, że sklep bombarduje ofertami co drugi dzień. Jeśli nie chcesz całkowicie rezygnować z takich mailingów, ale pragniesz odchudzić skrzynkę, z której korzystasz na co dzień, polecamy Ci tworzyć specjalne maile przeznaczone tylko do tego typu korespondencji. Z kolei aliasy, czyli alternatywne nazwy dla Twojego adresu e-mail przypisane do tej samej skrzynki pocztowej, mogą pomóc Ci zidentyfikować firmę, w której doszło do wycieku lub która wykorzystuje Twoje dane niezgodnie z prawem (np. gdy nagle zaczynasz dostawać dużo spamu).

Jeśli nie chcesz otrzymywać żadnych e-maili z ofertami, możesz z nich w każdej chwili zrezygnować bez podawania przyczyny. W przypadku newslettera w stopce powinien znajdować się link rezygnacji z subskrypcji: wystarczy go kliknąć i po sprawie. W sytuacjach, gdy sklep wysyła Ci rekomendacje w oparciu o poprzednie zamówienia, możesz zgłosić sprzeciw (patrz rozdział *Użyj RODO, czyli lekcje samoobrony*).

Karty lojalnościowe: kopalnia wiedzy

Kilka lat temu świat obiegła informacja, że amerykański sklep Target wysłał nastolatce oferty pieluszek i ubranek dziecięcych, jeszcze zanim o ciąży dowiedzieli się jej rodzice. Jak to możliwe? Amerykańskiej sieciówce udało się to ustalić w oparciu o dane o zakupach powiązanych z kartą lojalnościową. W wysnuwaniu wniosków na temat zakupów pomogła analiza statystyczna: np. Target zaobserwował, że kupowanie dużych ilości bezzapachowego balsamu jest charakterystyczne dla kobiet rozpoczynających drugi trymestr ciąży.

Klienci, którzy decydują się na kartę lojalnościową, mają do czynienia z transakcją wiązaną. Dostają zniżki i nagrody, a sklep – ich dane i informacje o nawykach zakupowych, które starannie analizuje na potrzeby swojego własnego marketingu (jak pokazuje przykład nastolatki w ciąży) lub którymi dzieli się z innymi firmami.

To, o jakie dane sklep może Cię poprosić przy zakładaniu karty lojalnościowej, jest podyktowane ogólnymi zasadami wynikającymi z RODO, w tym przede wszystkim wspomnianą już zasadą minimalizacji. Kilka lat temu klienci Biedronki, którzy chcieli dołączyć do jej programu lojalnościo-

wego, musieli podać oprócz imienia i numeru telefonu także adres zamieszkania. Biedronka wycofała się ze zbierania tego ostatniego w odpowiedzi na zarzuty naruszenia właśnie zasady minimalizacji. Niektóre sklepy mają jednak jeszcze bardziej rozbudowane formularze, które wymagają podania np. daty urodzenia. Jeśli sklep nie wyjaśnia, dlaczego te informacje są niezbędne do uczestnictwa w programie (lub to wyjaśnienie budzi Twoje wątpliwości), daj mu o tym znać. Niestety w praktyce bywa tak, że sklep nie ma ochoty zmienić swoich praktyk i stawia sprawę jasno: jeśli nie podzielisz się danymi, nie dostaniesz karty. Dlatego zastanów się dwa razy, czy udział w programie jest na pewno tego warty – albo zgłoś nadużycie do Prezesa UODO (w dalszej części podpowiadamy, jak to zrobić).

KLIENCI, KTÓRZY DECYDUJĄ SIĘ NA KARTĘ LOJALNOŚCIOWĄ, MAJĄ DO CZYNIENIA Z TRANSAKCJĄ WIĄZANĄ. DOSTAJĄ ZNIŻKI I NAGRODY, A SKLEP — ICH DANE I INFORMACJE O NAWYKACH ZAKUPOWYCH.

Usuwanie zbędnych danych

Prawo do bycia zapomnianym przez sklep nie zadziała w każdej sytuacji. Możesz „wypisać się" ze sklepu wtedy, gdy Twoje dane przestaną być potrzebne do realizacji celu, w którym sklep je zebrał. Czy zatem jeśli przesyłka już do Ciebie dotarła, to możesz poprosić sklep o skasowanie Twojego imienia i nazwiska, adresu i numeru konta? Niekoniecznie. Sklep może odmówić, powołując się na to, że dane mogą być mu nadal potrzebne choćby do rozpatrzenia Twojej reklamacji (masz na nią zgodnie z prawem 2 lata). Ustawa o rachunkowości natomiast nakłada na sklepy obowiązek przechowywania dokumentacji przez 5 lat.

Po upływie tego okresu sklep z własnej inicjatywy powinien usunąć dane (zgodnie z tzw. zasadą ograniczenia przechowywania danych). Jeśli z jakiegoś powodu zaniedba ten obowiązek, musi usunąć dane na Twoje żądanie. Wbrew praktykom niektórych sklepów nie powinno to oznaczać jedynie wypisania Cię z newslettera, lecz trwałe i nieodwracalne skasowanie danych.

Jeśli ciekawi Cię, jak RODO działa w praktyce, relacje ze sklepami umożliwiają przetestowanie niemal wszystkich przysługujących Ci praw (omawiamy je w dalszej części).

W KOŚCIELE

Kiedy w maju przez Polskę przeszła burza związana z RODO, jedna instytucja zachowała stoicki spokój: Kościół rzymskokatolicki. Jak Kościół poradził sobie z wprowadzeniem przepisów o ochronie danych, które do niedawna dotyczyły go jedynie w ograniczonym stopniu? Czy po wejściu w życie RODO prywatność wiernych jest lepiej chroniona?

Między RODO a dekretem

W nowych przepisach o ochronie danych przewidziano wyjątek dla kościołów i związków wyznaniowych – mogą one stosować własne zasady przetwarzania danych, o ile obowiązywały one w chwili uchwalenia RODO (czyli 27 kwietnia 2016 r.) i zostały dostosowane do nowych przepisów. Z tej furtki skorzystał Kościół rzymskokatolicki, wydając obowiązujący od 30 kwietnia 2018 r. dekret ogólny w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych.

Dekret w znacznej części stanowi „kopiuj-wklej" z RODO (m.in. powtarza zasady przetwarzania danych), dlatego w podstawowym zakresie ochrona danych w Kościele powinna wyglądać podobnie jak poza nim. Diabeł jak zwykle tkwi jednak w szczegółach. Z jednej strony nie jest wcale jasne, czy obowiązujące w polskim Kościele zasady ochrony danych były na tyle szczegółowe, by można było zastosować przewidziany w RODO wyjątek. Z drugiej – dekret pozwala kościelnym podmiotom na więcej niż RODO świeckim, ograniczając sankcje za łamanie prawa.

Prawo do informacji

W zakresie prawa do informacji prawo kościelne – przynajmniej w teorii – nie ustępuje świeckiemu. Administratorzy danych osobowych mają obowiązek informować osoby, których dane przetwarzają, m.in. o tym, w jakim celu to robią, na jakiej podstawie, jak długo oraz jakie prawa im

przysługują. Dotyczy to np. parafii, działających na podstawie kościelnego dekretu. Niektóre z nich realizują obowiązek informacyjny wprost z ambony, inne wywieszają klauzule o przetwarzaniu danych w przykościelnych gablotach. Odpowiednia informacja powinna też trafić do osób, które zgłaszają się do parafii przy różnych okazjach, np. ślubu czy chrztu.

PARAFIE MOGĄ PUBLIKOWAĆ LISTY OFIARODAWCÓW W SWOICH GAZETKACH, NA STRONACH INTERNETOWYCH I WYCZYTYWAĆ Z AMBONY – I TO BEZ ICH ZGODY.

Czy i jak to działa w praktyce, każdy wierny może się przekonać w swojej parafii. Może też skorzystać z prawa do uzyskania kopii danych (najlepiej zwrócić się do parafii chrztu, bo tam trafiają informacje o późniejszych sakramentach, nawet jeśli udzielono ich w innym miejscu).

Lista ofiarodawców nadal publiczna

Jedno z najbardziej kontrowersyjnych rozwiązań przewidzianych dekretem pozwala na ujawnianie listy ofiarodawców wraz z przekazanymi przez nich kwotami. Parafie mogą je publikować w swoich gazetkach, na stronie internetowej czy wyczytywać z ambony – i to bez zgody ofiarodawców. Osoby, które nie życzą sobie upubliczniania informacji o swojej ofiarności, muszą o tym poinformować. To odwrócenie jednej z najważniejszych zasad RODO, według którego rozwiązania chroniące prywatność powinny być stosowane domyślnie (*privacy by default*).

Ograniczone prawo do bycia zapomnianym

Z największą nadzieją na nowe zasady ochrony danych w Kościele oczekiwali ci, którzy próbują z niego wystąpić i zniknąć z jego archiwów. Do parafii zgłaszają się osoby, które żądają usunięcia swoich danych z ksiąg parafialnych, powołując się na RODO. Wygląda jednak na to, że w sytuacji apostatów niewiele się zmieni, bo Kościół uważa, że jego członkiem zostaje się na zawsze, a informacje o sakramentach są niewymazywalne – i dlatego odmawia tutaj prawa do zapomnienia. Dekret przyznaje apostatom jedynie prawo do ograniczenia przetwarzania danych: te pozostają w księgach tylko w celach archiwalnych i do ustalenia stanu kanonicznego, czyli

pozyskania informacji o przyjętych sakramentach (chyba że biskup wyrazi zgodę na wykorzystanie ich w innym celu).

Kościół w Internecie

Kamera na terenie parafii, arkusze kalkulacyjne z wpłatami na jej rzecz, transmisja mszy na YouTubie, zdjęcia parafian na profilach społecznościowych – nowoczesny Kościół nie stroni od technologii. W środowisku cyfrowym ochrona prywatności napotyka zgoła inne wyzwania, niż ma to miejsce w przypadku spisywanych piórem ksiąg parafialnych. To ważne, zwłaszcza w kontekście ochrony wizerunku. Dekret pozwala na przykład na zamieszczanie zdjęć parafian na Facebooku, ale prawo autorskie, poza ściśle określonymi wyjątkami, wymaga uzyskania zgody na publikację od osoby, która widnieje na zdjęciu.

W SYTUACJI APOSTATÓW NIEWIELE SIĘ ZMIENI, BO KOŚCIÓŁ UWAŻA, ŻE JEGO CZŁONKIEM ZOSTAJE SIĘ NA ZAWSZE, A INFORMACJE O SAKRAMENTACH SĄ NIEWYMAZYWALNE.

Kto pomoże wiernym?

Co możesz zrobić, jeśli uważasz, że Twoje prawa zostały naruszone? Jeśli na przykład na otrzymanym z Kościoła zaświadczeniu o bierzmowaniu znajdzie się informację o przynależności do partii i wypowiedziach przeciwko księżom (taka sytuacja spotkała młodego polityka z Pułtuska)? Albo gdy informacje o rodzinie adopcyjnej bez jej wiedzy i zgody zostaną udostępnione rodzinie biologicznej (jak w sprawie, w której do Episkopatu występowała Helsińska Fundacja Praw Człowieka)?

Według kościelnego dekretu możesz zwrócić się ze skargą do powołanego nim Kościelnego Inspektora Ochrony Danych. Jak będzie działał w praktyce, dopiero się przekonamy. Jednak pozycja KIOD jest zupełnie inna niż Prezesa Urzędu Ochrony Danych Osobowych. Ten ostatni musi przestrzegać przewidzianych w przepisach terminów rozpatrywania skarg i dysponuje realnymi karami, w tym finansowymi. W kościelnym dekrecie nie ma słowa o terminach, a KIOD dysponuje specyficznym wachlarzem kar (od nakazania naprawienia szkody przez nałożenie cenzury po pozbawienie urzędu). Od postanowienia KIOD można odwołać się tylko do Watykanu.

Jak na razie furtka do prawa świeckiego pojawia się jedynie w tych sytuacjach, w których Kościół wykracza poza istotę swojej działalności, np. gdy działalność kościelnych mediów podpada pod przepisy ogólne. Są jednak sytuacje, w których trudno powiedzieć, czy to jeszcze działalność Kościoła, czy już nie. Na przykład: czy kamery zamontowane w kościele mają funkcjonować zgodnie z RODO, czy z dekretem? Albo co z danymi przetwarzanymi przez pielgrzymkowe biuro podróży? Na odpowiedź trzeba poczekać do rozstrzygnięcia przez Prezesa UODO (a ostatecznie: sądy administracyjne), bo jeszcze może się okazać, że kościelny dekret w ogóle nie obowiązuje.

UŻYJ RODO, CZYLI LEKCJE SAMOOBRONY

Uważasz, że szpital lub pracodawca narusza Twoje prawo do prywatności? Do Twojej skrzynki po raz setny trafiła oferta sklepu, który nie wiadomo skąd ma Twój adres? Telemarketer znowu Cię zirytował napastliwym telefonem? A może zamierzasz starać się o kredyt i zastanawiasz się, jak wygląda Twój profil z perspektywy banku? Nad danymi, które już raz się od Ciebie odkleiły, trudno jest zapanować. Jednak sam fakt, że one „gdzieś tam krążą", jeszcze nie oznacza, że nic w tej sprawie nie możesz zrobić. Wręcz przeciwnie! RODO daje Ci konkretne uprawnienia, po które możesz sięgnąć, żeby odzyskać kontrolę nad swoimi danymi.

Nie damy Ci jednego przycisku, który załatwia wszystko. Zamiast tego przygotowaliśmy zbiór prostych instrukcji, które krok po kroku przeprowadzą Cię przez cały proces. Na naszej stronie znajdziesz też wzory wniosków, które możesz wypełnić i wysłać do administratora swoich danych (panoptykon.org/rodo-na-tacy-V).

1. SPRAWDŹ, JAK SIĘ MAJĄ TWOJE DANE

Twoje dane to Twoja sprawa. Ci, którzy mają do nich dostęp, są w stanie wpływać na Twoje decyzje (np. poprzez reklamę lub ofertę wykorzystującą Twoje słabości), zmieniać sposób, w jaki patrzysz na świat (np. poprzez odpowiednio sprofilowane treści w Internecie), a nawet postawić Cię w trudnym położeniu (np. podnosząc stawkę ubezpieczenia czy kwestionując Twoją wiarygodność kredytową). To niebezpieczne, jeśli jedna strona (firma, instytucja) wie dużo, a druga (klient, petent) – nawet nie zdaje sobie z tego sprawy. Dlatego dostęp do informacji o przetwarzanych danych to podstawa.

Masz prawo wymagać przejrzystości od wszystkich, którzy mają do czynienia z Twoimi danymi. Nie ma znaczenia, kiedy, w jakim celu i na jakiej podstawie te dane pozyskali: zawsze możesz do nich zapukać i zażądać

wyłożenia kart na stół. Takie żądanie może się odbić od ściany w przypadku organów, które działają w sposób tajny: Policji czy ABW, ale w sektorze prywatnym i w relacji z administracją publiczną powinno zadziałać.

TO NIEBEZPIECZNE, JEŚLI JEDNA STRONA (FIRMA, INSTYTUCJA) WIE DUŻO, A DRUGA (KLIENT, PETENT) – NAWET NIE ZDAJE SOBIE Z TEGO SPRAWY. DLATEGO DOSTĘP DO INFORMACJI O PRZETWARZANYCH DANYCH TO PODSTAWA.

Czasem o tym, że ktoś przetwarza Twoje dane, dowiadujesz się dopiero w bezpośrednim kontakcie (klasyczna sytuacja z telemarketerem dzwoniącym na Twój numer telefonu, do tego zwracającym się do Ciebie po imieniu...). Czasem możesz się tego tylko domyślać (np. kiedy na odwiedzanej przez Ciebie stronie internetowej wyświetla się zaskakująco trafnie spersonalizowana reklama). Możesz też z dużą dozą pewności założyć, że Twoje dane ma każda firma i instytucja, z którą wcześniej zdarzyło Ci się mieć do czynienia, choćby przelotnie. Nie namawiamy do tego, żeby odtwarzać pełną historię swoich zakupów, podróży i wizyt lekarskich. Ale jeśli intryguje Cię, jaki ślad pozostał po Tobie w prywatnej przychodni, korporacji taksówkarskiej czy sklepie internetowym – możesz to łatwo sprawdzić.

Jak to zrobić?

Zażądanie informacji o przetwarzanych danych nie jest trudne. Oto parę praktycznych wskazówek na początek:

- możesz złożyć takie żądanie w dowolnej formie (list, e-mail, formularz online etc.);
- adresat ma miesiąc na reakcję: w tym czasie powinien spełnić Twoje żądanie, odmówić albo poinformować Cię o przedłużeniu realizacji żądania ze względu na skomplikowany charakter sprawy;
- sposób udostępnienia informacji powinien być dopasowany do Twoich potrzeb (np. jeśli pytanie zostało wysłane mailem, odpowiedź też powinna wrócić drogą elektroniczną).

Firma/instytucja, do której kierujesz swoje żądanie, musi wiedzieć, że „Ty to Ty", a więc że dane, o które pytasz, rzeczywiście dotyczą Ciebie. Ale to nie oznacza, że do każdego takiego wniosku trzeba dołączyć skan dowodu osobistego. Żeby uwiarygodnić swoje żądanie, możesz wykorzystać każdą informację, która identyfikuje Cię w tej konkretnej relacji. Na przykład: jeśli pytasz o dane przetwarzane w sklepie internetowym, wyślij wiadomość z pytaniem z adresu e-mail użytego do założenia konta albo złożenia zamówienia. Jeśli administrator nadal ma uzasadnione wątpliwości, sam powinien zaproponować sposób zweryfikowania Twojej tożsamości.

Czego konkretnie możesz się dowiedzieć?

Możesz dowiedzieć się:

- w jakim celu i na jakiej podstawie Twoje dane są przetwarzane (np. że sklep internetowy uznał, że kiedyś zrobione zakupy dają mu prawo przetwarzać Twoje dane także w celach marketingowych);
- komu Twoje dane są przekazywane (np. że dane o Twojej lokalizacji zbierane przez aplikację mobilną są przekazywane takim firmom jak Selectivv i że dzieje się to za Twoją „zgodą", udzieloną przy okazji akceptowania polityki prywatności);
- jak to się stało, że Twoje dane znalazły się tym miejscu (np. że Twój adres trafił do bazy telemarketingowej od operatora, z którym już dawno nie masz umowy);
- jak długo Twoje dane są przechowywane i dlaczego tak długo (np. że sklep czy portal internetowy planuje je trzymać jeszcze przez trzy lata po rozwiązaniu umowy ze względu na możliwe roszczenia);
- jakie masz w związku z tym uprawnienia (np. że możesz zażądać usunięcia lub sprostowania danych).

Co dalej? Masz kilka możliwości

W zależności od tego, jakie (i jak silne) emocje wzbudziła w Tobie informacja uzyskana w pierwszym kroku (kto, po co i na jakiej podstawie przetwarza Twoje dane, skąd je pozyskał, komu przekazuje i jak długo trzyma), masz kilka możliwości.

2. ODZYSKAJ SWOJE DANE

Jeśli udało Ci się ustalić, że konkretna firma/instytucja przetwarza Twoje dane, możesz pójść krok dalej i skorzystać z innych praw, jakie daje Ci RODO. W miarę możliwości administrator powinien udostępnić bezpieczny system, w którym (po zalogowaniu) każdy może sam przeglądać i weryfikować swoje dane, a – w razie potrzeby – również je pobierać. W przypadku braku takiego ułatwienia, możesz zrealizować swoje prawa za pomocą prostych wniosków.

Uzyskanie kopii danych

Trudno w to uwierzyć, ale przed RODO możliwość uzyskania kopii danych wcale nie była oczywista. Zgodnie z polskim prawem można było się dowiedzieć, jakie kategorie (rodzaje) danych ktoś przetwarza na nasz temat, ale już niewiele więcej. Teraz jest inaczej. Bez względu na rodzaj przetwarzanych danych – czyli na to, czy w grę wchodzą wiadomości tekstowe, nagrania rozmów, czy metadane – masz prawo dostać ich kopię na własny użytek.

PRZED RODO MOŻLIWOŚĆ UZYSKANIA KOPII DANYCH WCALE NIE BYŁA OCZYWISTA. MOŻNA BYŁO SIĘ DOWIEDZIEĆ, JAKIE KATEGORIE DANYCH KTOŚ PRZETWARZA, ALE JUŻ NIEWIELE WIĘCEJ. TERAZ JEST INACZEJ.

Co Ci daje uzyskanie kopii danych? Przede wszystkim pełny wgląd w to, co na Twój temat zostało zgromadzone w danej bazie. Jeśli w grę wchodzą tylko podstawowe informacje, takie jak e-mail, numer telefonu czy adres, żądanie przekazania ich kopii to trochę zawracanie głowy. Ale kiedy mowa o historii, jaką za sobą zostawiasz w banku, wyszukiwarce internetowej czy na portalu społecznościowym, warto podjąć ten wysiłek. Możesz się przekonać, że tego typu podmioty mają lepszą pamięć Twojego cyfrowego życia niż Ty...

O ile nie zażądasz odpowiedzi w innej formie, administrator powinien Ci przekazać kopię Twoich danych drogą elektroniczną. Za jej przygotowanie i przesłanie nie ma prawa pobrać opłaty, jeśli to jest pierwsze takie żądanie z Twojej strony. Przy kolejnych tego typu prośbach może zacząć pobierać opłaty, ale tylko w rozsądnej wysokości wynikającej z kosztów, jakie sam ponosi.

Przeniesienie danych w ustrukturyzowanym formacie

Prawo do przeniesienia danych to tak naprawdę modyfikacja poprzedniego kroku, polegająca na tym, że dostajesz kopię swoich danych w ustrukturyzowanym, powszechnie używanym formacie. Dzięki temu mogą być one od razu przekazane do bazy innej firmy (uwaga: ta możliwość nie dotyczy organów publicznych). Nie musi się to wiązać z zakończeniem istniejącej relacji – możesz zażądać przeniesienia swoich danych, nie wymagając jednocześnie ich usunięcia u źródła (np. jeśli występujesz o kredyt w kilku bankach i nie chcesz wypełniać kilka razy tej samej dokumentacji).

Przygotowanie Twoich danych do przeniesienia wymaga nieco więcej nakładów i wysiłku po stronie administratora, dlatego nie zawsze możesz się tego domagać.

Masz prawo zażądać przeniesienia Twoich danych, jeśli są spełnione dwa warunki:

- są one przetwarzane w sposób zautomatyzowany;
- są to dane dostarczone bezpośrednio przez Ciebie: albo z Twojej inicjatywy (w oparciu o udzieloną zgodę), albo na podstawie umowy (dane niezbędne do realizacji umowy).

Pierwszy warunek w dzisiejszych czasach spełnia już prawie każda firma (odmówić mogłaby Ci tylko taka, która nie korzysta z systemów informatycznych). Natomiast ten drugi w praktyce może rodzić więcej problemów: czy chodzi tylko o dane, które własnoręcznie wprowadzasz do systemu (np. wypełniając formularz internetowy), czy też o te, które generujesz, korzystając z danej usługi (np. historia transakcji bankowych, zakupów online czy konwersacji na portalu społecznościowym)? Na szczęście wytyczne dotyczące stosowania RODO (przyjęte przez Grupę Roboczą Artykułu 29) promują szerszą interpretację prawa do przenoszenia danych i objęcie nim również wygenerowanych danych.

3. POWIEDZ „DOŚĆ!”

Jeśli nie podoba Ci się to, w jaki sposób Twoje dane zostały pozyskane lub są przetwarzane (np. nie przypominasz sobie udzielenia zgody, na którą powołuje się administrator, albo uważasz, że dane nie są już potrzebne do celu, w którym zostały zebrane), możesz wziąć sprawy w swoje ręce i powiedzieć „dość!”. Nie zawsze wystarczy po prostu zażądać natychmiastowego usunięcia swoich danych, żeby osiągnąć pożądany efekt.

Może się okazać, że administrator ma zgodne z prawem powody, żeby Twoje dane przetwarzać, albo że na ich usunięcie musisz jeszcze chwilę poczekać. Warto jednak próbować, choćby po to, żeby się przekonać, jak to wszystko działa.

Sprzeciw wobec przetwarzania danych

Typową sytuacją, w której możesz zgłosić sprzeciw, jest przetwarzanie Twoich danych w celach marketingowych. Za tym celem mogą się kryć rozmaite praktyki o różnym stopniu ingerencji w prywatność: od okazjonalnej wysyłki reklamowego mailingu na Twój adres, przez zbieranie okruchów Twoich danych z różnych źródeł i tworzenie spójnego profilu, po monitorowanie Twojej lokalizacji i analizowanie historii transakcji. Każdy może gdzie indziej wytyczać swoją osobistą granicę, za którą zaczyna się naruszenie prywatności. Ale dzięki RODO każdy może zgłosić sprzeciw, jeśli poczuje, że to jest ten moment.

ZGODNIE Z RODO WYCOFANIE ZGODY POWINNO BYĆ RÓWNIE PROSTE JAK JEJ UDZIELENIE.

Jeśli już wiesz, że konkretna firma przetwarza Twoje dane po to, żeby się skuteczniej reklamować i oferować Ci kolejne produkty/usługi, a Ty nie masz ochoty na taką komunikację (bo jest irytująca, zajmuje czas albo po prostu nie trafia w Twoje potrzeby), wystarczy, że powiesz „nie, dziękuję". Takiego sprzeciwu nie musisz uzasadniać. Możesz go też zgłosić w dowolnej formie. Co więcej: administrator powinien wyjść Ci naprzeciw i zachować maksymalną elastyczność (nie może np. wymagać, żeby sprzeciw został złożony na specjalnym formularzu albo w jego siedzibie).

Prawo wniesienia sprzeciwu komplikuje się, jeśli powodem przetwarzania Twoich danych są inne cele niż marketing. Twoje dane mogą być przetwarzane przez firmę w innym uzasadnionym interesie (np. po to, żeby ulepszać działanie serwisu, przeciwdziałać awariom albo prowadzić statystyki strony), a nawet w interesie publicznym (np. żeby monitorować, czy nie wrzucasz na portal społecznościowy nielegalnych treści). Jeśli taki cel Cię nie przekonuje i nadal chcesz się sprzeciwić, możesz to zrobić, ale musisz wykazać swoją „szczególną sytuację". Sprowadza się to do wykazania, że względy, na które powołuje się administrator, nie są na tyle ważne, żeby uzasadnić ograniczenie Twojego prawa do prywatności. Akurat w tym zakresie przepisy RODO nie są precyzyjne i będą działać na

korzyść przetwarzających dane – więc tę ścieżkę polecamy tylko mocno zdeterminowanym.

Wycofanie wcześniej udzielonej zgody

Jeśli po wykonaniu pierwszego kroku wiesz już, że firma/instytucja wykorzystuje Twoje dane na podstawie udzielonej w przeszłości zgody, pamiętaj, że zawsze możesz ją wycofać. To Twoje bezwzględne prawo, a obowiązkiem administratora jest Ci ułatwić skorzystanie z niego. Zgodnie z RODO wycofanie zgody powinno być równie proste jak jej udzielenie. A więc jeśli zgoda na przetwarzanie danych została wyrażona jednym kliknięciem w formularzu, który był dobrze wyeksponowany na stronie internetowej, do wycofania zgody też powinno wystarczyć jedno kliknięcie w analogicznym miejscu.

Swojej decyzji nie musisz uzasadniać. Od tego momentu administrator nie może już powoływać się na zgodę jako podstawę przetwarzania Twoich danych. Jeśli więc zgoda obejmowała udostępnienie Twojej lokalizacji, a nawet przekazywanie jej innym firmom w celach marketingowych, po wycofaniu zgody administrator powinien takie dane usunąć i zażądać tego samego od firm, którym je przekazał.

Żądanie usunięcia danych

Wiesz już, jakie dane na Twój temat są przetwarzane? A może nawet udało Ci się uzyskać ich kopię? Jeśli zakres tych informacji dał Ci do myślenia i uważasz, że jest tego wszystkiego za dużo, albo nie widzisz podstawy do dalszego przetwarzania (przynajmniej niektórych) danych, możesz zażądać ich usunięcia. Pamiętaj jednak, że to uprawnienie nie działa automatycznie i może napotkać pewien opór. Jeśli administrator znajdzie podstawę, żeby Twoje dane nadal przetwarzać (np. ustali, że jest to niezbędne do realizacji umowy albo wymaga tego od niego obowiązujące prawo), będzie mógł odmówić.

Żądanie usunięcia danych ma największe szanse powodzenia, jeśli:

- cel, w jakim Twoje dane zostały zebrane, został już zrealizowany (np. chodziło o ocenę Twojej wiarygodności kredytowej, a bank już udzielił Ci kredytu);
- wcześniej udzieliłaś/-eś zgody na zbieranie dodatkowych danych, ale później zmieniłaś/-eś zdanie i tę zgodę wycofałaś/-eś;

- chodzi o dane „niewiadomego pochodzenia", na których przetwarzanie nigdy nie udzielałaś/-eś zgody, a nawet o tym nie wiedziałaś/-eś.

4. WYCIĄGNIJ KONSEKWENCJE

Nadal nie wiesz, na jakiej podstawie Twoje dane są przetwarzane albo skąd się wzięły w rękach telemarketerów? Już dawno minął miesiąc od Twojego żądania informacji na temat przetwarzanych danych, a po drugiej stronie cisza? A może dotarła do Ciebie właśnie informacja, że Twoje dane wyciekły albo bez podstawy prawnej zostały przekazane do innej firmy, która nie ma zamiaru ich usunąć? Cóż, może się tak zdarzyć... Ale Ty nie musisz tego tolerować! Jeśli na etapie zbierania informacji albo przy próbie zrealizowania innych uprawnień nabierzesz przekonania, że druga strona narusza prawo, możesz zrobić kolejny krok i wyciągnąć konsekwencje.

NAJPROSTSZYM I NIEMAL DARMOWYM ŚRODKIEM PRAWNYM, Z KTÓREGO MOŻESZ SKORZYSTAĆ, JEST SKARGA DO PREZESA URZĘDU OCHRONY DANYCH OSOBOWYCH.

Skarga do Prezesa UODO

Najprostszym i niemal darmowym środkiem prawnym, z którego możesz skorzystać, jest skarga do Prezesa Urzędu Ochrony Danych Osobowych (UODO). Taka skarga powinna dotyczyć naruszenia przepisów RODO (np. braku informacji o tym, jakie dane są przetwarzane, albo tego, że ktoś przetwarza Twoje dane bez podstawy prawnej). Wnosząc ją, nie musisz wykazywać ani krzywdy, ani szkody z tym związanej. Prezes UODO bada przede wszystkim to, czy doszło do naruszenia obowiązującego prawa.

W swojej skardze możesz się domagać:

- zmuszenia firmy/instytucji do tego, żeby wreszcie zareagowała na Twoje żądanie (np. usunęła niepotrzebne dane, udzieliła Ci informacji, przestała przekazywać Twoje dane innym podmiotom, skoro się na to nie zgadzasz);
- nałożenia na nią administracyjnej kary pieniężnej. Taka kara może być bardzo dotkliwa (do 4% globalnego obrotu), więc ma silne działanie dys-

cyplinujące. Pamiętaj jednak, że trafia ona do budżetu państwa i nie ma nic wspólnego z odszkodowaniem (o nim piszemy w kolejnym punkcie).

Postępowanie przed Prezesem jest jednoinstancyjne. Jego przebieg reguluje kodeks postępowania administracyjnego (z wyjątkami wynikającymi z ustawy o ochronie danych osobowych).

Skargę możesz wnieść do organu ochrony danych osobowych w Polsce (jeśli zwykle tu przebywasz: mieszkasz lub pracujesz) albo w innym kraju, jeśli łączy Cię z nim podobny związek (mieszkanie lub praca). Ze względów taktycznych możesz też wybrać kraj, w którym doszło do naruszenia Twoich praw (np. zostały zebrane nielegalnie Twoje dane). Przy wnoszeniu skargi nie ma znaczenia adres firmy, która mogła naruszyć prawo, więc tego czynnika w ogóle nie musisz brać pod uwagę.

Jeśli Twoja sprawa została wszczęta w Polsce, ale dotyczy firmy mającej siedzibę za granicą (albo naruszenia prawa, do którego doszło za granicą), Prezes UODO będzie współpracował z zagranicznymi organami, ale Ty tego specjalnie nie odczujesz, ponieważ cała komunikacja z Tobą będzie się odbywać po polsku.

PRZED SĄDEM CYWILNYM MOŻESZ DOCHODZIĆ NIE TYLKO STWIERDZENIA, ŻE DOSZŁO DO NARUSZENIA TWOICH PRAW, ALE TEŻ ODSZKODOWANIA.

Pozew do sądu

Bez względu na to, czy postanowisz złożyć skargę do Prezesa UODO, czy nie, możesz dochodzić swoich praw bezpośrednio przed sądem cywilnym. To niezależna, choć nieco bardziej skomplikowana i kosztowna ścieżka (przy składaniu pozwu czeka Cię podstawowa opłata w wysokości 600 zł; jeśli dodatkowo wnosisz o odszkodowanie, wysokość opłaty będzie uzależniona od wysokości dochodzonej kwoty).

Sprawę sądową możesz wnieść w tym kraju, w którym mieszkasz, lub w kraju, w którym ma swoją siedzibę firma lub instytucja, którą zamierzasz pozwać (przy czym chodzi o jakąkolwiek jednostkę organizacyjną, np. biuro marketingowe). Wybór należy do Ciebie. Jedynym wyjątkiem jest pozew przeciwko organom publicznym: można je pozwać tylko na terytorium państwa, w którym funkcjonują. Do spraw z zakresu ochrony danych osobowych w Polsce zawsze będzie właściwy sąd okręgowy.

Jeśli zdecydujesz się wnieść pozew, sąd zawiadomi o tym Prezesa UODO. Jeśli przed Prezesem UODO toczy się akurat postępowanie w sprawie tego samego naruszenia, sąd zostanie o tym poinformowany i będzie musiał zawiesić Twoją sprawę, żeby poczekać na rozstrzygnięcie Prezesa UODO. A jeśli Twoja sprawa została już rozstrzygnięta przez Prezesa UODO, jego ustalenie będzie wiążące dla sądu.

Przed sądem cywilnym możesz dochodzić nie tylko stwierdzenia, że doszło do naruszenia Twoich praw, oraz zobowiązania administratora do ich przestrzegania, ale też odszkodowania, jeśli takie naruszenie spowodowało w Twoim życiu konkretne straty (moralne czy majątkowe). Żeby mieć szansę na odszkodowanie, musisz udowodnić, że te szkody rzeczywiście wystąpiły (np. ze względu na informacje, które wyciekły lub zostały nielegalnie zebrane, straciłaś/-eś obiecujący kontrakt, miałaś/-eś nieprzyjemności towarzyskie albo problemy w pracy). Po stronie pozwanej firmy lub instytucji leży natomiast udowodnienie, że nie ponosi ona winy za zdarzenie, które doprowadziło do powstania szkody (np. zrobiła wszystko, czego wymagało prawo, żeby dobrze zabezpieczyć dane).

CO JESZCZE MOŻESZ ZROBIĆ

Mamy nadzieję, że namówiliśmy Cię do skorzystania z uprawnień, jakie daje RODO. Ale na tym jednak nie koniec. Oto, co jeszcze możesz zrobić:

PODZIEL SIĘ WIEDZĄ

Zachęć osoby w Twoim otoczeniu do skorzystania z prawa dostępu do danych, poleć nasz poradnik (panoptykon.org/RODO-masz-prawo) i przygotowane przez nas wzory pism (panoptykon.org/rodo-na-tacy-V).

NIE IGNORUJ ABSURDÓW

Mity krążące wokół RODO sprawiają, że ludzie zniechęcają się do ochrony danych i nie korzystają ze swoich praw.

WESPRZYJ DZIAŁANIA PANOPTYKONU

Pomóż nam walczyć o to, by prawo chroniło prywatność oraz by firmy i administracja nie mogły go ignorować – dołóż swoją darowiznę i 1% podatku.
Numer konta: 43 1440 1101 0000 0000 1044 6058
KRS: 0000327613

RODO

A PANOPTYKON

W prace nad reformą ochrony prywatności w Unii Europejskiej Fundacja Panoptykon była zaangażowana od początku, czyli od 2010 r. Po sześciu latach konsultacji, uzgodnień, trialogów, przeciągania liny przez różne grupy interesów – w kwietniu 2016 r. Parlament Europejski przyjął RODO w kształcie, który uwzględniał wiele naszych postulatów.

To jednak nie był koniec naszej pracy. Rozporządzenie stosowane jest w krajach członkowskich bezpośrednio, ale daje władzom państwowym odrobinę swobody w dostosowywaniu rodzimego prawa. Kolejne dwa lata poświęciliśmy więc na obronę zdobyczy na rodzimym gruncie. Udało się wywalczyć m.in. niezależność organu ochrony danych osobowych i krótkie terminy rozpatrywania skarg. Ale najważniejsze – czyli to, jak nowe prawo zadziała w praktyce – było jeszcze przed nami.

Z myślą o administratorach danych osobowych straszonych przyszłymi karami przygotowaliśmy poradnik pomagający dobrze przygotować się na RODO (panoptykon.org/rodo). W mediach i na naszej stronie tłumaczyliśmy wszystkim zainteresowanym, na czym polegają zmiany, jakie uprawnienia daje RODO, jak będzie można z nich skorzystać. Z myślą o nauczycielach przygotowaliśmy poradnik o RODO jako szansie edukacyjnej. Kiedy 25 maja 2018 r. reforma wreszcie stała się faktem, zaczęliśmy bliżej przyglądać się temu, jak nowe prawo funkcjonuje w różnych branżach, analizować dobre i złe praktyki, odnosić się do najbardziej absurdalnych interpretacji.

Sami – jako osoby związane z Panoptykonem – również testujemy uprawnienia, które daje RODO: pytamy np. banki czy portale internetowe o to, co o nas wiedzą i jak tę wiedzę wykorzystują. W wielu miejscach wciąż odbijamy się od ściany i dlatego szykujemy się na dłuższą batalię.

Mamy RODO i nie zawahamy się go użyć! Wszystko po to, żeby państwo i firmy szanowały prywatność – także Twoją.

Batman, Skrzat i Muminek – oto kilka przykładowych pseudonimów, jakimi zostali obdarzeni pacjenci jednej z przychodni. W niektórych szkołach nauczyciele obawiali się odczytywać na głos listę obecności uczniów i podpisywać prace zwycięzców konkursów. A w Internecie rozprzestrzeniały się dowcipy o tym, że teraz już noworodki będą podpisywać grube pliki zgód na przetwarzanie danych osobowych.

Wysyp absurdów sprawił, że wielu osobom unijne rozporządzenie o ochronie danych osobowych kojarzy się raczej z biurokratyczną mitręgą niż lepszą ochroną prywatności. Czy to zasłużona opinia?

W tej publikacji rozprawiamy się z mitami, które narosły wokół RODO. Tłumaczymy, co naprawdę się zmieniło i jak ochrona danych funkcjonuje w różnych sferach życia (u lekarza, w szkole, w pracy, w sklepie czy w Kościele). Pokazujemy, jak w praktyce korzystać ze swoich praw.

* * *