KANCELARIA PRAWNA
answer
WOJCIECHOWSKI I PARTNERZY

DZIENNIK GAZETA PRAWNA

RODO w praktyce

• zasady przetwarzania danych osobowych szczególnych kategorii • ograniczenia czasowe w przechowywaniu danych osobowych • zgody marketingowe i ich wycofywanie • monitoring – gdzie i jak może być stosowany • przetwarzanie danych osobowych z publicznie dostępnych źródeł • jakie prawa mają osoby, których dotyczą dane osobowe • dokumentacja administratora danych osobowych

DZIENNIK
GAZETA PRAWNA

Adres redakcji: 01-042 Warszawa, ul. Okopowa 58/72,
www.dziennik.pl, www.gazetaprawna.pl, www.forsal.pl

Autorzy: Bartosz Wojciechowski, Kamila Kozera, Marcin Dratwiński,
Kamil Szczur, Martyna Kośmicka, Michał Sobczak,
Elżbieta Białobrodzka-Skrzypiec

Redaktor merytoryczny: Artur Borkowski
Redaktor prowadzący: Mariusz Łukasik
Korekta: Mirosława Jasińska-Nowacka
Projekt graficzny okładki: Kinga Pisarczyk
DTP: Agnieszka Borek

Biuro Obsługi Klienta: 01-042 Warszawa, ul. Okopowa 58/72,
tel. 22 761 31 27, 801 626 666, e-mail: bok@infor.pl

Wydanie I/2020, czerwiec 2020 r.
ISBN: 978-83-66316-66-9

Spis treści

Rozdział 1.
Wprowadzenie

25 maja 2018 r. zaczęło obowiązywać nowe prawo dotyczące ochrony danych osobowych uregulowane rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679, znanym szerzej jako „ogólne rozporządzenie o ochronie danych osobowych" lub krótko: „RODO".

W niniejszym poradniku przybliżamy Czytelnikom zasady, na jakich opierają się regulacje dotyczące ochrony danych osobowych i jak należy je prawidłowo implementować w przedsiębiorstwach. Chcemy w ten sposób pomóc w rozumieniu rzeczywistości prawnej. W naszej praktyce napotkaliśmy bowiem różne przypadki, czasem bardzo skrajne, podchodzenia do przetwarzania danych osobowych: od obojętności wobec zmian w prawie, do panicznego utajniania bądź nawet odchodzenia od posiadania niektórych, wydawałoby się potrzebnych, zbiorów danych osobowych w ogóle.

Od chwili rozpoczęcia obowiązywania ogólnego rozporządzenia o ochronie danych osobowych interpretacje przepisów tego aktu prawnego znacznie się wzbogaciły o wydawane na jego kanwie decyzje oraz orzeczenia. Daje nam to jeszcze lepsze podstawy do przewidywania tego, jak działania dotyczące przetwarzania danych osobowych oceniane będą przez organy sankcjonujące stosowanie prawa. Stąd zaproszenie Państwa do zapoznania się z RODO, ustalonymi nim zasadami i sposobem postępowania, dzięki któremu można uniknąć surowych i niepożądanych konsekwencji.

Niniejszy poradnik to zbiór wiedzy i praktycznych doświadczeń, jak przetwarzać dane osobowe oraz jak przestrzegać związanych z tym regulacji. W poradniku najważniejsze obowiązki przewidziane przez RODO zostały omówione na podstawie wydanych decyzji organów nadzorczych na terenie Unii Europejskiej. Takie podejście do zagadnień i obowiązków w zakresie ochrony danych osobowych przybliża Czytelnikowi praktyczne rozumienie przepisów RODO. W obliczu wydanych decyzji można spostrzec rozwiązania, na które warto zwrócić uwagę przy przetwarzaniu danych.

Poradnik przedstawia wybrane obowiązki i przykłady dla organizacji, które przetwarzają dane osobowe, biorąc przy tym pod uwagę powin-

ność zagwarantowania osobom, których dane dotyczą, bezpieczeństwa. Administratorzy między innymi zobowiązani są stosować się do zasad przetwarzania danych osobowych, przetwarzać dane osobowe zgodnie z prawidłową podstawą prawną i wypełniać obowiązki informacyjne. Przedstawione decyzje organów nadzorczych przybliżają również problematykę kar pieniężnych za niewypełnianie powinności wynikających z przepisów RODO.

Rozdział 2.
Zasady przetwarzania danych osobowych

Kluczowym aspektem prawidłowych działań w zakresie danych osobowych jest przestrzeganie zasad ich przetwarzania. Nie bez powodu unijny prawodawca usytuował ogólne zasady przetwarzania danych osobowych w początkowej części RODO, kładąc nacisk na ich nadrzędność w stosunku do pozostałych norm rozporządzenia. Dlatego pozostałe przepisy należy odczytywać przy zastosowaniu kryterium spójności z omawianymi w niniejszym dziale regułami.

Prawidłowe przestrzeganie zasad przetwarzania danych osobowych ma tym większe znaczenie, że przepisy regulujące te kwestie przewidują możliwość nakładania kar administracyjnych przez organ ochrony danych za ich nieprzestrzeganie. A mogą one być ogromne. Przepisy przewidują w takim przypadku najwyższe na gruncie rozporządzenia sankcje w wysokości do 20 mln euro, a w przypadku przedsiębiorstwa – do 4% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa (art. 83 ust. 5 lit. a RODO).

Tabela. Zasady przetwarzania danych (art. 5 RODO)

Zasada	Istota zasady	Dozwolone/zabronione
Zgodności z prawem, rzetelności i przejrzystości	przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dotyczą dane;	✓ przetwarzanie danych osobowych w ankiecie na podstawie zgody; × nieposiadanie podstawy prawnej na przetwarzanie danych osobowych zawartych w przeprowadzanej ankiecie;
Celowości (ograniczenia celu przetwarzania danych)	dane mogą być zbierane tylko w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami (dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych albo do celów statystycznych nie jest uznawane za niezgodne z pierwotnymi celami);	✓ przetwarzanie danych kontaktowych w postaci adresu e-mail w celu wysyłki newslettera; × przetwarzanie adresu e-mail podanego w celach korzystania z usługi newsletter w innych celach przez administratora;

Adekwatności (minimalizacji) danych	dane muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;	× przetwarzanie numeru PESEL w rekrutacji na dane stanowisko;
Merytorycznej poprawności (prawidłowości danych)	dane muszą być prawidłowe i w razie potrzeby uaktualniane, należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub poprawione;	✓ zapewnienie klientom możliwości uaktualnienia danych osobowych;
Ograniczenia czasowego (ograniczenia przechowywania danych)	dane mogą być przechowywane w formie umożliwiającej identyfikację osoby, której dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane (dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane za niezgodne z pierwotnymi celami);	✓ przetwarzanie danych osobowych w celach marketingu bezpośredniego do momentu zgłoszenia sprzeciwu lub cofnięcia zgody; × przetwarzanie danych osobowych byłych klientów po upływie przedawnienia roszczeń lub przedawnienia przewidzianego w przepisach podatkowych;
Zabezpieczenia danych (integralności i poufności danych)	dane osobowe muszą być przetwarzane w sposób, który zapewni odpowiednie bezpieczeństwo danych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem;	× niezabezpieczanie przetwarzanych danych osobowych, niestosowanie haseł, pozostawianie dokumentacji papierowej w miejscu ogólnodostępnym itp.;
Rozliczalności	administrator danych jest odpowiedzialny za przestrzeganie przepisów i musi być w stanie wykazać ich przestrzeganie.	✓ wdrożenie procedur dotyczących przetwarzania danych osobowych, np. sprawdzania podstaw przetwarzania danych, postępowania w przypadku incydentów.

2.1. Bezpieczeństwo danych (zasada poufności i integralności)

Dane osobowe muszą być przetwarzane w sposób zapewniający ich odpowiednie bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą,

zniszczeniem lub uszkodzeniem. Bezpieczeństwo danych należy zapewnić poprzez odpowiednie środki techniczne i organizacyjne (art. 5 ust. 1 lit. f RODO).

Regulacja ta zwana jest zasadą poufności i integralności. Polega ona na zobowiązaniu administratora danych osobowych do zapewnienia bezpieczeństwa tych danych, w szczególności przed dostępem do nich osób nieuprawnionych, ale także przed ryzykiem ich usunięcia czy przypadkowym zmodyfikowaniem. Reguła ta opiera się na wątłej konstrukcji trafności dobrania środków, które mają służyć zabezpieczeniu danych osobowych. Formuła tej zasady operuje słowem „odpowiednie", co może powodować duży dyskomfort i niepewność, co do prawidłowego zastosowania zasady poufności i integralności w praktyce. Z jednej bowiem strony RODO nie wskazuje wprost, jakie środki techniczne i organizacyjne należy przyjąć przy przetwarzaniu danych osobowych, dając w tym względzie swobodę do ich określenia podmiotowi, który dane te przetwarza. Z drugiej strony przerzuca na administratora obowiązek prawidłowej oceny, jakie zabezpieczenia będą adekwatne dla danego przetwarzania i właściwego ich zastosowania. Wskazówki określające poziom właściwych do zastosowania środków technicznych i organizacyjnych wskazane są w art. 24 ust. 1, art. 25 ust. 1, art. 32 ust. 1 lit. b i d oraz art. 32 ust. 2 RODO.

Zgodnie z treścią art. 24 ust. 1 RODO administrator, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze, powinien wdrożyć odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z prawem i aby móc to wykazać. Środki te powinny być w razie potrzeby poddawane przeglądom i uaktualniane. Administrator powinien dbać o bezpieczeństwo danych na każdym etapie, zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania (tzw. uwzględnianie ochrony danych w fazie projektowania).

Przy wdrażaniu odpowiednich środków technicznych i organizacyjnych administrator i podmiot przetwarzający powinien uwzględnić stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze

zagrożenia. Należy to zrobić w taki sposób, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku (por. art. 32 RODO), w tym między innymi w stosownym przypadku poprzez:

1) pseudonimizację i szyfrowanie danych osobowych;
2) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
3) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
4) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania;
5) poddawanie środków bezpieczeństwa przeglądom i uaktualnianiu.

PRZYKŁAD

Zdolność do zapewnienia poufności i integralności może zostać osiągnięta za pomocą wielu narzędzi programistycznych w postaci: logowania do systemu za pomocą hasła lub innej metody uwierzytelniającej (kod PIN, linie papilarne), bezpiecznego połączenia typu VPN czy stosowania odpowiednich procedur organizacyjnych w postaci zobowiązania pracowników do zachowania poufności danych osobowych.

Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko związane z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych. Warto oprzeć się tu na określonych standardach stosowania środków technicznych i organizacyjnych. Najpewniejszym sposobem wywiązywania się z tych obowiązków jest wykazanie stosowania zatwierdzonego kodeksu postępowania (opracowanego przez zrzeszenia lub inne podmioty reprezentujące administratorów lub podmioty przetwarzające) lub zatwierdzonego mechanizmu certyfikacji w zakresie ochrony danych osobowych. Konstruując bezpieczne metody przetwarzania danych i eliminowania ryzyka, można posiłkować się standardami czy normami wypracowanymi przez

organizacje o określonej renomie w dziedzinie przetwarzania danych bądź bezpieczeństwa informacji.

2.1.1. Przypadek Morele.net

Sklep internetowy Morele.net to jeden z największych graczy na rynku e-commerce w Polsce z blisko 20-letnią historią. Zespół utalentowanych menedżerów i specjalistów od sprzedaży online doprowadził Morele.net do fantastycznego rozwoju, nagrodzonego wieloma wyróżnieniami, i wypracowania renomy i zaufania wśród klientów.

W listopadzie 2018 r. osoby, które dokonały zakupów w sklepie Morele.net, zaczęły otrzymywać SMS-y z informacją: „MORELE.NET – WYMAGANA dopłata do zamówienia (1.00 PLN). Opłać teraz...". Wiadomość zawierała link, który kierował kupujących do strony płatności. Niestety, zarówno SMS-y, jak i strona internetowa dotycząca dokonania wpłat były fałszywe, a jej celem było wyłudzenie od ofiary loginu i hasła do konta w banku oraz kodu autoryzacji przelewu wysyłanego ofierze przez bank SMS-em. Metoda takiego oszustwa zwana jest powszechnie phishingiem. Co więcej, w niniejszej sprawie zastosowano phishing personalizowany (tzw. spearphishing), ściśle związany z sytuacją osób, które dokonywały w nieodległym czasie transakcji zakupowej w Morele.net. Sprawiło to, że wiadomość o konieczności dopłaty była odbierana przez klientów jako wysoce wiarygodna. W konsekwencji jednak ofiara traciła pieniądze, jakie miała na swoim rachunku bankowym. Z szacunków serwisu Niebezpiecznik.pl wynika, że zyski przestępcy z tego procederu sięgały nawet kilkaset tysięcy złotych dziennie.

Zaalarmowany o zdarzeniu sklep poinformował prezesa Urzędu Ochrony Danych Osobowych (dalej równiej jako „prezes UODO") oraz opublikował informacje na swojej stronie internetowej, ostrzegając klientów o potencjalnej próbie oszustwa i wyłudzenia oraz o tym, że nigdy nie wysyła SMS-ów z prośbą o dopłaty do zamówienia. Jednocześnie Morele.net zapewniło, że nie jest źródłem danych wykorzystywanych przez oszustów i że posiada ściśle chronioną bazę danych swoich klientów. W pierwszym tygodniu grudnia sklep jednak wycofał się z wcześniejszego zapewnienia, a 18 grudnia 2018 r. oficjalnie poinformował klientów, że ich dane teleadresowe i hasła zostały wykradzione. Dwa dni później w serwisie Wykop.pl, jeden z użytkowników ujawnił, że od 28 listopada rozpoczęły się negocjacje w sprawie

okupu za wykradzioną bazę zawierającą dane ponad 2,2 mln klientów, w tym ich imiona, nazwiska, adresy, e-maile, numery telefonów, ale i w niektórych przypadkach numery PESEL z wniosków kredytowych, a także skany dowodów osobistych. Włamywacz domagał się 500 tys. zł, ale przerwał negocjacje, gdy zorientował się, że jest namierzany. Urząd Ochrony Danych Osobowych (dalej również jako „UODO") ustalił, że nie dochowano należytej staranności w prawidłowej ocenie ryzyka związanego z przetwarzaniem danych osobowych, w szczególności pomimo deklaracji monitorowania systemu sieciowego i reagowania na zagrożenia w systemie 24/7, nie stwierdzono w czasie rzeczywistym zwiększonego ruchu na bramie sieciowej serwera i nie podjęto żadnych działań zaradczych celem uniemożliwienia nieuprawnionym dostępu do danych osobowych. Jednocześnie UODO stwierdził, że Morele.net wykorzystywało nieskuteczny środek uwierzytelniania, który przyczynił się do zdarzenia polegającego na uzyskaniu nieuprawnionego dostępu do danych klientów.

10 września 2019 r. prezes UODO nałożył na spółkę Morele.net karę w wysokości ponad 2 830 410 zł (równowartość 660 tys. euro)[1] . W decyzji wyjaśniono, że spółka, nie stosując wystarczających środków technicznych ochrony danych, naruszyła m.in. określoną w art. 5 ust. 1 lit. f RODO zasadę poufności. W związku z tym doszło do nieuprawnionego dostępu do danych klientów i do uzyskania tych danych. Organ uznał, że miało miejsce zastosowanie nieskutecznego środka uwierzytelniania dostępu do informacji. Dodatkowe środki zabezpieczenia technicznego spółka wdrożyła już po wykrytym naruszeniu. W toku postępowania ustalono, że do naruszenia doszło także z uwagi na brak odpowiednich środków technicznych (niewystarczające zabezpieczenia) i organizacyjnych (dotyczących monitorowania potencjalnych zagrożeń, związanych z nietypowymi działaniami w sieci), co w konsekwencji przesądziło o nałożeniu kary. Przy ustalaniu jej wysokości prezes UODO wziął jednak pod uwagę okoliczności łagodzące, jak np.: podjęcie przez spółkę działań zmierzających do usunięcia naruszenia, dobrą współpracę z administratorem oraz to, że wcześniej spółka nie dopuściła się naruszenia przepisów o ochronie danych osobowych.

[1] Decyzja prezesa Urzędu Ochrony Danych Osobowych z 10 września 2019 r., sygn. ZSPR.421.2.2019.

W uzasadnieniu swojej decyzji prezes UODO wskazał, że podstawowym środkiem bezpieczeństwa danych osobowych jest kontrola dostępu do nich i uwierzytelnianie, które zapewniają ochronę przed nieautoryzowanym dostępem do systemu informatycznego wykorzystywanego do przetwarzania danych osobowych. Prezes UODO zwrócił uwagę, że wskazówek konkretyzujących w przedmiocie odpowiedniego bezpieczeństwa dostarczają obowiązujące standardy i normy, w szczególności normy ISO, które ulegają również ciągłym przeglądom i zmianom warunkowanym postępem technologicznym. Jednocześnie wskazał na normę ISO – PN-EN ISO/IEC 27001:2017-06 („Technika informatyczna – Techniki bezpieczeństwa – Ramy uzasadnionej pewności poziomów uwierzytelnienia") jako wzorzec postępowania, który należało stosować w celu zapobiegania nieuprawnionemu dostępowi do systemów i usług[2]. W ocenie prezesa UODO nieskuteczne monitorowanie potencjalnych zagrożeń dla praw i wolności klientów, których dane są przetwarzane przez Morele.net, przyczyniło się do zdarzenia polegającego na uzyskaniu nieuprawnionego dostępu do danych z baz danych tego sklepu internetowego. Wskazano, że przyjęte środki mogłyby być skuteczne, gdyby były odpowiednio dostosowane oraz gdyby wdrożono procedurę reagowania na zdarzenia niepożądane, takie jak nietypowy ruch sieciowy. W wytycznych Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA) dotyczących bezpieczeństwa przetwarzania danych osobowych również wskazuje się, że monitorowanie zdarzeń w systemach informatycznych jest istotnym elementem umożliwiającym identyfikację potencjalnych wewnętrznych lub zewnętrznych zagrożeń dla tych systemów. Zadanie to powinno być realizowane w postaci odpowiednich, wdrożonych procedur i systemu powiadamiania o zdarzeniach niepożądanych. Przetwarzanie danych osobowych ponad 2,2 mln użytkowników uznano za przetwarzanie danych osobowych na dużą skalę, a biorąc pod uwagę zakres danych i kontekst przetwarzania, prezes UODO uznał, że należało skuteczniej na bieżąco oceniać i monitorować potencjalne zagrożenia dla praw i wolności osób, których dane przetwarzano.

[2] Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (ENISA) w swoich wytycznych dotyczących bezpieczeństwa przetwarzania danych osobowych wydanych w 2016 r. z uwzględnieniem normy PN-EN ISO/IEC 27001 (w wersji z 2013 r.) oraz przepisów rozporządzenia 2016/679, w ramach kontroli dostępu i uwierzytelniania rekomenduje stosowanie mechanizmu uwierzytelniania dwuetapowego dla systemów obejmujących dostęp do danych osobowych.

WAŻNE

Regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych osobowych jest obowiązkiem każdego administratora oraz podmiotu przetwarzającego. Administrator zobowiązany jest więc do weryfikacji zarówno doboru, jak i poziomu skuteczności stosowanych środków technicznych. Kompleksowość tej weryfikacji powinna być oceniana przez pryzmat adekwatności do ryzyka oraz proporcjonalności w stosunku do stanu wiedzy technicznej, kosztów wdrażania oraz charakteru, zakresu, kontekstu i celów przetwarzania.

W ocenie prezesa UODO Morele.net nie podejmowało działań mających na celu ocenę doboru środków technicznych i organizacyjnych przez pryzmat adekwatności do ryzyka. Morele.net zastosowało środki techniczne i organizacyjne, które przyczyniły się w ograniczonym stopniu do wypełnienia wymogów RODO, gdyż przewidywalne ryzyko nie zostało odpowiednio zminimalizowane i ograniczone w czasie przetwarzania.

Przypadek Morele.net nie jest odosobnionym aktem wycieku danych ze sklepu internetowego. W technologii internetowej nie ma takiej funkcji, która nie posiada żadnego błędu czy słabego punktu. Zdarzają się problemy ze źle zaprojektowanymi procesami, rotacją pracowników, przekazywaniem wiedzy, szkoleniami, holistycznym spojrzeniem na zmieniającą się technologię i permanentnym brakiem czasu. Wszystko to sprawia, że każdy sklep internetowy wcześniej czy później może paść ofiarą ataku hakerskiego i nawet nie mieć pojęcia o skali kradzieży informacji. Computerworld podaje, że 97% korporacji z listy Fortune 500 co najmniej raz ucierpiało z powodu naruszenia bezpieczeństwa IT. Według raportu „Stan Cyberbezpieczeństwa Polskiej Branży E-commerce", wykonanego przez TestArmy CyberForces z lipca 2018 r., 80% polskich sklepów internetowych padło ofiarą cyberataku, a 40% przyznaje, że przeprowadza testy penetracyjne podnoszące bezpieczeństwo.

Kary, która dotknęła Morele.net, nie należy zatem odbierać jako ceny za atak hakerski, a jedynie jako ocenę tego, co operator sklepu wykonywał, aby unikać podobnego zagrożenia. Firmy mogą zatem ograniczać

ryzyko (także potencjalnych kar regulacyjnych) poprzez dokonywanie cyklicznych przeglądów zabezpieczeń oraz unikania przechowywania danych w zakresie już zbędnym (dane użytkowników, którzy rozwiązali umowy, dane niekonieczne do wykonywania umowy).

PRZYKŁADOWA LISTA KONTROLNA (CHECKLIST)

- Ustal, jakie dane osobowe przetwarzasz i gdzie (w tym komu powierzono przetwarzanie danych osobowych i na jakich warunkach).
- Dobierz skuteczne i adekwatne do ryzyka środki organizacyjne i techniczne.
- Regularnie testuj, mierz i oceniaj skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo danych osobowych.
- Posiadaj procedurę postępowania na wypadek zaistnienia incydentu.

2.2. Cel przetwarzania danych (zasada celowości i adekwatności)

Dane osobowe zbierane są w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami (art. 5 ust. 1 lit. b RODO). Ponadto, zgodnie z art. 5 ust. 1 lit. c RODO, dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych").

PRZYKŁAD

Przykładem nieadekwatności będzie przetwarzanie np. numeru PESEL, numeru dowodu osobistego, imion rodziców, użytkownika serwisu dla celów złożenia przez niego zamówienia w sklepie internetowym.

2.2.1. Przypadek portugalskiego szpitala Barreiro Montijo

Naruszenie zasady celowości i adekwatności (minimalizacji danych) najlepiej widać na przykładzie sprawy szpitala Barreiro Montijo, położonego vis-à-vis Lizbony, na przeciwległym brzegu rzeki Tag. Głównym powodem prowadzenia przez krajowy organ nadzorczy postępowania

w tym przypadku było sprawdzenie uprawnień poszczególnych osób w zakresie dostępu do danych klinicznych pacjentów.

W szpitalu było zatrudnionych 296 lekarzy, zaś system informatyczny, którym dysponował ten podmiot, umożliwiał dostęp do danych klinicznych pacjentów z aż 985 aktywnych kont – jak się bowiem okazało byli pracownicy szpitala nie zostali pozbawieni do nich dostępu. Comissão Nacional de Proteção de Dados (CNPD – organ nadzorczy ochrony danych osobowych w Portugalii) w toku przeprowadzonej kontroli uznał, że głównym naruszeniem, którego szpital się dopuścił, był dostęp do danych pacjentów poprzez świadome powiązanie profilu lekarza z profilem, który powinien być profilem czysto technicznym. Wśród uchybień organ wskazał także na to, że do danych medycznych, do których co do zasady powinni mieć dostęp wyłącznie lekarze prowadzący pacjenta, upoważnieni byli także inni lekarze oraz pracownicy szpitala. Zawiodła także metoda uwierzytelniania, która nie uwzględniała danych identyfikacyjnych pozwalających na połączenie danego specjalisty z obszarem przez niego nadzorowanym. Każdy lekarz o dowolnej specjalizacji był w stanie w każdym momencie uzyskać dostęp do danych pacjentów z różnych ośrodków szpitalnych. Z konta testowego utworzonego przez ekspertów wyznaczonych przez organ nadzorczy możliwe było uzyskanie dostępu do danych pacjentów nie tylko szpitala w Barreiro, ale też do plików cyfrowych szpitala Santa Cruz w mieście Carnaxide. Nadto w toku przeprowadzonych czynności kontrolnych organ wykazał również, że szpital nie posiada wewnętrznych regulacji opisujących zasady tworzenia kont pracowniczych – aby stworzyć takie konto, wystarczyło napisać wiadomość e-mailową do współpracującego ze szpitalem informatyka. Metoda uwierzytelniania użytkowników nie zakładała więc identyfikacji indywidualnej pozwalającej na dostęp do określonych danych, co w efekcie powodowało, że technicy pracujący w szpitalu mieli taki sam dostęp do danych klinicznych jak lekarze. CNPD stwierdził także zaniechanie przez szpital niezbędnych kroków celem weryfikacji i ustalenia dezaktywacji kont byłych pracowników, a także podjęcia stosownych środków do zapewnienia trwałego usunięcia kont lekarzy, którzy zakończyli pracę w placówce.

Organ w toku przeprowadzonej kontroli ustalił, że doszło do naruszenia art. 5 ust. 1 lit. c i f w związku z art. 83 ust. 5 lit. a oraz art. 32 ust. 1 lit. b RODO. Zidentyfikował więc trzy naruszenia, tj.:

1) naruszenie zasady integralności i poufności danych,
2) naruszenie zasady minimalizacji danych, a także
3) brak zapewnienia przez administratora odpowiednich środków technicznych gwarantujących zachowanie poufności, integralności, dostępności i odporności systemów i usług przetwarzania danych.

Za wymienione wyżej naruszenia szpital obarczono sankcją w łącznej wysokości 400 tys. euro, na którą złożyły się odpowiednio po 150 tys. euro za naruszenie zasady integralności i poufności danych i naruszenie zasady minimalizacji danych oraz 100 tys. euro za brak zapewnienia odpowiednich środków bezpieczeństwa. Okolicznością wpływającą na wymiar kary był przede wszystkim fakt, że w ocenie Komisji szpital miał pełną świadomość tego, iż był zobowiązany do zastosowania technicznych i organizacyjnych środków niezbędnych do identyfikacji i uwierzytelniania użytkowników, a także do ustalania zakresu ich dostępu do profili informacyjnych stosownie do zakresu obowiązków pracowniczych, mimo to nigdy nie podjęto czynności w celu doprowadzenia do stanu zgodnego z prawem. W decyzji CNPD możemy natrafić na poniższe uzasadnienie:

(...) Podmiot działał umyślnie, wiedząc, że był zobowiązany do zastosowania technicznych i organizacyjnych środków niezbędnych do identyfikacji i uwierzytelniania użytkowników, a także do zarządzania i rozgraniczania ich dostępu do profili informacyjnych, warstwując je zgodnie z różnymi przywilejami (...).

Następstwem zaniedbań była możliwość za pośrednictwem rejestru zapoznania się osób, które nie powinny mieć takiej sposobności, z danymi osobowymi pacjentów. Mowa tu zarówno o lekarzach mających dostęp do cudzych pacjentów, jak i osób z nimi współpracujących. Niewątpliwie skala oraz długotrwałość naruszeń wpłynęły w tej sprawie na wysokość sankcji.

WAŻNE

Przypomnieć należy, że RODO przewiduje w zależności od rodzaju naruszenia kary pieniężne w wysokości do 10 mln euro w sprawach mniejszej wagi lub w wysokości do 20 mln euro przy naruszeniach w większej skali. W przypadku przedsiębiorstwa, gdzie wysokość kary również zależy od wagi naruszenia, kary oscylują w wysokości 2% lub 4% całkowitego, rocz-

nego światowego obrotu podmiotu z poprzedniego roku obrotowego, chyba że kara ustalona kwotowo jest wyższa – wtedy ona znajduje zastosowanie.

Władze szpitala nie zgodziły się z decyzją CNPD, argumentując, że aktywność takiej liczby kont była spowodowana przejściowym incydentem związanym z technicznymi ograniczeniami programu do przechowywania danych pacjentów dostarczanego przez firmy trzecie.

Sprawa szpitala Barreiro Montijo vs. CNPD doskonale ukazuje, jak istotna jest świadomość i wiedza administratora danych podczas ich przetwarzania. Odpowiednie procedury oraz zastosowane mechanizmy systemowe mogłyby zapobiec naruszeniom i wysokiej karze finansowej.

PRZYKŁADOWA LISTA KONTROLNA (CHECKLIST)

- Ustal, jakie dane osobowe przetwarzasz.
- Posiadaj procedurę nadawania upoważnień do przetwarzania danych osobowych.
- Zadbaj, aby dostęp do określonych danych osobowych miały jedynie osoby upoważnione do przetwarzania tych danych w przedsiębiorstwie administratora.
- Posiadaj mechanizmy ograniczające dostępność do danych oraz mechanizmy uwierzytelniania.

2.3. Przetwarzanie zgodne z prawem (zasada zgodności z prawem)

Przetwarzanie danych jest zgodne z prawem pod warunkiem, że następuje na podstawie ustawy lub aktu prawnego wydanego na podstawie ustawy oraz jest niezbędne do osiągnięcia uzasadnionego celu. Obowiązek zapewnienia przez administratora, aby dane były przetwarzane zgodnie z prawem, oznacza przetwarzanie ich na wszystkich płaszczyznach zarządzania danymi, to jest już od momentu ich zebrania aż do momentu ich usunięcia na podstawie co najmniej jednej z podstaw prawnych przetwarzania bliżej opisanych w rozdziale 3 (art. 6 i art. 9 ust. 2 RODO). W art. 6 i 9 ust. 2 RODO przewidziano warunki zgodnego z prawem przetwarzania danych osobowych i opisano podstawy zgod-

ne z prawem, na których administrator może się opierać. Zastosowanie jednej z tych podstaw musi zostać ustalone przed przetwarzaniem i w odniesieniu do określonego celu.

WAŻNE

Zasada zgodności z prawem – dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą (art. 5 ust. 1 lit. a RODO).

Niedopuszczalne jest natomiast przetwarzanie danych w sposób pozbawiony podstawy prawnej i bez określonego celu.

PRZYKŁAD

1. Sprzedający legalnie przetwarza dane osobowe użytkownika sklepu internetowego, który wypełniając formularz kontaktowy wpisał swoje dane: imię i nazwisko oraz adres e-mailowy w celu otrzymania odpowiedzi na zadane sprzedającemu zapytanie dotyczące towaru lub świadczonej usługi. Przyjąć bowiem należy, że przetwarzanie podanych danych osobowych znajduje podstawę prawą w art. 6 ust. 1 lit. b RODO.
2. W przypadku świadczenia usługi typu newsletter przetwarzanie danych będzie zgodne z prawem, gdy osoba, na rzecz której świadczona ma być usługa, wyrazi na to zgodę lub zamówi usługę. Przyjąć bowiem należy, że w celu przesyłania informacji dotyczących oferty lub treści marketingowych dotyczących administratora drogą e-mailową w ramach newslettera – podstawą prawną przetwarzania, w tym profilowania, jest uzasadniony interes administratora (art. 6 ust. 1 lit. f RODO) w związku z wyrażoną zgodą na otrzymywanie newslettera.

2.3.1. Przypadek Österreichische Post AG

Przykładem braku zgodności z prawem było przetwarzanie przez austriacką pocztę Österreichische Post AG („ÖPAG") danych o politycznych afiliacjach odbiorców przesyłek. W ramach przeprowadzonego postępowania dowodowego austriacki organ ochrony danych uznał za

udowodnione, że ÖPAG naruszyła przepisy RODO, przetwarzając dane osobowe na temat upodobań politycznych swoich klientów. W ramach postępowania uznano, że ÖPAG zebrała dane o afiliacjach politycznych od 2,2 mln osób. Obok takich danych, jak imię i nazwisko, adres austriacka poczta przechowywała dane o przynależności do partii, które następnie wykorzystała do zaoferowania określonych opcji marketingowych partiom politycznym lub nawet sprzedaży partiom politycznym baz danych umożliwiających wysyłkę ukierunkowanej reklamy. 23 października 2019 r. austriacki organ ochrony danych osobowych wydał decyzję i nałożył na ÖPAG karę administracyjną w wysokości 18 mln euro. Decyzja ta obecnie (stan na kwiecień 2020 r.) nie jest prawomocna, gdyż ÖPAG odwołała się od niej. ÖPAG broni stosowanej procedury jako legalnej pod względem marketingowym, wskazuje przy tym, że partie powinny mieć możliwość wysyłania ukierunkowanych reklam wyborczych.

Analizując przykład ÖPAG, należy przypomnieć, że zgodnie z art. 9 ust. 1 RODO zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby. Poglądy polityczne zatem zalicza się do danych szczególnych kategorii i ich przetwarzanie może odbywać się tylko w oparciu o podstawę określoną w art. 9 ust. 2 RODO.

Ustawodawca unijny we wspomnianym art. 9 ust. 2 RODO przewidział dziesięć podstaw legalizujących przetwarzanie danych osobowych szczególnych kategorii. Jedną z najczęściej spotykanych jest zgoda osoby, której dane dotyczą. Jednak należy pamiętać, że prawo unijne lub prawo krajowe może przewidywać, iż nawet udzielenie zgody przez osobę, której dane dotyczą, nie uchyla zakazu przetwarzania danych szczególnych kategorii. Należy też wziąć pod uwagę, że wyrażona na prośbę administratora pisemna zgoda na przetwarzanie danych osobowych szczególnych kategorii może wiązać się z nieadekwatnością przetwarzania określonych danych do wybranego przez administratora celu (por. Cel przetwarzania danych (zasada celowości i adekwatności – pkt 2.2).

WAŻNE

Aby zachować zasadę zgodności z prawem przetwarzania, każdy administrator jest zobowiązany do:
1) określenia podstawy prawnej przetwarzanych danych przy uwzględnieniu celu przetwarzania;
2) stosowania określonej podstawy prawnej wobec przetwarzanych danych.

Przy naruszeniu omawianej zasady należy nie tylko brać pod uwagę naruszenie administracyjne, ale również zwrócić uwagę, że nielegalne przetwarzanie danych osobowych może bez wątpienia powodować poważne problemy z punktu widzenia prawa cywilnego.

Zgodnie z przepisem art. 82 RODO każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia niniejszego rozporządzenia, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę.

RODO nie zawiera żadnych szczegółowych zasad określania kwoty roszczenia z tytułu niematerialnych szkód. Zastosowanie mają ogólne zasady dochodzenia roszczeń (niematerialnych). Na kanwie austriackiej sprawy doszło również do orzeczenia rekompensaty na rzecz osoby, której dane dotyczą, za niematerialne szkody wynikające z niezgodnego z prawem przetwarzania jej danych osobowych. Z publicznie dostępnych informacji wynika, że klienci ÖPAG nie byli informowani ani nie wyrażali zgody na przetwarzanie swoich danych. W ramach sporu sądowego powód twierdził, że czuł się zaniepokojony tym, iż został tak wyprofilowany bez swej wiedzy i zgody. Sąd pierwszej instancji orzekł, że samo poczucie zakłócenia przez niezgodne z prawem przetwarzanie danych o upodobaniach politycznych już samo w sobie stanowi niematerialną szkodę i zasądził na rzecz powoda 800 euro z 2500 euro, o które ten wystąpił.

Biorąc pod uwagę, że niezgodne z prawem przetwarzanie danych osobowych ma z natury wpływ na dużą liczbę osób, należy ściśle monitorować przyszły rozwój sporów dotyczących ochrony danych i zasądzanych odszkodowań.

LISTA KONTROLNA (CHECKLIST)

- Ustal, jakie dane osobowe przechowujesz, na jakiej podstawie prawnej oraz w jakim celu.
- Dokładnie rozważ i uzasadnij stosowaną podstawę prawną wobec przetwarzania danych w danym celu.

2.4. Ograniczenie przechowywania danych (zasada retencji/czasowości)

Dane osobowe powinny być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy niż jest to niezbędne do celów, dla realizacji których dane te są przetwarzane (art. 5 ust. 1 lit. e RODO). Stosowanie ograniczenia przechowywania, czyli retencji, przede wszystkim może następować poprzez wewnętrzne procedury określające zasady i okresy usuwania danych osobowych, wynikające z przepisów prawa lub celów administratora.

WAŻNE

Wyrażona w tym przepisie zasada ograniczenia przechowywania wskazuje, że dane nie mogą być przetwarzane bez ograniczeń czasowych i na każdym etapie należy ocenić, czy dla danego podmiotu są one niezbędne w kontekście realizacji konkretnych celów.

2.4.1. Przypadek Deutsche Wohnen SE

Zasady retencji można omówić na przykładzie sprawy Deutsche Wohnen SE. Według organu nadzoru Deutsche Wohnen SE dopuścił się wielu naruszeń RODO, w tym polegających na tym, że używał systemu do przechowywania danych osobowych najemców ze świadomością, iż system ten nie jest w stanie właściwie usuwać danych, które nie są już potrzebne.

Podmiot przetwarzał również dane osobowe bez sprawdzania, czy ich przechowywanie było konieczne oraz czy w ogóle było to dozwolone. W indywidualnych przypadkach badanie wykazało, że można było prze-

glądać prywatne dane byłych najemców, nawet jeśli cel pierwotnego badania nie był już dostępny. Były to dane dotyczące osobistej i finansowej sytuacji najemców, takie jak zaświadczenia o wynagrodzeniach, formularze do samodzielnego ujawnienia, wyciągi z umów o pracę i szkolenia, dane podatkowe, informacje dotyczące ubezpieczenia społecznego i zdrowotnego oraz wyciągi bankowe.

Po kontroli organ nadzoru wydał pilną rekomendację dla Deutsche Wohnen SE, aby w niezbędnym zakresie przekształcić system przechowywania i archiwizacji tak, aby był zgodny z przepisami RODO. Podmiot nie spełnił jednak, a przynajmniej niewystarczająco, tego żądania. W marcu 2019 r., po ponad półtora roku po pierwszej kontroli, podmiot nie był w stanie wykazać stosownej procedury usunięcia informacji w przypadku starszych baz danych lub prawnych, a także podstaw prawnych do trwałego przechowywania danych osobowych. Podmiot próbował zaradzić tej sytuacji, podejmując pierwsze przygotowania. Nie wystarczyło to jednak organowi nadzorczemu, ponieważ przedsięwzięte środki nie doprowadziły do stanu zgodnego z prawem przetwarzania danych.

Na podstawie rocznego raportu obroty Deutsche Wohnen SE w 2018 r. wyniosły ponad miliard euro, co stanowiło ramy dla ustalenia grzywny dla ustalonych naruszeń ochrony danych na poziomie około 28 mln euro. Za główne naruszenie uznany został fakt, iż Deutsche Wohnen SE celowo utworzył strukturę archiwum danych osobowych, które przetwarzane były z naruszeniem zasad. Jako okoliczność łagodzącą wysokość grzywny uznano to, iż podmiot zrobił pierwsze kroki w celu zmiany niezgodnego z prawem stanu rzeczy i podjął współpracę z organem nadzorczym. Organ nadzorczy postrzegał wadliwy stan systemu przechowywania i archiwizacji danych jako rażące naruszenie art. 5 RODO i art. 25 ust. 1 RODO. Grzywna we wskazanej powyżej wysokości była zatem niezbędna i uzasadniona z punktu widzenia władzy. Jak wskazują organy nadzorcze, kary powinny być nie tylko skuteczne i proporcjonalne, ale także odstraszające. Jak informują przedstawiciele organów nadzorczych, często spotykane są tzw. cmentarze danych. Zazwyczaj wiedza organów o przedmiotowych nadużyciach pojawia się w momencie, gdy cyberataki doprowadzają do niewłaściwego dostępu do ogromnej ilości zgromadzonych tam danych. Jednak również jak we wskazanym powyżej przypadku, gdzie nie dochodzi do tak poważnych konsekwencji, mamy do czynienia z rażącym naruszeniem zasad ochrony danych osobowych.

Każdy administrator, uwzględniając między innymi charakter, zakres, kontekst i cele przetwarzania danych osobowych, jest obowiązany wdrożyć odpowiednie środki techniczne i organizacyjne zapewniające usuwanie tych informacji, których cel przetwarzania już minął, tak by spełnić wymogi RODO oraz chronić prawa osób, których dane dotyczą.

WAŻNE

Dane muszą być przechowywane przez możliwie najkrótszy czas. Okres ten powinien uwzględniać powody, dla których przedsiębiorca musi przetwarzać dane, a także wszelkie prawne zobowiązania do przechowywania danych przez określony czas (na przykład krajowe przepisy prawa pracy, podatków lub zwalczania nadużyć finansowych, które wymagają przechowywania danych osobowych swoich pracowników przez określony czas, okres gwarancji produktu itp.).

Przedsiębiorca powinien ustalić limity czasowe na usunięcie lub przegląd przechowywanych danych, np. poprzez wdrożenie polityki retencji danych.

Gdy dane osobowe przechowywane są dłużej, niż jest to potrzebne, administrator powinien je usunąć lub zanonimizować. Anonimizacja jest techniką maskowania danych, czyniąc je takimi, aby jakiekolwiek ich powiązanie ze stanem pierwotnym (w tym osobą, której dotyczą) było niemożliwe. Anonimizację należy odróżnić od pseudonimizacji, tak zwanego kodowania kluczem, umożliwiającego identyfikację. Pseudonimizacja może być użytecznym narzędziem służącym do zachowania zgodności z innymi zasadami, takimi jak minimalizacja danych i bezpieczeństwo.

LISTA KONTROLNA (CHECKLIST)

- Ustal, jakie dane osobowe przechowujesz i dlaczego ich potrzebujesz.
- Dokładnie rozważ i uzasadnij, jak długo należy przechowywać dane osobowe.
- Nie przechowuj danych osobowych dłużej, niż jest to potrzebne.

- Analizuj – i uzasadniaj – jak długo przechowujesz dane osobowe, co zależy od celów przechowywania danych.
- Wprowadź procedurę określającą standardowe okresy przechowywania danych, jeśli jest to możliwe, zgodnie z obowiązkami dotyczącymi dokumentacji.
- Sprawdzaj okresowo posiadane dane oraz usuwaj je lub anonimizuj, gdy nie są już potrzebne.
- Przechowuj dane osobowe dłużej jedynie wtedy, gdy przepisy na to pozwalają.

2.5. Podsumowanie

Wszelkie procesy przetwarzania danych osobowych muszą być zgodne ze wszystkimi zasadami przetwarzania łącznie. Naruszenie choćby jednej z nich powoduje, że przetwarzanie danych osobowych będzie niezgodne z obowiązującymi przepisami prawa w tym zakresie. Zasady precyzują sposoby przetwarzania danych osobowych oraz procesy administrowania nimi, stanowiąc źródło obowiązków ciążących na administratorze i innych podmiotach przetwarzających dane i jednocześnie zwiększając ich samodzielność w zakresie przetwarzania danych osobowych.

Przedsiębiorcy muszą samodzielnie ocenić, jakie ryzyko wiąże się z przetwarzaniem danych osobowych i jakie w związku z tym należy przedsięwziąć środki (jakie zabezpieczenia, dokumentację oraz procedury przetwarzania wdrożyć) – biorąc pod uwagę charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych – z zachowaniem określonych wytycznych wynikających z przywołanych zasad. Respektowanie wymienionych zasad niejako zmusza podmioty do skontrolowania prowadzonej działalności pod kątem wypełniania wymogów w zakresie ochrony danych osobowych, w tym zweryfikowania m.in.: jakie dane osobowe przetwarzają, w jaki sposób, na jakiej podstawie prawnej, w oparciu o jaką dokumentację wewnętrzną, jakie stosują środki techniczne i organizacyjne w zakresie zabezpieczenia danych osobowych, a także jakim podmiotom przekazują dane i czy są to podmioty spoza Europejskiego Obszaru Gospodarczego.

Rozdział 3.
Podstawy prawne przetwarzania danych

Przez pojęcie przetwarzania danych osobowych należy rozumieć każdą operację lub zestaw operacji wykonywanych na danych osobowych. W szczególności przetwarzanie danych osobowych może polegać na ich zbieraniu, porządkowaniu, pobieraniu, przechowywaniu, a także niszczeniu. Dane osobowe zgodnie z RODO można przetwarzać wyłącznie w określonych przypadkach i przy poszanowaniu zasad przetwarzania wynikających z przepisów prawa. Szczegółowo określone podstawy przetwarzania danych osobowych zawarte są w art. 6 ust. 1 RODO.

Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków (art. 6 ust. 1 RODO):

a) osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych

Warunki te stanowią katalog zamknięty podstaw prawnych przetwarzania danych osobowych.

Tabela. Przetwarzanie zgodne z prawem – warunki

Warunki przetwarzania zgodnego z prawem	Opis	Przykłady
Zgoda na przetwarzanie	Aby zgoda była prawidłowa, musi być wyrażona dobrowolnie (nie może być wymuszona), konkretnie (cel przetwarzania danych oraz zakres przetwarzania muszą być precyzyjnie określone), świadomie oraz jednoznacznie (okazanie woli w formie oświadczenia lub wyraźnego działania). Ponadto każdy administrator danych powinien wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie. W kontekście zgody na przetwarzanie danych niezwykle istotne jest również to, że osoba wyrażająca zgodę musi mieć zapewnione prawo do cofnięcia zgody w dowolnym momencie i to w równie łatwy sposób, jak wyrażenie zgody. Cofnięcie zgody nie powoduje przy tym, że przetwarzanie danych przed cofnięciem zgody staje się niezgodne z prawem. O tej ostatniej okoliczności osoba wyrażająca zgodę powinna zostać poinformowana jeszcze przed jej wyrażeniem.	Przykłady przetwarzania danych opartych na zgodzie: ✓ dane osób ankietowanych, ✓ dane osób w celach marketingowych, ✗ dane kontrahentów będących osobami fizycznymi – w związku z zawarciem umowy podstawą przetwarzania jest niezbędność realizacji umowy (art. 6 ust. 1. lit. b RODO), w takim przypadku nieprawidłowe jest pobieranie zgody na przetwarzanie danych w celu realizacji umowy.
Przetwarzanie niezbędne do wykonania umowy lub podjęcia działań przed zawarciem umowy	Ustawodawca europejski przewidział w art. 6 ust. 1 lit. b RODO sytuację, w której zgodne z prawem jest przetwarzanie danych koniecznych dla prawidłowego wykonania umowy lub podjęcia działań przed zawarciem umowy. Zakres danych, które są wymagane, zależy od charakteru umowy, rodzaju świadczenia lub innych okoliczności istotnych z punktu widzenia celu przetwarzania danych. Czasem wystarczające są podstawowe informacje identyfikujące osobę, której dane dotyczą, a innymi razem zakres potrzebnych danych może być znacznie szerszy. Ważne jednak, aby zakres przetwarzanych danych był adekwatny do celu, który ma zostać osiągnięty, oraz aby nie były gromadzone dane zbędne z punktu widzenia celu ich przetwarzania.	✓ zamówienie w sklepie internetowym, ✓ skorzystanie z wybranych usług

Przetwarzanie niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze	Aby przetwarzanie na tej podstawie było w pełni legalne, konieczne jest współistnienie krajowego lub unijnego przepisu prawa nakładającego na administratora określony obowiązek. Nie jest to zatem samodzielna podstawa przetwarzania danych. W przypadku przetwarzania danych na tej podstawie prawo osoby, której dane dotyczą, do bycia zapomnianym jest wyłączone w zakresie, w jakim przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego spoczywającego na administratorze danych.	✓ przetwarzanie danych pracowników przez pracodawcę, ✓ przetwarzanie danych kontrahentów po zakończeniu współpracy z uwagi na przepisy podatkowe lub rachunkowe
Przetwarzanie niezbędne do ochrony żywotnych interesów	Przetwarzanie danych osobowych należy uznać za zgodne z prawem także wtedy, gdy jest ono niezbędne dla ochrony interesu, który ma istotne znaczenie dla ochrony życia osoby, której dane dotyczą, lub innej osoby fizycznej. Żywotny interes osoby fizycznej może stać się podstawą przetwarzania danych wyłącznie wtedy, gdy nie jest możliwe przetwarzanie na innej podstawie prawnej.	✓ przetwarzanie jest niezbędne do celów humanitarnych, ✓ przetwarzanie w celach monitorowania epidemii i ich rozprzestrzeniania się
Przetwarzanie niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi	Kolejna przesłanka stanowi podstawę przetwarzania danych osobowych w przypadku organów i podmiotów publicznych, które co do zasady działają w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. Dla zastosowania tej przesłanki, podobnie jak w przypadku przetwarzania danych w celu wypełnienia prawnego obowiązku ciążącego na administratorze, konieczne jest istnienie podstawy prawnej w przepisach prawa krajowego lub unijnego. Wystarczające jest uregulowanie prawne, które stanowi podstawę, że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej.	✓ przetwarzanie danych osobowych w związku z wykonywaniem zadań publicznych wynikających z ustaw samorządowych
Przetwarzanie niezbędne dla celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią	Przetwarzanie danych osobowych może mieć miejsce wówczas, gdy jest niezbędne dla celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub osobę trzecią. Chodzi więc o takie sytuacje, kiedy administrator nie może powołać się na zgodę osoby, której dane dotyczą, przepis bądź realizację umowy, a mimo to ma możliwość przetwarzania danych, ponieważ za dopuszczalnością przetwarzania przemawia prawnie uzasadniony interes. Aby móc powołać się na tę podstawę przetwarzania, konieczne jest kumulatywne spełnienie następujących przesłanek:	✓ przetwarzanie danych osobowych w związku z przeprowadzanym konkursem dla klientów, ✓ przetwarzanie danych osobowych klientów w celu marketingu bezpośredniego

	1) istnienie prawnie uzasadnionego interesu realizowanego przez administratora lub osobę trzecią, 2) niezbędność przetwarzania dla realizacji celu wynikającego z uzasadnionego interesu prawnego; 3) niewystępowania interesów lub podstawowych praw i wolności podmiotu danych, które mają charakter nadrzędny wobec prawnie uzasadnionych interesów administratora lub strony trzeciej. Tak więc dla możliwości przetwarzania danych na tej podstawie konieczne jest odpowiednie wyważenie dwóch prawnie chronionych dóbr. Z jednej strony prawnie uzasadnionego interesu administratora lub osoby trzeciej, a z drugiej podstawowych praw i wolności podmiotu danych. Aby jednak dokonać prawidłowej oceny, należy odpowiedzieć na pytanie, czym jest prawnie uzasadniony interes. Ustawodawstwo Unii Europejskiej nie określa zamkniętego katalogu okoliczności, które można za taki uzasadniony interes uznać. Posiłkując się jednak motywami 47-49 preambuły rozporządzenia, za taki cel można uznać m.in. cele marketingu bezpośredniego, przesyłanie danych osobowych w ramach grupy przedsiębiorstw do wewnętrznych celów administracyjnych czy przetwarzanie danych w zakresie bezwzględnie niezbędnym i proporcjonalnym do zapewnienia bezpieczeństwa sieci i informacji, ale także przetwarzanie danych w celu zapobiegania oszustwom.	

WZÓR. ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH

[...] (miejscowość), [...] data

ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH

Ja niżej podpisany/a [...], wyrażam zgodę na przetwarzanie moich danych osobowych przez [...] w celu [...].
Oświadczam, że zostałem pouczony/a o prawie do wycofania niniejszej zgody w każdym czasie, a także o tym, że wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem

.....
(podpis)

3.1. Przetwarzanie danych osobowych szczególnych kategorii

Ustawodawca europejski ustanowił generalny zakaz przetwarzania danych osobowych należących do szczególnych kategorii. Chodzi o dane dotyczące pochodzenia rasowego lub etnicznego, poglądów politycznych, przekonań religijnych lub światopoglądowych, przynależności do związków zawodowych, dane genetyczne, dane biometryczne, dane dotyczące zdrowia, seksualności lub orientacji seksualnej osoby, której dotyczą. W treści art. 9 ust. 2 RODO przewidziane zostały jednak przypadki, kiedy zakaz ten może zostać uchylony. Dotyczy to, co do zasady, sytuacji gdy:

1) osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu, o którym mowa w ust. 1;
2) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą;
3) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;
4) przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą;
5) przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;

6) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;
7) przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą;
8) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem warunków i zabezpieczeń, o których mowa w ust. 3;
9) przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową;
10) przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

W zakresie zgody na przetwarzanie danych szczególnych kategorii należy pamiętać, że prawo unijne lub prawo krajowe może przewidywać, iż nawet udzielenie zgody przez osobę, której dane dotyczą, nie uchyla zakazu przetwarzania danych należących do szczególnych kategorii. Wskazana regulacja może odnosić się na przykład do danych

osobowych szczególnej kategorii pracowników (np. w wielu przypadkach nieuprawnione będzie przetwarzanie danych biometrycznych pracowników). Z punktu widzenia administratora zgodę na przetwarzanie danych szczególnych kategorii warto uzyskać w formie pisemnej. Z jednej strony pozwala to bowiem na wykazanie, że zgoda została wyrażona w sposób wyraźny, a z drugiej strony gwarantuje wywiązanie się z zasady rozliczalności. Tworząc treść takiej zgody, należy pamiętać, że oświadczenie o „przyjęciu do wiadomości" nie może być traktowane jako udzielenie wyraźnej zgody.

WZÓR. ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH SZCZEGÓLNYCH KATEGORII

[...] (miejscowość), [...] (data)

ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH SZCZEGÓLNYCH KATEGORII

Wyrażam zgodę na przetwarzanie moich danych osobowych przez [...] (nazwa, adres oraz inne dane identyfikujące administratora np. NIP, KRS), w tym szczególnych kategorii danych osobowych dotyczących mojego zdrowia, zgodnie z warunkami przedstawionymi w informacji dla pacjenta w celu wzięcia udziału w badaniu klinicznym.

Oświadczam, że niniejsza zgoda może być odwołana w każdym czasie.

Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem.

.....
(podpis)

W zakresie przetwarzania danych szczególnych kategorii dla ochrony żywotnych interesów wskazać należy, że zgodnie z treścią motywu 46 RODO żywotny interes innej osoby fizycznej powinien być podstawą przetwarzania danych osobowych zasadniczo wyłącznie wówczas, gdy przetwarzania nie da się oprzeć na innej podstawie prawnej. Należy również pamiętać o konieczności wystąpienia warunku wprost wskazanego w przepisie art. 9 ust. 2 lit. c RODO w postaci niezdolności do wyrażenia zgody na przetwarzanie danych przez osobę, której dane dotyczą.

PRZYKŁAD

W następstwie wypadku komunikacyjnego konieczne jest przetwarzanie danych osobowych dotyczących zdrowia osoby, która ucierpiała w wypadku i nie jest w stanie wyrazić zgody. Natomiast przetwarzanie tego rodzaju danych jest niezbędne dla ratowania jej zdrowia, a nawet życia.

3.2. Publikowanie danych osobowych – przypadek DZPN

Co roku do UODO wpływa kilka tysięcy skarg na niezgodne z prawem przetwarzanie danych osobowych. Znaczna część z nich dotyczy przetwarzania danych bez odpowiedniej podstawy prawnej. Jednym z ciekawszych przypadków jest sprawa dotycząca Dolnośląskiego Związku Piłki Nożnej (dalej również jako „DZPN")[3].

Związek w lipcu 2018 r. zgłosił prezesowi UODO naruszenie ochrony danych osobowych polegające na niezamierzonej publikacji danych osobowych 585 osób, którym przyznano licencje sędziowskie w roku 2015, w zakresie imienia, nazwiska, numeru PESEL oraz adresu zamieszkania, które zostały umieszczone na stronie internetowej DZPN. W zgłoszeniu wskazano, że okres naruszeń trwał od października 2015 r. do lipca 2018 r. Jednocześnie pismem z sierpnia 2018 r. związek powiadomił UODO o zakończeniu procesu powiadamiania osób, których dane dotyczą, o naruszeniu ich danych oraz o usunięciu tego naruszenia.

W toku postępowania prezes UODO ustalił, że w związku z zakończeniem procesu przyznawania licencji sędziowskich w 2015 r., na podstawie zgłoszeń przesłanych przez kolegium sędziowskie, DZPN opublikował w październiku listę osób, którym przyznano licencje sędziowskie w roku 2015. Publikacja obejmowała: imię, nazwisko, numer PESEL oraz adres zamieszkania i została opublikowana na stronie internetowej DZPN. Następnie DZPN podjął działania mające na celu usunięcie plików z danymi oraz powiadomienie dostawców wyszukiwarek o konieczności usunięcia danych z wyników wyszukiwania. Usunięcie danych miało nastąpić w lipcu 2018 r. Pomimo teoretycznego usunięcia

[3] Decyzja prezesa Urzędu Ochrony Danych Osobowych z 25 kwietnia 2019 r., sygn. ZSPR.440.43.2019.

danych związek w styczniu 2019 r. otrzymał telefoniczną informację, że usunięte dane nadal są dostępne w jednej z wyszukiwarek internetowych, a plik z danymi wyświetla się w internecie. Po wszczęciu postępowania przez prezesa UODO związek ostatecznie i skutecznie usunął dane ze swojej strony internetowej.

Wydając decyzję, prezes UODO wskazał, że dokonując zgłoszenia DZPN miał świadomość, iż zakres danych, jaki został udostępniony na jego stronie internetowej, jest nieprawidłowy, jednak nie wdrożył odpowiednich środków technicznych i organizacyjnych, aby zapewnić odpowiedni stopień bezpieczeństwa w procesie przetwarzania tych danych, przez co dane te były dostępne na stronie internetowej również po dacie dokonania zgłoszenia. W kontekście podstawy przetwarzania danych osobowych organ wskazał natomiast, że zgodnie z art. 6 ust. lit. f RODO przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy i w takim zakresie przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem. Jednocześnie organ dostrzegł, że DZPN jako wojewódzki związek piłki nożnej jest zobowiązany do prowadzenia ewidencji przyznanych licencji i ich publikacji na stronie internetowej, co wynika wprost z § 13 uchwały Zarządu Polskiego Związku Piłki Nożnej (PZPN) z 19 kwietnia 2012 r., nr IV/74, w sprawie licencji dla sędziów piłkarskich (nr VI/90, z 13 maja 2015 r., j.t.). Jednakże zwrócił uwagę na to, że ww. uchwała nie określa zakresu danych, które powinny zostać opublikowane. Nie ma również przepisu prawa, który regulowałby tę kwestię. Dlatego też w ocenie organu przetwarzając dane osobowe DZPN powinien mieć na uwadze zasadę minimalizacji danych określoną w art. 5 ust. 1 lit. c rozporządzenia. Zgodnie z jego treścią przetwarzane dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane. W ocenie prezesa cel określony w § 13 uchwały Zarządu PZPN zostałby osiągnięty, gdyby na stronie internetowej związku udostępnione zostały dane osobowe osób, którym przyznano licencję w zakresie imienia i nazwiska oraz miejscowości zamieszkania. Natomiast udostępnianie numeru PESEL oraz adresu zamieszkania wykracza poza ten cel. Udostępnianie danych w tak

szerokim zakresie stwarza bowiem potencjalne ryzyko wykorzystania ich w celach bezprawnych, np. do zawierania stosunków prawnych lub zaciągania zobowiązań w imieniu osób, których dane ujawniono, bez ich wiedzy, a także do rozporządzania ich prawami.

Mając na uwadze to, że DZPN przetwarzał dane w postaci numeru PESEL oraz adresu zamieszkania bez podstawy prawnej oraz nie wdrożył odpowiednich środków technicznych i organizacyjnych, aby zapewnić odpowiedni stopień bezpieczeństwa w procesie przetwarzania tych danych, prezes UODO nałożył na związek karę pieniężną w wysokości 55 750,50 zł.

3.3. Podstawa prawna działań marketingowych

Działania marketingowe mogą być prowadzone przy uwzględnieniu jednej z dwóch podstaw prawnych. Pierwszą jest zgoda, czyli zgodnie z art. 6 ust. 1 lit. a RODO. Drugą jest uzasadniony interes administratora, czyli zgodnie z art. 6 ust. 1 lit. f RODO.

WAŻNE

W przypadku zgody należy pamiętać, że musi być ona wyrażona dobrowolnie, konkretnie (cel przetwarzania danych oraz zakres przetwarzania muszą być precyzyjnie określone), świadomie.

Osoba wyrażająca zgodę musi zostać pouczona oraz musi mieć zapewnione prawo do cofnięcia zgody w dowolnym momencie i to w równie łatwy sposób jak wyrażenie zgody. Cofnięcie zgody nie powoduje przy tym, że przetwarzanie danych przed cofnięciem zgody staje się niezgodne z prawem. O tej ostatniej okoliczności osoba wyrażająca zgodę powinna zostać poinformowana jeszcze przed jej wyrażeniem (por. pkt 3.3.2. Możliwość prostego wycofania zgody na przetwarzanie danych osobowych w celach marketingowych).

Odnośnie do drugiej podstawy przetwarzania, to właśnie w motywie 47 RODO ustawodawca unijny przyjął, że przetwarzanie danych osobowych do celów marketingu bezpośredniego można uznać za działanie wykonywane w prawnie uzasadnionym interesie. Wówczas nie jest wymagane zbieranie odrębnych zgód na przetwarzanie danych. Prawi-

dłowe jest samodzielne istnienie prawnie uzasadnionego interesu realizowanego przez administratora powiązanego z niezbędnością przetwarzania danych w celu jego realizacji. Co więcej, osoba, której dane dotyczą, ma prawo do złożenia sprzeciwu wobec przetwarzania jej danych osobowych.

WAŻNE

Jeżeli osoba, której dane dotyczą, wniesie sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, danych osobowych nie wolno już przetwarzać do takich celów.

3.3.1. Brak zgody na działania marketingowe – przypadek TIM S.p.A.

Jedna z najwyższych kar za złamanie przepisów RODO została nałożona przez włoski organ ochrony danych osobowych (Il Garante per la protezione dei dati personali) na spółkę telekomunikacyjną TIM S.p.A. Wysokość kary wyniosła dokładnie 27 802 946 euro, co stanowi równowartość ponad 100 mln zł. Podstawą do wszczęcia postępowania wobec spółki były setki skarg składane w okresie pomiędzy styczniem 2017 r. a początkiem roku 2019. Osoby, których dane dotyczyły, informowały organ o niezgodnych z prawem praktykach spółki polegających m.in. na telefonicznym przekazywaniu informacji marketingowych osobom, które nie wyraziły na to zgody, a także osobom, które wprost skorzystały z prawa sprzeciwu. W toku przeprowadzonego postępowania potwierdzone zostały nieprawidłowości wskazywane w skargach. Ustalono między innymi, że z jednym numerem telefonu pracownicy spółki kontaktowali się do 155 razy w miesiącu. Nie zważano przy tym na wpisy osób, do których dzwoniono, w publicznym rejestrze sprzeciwów. Tym samym spółka przetwarzała dane osobowe bez podstawy prawnej.

Organ wykrył także wiele innych nieprawidłowości, polegających m.in. na uzależnianiu udziału w programie promocyjnym od wyrażenia zgody na przetwarzanie danych także w innych celach, czy zbieranie na jednym formularzu zgody na różne cele, a także wykorzystywanie danych niezgodnie z celem, dla którego zostały pobrane. Wątpliwości

budziła również realizacja obowiązku informacyjnego przez operatora. Informacje przekazywane podmiotom danych były niejasne, a co za tym idzie, nie spełniały wymogów stawianych przez RODO. Ujawniono także nieprawidłowości w kontekście procedur związanych z naruszeniem danych osobowych oraz systemów mających na celu zabezpieczenie danych. Uchybienia znaleziono także w zakresie czarnych list, a więc list podmiotów, które nie wyrażały zgody na kontakt telefoniczny. Jedynie część kontaktów znajdujących się na listach partnerów spółki znalazła się na czarnej liście TIM S.p.A. W efekcie część osób nadal otrzymywała telefony, pomimo że nie wyrażała na to zgody. Warto zaznaczyć, że rozbieżności te dotyczyły setek tysięcy numerów. Przeprowadzone postępowanie wykazało również inne uchybienia spółki, takie jak np. brak jasno wyrażonych okresów przechowywania danych.

Na wysokość kary z pewnością złożyła się liczba naruszeń, których dopuściła się spółka, jednakże ogromne znaczenie miało również to, że uchybienia dotyczyły milionów osób, których danymi ona dysponowała. Organ nadzoru, korzystając ze swoich uprawnień, obok kary pieniężnej zastosował wobec firmy również środki naprawcze, o których mowa w art. 58 RODO. W celu zapewnienia możliwości realizacji uprawnień przez osoby, których dane dotyczyły, organ nakazał wdrożenie adekwatnych środków technicznych i organizacyjnych przez spółkę. Chcąc umożliwić efektywne reagowanie na potencjalne naruszenia w przyszłości, organ wskazał również na konieczność implementacji procedury organizacyjnej, która je umożliwi.

3.3.2. Możliwość prostego wycofania zgody na przetwarzanie danych osobowych w celach marketingowych

O tym, że znaczenie problemu ochrony danych osobowych osób fizycznych w państwach należących do Unii Europejskiej jest doniosłe, nikogo nie trzeba dzisiaj przekonywać. Ochrona każdej osoby fizycznej w związku z przetwarzaniem jej danych osobowych należy do praw podstawowych tej osoby. Znajduje to swoje odzwierciedlenie w treści art. 8 ust. 1 Karty praw podstawowych Unii Europejskiej oraz w art. 16 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej. Podstawowym sposobem zapewnienia przedmiotowej ochrony jest wprowadzenie na mocy ogólnego rozporządzenia o ochronie danych zasady przetwarzania danych osobowych wyłącznie na odpowiedniej podstawie prawnej. Zgodnie z rozporządzeniem RODO przetwarzanie danych osobowych

zgodnie z prawem nie jest możliwe, jeżeli nie jest spełniony przynajmniej jeden z sześciu przewidzianych przez rozporządzenie RODO warunków uznania przetwarzania danych osobowych za zgodne z prawem. Jak pokazuje praktyka, istotną częścią problematyki związanej z przetwarzaniem danych osobowych na podstawie zgody osoby, której te dane dotyczą, jest niezbywalne prawo tej osoby do wycofania zgody w dowolnym momencie, co zostało zagwarantowane w art. 7 ust. 3 rozporządzenia RODO.

WAŻNE

Warto wiedzieć, że rozporządzenie RODO określa nie tylko treść prawa do wycofania zgody, lecz także sposób wykonywania tego prawa. Jak wynika z brzmienia art. 7 ust. 3 rozporządzenia RODO, wycofanie zgody na przetwarzanie danych musi być równie łatwe, jak jej wyrażenie.

Tworząc bazy danych zwierające dane osobowe pozyskane za pośrednictwem środków komunikacji elektronicznej, dość łatwo można przeoczyć subtelną różnicę między wyrażeniem „łatwe wycofanie zgody" i „wycofanie zgody równie łatwe jak jej wyrażenie". Podczas gdy sens pierwszego wyrażenia sprowadza się do konstatacji, że wycofanie zgody powinno być możliwe przez dokonanie takiego zespołu czynności, które same w sobie nie są trudne, drugie wyrażenie oznacza, że wycofanie zgody powinno być możliwe przez dokonanie takiego zespołu czynności, które nie mogą być bardziej wymagające niż zespół czynności, w wyniku których podlegająca wycofaniu zgoda została udzielona. W konsekwencji proces wycofania zgody dotyczącej przetwarzania danych osobowych podlega dwustopniowej ocenie. W pierwszym etapie ocenie podlega obiektywna prostota procesu, a więc to, czy wycofanie udzielonej zgody jest proste czy trudne, zaś w drugim etapie – istniejąca między procesem udzielenia zgody i jej wycofaniem relacja, a więc to, czy zespół czynności koniecznych do wycofania zgody jest adekwatnym odpowiednikiem zespołu czynności koniecznych do udzielenia zgody.

Można w tym miejscu zadać pytanie, czy przedsiębiorca przetwarzający dane osobowe ma bezwzględny obowiązek stosowania takich środków technicznych i organizacyjnych, które zapewnią, że proces

wycofania zgody będzie wiernym odbiciem procesu udzielenia zgody. W aktualnym stanie prawnym na takie pytanie należy odpowiedzieć negatywnie. Istotą omawianej regulacji jest bowiem wyłącznie to, aby proces wycofania zgody nie był trudniejszy od procesu udzielenia zgody. Tym samym nie ma żadnych przeszkód, aby przedsiębiorca przetwarzający dane osobowe stosował takie rozwiązania techniczne i organizacyjne, w wyniku których wycofanie zgody na przetwarzanie danych osobowych jest znacznie łatwiejsze niż jej udzielenie.

WAŻNE

Przedsiębiorca przetwarzający dane osobowe może stosować takie rozwiązania techniczne i organizacyjne, w wyniku których wycofanie zgody na przetwarzanie danych osobowych jest znacznie łatwiejsze niż jej udzielenie.

3.4. Wycofanie zgody – przypadek polskiego przedsiębiorcy

Za poświęceniem należytej uwagi problematyce wycofania zgody na przetwarzanie danych osobowych przemawia argument natury ekonomicznej. Zgodnie z treścią art. 83 ust. 5 lit. a RODO niezapewnienie przez administratora danych osobowych właściwego stopnia prostoty wycofania udzielonej zgody na przetwarzanie danych osobowych podlega administracyjnej karze pieniężnej w wysokości do 20 mln euro, a w przypadku przedsiębiorstwa – w wysokości do 4% jego całkowitego rocznego światowego obrotu. Przekonał się o tym niedawno jeden z warszawskich przedsiębiorców, który, w wyniku przeprowadzonej kontroli i stwierdzonych nieprawidłowości w zakresie umożliwienia wycofania zgody na przetwarzanie danych osobowych został ukarany przez prezesa UODO karą pieniężną w wysokości ponad 200 tys. zł[4].

Przedsiębiorca posiadał bazę danych, w której przetwarzał dane osobowe osób fizycznych między innymi w celu prowadzenia działań marketingowych realizowanych na rzecz swoich kontrahentów, wobec których przedsiębiorca dobrowolnie zobowiązał się, że zapewni osobom,

[4] Decyzja prezesa Urzędu Ochrony Danych Osobowych z 16 października 2019 r., sygn. ZSPR.421.7.2019.

do których będzie kierowana kampania marketingowa, możliwość łatwego i prostego odwołania udzielonych zgód na przetwarzanie ich danych osobowych. Od strony formalnej proces wycofania zgody nie został uporządkowany w sposób zbyt szczegółowy. Możliwość wycofania zgody miał zapewnić link, który przedsiębiorca zobowiązał się zamieścić w każdej wiadomości e-mail lub SMS, kierowanej do adresata kampanii marketingowej w ramach tej kampanii. Ponadto przedsiębiorca zobowiązał się niezwłocznie zaprzestać prowadzenia kampanii marketingowej wobec osoby, o której pozyska informację, że nie wyraża zgody na dalsze przetwarzanie jej danych osobowych bądź nie wyraża chęci uczestniczenia w danej kampanii marketingowej.

W praktyce osoba, która korzystała z przesłanego linku, oznaczonego jako „odwołanie zgody", była przekierowywana na stronę, na której zmuszona była wybrać jedną z dwóch podanych przyczyn rezygnacji z udziału w kampanii marketingowej. Brak zaznaczenia jednej z opcji uniemożliwiał kontynuację procesu wycofywania zgody na przetwarzanie danych osobowych, a co za tym idzie – jeżeli osoba nie udzieliła odpowiedzi na pytanie o powód rezygnacji z kampanii marketingowej, nie mogła przejść do kolejnego etapu procesu wycofania zgody i w konsekwencji nie mogła wycofać swojej zgody w tym trybie. Zaznaczenie jednego z powodów rezygnacji z udziału w kampanii marketingowej skutkowało przeniesieniem na kolejną stronę, na której znajdowały się dwa komunikaty – pierwszy o treści: „Pani odwołanie zgody dziś (...)!", i kolejny, zamieszczony pod pierwszym komunikatem, o treści: „Dziękuję za odpowiedź! W takiej sytuacji informuję, że przysługuje Pani prawo dostępu do danych, ich usunięcia, ograniczenia przetwarzania, przenoszenia, wniesienia sprzeciwu, żądania sprostowania oraz cofnięcia zgód w każdym czasie pod adresem (...), w tym również prawo do złożenia skargi do Prezesa Urzędu Ochrony Danych Osobowych. Z mojej strony to wszystko. (...) (...)". Zatem – choć link był oznaczony wyrażeniem „odwołanie zgody", rezultatem skorzystania z niego było w rzeczywistości jedynie uzyskanie informacji o prawach, jakie przysługują w związku z przetwarzaniem danych osobowych osobie, której dane są przetwarzane. Tak skonstruowany mechanizm wymagał więc od osoby, która chciała wycofać swoją zgodę, podjęcia dodatkowych czynności w celu skutecznego wycofania zgody na przetwarzanie danych osobowych.

Zastosowany przez przedsiębiorcę mechanizm wycofywania zgody na przetwarzanie danych osobowych został uznany przez prezesa UODO nie tylko za niezgodny z treścią przyjętego przez tego przedsiębiorcę zobowiązania do umożliwienia adresatom kampanii marketingowych rezygnacji z tych kampanii, lecz także za naruszający art. 7 ust. 3 rozporządzenia RODO. Prezes UODO zarzucił przedmiotowemu mechanizmowi przede wszystkim to, że nie spełnia on kryteriów prostego i szybkiego odwołania zgody. Jak stwierdził: przedsiębiorca stosował mechanizm, w wyniku którego pozyskanie zgody na przetwarzanie danych osobowych polegało jedynie na zaznaczeniu odpowiedniego pola w formularzu (tzw. checkbox), zaś wycofanie zgody – mimo wprowadzenia procesów sugerujących automatyzm – w praktyce wymagało samodzielnego sporządzenia oświadczenia o wycofaniu zgody na przetwarzanie danych osobowych przez osobę, której te dane dotyczą, i wysłania tego oświadczenia za pośrednictwem poczty elektronicznej na wskazany przez przedsiębiorcę adres poczty elektronicznej.

Problematyka wycofania zgody na przetwarzanie danych osobowych jest nie tylko fragmentem zagadnień związanych z legalnymi podstawami przetwarzania danych osobowych, na które zwrócono uwagę w poprzedniej części rozważań. Problematyka wycofania zgody na przetwarzanie danych osobowych jest również ściśle związana z unormowanym na mocy rozporządzenia RODO prawem do bycia zapomnianym. Zgodnie z art. 17 ust. 1 rozporządzenia RODO osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki dane osobowe usunąć, jeżeli spełnione są przewidziane w rozporządzeniu warunki. W myśl art. 17 ust. 1 lit. b obowiązek administratora danych osobowych do usunięcia danych aktualizuje się, jeżeli podstawą przetwarzania przez niego danych jest udzielona mu zgoda osoby, której te dane dotyczą, a osoba ta cofnęła swoją zgodę i nie ma innej podstawy prawnej do przetwarzania jej danych osobowych. Prawo do bycia zapomnianym korzysta w obowiązującym porządku prawnym ze szczególnej ochrony prawnej. W świetle art. 12 ust. 2 rozporządzenia RODO administrator danych osobowych jest zobowiązany ułatwić osobie, której dane osobowe przetwarza, wykonanie przysługujących jej praw, w tym także prawa do bycia zapomnianym. Tym samym należy przyjąć, że administrator danych osobowych jest odpowiedzialny nie tylko za stworzenie mechanizmów umożliwiających wycofanie zgody

w sposób równie łatwy jak sposób jej wyrażenia, lecz także jest zobowiązany do współdziałania z osobą, której dane osobowe przetwarza, w zakresie wykonywania przez tę osobę praw przysługujących jej na mocy rozporządzenia RODO, w tym prawa do wycofania zgody na przetwarzanie jej danych.

WAŻNE

Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki dane osobowe usunąć, jeżeli spełnione są przewidziane w rozporządzeniu RODO warunki.

W analizowanym przypadku przedsiębiorca nie tylko nie przewidział wystarczająco prostych mechanizmów wycofywania zgody na przetwarzanie danych osobowych przez osoby, których te dane dotyczą, lecz także nie podejmował żadnych działań, mających na celu ułatwienie osobom, których dane przetwarzał, skorzystania z przysługujących im praw. Uchybienie w tym zakresie polegało na tym, że przedsiębiorca pozostawiał bez rozpoznania wpływające do niego e-maile, jeżeli nie zawierały one treści żądania dotyczącego danych osobowych.

Brak treści e-maila powodował, że wniosek dotyczący przetwarzania danych osobowych był niekompletny – i co za tym idzie – nieskuteczny, o czym jednak przedsiębiorca nie informował osób, które przedmiotowe wnioski składały, mimo iż dysponował ich adresami poczty elektronicznej. W ocenie prezesa UODO działanie takie stanowiło naruszenie obowiązków administratora danych osobowych wynikających z art. 12 ust. 2 rozporządzenia RODO. Jak podkreślił prezes UODO administrator powinien był w tej sytuacji podjąć działania zmierzające do ustalenia, jakie prawo w zakresie ochrony danych osobowych zamierza wykonać osoba, której dotyczą dane podane w e-mailu, oraz wskazać, w jaki sposób osoba ta może dane prawo wykonać.

Obowiązek administratora danych osobowych do ułatwienia wykonywania praw przez osobę, której dane dotyczą, nie wyczerpuje się jedynie w nakazie współdziałania z tą osobą.

WAŻNE

Na podstawie art. 24 ust. 1 rozporządzenia RODO administrator danych osobowych jest zobowiązany wdrożyć takie środki techniczne i organizacyjne, które zapewnią przetwarzanie danych osobowych zgodnie z przepisami rozporządzenia RODO. Co więcej, to na administratorze danych ciąży obowiązek wykazania, że stosowane środki techniczne i organizacyjne są odpowiednie.

Tym samym administrator danych osobowych jest odpowiedzialny za wdrożenie takiego mechanizmu, który umożliwi przekazanie osobie, której dane osobowe są przetwarzane, łatwo dostępnej, zwięzłej, przejrzystej i zrozumiałej informacji o możliwości skutecznego wycofania zgody na przetwarzanie danych osobowych. Istotą takiego rozwiązania jest to, aby osoba, której dane osobowe są przetwarzane, mogła w dowolnym momencie skutecznie skorzystać ze swojego prawa do wycofania udzielonej zgody oraz do prawa bycia zapomnianym, dlatego też administrator odpowiada za stosowanie odpowiednich środków technicznych i organizacyjnych nie tylko w ramach swojej działalności, lecz także w ramach działalności innych podmiotów zaangażowanych w proces przetwarzania danych osobowych.

Na koniec omawiania tej sprawy warto się jeszcze przyjrzeć uzasadnieniu decyzji o nałożeniu na przedsiębiorcę kary administracyjnej, w którym prezes UODO stwierdził, że wskazane naruszenia mają charakter umyślny. Jak podkreślił organ, ze sporządzonych przez przedsiębiorcę dokumentów jednoznacznie wynika, że przedsiębiorca posiadał wiedzę o tym, że proces odwołania zgody na przetwarzanie danych osobowych powinien być łatwy i przebiegać w sposób prosty i skuteczny. Jednak mimo to zastosowany mechanizm nie uwzględniał wymogów, jakie przed administratorem danych osobowych stawia rozporządzenie RODO. W tej sytuacji trafna wydaje się konstatacja, że każdy przedsiębiorca, który jest administratorem danych osobowych, powinien dołożyć należytej staranności nie tylko w zakresie sporządzenia dokumentacji, która będzie czynić zadość przewidzianym w prawie wymogom formalnym, lecz także w zakresie zaprojektowania procesów, które zapewnią realizację obowiązków administratora danych także w aspekcie praktycznym.

3.5. Podstawy prawne przetwarzania danych osobowych w przypadku monitoringu

Rozwój nowych technologii powoduje, że koszty zakupu, montażu i eksploatacji systemu kamer i rejestratorów nagrań nie stanowią dużego wydatku. Urządzenia takie stają się coraz bardziej precyzyjne i umożliwiają nawet zdalne i w czasie rzeczywistym obserwowanie objętego nimi obszaru. Dzięki temu monitoring wizyjny stał się jednym z najczęściej stosowanych sposobów mających służyć podwyższeniu bezpieczeństwa.

Filmowanie określonego obszaru, na którym znajdują się ludzie, będzie przedmiotem podlegającym regulacjom przepisów o ochronie danych osobowych. Przypomnijmy, że zgodnie z art. 4 pkt 1 RODO dane osobowe oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Możliwą do zidentyfikowania osobą jest natomiast osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej. Nie ma wątpliwości, że celem stosowania monitoringu jest właśnie identyfikacja, a utrwalony na nagraniu z kamer wizerunek osoby pozwala na określenie jej cech fizycznych i w ten sposób staje się formą przetwarzania danych osobowych. Co więcej, prezes UODO określił monitoring jako jedną z najbardziej inwazyjnych form przetwarzania danych osobowych, a jego stosowanie zalecił ograniczać jedynie do sytuacji, kiedy nie istnieją inne, mniej ingerujące w prywatność środki umożliwiające zapewnienie bezpieczeństwa

WAŻNE

Dane osobowe mogą mieć zatem formę nie tylko słowną, ale również postać obrazu.

Skoro zatem wizerunek osoby uchwyconej przez kamerę stanowi dane osobowe, przetwarzając takie nagranie należy postępować zgodnie z zasadami określonymi w przepisach o ochronie danych osobowych. W szczególności zgodnie z zasadą integralności i poufności administra-

tor musi zapewnić, by przetwarzanie odbywało się przy zastosowaniu odpowiednich do sposobu przetwarzania danych środków bezpieczeństwa, w tym zawęzić dostęp do danych z monitoringu wyłącznie do kręgu osób, które tego dostępu potrzebują, np. w związku z wykonywaniem obowiązków służbowych, oraz aby osoby te zobowiązane zostały do zachowania poufności.

Podstawy prawne dla przetwarzania danych osobowych w związku z instalowaniem kamer i rejestrowaniem danych będą inne w zależności od tego, czy dane zbiera podmiot publiczny czy osoba prywatna. Dla podmiotów prywatnych podstawy takiej należy poszukiwać w art. 6 ust. 1 lit. f RODO, chodzi więc o prawnie uzasadniony interes administratora. W tym przypadku uzasadnionym interesem będzie przede wszystkim ochrona osób i mienia. Uznanie takiej ochrony za uzasadniony interes potwierdził w swoim stanowisku Trybunał Sprawiedliwości UE (wyrok z 11 grudnia 2014 r. w sprawie C-212/13 Ryneš).

WAŻNE

Monitoring wizyjny odnosi się do rejestrowania obrazu (wizja), a nie dźwięku (fonia). Wykorzystywanie mikrofonów może okazać się nie tylko nadmiarową formą przetwarzania danych osobowych, ale również procederem nielegalnym wiążącym się z odpowiedzialnością administracyjną i cywilną, a nawet karną. Uprawnienie do nagrywania dźwięku posiadają jedynie służby porządkowe i specjalne.

Zgodnie z motywem 47 RODO prawnie uzasadniony interes administratora nie powinien mieć jednak zastosowania jako podstawa prawna do przetwarzania danych, którego dokonują organy publiczne w ramach realizacji swoich zadań. Dlatego też w przypadku podmiotów publicznych oraz podmiotów prywatnych realizujących zadania publiczne muszą opierać się na przepisach dopuszczających albo nakazujących taką formę wykonywania ich zadań. Podstawę instalacji kamer stanowić tu może:

- art. 6 ust. 1 lit. c RODO – w przypadku, gdy przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze (ma zastosowanie, jeśli odrębny przepis prawa jasno wskazuje taki obowiązek) lub

- art. 6 ust. 1 lit. e RODO – przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

3.5.1. Monitoring w szkole

Na przykład monitoring wizyjny w szkole w Polsce znajdzie swoje uzasadnienie w art. 6 ust. 1 lit. e RODO w związku z art. 108a ustawy – Prawo oświatowe, jeżeli jest to niezbędne do zapewnienia bezpieczeństwa uczniów i pracowników lub ochrony mienia. Decyzję taką może podjąć dyrektor szkoły lub placówki, w uzgodnieniu z organem prowadzącym szkołę lub placówkę oraz po przeprowadzeniu konsultacji z radą pedagogiczną, radą rodziców i samorządem uczniowskim.

Dyrektor powinien poinformować uczniów i pracowników szkoły o wprowadzeniu monitoringu w sposób przyjęty w danej szkole, nie później niż 14 dni przed uruchomieniem monitoringu. W przypadku wprowadzenia monitoringu dyrektor szkoły oznacza pomieszczenia i teren monitorowany w sposób widoczny i czytelny, za pomocą odpowiednich znaków lub ogłoszeń dźwiękowych, nie później niż dzień przed jego uruchomieniem.

Monitoring może dotyczyć nadzoru nad pomieszczeniami szkoły lub terenem wokół szkoły. Monitoring nie powinien jednak stanowić środka nadzoru nad jakością wykonywania pracy przez pracowników szkoły.

Tabela. Zakaz stosowania monitoringu w szkole i placówkach oświatowych

Monitoring nie może być stosowany w szkole i placówkach oświatowych w pomieszczeniach:		
A	w których odbywają się zajęcia dydaktyczne, wychowawcze i opiekuńcze	chyba że stosowanie monitoringu w tych pomieszczeniach jest niezbędne ze względu na istniejące zagrożenie dla realizacji bezpieczeństwa osób lub ochrony mienia i nie naruszy to godności oraz innych dóbr osobistych uczniów, pracowników i innych osób, w szczególności zostaną zastosowane techniki uniemożliwiające rozpoznanie przebywających w tych pomieszczeniach osób.
B	w których uczniom jest udzielana pomoc psychologiczno-pedagogiczna	
C	przeznaczonych do odpoczynku i rekreacji pracowników	
D	sanitarnohigienicznych	
E	gabinetu profilaktyki zdrowotnej	
F	szatni i przebieralni	

Nagrania obrazu zawierające dane osobowe uczniów, pracowników i innych osób, których w wyniku tych nagrań można zidentyfikować, szkoła lub placówka przetwarza wyłącznie do celów, dla których zostały zebrane, i przechowuje przez okres nie dłuższy niż 3 miesiące od dnia nagrania. Po upływie tego okresu uzyskane w wyniku monitoringu nagrania obrazu zawierające dane osobowe uczniów, pracowników i innych osób, które w wyniku tych nagrań można zidentyfikować, podlegają zniszczeniu, o ile przepisy odrębne nie stanowią inaczej.

Czy można jednak korzystać z monitoringu wizyjnego w szkole, by dbać nie tylko o bezpieczeństwo, ale np. sprawdzać obecność uczniów? Takie nowoczesne narzędzie wprowadziła do testów gmina Skellefteå w Szwecji. Rejestrator nagrań wizyjnych z kamer był połączony z systemem rozpoznawania twarzy w celu monitorowania frekwencji uczniów w szkole. Miało to w zamyśle rozładować pracę nauczycieli, którzy poświęcali łącznie blisko 17 tys. godzin rocznie na kontrolę obecności uczniów. System był testowany przez ponad trzy tygodnie i obejmował 22 uczniów jednej z klas, którzy wyrazili zgody na takie przetwarzanie ich danych. Szwedzki Datainspektionen (odpowiednik polskiego UODO) nie podzielił entuzjazmu nowatorskiej gminy i nałożył na nią karę, o czym szerzej w 3.6.1. Przypadek szwedzkiej szkoły.

3.5.2. Monitoring w miejscu pracy

Pracodawca jest uprawniony do stosowania wizyjnego systemu dozoru w zakładzie pracy, jednak nie może go wykorzystywać jako środka nadzoru nad realizacją zadań pracowników. Pracodawcy mogą zdecydować się na nadzór wizyjny, jeżeli służy on do zapewnienia bezpieczeństwa pracownikom, ochrony mienia lub kontroli produkcji, a także jeśli jest niezbędny do zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę. Pracodawca zobowiązany jest zadbać o to, by cel, zakres oraz sposób zastosowania monitoringu wizyjnego ustalony został w układzie zbiorowym pracy lub w regulaminie pracy albo w obwieszczeniu, jeżeli pracodawca nie jest objęty układem zbiorowym pracy lub nie jest obowiązany do ustalenia regulaminu pracy. W przypadku pracowników, który zostali już dopuszczeni do pracy, pracodawca powinien poinformować ich o zamiarze wprowadzenia monitoringu w sposób przyjęty u danego pracodawcy, nie później niż 2 tygodnie przed jego uruchomieniem. W przypadku nowych pracowników realizacja tego obowiązku powinna nastąpić przed dopuszczeniem ich do pracy.

Tabela. Zakaz stosowania monitoringu w zakładzie pracy

Monitoring w zakładzie pracy nie może obejmować:		
A	pomieszczeń sanitarnych[5]	chyba że stosowanie monitoringu w tych pomieszczeniach jest niezbędne do realizacji celu przetwarzania i nie naruszy to godności oraz innych dóbr osobistych pracownika, w szczególności poprzez zastosowanie technik uniemożliwiających rozpoznanie przebywających w tych pomieszczeniach osób.
B	szatni	
C	stołówek	
D	palarni	
E	pomieszczeń udostępnianych zakładowej organizacji związkowej	

Pracodawca nie powinien dopuszczać do przetwarzania danych z kamer w innych celach niż tylko te, dla których dane owe zostały zebrane. Oznacza to, że pracodawca nie może na podstawie nagrań z monitoringu np. wyciągać konsekwencji w stosunku do pracowników za sposób, w jaki wykonują swoją pracę.

Nagrania z monitoringu powinny być, zgodnie z kodeksem pracy, przechowywane przez okres nieprzekraczający 3 miesięcy liczony od dnia nagrania. W przypadku, kiedy nagrania obrazu stanowią dowód w postępowaniu prowadzonym na podstawie prawa lub pracodawca powziął wiadomość, iż mogą one stanowić dowód w takim postępowaniu, termin ten ulega przedłużeniu do czasu prawomocnego zakończenia postępowania. Po upływie czasu dozwolonego przetwarzania uzyskane w wyniku monitoringu nagrania obrazu zawierające dane osobowe podlegają zniszczeniu, chyba że konkretne przepisy odrębne stanowią inaczej.

WZÓR. OBWIESZCZENIE O WPROWADZENIU MONITORINGU WIZYJNEGO

OBWIESZCZENIE O WPROWADZENIU MONITORINGU WIZYJNEGO

Z dniem (dzień, miesiąc, rok) na podstawie przepisu art. 22^2 ustawy – Kodeks pracy wprowadza się na terenie przedsiębiorstwa [nazwa] techniczne środki bezpieczeństwa umożliwiające rejestrację obrazu na terenie zakładu pracy oraz wokół zakładu pracy, tj. monitoring wizyjny w celu:

[5] Monitoring pomieszczeń sanitarnych wymaga uzyskania uprzedniej zgody zakładowej organizacji związkowej, a jeżeli u pracodawcy nie działa zakładowa organizacja związkowa – uprzedniej zgody przedstawicieli pracowników wybranych w trybie przyjętym u danego pracodawcy.

1) zapewnienia bezpieczeństwa pracowników oraz współpracowników pracodawcy,
2) ochrony mienia pracodawcy,
3) zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę.

I. Zakres monitoringu

1. Monitoring wizyjny polegający na rejestrowaniu obrazu przez zamontowane w zakładzie pracy kamery przemysłowe i inne podobne urządzenia, obejmuje następujące pomieszczenia: (...).
2. Monitoring nie obejmuje pomieszczeń sanitarnych, szatni, stołówek oraz palarni, chyba że stosowanie monitoringu w tych pomieszczeniach jest niezbędne do realizacji celów wyżej określonych i nie narusza godności oraz innych dóbr osobistych pracownika, w szczególności poprzez zastosowanie technik uniemożliwiających rozpoznanie przebywających w tych pomieszczeniach osób.
3. Monitoring nie obejmuje pomieszczeń udostępnianych zakładowej organizacji związkowej, jeżeli taka będzie funkcjonować.

II. Czas przechowywania danych

1. Nagrania obrazu pracodawca przetwarza wyłącznie do celów, dla których zostały zebrane, i przechowuje przez okres nieprzekraczający trzech miesięcy od dnia nagrania.
2. W przypadku, kiedy nagrania obrazu stanowią dowód w postępowaniu prowadzonym na podstawie prawa lub pracodawca powziął wiadomość, iż mogą one stanowić dowód w postępowaniu, termin przechowywania ulega przedłużeniu do czasu prawomocnego zakończenia postępowania.
3. Po upływie okresu przechowywania uzyskane w wyniku monitoringu nagrania obrazu zawierające dane osobowe podlegają zniszczeniu, o ile przepisy odrębne nie stanowią inaczej.

III. Wewnętrzna regulacja monitoringu

1. Urządzenia rejestrujące obraz znajdują się w wyłącznej dyspozycji pracodawcy.
2. Do przeglądania zarejestrowanego obrazu oraz do kontroli urządzeń rejestrujących obraz mogą zostać jedynie upoważnione przez pracodawcę osoby. Osoby wyznaczone otrzymują imienne upoważnienia do czynności związanych z monitoringiem i nadzorem nad urządzeniami.
3. Wejścia do budynków oraz pomieszczenia objęte monitoringiem są oznakowane tablicami z rysunkiem kamery i napisem „Teren monitorowany" lub „Pomieszczenie monitorowane". Tablica może znajdować się nad drzwiami wejściowymi do określonych pomieszczeń.

IV. Prawa osób objętych monitoringiem

1. Dane zarejestrowane na nośniku podlegają ochronie, nie stanowią informacji publicznej, są informacjami poufnymi w rozumieniu ochrony danych osobowych oraz informacji objętych prawem tajemnicy przedsiębiorstwa, i nie podlegają udostępnieniu nieuprawnionym podmiotom.
2. Dane zarejestrowane na nośniku przetwarzane są w celu prowadzenia wewnętrznych postępowań wyjaśniających oraz mogą być udostępniane wyłącznie upoważnionym instytucjom w zakresie prowadzonych przez nie spraw czy postępowań (np. Policji, sądom, prokuraturom oraz innym podmiotom prowadzącym czynności dochodzeniowo-śledcze) na podstawie pisemnego wniosku.

3. Osoby biorące udział w zdarzeniach zarejestrowanych w systemie monitoringu mogą wnioskować do pracodawcy o zabezpieczenie nagrania w celu przekazania uprawnionym organom.

V. Pozostałe zagadnienia

1. Zasady monitoringu wizyjnego wprowadzone zostają niniejszym obwieszczeniem.
2. Obwieszczenie wchodzi w życie po upływie dwóch tygodni od podania go pracownikom do wiadomości w sposób zwyczajowo przyjęty u pracodawcy (rozesłanie na imienne firmowe adresy poczty elektronicznej oraz wyłożenie w siedzibie pracodawcy do wglądu i kopiowania w razie potrzeb przez każdego pracownika).
3. Każdy nowy pracownik przed dopuszczeniem do pracy otrzymuje niniejsze obwieszczenie na piśmie.
4. Klauzula informacyjna wymagana przepisami RODO stanowi załącznik do obwieszczenia.

O istocie informacji o stosowanym monitoringu w miejscu pracy więcej w pkt 4.4. Informacja o stosowanym monitoringu na podstawie przykładu francuskiego pracodawcy.

3.5.3. Obszar monitoringu wizyjnego

Jak już wcześniej podkreślano, rejestrowanie wizerunku poprzez system monitoringu ma służyć bezpieczeństwu osób i mienia. Nie bez znaczenia jest zatem, w jaki sposób skierowane zostaną kamery i jaki obraz obejmą swoim zasięgiem. Pamiętamy bowiem, że zgodnie z zasadą minimalizacji danych określoną w art. 5 ust. 1 lit. a RODO, dane osobowe powinny być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane.

O ile podmioty publiczne w związku z realizowaniem swoich ustawowych obowiązków lub zadań mogą dokonywać rejestrowania zdarzeń na terenach ogólnodostępnych, to monitoring prowadzony przez podmioty prywatne nie powinien dotyczyć filmowania przestrzeni publicznej lub miejsc, które pozostają poza racjonalnie wymaganą kontrolą czy ochroną administratora danych osobowych.

W grudniu 2018 r. austriacki odpowiednik UODO nałożył grzywnę w wysokości 2200 euro na mieszkańca pewnego kompleksu apartamentowego, który korzystał z monitoringu wizyjnego. Warto w tym miejscu zaznaczyć, że przepisy o ochronie danych osobowych nie mają zastosowania do przetwarzania danych przez osoby fizyczne w celach o czysto osobistym lub domowym charakterze.

W praktyce oznacza to, że RODO nie znajdzie zatem zastosowania do monitoringu własnej posesji przez osobę fizyczną. Jednakże system

wideo wprowadzony przez ukaranego mieszkańca obejmował obszary przeznaczone do ogólnego użytku mieszkańców kompleksu mieszkalnego, w tym: parkingi, chodniki, dziedziniec, ogród i obszary dostępu do budynków, a nawet ogródki przylegającej nieruchomości. Ustalono, że monitoring nie został więc ograniczony tylko do własnego mieszkania. Rejestrowanie obrazu ciągów komunikacyjnych wielorodzinnego domu, utrwalanie wizerunku osób wchodzących i wychodzących z okolicznych apartamentów wykraczało poza uprawnienia osoby fizycznej i naruszało – zdaniem urzędu – osobistą przestrzeń życiową innych osób, bez zgody na rejestrowanie obrazu.

WAŻNE

Przepisy o ochronie danych osobowych nie mają zastosowania do przetwarzania danych przez osoby fizyczne w celach o czysto osobistym lub domowym charakterze.

Podobnie krytycznie austriackie władze odniosły się do przedsiębiorcy prowadzącego punkt przyjmowania zakładów bukmacherskich, który wprowadził nadzór wideo nie tylko nad swoim obiektem, ale również nad dużą częścią chodnika okalającego obiekt. Organ uznał, że nastąpiło niedozwolone monitorowanie przestrzeni publicznej na dużą skalę i ukarał przedsiębiorcę karą 4800 euro. Podobne kary nakładał hiszpański i francuski odpowiednik UODO, a ich przedmiotem było za każdym razem nadmiarowe śledzenie okiem kamer obszaru publicznego, zupełnie zbędnie do celów zapewnienia bezpieczeństwa administratora danych.

Czy oznacza to, że przestrzeń wokół obiektu prywatnego nie powinna być w żadnym wypadku pod obserwacją kamer? Nie należy wysnuwać aż tak kategorycznego wniosku. W określonych przypadkach ustawienie kamer w taki sposób, by rejestrowały obraz wykraczający poza własny obiekt i filmujący także fragment przestrzeni publicznej może być konieczne do zapewnienia bezpieczeństwa. Przykładem takiego przetwarzania jest filmowanie miejsca znajdującego się tuż przed witryną sklepu, jeżeli istnieje ryzyko kradzieży przedmiotów z wystawy. Ponieważ takiej kradzieży można dokonać z zewnątrz sklepu, identyfikacja sprawcy kradzieży byłaby niemożliwa, gdyby monitoring obejmował

wyłącznie przestrzeń sklepu. Aby jednak ustalić, że takie działanie jest niezbędne, warto jest przeprowadzić ocenę skutków takiego przetwarzania dla ochrony danych zgodnie z art. 35 ust. 3 lit. c RODO[6].

Podstawowym prawem osób, których dane są przetwarzane w ramach monitoringu, jest uzyskanie informacji wynikających z art. 13 RODO, w tym informacji o fakcie filmowania ich wizerunku, o osobie administratora danych, o celu, w jakim dane będą wykorzystywane, okresie przechowywania danych czy ich odbiorcach. Prezes UODO dopuszcza udzielenie tej informacji w sposób warstwowy: pierwszą warstwę informacji stanowi krótka informacja umieszczona w miejscach objętych monitoringiem, również w formie piktogramu. Informacja powinna być wyraźnie widoczna dla osób objętych monitoringiem. Druga warstwa informacji stanowi już pełną realizację obowiązku informacyjnego z art. 13 RODO, powinna być łatwo dostępna dla osób odwiedzających obiekt np. w punkcie ochrony czy stronie internetowej. Brak informacji o stosowaniu monitoringu wizyjnego był przedmiotem wielu kar nakładanych przez urzędy ochrony danych osobowych, m.in. we Francji i w Austrii.

Osoba monitorowana ma ponadto prawo żądania dostępu do danych z monitoringu, które jej dotyczą. Warto przy tym zwrócić uwagę na to, że prawo to musi być realizowane z poszanowaniem praw innych osób, których wizerunki zostały utrwalone wraz z wizerunkiem osoby, która domaga się dostępu do danych. W grudniu 2018 r. węgierski odpowiednik UODO nałożył karę w wysokości 3200 euro za 1) nieudzielenie podmiotowi danych nagrań z monitoringu wizyjnego; 2) niezatrzymywanie nagrań do dalszego wykorzystania przez osobę, której dane dotyczą, oraz 3) niepoinformowanie osoby, której dane dotyczą, o prawie do złożenia skargi do organu nadzorczego.

3.6. Przetwarzanie danych szczególnych kategorii a niezbędność celu

Ustawodawca unijny przewidział dziesięć podstaw legalizujących przetwarzanie danych osobowych szczególnych kategorii. Jedną z najczęściej spotykanych jest zgoda osoby, której dane dotyczą. Jednak na-

[6] Zgodnie z komunikatem prezesa UODO z 17 sierpnia 2018 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony wprowadzenie monitoringu wizyjnego, w których obraz jest nagrywany i wykorzystywany tylko na potrzeby analizy incydentów naruszeń prawa, nie wymaga dokonywania oceny skutków przetwarzania dla ochrony danych osobowych.

leży pamiętać, że prawo unijne lub prawo krajowe może przewidywać, iż nawet udzielenie zgody przez osobę, której dane dotyczą, nie uchyla zakazu przetwarzania danych szczególnych kategorii.

3.6.1. Przypadek szwedzkiej szkoły

Szwedzki organ ochrony danych (Datainspektionen) przeprowadził audyt na okoliczność gromadzenia i przetwarzania danych osobowych po otrzymaniu medialnych doniesień, że rada szkolna gminy Skellefteå w ramach prowadzonego projektu w szkole średniej Anderstorps wykorzystała technologię rozpoznawania twarzy do rejestracji obecności uczniów przez kilka tygodni.

Rada szkoły wykorzystała oprogramowanie do rozpoznawania twarzy za pomocą kamery, aby zarejestrować udział 22 uczniów w zajęciach. W dalszych krokach planowane było wdrożenie tej technologii na stałe. U podstaw wdrożenia tego rozwiązania leżało dalsze usprawnienie i automatyzacja prowadzenia rejestru obecności uczniów poszczególnych klas, albowiem zadanie to zwykle zajmuje nauczycielom 10 minut na klasę. Rada twierdziła, że automatyzacja rejestrów klasowych pozwoliłaby zaoszczędzić 17 280 godzin pracy każdego roku w szkole.

Dane biometryczne zostały przechwycone przez kamery w postaci zdjęć twarzy uczniów, a później dopasowane do ich pełnych nazwisk. Informacje były przechowywane na lokalnym komputerze bez połączenia z internetem, który był przechowywany w zamkniętej szafce. Uzyskano wyraźną zgodę od opiekunów na przetwarzanie biometrycznych danych osobowych uczniów i można było powstrzymać się od wzięcia udziału w rozprawie. Nie przeprowadzono jednak oceny ryzyka ani wcześniejszych konsultacji ze szwedzkim organem ochrony danych. 20 sierpnia 2019 r. szwedzki organ ochrony danych nałożył na szkołę grzywnę w wysokości 200 tys. koron (82 tys. zł), pierwszą grzywnę na podstawie RODO i wydał ostrzeżenie przed dalszym przetwarzaniem danych osobowych.

W swoim orzeczeniu szwedzki organ ochrony danych stwierdził, że szkoła naruszyła przepisy RODO w trzech zakresach:

1) naruszenie podstawowych zasad art. 5 poprzez przetwarzanie danych osobowych w bardziej inwazyjny sposób niż to konieczne w stosunku do celu (obecności),

2) art. 9 poprzez przetwarzanie danych osobowych szczególnych kategorii (dane biometryczne) bez podstawy prawnej,
3) art. 35 i 36 poprzez niespełnienie wymogów oceny wpływu na ochronę danych i uprzednich konsultacji.

Artykuł 9 ust. 1 RODO stanowi o przetwarzaniu biometrycznych danych osobowych w celu jednoznacznej identyfikacji osoby fizycznej. Punktem wyjścia jest to, że zabrania się wykorzystywania takich wrażliwych informacji. Do przetwarzania danych osobowych szczególnych kategorii musi mieć zastosowanie wyjątek od zakazu określonego w art. 9 ust. 2 RODO (patrz rozdział 3).

Jak stwierdzono powyżej, rada szkoły potwierdziła, że opiekunowie wyrazili zgodę na zbieranie wizerunków uczniów w związku z ich bieżącym przetwarzaniem. Jednak szwedzki organ ochrony danych podkreślił znaczącą nierówność w relacjach między radą szkoły a uczniami oraz fakt, że zapisy obecności są jednostronnym środkiem kontroli. Dlatego szwedzki organ ochrony danych stwierdził, że zgody nie można wykorzystać jako podstawy prawnej, ponieważ zgody nie można uznać za dobrowolną.

WAŻNE

Zgoda nie może zatem zostać wykorzystana jako wyjątek od zakazu wykorzystywania danych osobowych szczególnych kategorii w rozpatrywanej sprawie.

Szwedzki organ ochrony danych stwierdził również, że zarządzanie rejestrami obecności nie jest działaniem niezbędnym i nie jest konieczne w istotnym interesie publicznym.

Naruszenie art. 35 i 36 RODO: ocena wpływu na ochronę danych i wcześniejsze konsultacje

Rada szkolna dokonała pewnego rodzaju oceny ryzyka, w której stwierdziła, że bezpieczeństwo i podstawa prawna (zgoda i interes publiczny) doprowadziły do podjęcia decyzji, że nie ma wysokiego ryzyka naruszenia interesów osób, których dane dotyczą. Nie przeprowadzono jednak oceny wpływu eksperymentu na ochronę danych osobowych. Szwedzki or-

gan ochrony danych stwierdził, że ocena ryzyka przeprowadzona przez zarząd szkoły nie zawiera oceny ryzyka, jakie istnieje dla praw i wolności osób, których dane dotyczą, a także oceny proporcjonalności przetwarzania w stosunku do jego celów. Zatem wymogi art. 35 nie zostały spełnione.

Grzywna

Niewątpliwie stwierdzić należy, że grzywna w wysokości 200 tys. koron (82 tys. zł) może nie wydawać się surowa w porównaniu do grzywien wymierzanych w sektorze prywatnym. Należy jednak pamiętać, że maksymalny poziom grzywien w sektorze publicznym został ograniczony w Szwecji do 10 mln koron (około 4,091 mln zł). Grzywna stanowi 2% maksymalnej kwoty grzywny (ta wynosi 10 mln koron), co może oznaczać, że gdyby szkoła była w sektorze prywatnym, grzywna wyniosłaby co najmniej 4,3 mln koron (około 1,76 mln zł). Biorąc pod uwagę założenie, że szwedzki organ ochrony danych zbadał również inne potencjalne naruszenia (takie jak obowiązek informowania lub poziom bezpieczeństwa), grzywna z pewnością byłaby jeszcze wyższa.

Podkreślenia wymaga fakt, iż grzywna dotyczyła 22 uczniów rejestrowanych przez okres kilku tygodni i że odbiorca jest jednostką finansowaną z podatków, a szwedzki organ ochrony danych ustala dość wysoki standard kar za nadchodzące działania egzekucyjne.

Stanowisko Najwyższego Sądu Administracyjnego w Szwecji

Rada szkoły jest organem publicznym i dlatego zwykle będzie musiała posiadać zezwolenie na korzystanie z kamery, aby stosować nadzór w miejscach, do których społeczeństwo ma dostęp. Pytanie brzmi zatem, czy szkoła to przestrzeń, do której społeczeństwo ma dostęp. Zgodnie z orzecznictwem, szkoły zwykle nie są uważane za miejsca, do których jest ogólny dostęp, chociaż wskazać należy, iż w szkołach są strefy, do których, jak się przyjmuje, dostęp jest możliwy dla wszystkich. Przykłady takich obszarów obejmują główne wejścia i korytarze, które prowadzą do budynku. Postępowanie szwedzkiego regulatora wykazało, że uczniowie byli rejestrowani za pomocą systemu rozpoznawania twarzy za każdym razem, gdy wchodzili do klasy. Klasa nie jest uważana za miejsce ogólnodostępne.

Na podstawie informacji, które pojawiły się na temat miejsca, w którym miał miejsce nadzór, szwedzki organ ochrony danych stwierdził, że nie jest to miejsce, do którego społeczeństwo ma dostęp. Nie ma zatem

wymogu ubiegania się o zezwolenie. W ocenie organu powyższy fakt nie daje jednakże nieograniczonego prawa do nadzoru wizyjnego. Jeśli nadzór z wykorzystaniem aparatu/kamery obejmuje przetwarzanie danych osobowych, nadzór ten powinien odbywać się z poszanowaniem przepisów rozporządzenia RODO, w szczególności z zachowaniem obowiązku dostarczenia jasnych informacji dotyczących funkcjonowania systemu nadzoru i sposobu przetwarzania danych.

3.6.2. Przypadek gdańskiej szkoły

Szkoła Podstawowa nr 2 w Gdańsku zbierała odciski palców uczniów bez posiadania konkretnej podstawy prawnej do takich działań. Dane wykorzystywane były przy weryfikacji uczniów podczas wchodzenia na szkolną stołówkę – weryfikacja dokonanej opłaty za posiłek. Szkoła posiadała zgodę rodziców, która w zaistniałej sytuacji nie jest wystarczająca. Prezes UODO uznał działanie ze strony szkoły za środek nieproporcjonalny i jak najbardziej możliwy do zastąpienia innym. Przepisy RODO wymagają, by przetwarzanie danych osobowych było między innymi niezbędne do zrealizowania stawianego przed nim celu. W przeciwnym wypadku staje się ono bezprawne[7].

Szkoła próbowała tłumaczyć się, że co prawda pobierała odciski palców, lecz nie przetwarzała danych osobowych. Dane związane z czytnikiem odcisków palca miały być gromadzone tylko w samym czytniku. Podkreślić należy, iż zgodnie z przepisami rozporządzenia dane daktyloskopijne w takiej formie mieszczą się w definicji „danych biometrycznych" zawartej w art. 4 pkt 14 RODO.

ART. 4 PKT 14 RODO

(...)
14) „dane biometryczne" oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne.

[7] Decyzja prezesa Urzędu Ochrony Danych Osobowych z 18 lutego 2020 r., sygn. ZSZZS.440.768.2018.

Grzywna nałożona na Szkołę Podstawową nr 2 w Gdańsku wyniosła 20 tys. zł.

3.7. Podsumowanie

Dane osobowe można przetwarzać wyłącznie w określonych przypadkach i z uwzględnieniem zasad wynikających z przepisów prawa. Biorąc pod uwagę wytyczne oraz przepisy RODO, do każdej operacji przetwarzania danych osobowych niezbędne jest posiadanie odpowiedniej podstawy prawnej. Należy przy tym pamiętać, że nie chodzi o to, aby posiadać do takiej każdej operacji zgodę od osoby, której dane dotyczą. Nie zawsze bowiem zgoda jest prawidłową podstawą, a co więcej, czasem żadna z podstaw nie uzasadnia przetwarzania określonych danych osobowych w określonym celu.

Podstawy prawne ustawodawca ujął w przepisie art. 6 ust. 1 RODO – jeśli chodzi o dane osobowe zwykłe, a także w przepisie art. 9 ust. 2 RODO – jeśli chodzi o dane osobowe szczególnych kategorii. Każdorazowo w sposób indywidualny należy oceniać dopuszczalność przetwarzania danych osobowych, biorąc pod uwagę dane okoliczności oraz cele przetwarzania.

Rozdział 4.
Obowiązek informacyjny

Już w preambule do RODO zawarto postulaty, by osobom fizycznym uświadomić ryzyko, zasady, zabezpieczenia i prawa związane z przetwarzaniem ich danych osobowych. Administrator musi wypełnić obowiązek informacyjny wobec osób, których dane przetwarza, aby móc legalnie przetwarzać dane osobowe. W skrócie obowiązek ten sprowadza się do poinformowania o tym, kto, na jakiej podstawie i w jakim celu zbiera dane osobowe.

Każda osoba, której dane mają być przetwarzane, ma prawo do zwięzłych, łatwo dostępnych i zrozumiałych informacji w zakresie przetwarzania jej danych osobowych. Klauzula informacyjna administratora danych osobowych powinna zawierać:

1) tożsamość i dane kontaktowe administratora oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe przedstawiciela;
2) gdy ma to zastosowanie – dane kontaktowe inspektora ochrony danych;
3) cele przetwarzania danych osobowych oraz podstawę prawną przetwarzania;
4) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f – prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią;
5) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
6) gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej;
7) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
8) informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
9) jeżeli przetwarzanie odbywa się na podstawie zgody – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu

na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
10) informacje o prawie wniesienia skargi do organu nadzorczego;
11) informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
12) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, oraz istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

WAŻNE

Obowiązek informacyjny należy wypełnić już w momencie pozyskiwania danych osobowych, a nie po ich zebraniu.

W zależności od tego, czy dane będą zbierane bezpośrednio od osoby, której dotyczą, czy też nie, obowiązek informacyjny będzie kształtował się nieco odmiennie. Wypełnienie obowiązku informacyjnego spoczywa na podmiocie, który pozyskuje dane bezpośrednio od osoby, której dane dotyczą, jak również gdy dane zostały przez niego pozyskane z innego źródła niż bezpośrednio od osoby. Wówczas administrator będzie musiał wypełnić wtórny obowiązek informacyjny, nie później niż w ciągu miesiąca po uzyskaniu danych. Analizując konieczność spełnienia odpowiednio obowiązku informacyjnego „bezpośredniego" bądź „pośredniego", wskazać należy, że zakres pozyskania informacji jest w zasadzie taki sam. Jednak przy pozyskiwaniu danych pośrednio wtórny obowiązek informacyjny dodatkowo obejmuje wskazanie źródła, z którego administrator pozyskał dane, oraz kategorii przetwarzanych danych.

Obowiązki informacyjne mają zastosowanie do wszystkich administratorów. Administrator zwolniony jest jednak z udzielania informacji, które wynikają z wypełnienia wtórnego obowiązku informacyjnego w sytuacjach, gdy:
1) osoba, od której zbiera dane, już nimi dysponuje,
2) udzielenie takich informacji jest niemożliwe lub wymaga niewspółmiernie dużego wysiłku,

3) pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem państwa członkowskiego,
4) konieczne jest zachowanie tajemnicy zawodowej.

4.1. Transparentność obowiązku informacyjnego – przypadek Google LLC

Jedną z najważniejszych zasad przetwarzania danych osobowych osób fizycznych jest zasada przejrzystości (motyw 39 RODO). Zgodnie z tą zasadą wszelkie informacje i komunikaty związane z przetwarzaniem danych osobowych powinny być łatwo dostępne i zrozumiałe, a także sformułowane jasnym i prostym językiem. Ponadto na mocy art. 12 ust. 1 RODO wszelka komunikacja dotycząca przetwarzania danych osobowych musi odbywać się z uwzględnieniem poszczególnych praw podmiotu tych danych, określonych w art. 15–22 i 34 RODO, w zależności od podstawy przetwarzania danych osobowych.

Każda osoba, której dane mają być przetwarzane, ma prawo do informacji w zakresie przetwarzania jej danych osobowych. Wszystkie informacje związane z przetwarzaniem danych osobowych powinny być zwięzłe, przejrzyste, zrozumiałe i łatwo dostępne. Nieuwzględnienie powyższych wymogów w swojej działalności naraża przedsiębiorcę na dodatkowe koszty, o czym w nieodległej przeszłości miała okazję przekonać się spółka Google LLC, na którą francuska Krajowa Komisja Ochrony Danych Osobowych (Commission Nationale de l'Informatique et des Libertés, francuski organ nadzorczy, dalej również jako „CNIL") nałożyła karę wysokości 50 mln euro.

WAŻNE

Każda osoba, której dane mają być przetwarzane, ma prawdo do informacji w zakresie przetwarzania jej danych osobowych. Wszelkie informacje i komunikaty związane z przetwarzaniem danych osobowych powinny być łatwo dostępne i zrozumiałe, a także sformułowane jasnym i prostym językiem.

W związku ze złożonymi w 2018 r. zbiorowymi skargami, które wpłynęły do CNIL w imieniu blisko 10 tys. osób fizycznych za pośrednictwem

dwóch francuskich stowarzyszeń, None of Your Business i La Quadrature du Net, przeprowadzone zostało postępowanie kontrolne. Zbadano w nim zasadność podniesionych w skargach zarzutów, dotyczących wymuszania przez Google LLC na użytkownikach urządzeń mobilnych z systemem operacyjnym Android akceptacji polityki prywatności i ogólnych warunków świadczenia usług oraz przetwarzania danych osobowych w celach związanych z analizą behawioralną i reklamą ukierunkowaną bez wymaganej przez prawo podstawy prawnej.

CNIL przyjrzała się między innymi temu, w jaki sposób Google LLC wypełnia ciążące na niej, jako administratorze danych osobowych, obowiązki w zakresie ochrony danych. Wyniki przeprowadzonej w spółce kontroli bynajmniej nie były tak imponujące, jak osiągane przez nią wyniki finansowe, bowiem CNIL stwierdziła liczne naruszenia – między innymi w postaci niewystarczającej przejrzystości informacji związanych z przetwarzaniem danych osobowych, nieprzekazywania wszystkich wymaganych przez prawo informacji oraz niezgodnego z prawem pozyskiwania zgody na przetwarzanie danych osobowych.

CNIL wypunktowała Google LLC za nienależytą realizację obowiązków informacyjnych ciążących na administratorze danych osobowych, podkreślając w szczególności praktykę formułowania niezrozumiałych komunikatów oraz praktykę realizowania obowiązków informacyjnych w formie niewystarczająco zwięzłej, która utrudnia użytkownikom dostęp do informacji, które ich dotyczą. CNIL negatywnie oceniła praktykę Google LLC, w wyniku której spółka realizowała obowiązek informacyjny związany z przetwarzaniem danych osobowych przez umieszczanie istotnych informacji w odrębnych dokumentach. Wprawdzie dokumenty te były ze sobą powiązane, bowiem spółka stosowała liczne odesłania w postaci linków, jednakże taki sposób wypełniania obowiązków informacyjnych powodował, że osoba pragnąca zrealizować swoje prawo dostępu do informacji o sposobie przetwarzania jej danych osobowych, zmuszona była samodzielnie poszukiwać relewantnych informacji, przełączając się za pomocą kliknięć między różnymi dokumentami. Jako przykład nieprawidłowo realizowanego obowiązku informacyjnego wskazano stosowany przez Google LLC mechanizm udostępniania informacji dotyczących przetwarzania danych osobowych w odniesieniu do personalizacji treści reklamowych oraz geolokalizacji. W obu przypadkach realizacja prawa dostępu do danych przez osobę, której te dane dotyczą, wymuszała na tej osobie przynajmniej kilka czynności – pię-

ciu w związku z personalizacją treści reklamowych i sześciu w związku z usługami opartymi na geolokalizacji.

Tym samym francuski organ nadzorczy zaakcentował, jak się wydaje, znaczenie kryterium zwięzłości formy, w jakiej administrator danych osobowych wypełnia ciążący na nim obowiązek informacyjny.

WAŻNE

Jednocześnie warto podkreślić, że nakaz wykonywania obowiązku informacyjnego w sposób zwięzły ma na celu nie tyle ukształtowanie praktyki zamieszczania wszystkich niezbędnych informacji w ramach jednego dokumentu czy też w ramach innej, wyraźnie wyodrębnionej jednostki redakcyjnej, ile zapewnienie osobom fizycznym rzeczywistej możliwości zapoznania się z informacjami, które dotyczą przetwarzania ich danych osobowych, zrozumienia tych informacji oraz ich znaczenia dla osoby, której one dotyczą.

Przyjęty przez CNIL sposób interpretacji przepisów RODO nie pozostawia wątpliwości, że każdy administrator danych osobowych jest odpowiedzialny za ukształtowanie takich mechanizmów informowania o przetwarzaniu danych, które umożliwiają pozyskanie pełnej informacji w sposób maksymalnie prosty, a więc redukujący do minimum poziom osobistego zaangażowania osoby fizycznej w proces realizacji przysługującego jej prawa dostępu do danych, które jej dotyczą.

W postępowaniu kontrolnym w spółce Google LLC organ nadzorczy zwrócił uwagę również na inny negatywny aspekt nadmiernego rozproszenia informacji o przetwarzaniu danych. Zgodnie z art. 15 ust. 1 RODO administrator danych osobowych ma obowiązek ujawnić informacje dotyczące przetwarzania danych osobowych, wymienione w punktach a–h tego artykułu. Przedmiotowe informacje odnoszą się zarówno do całości danych osobowych, jak i do ich części, przetwarzanej na przykład w związku z określoną usługą. Umieszczenie wszystkich wymaganych danych osobowych w ramach jednego dokumentu zwiększa prawdopodobieństwo poprawnej realizacji obowiązku informacyjnego, bowiem każda z zamieszczonych informacji, o ile nic innego nie

wynika z jej treści, będzie – w razie wątpliwości – dotyczyć wszystkich przetwarzanych danych osobowych.

WAŻNE

Rozproszenie informacji w kilku czy nawet kilkunastu dokumentach zwiększa natomiast ryzyko, że w odniesieniu do niektórych danych osobowych nie zostaną ujawnione wymagane informacje bądź informacje te zostaną ujawnione w nieprawidłowy sposób.

W zakresie sposobu realizowania obowiązku informacyjnego przez Google LLC negatywnie oceniono zarówno stopień wywiązania się przez spółkę z obowiązku udzielenia informacji dotyczących okresu przechowywania danych osobowych, jak i praktykę stosowania nieadekwatnego do treści nazewnictwa dokumentów i zakładek.

Jak nietrudno się domyślić, entuzjazmu CNIL nie wzbudziła też stosowana przez Google LLC praktyka pozyskiwania i przetwarzania nadzwyczajnej ilości różnorodnych danych osobowych, pozyskiwanych przede wszystkim za pośrednictwem oferowanych przez Google LLC usług. W ocenie CNIL, ze względu na doniosłe skutki, jakie niesie ze sobą pozyskiwanie i przetwarzanie tak dużej i różnorodnej ilości danych osobowych, absolutnym priorytetem jest całkowita jasność i komunikatywność przekazywanych przez administratora danych osobowych informacji. Jak się wydaje, również w tej kwestii punkt ciężkości został przeniesiony na szczególny cel, w jakim administrator zobowiązany jest do wykonywania obowiązku informacyjnego wobec osób, których dane przetwarza. Nie ulega wątpliwości, że tym celem jest przede wszystkim ukształtowanie takiego stanu faktycznego, w którym osoba, której dane osobowe są przetwarzane, ma pełną świadomość zakresu przetwarzania jej danych przez konkretnego administratora, i w którym osoba ta ma faktyczną możliwość rozpoznania ryzyka związanego z udostępnieniem administratorowi zarówno poszczególnych danych, jak i całego ich zespołu. W ocenie CNIL powyższe cele nie zostały zrealizowane przez Google LLC w związku z obowiązkiem informacyjnym dotyczącym personalizacji treści reklamowych, bowiem w sekcji oznaczonej nazwą „Personalizacja reklam" nie ujawniono, że przetwarzanie

danych osobowych następuje przy wykorzystaniu danych pochodzących z wielu usług i aplikacji, takich jak wyszukiwarka Google, YouTube, dom Google, mapy Google, Playstore, zdjęcia Google, powiązanych z licznymi źródłami, takimi jak pamięć telefonów, poczta elektroniczna Gmail czy pliki cookie. Jak oceniła CNIL, Google LLC nie przekazała użytkownikom pełnej informacji o liczbie przetwarzanych danych ani o tym, że są one ze sobą konsolidowane.

Problematyka poprawności realizowania obowiązku informacyjnego przez administratora danych osobowych zazębia się w pewnym stopniu także z problematyką zgody na przetwarzanie danych osobowych. Jak już wielokrotnie podkreślono, przetwarzanie danych osobowych może odbywać się wyłącznie wtedy, gdy istnieje ku temu określona podstawa prawna. W przypadku przedsiębiorców działających w branży e-commerce przetwarzanie danych osobowych następuje z reguły na podstawie zgody udzielonej przez osobę, której te dane dotyczą. W swoim rozstrzygnięciu CNIL zwróciła uwagę, że zgodnie z zawartą w rozporządzeniu definicją zgoda na przetwarzanie danych osobowych może stanowić podstawę prawną przetwarzania danych wyłącznie wtedy, gdy można jej przyznać walor dobrowolnego, konkretnego, świadomego i jednoznacznego okazania woli, przyzwalającego na przetwarzanie danych. W praktyce oznacza to, że legalność przetwarzania danych osobowych na podstawie zgody udzielonej przez osobę, wobec której nie wykonano należycie obowiązku informacyjnego w zakresie przetwarzania danych osobowych, może zostać zakwestionowana.

WAŻNE

Przetwarzanie danych osobowych może odbywać się wyłącznie wtedy, gdy istnieje ku temu określona podstawa prawna.

Jak ustaliła CNIL, podstawą prawną przetwarzania danych osobowych przez Google LLC była zgoda udzielona przez osobę, której te dane dotyczą. Jednocześnie, ze względu na brak wyczerpujących informacji o rodzaju, ilości i sposobie przetwarzania danych osobowych udzielonej przez użytkowników zgody nie można uznać jej za konkretną i jednoznaczną. Kryterium konkretności wymaga między innymi, aby zgoda dotyczyła oznaczonego celu przetwarzania danych osobowych. W prak-

tyce oznacza to zatem obowiązek administratora danych osobowych ujawnienia informacji o grupie danych, które podlegają przetwarzaniu w konkretnym celu oraz o celu, w jakim ta grupa danych jest przetwarzana.

Mechanizm tworzenia konta Google bazował na tym, że w celu utworzenia konta użytkownik był zmuszony zaznaczyć łącznie dwie opcje – „Wyrażam zgodę na warunki korzystania z usługi Google" oraz „Wyrażam zgodę na przetwarzanie moich danych osobowych zgodnie z powyższym opisem i zgodnie z wyjaśnieniami w Polityce prywatności". Zaznaczenie obu opcji skutkuje rozpoczęciem przez Google LLC przetwarzania danych osobowych w pełnym zakresie działalności Google LLC, w tym na przykład w zakresie personalizowania treści reklamowych na podstawie danych pozyskanych z historii przeglądarki Google, w wyniku monitorowania aktywności w serwisie YouTube czy korzystania z funkcji rozpoznawania głosu. Zdaniem CNIL taki mechanizm pozyskania zgody na przetwarzanie danych jest nieprawidłowy, ponieważ administrator nie realizuje obowiązku udzielenia użytkownikowi pełnej informacji dotyczącej celu przetwarzania danych osobowych, nie uzyskuje zgody na poszczególne cele przetwarzania danych osobowych i nie umożliwia użytkownikowi podjęcia decyzji o zakresie zgody na przetwarzanie jego danych osobowych.

Co więcej, w przyjętej przez Google LLC praktyce uzyskiwania zgody na przetwarzanie danych osobowych zarzucono, że w nieuzasadniony sposób wymusza ona na użytkowniku wykazanie się aktywnością w celu powstrzymania się od wyrażenia zgody na przetwarzanie danych. Jak podkreśliła CNIL, wyrażenie zgody na przetwarzanie danych osobowych jest dobrowolne, zaś obowiązek uzyskania zgody ciąży na administratorze, w związku z czym wymuszanie na użytkowniku podjęcia czynności w celu okazania braku woli wyrażenia zgody poprzez domyślne zaznaczenie przez administratora wymaganych zgód oraz przerzucenie na użytkownika czynności odznaczenia zgód w procesie rejestracji jest praktyką niezgodną z prawem. Co więcej, warunkiem legalności przetwarzania danych osobowych na podstawie udzielonej zgody na przetwarzanie danych jest jednoznaczność udzielonej zgody. Jak wyjaśniła CNIL, zgoda jest jednoznaczna tylko wtedy, gdy jej udzielenie następuje w wyniku wyraźnego działania strony uprawnionej do jej udzielenia. A zatem nie wystarczy samo umożliwienie użytkowniko-

wi modyfikowania określonych opcji przez ich odznaczanie – zgoda na przetwarzanie danych osobowych w określonym celu musi być udzielona w sposób wskazujący na świadome i aktywne działanie osoby, która tę zgodę wyraża. W przypadku Google LLC wyraźnie wskazano, że z inicjatywą zaznaczenia poszczególnych opcji powinien wyjść użytkownik, a nie administrator jego danych osobowych.

WAŻNE

Warunkiem legalności przetwarzania danych osobowych na podstawie udzielonej zgody na przetwarzanie danych jest jednoznaczność udzielonej zgody. Zgoda jest jednoznaczna tylko wtedy, gdy jej udzielenie następuje w wyniku wyraźnego działania strony uprawnionej do jej udzielenia, tj. poprzez świadome i aktywne działanie osoby, która tę zgodę wyraża.

Analiza przypadku Google LLC bez wątpienia znakomicie ilustruje kolosalne znaczenie nałożonego na administratora danych osobowych obowiązku informacyjnego oraz poważne konsekwencje niewypełniania bądź nieprawidłowego wypełniania tego obowiązku. Choć nałożona na Google LLC kara pieniężna ostatecznie wcale nie okazała się dolegliwa, warto pamiętać, że została ona nałożona we wczesnym okresie obowiązywania rozporządzenia RODO o ochronie danych osobowych, a co za tym idzie – kolejne kary nakładane przez organy nadzoru mogą być – i prawdopodobnie będą – wyższe.

4.2. Przetwarzanie danych osobowych z publicznie dostępnych źródeł a wypełnienie obowiązku informacyjnego – przypadek polskiej spółki

Wiele podmiotów nurtuje pytanie, czy można w swoich bazach danych przetwarzać dane, które zawarte są w ogólnodostępnych rejestrach, na przykład w Centralnej Ewidencji i Informacji o Działalności Gospodarczej („CEIDG"). Niezwykle ważne jest wzięcie pod uwagę sprawy dotyczącej polskiej spółki, na którą prezes UODO w marcu 2019 r. nałożył karę administracyjną w wysokości 943 470,00 zł[8].

[8] Decyzja prezesa Urzędu Ochrony Danych Osobowych z 15 marca 2019 r., sygn. ZSPR.421.3.2018.

Prezes UODO nałożył na spółkę karę administracyjną w związku ze stwierdzeniem naruszenia obowiązku informacyjnego (art. 14 ust. 1–3 RODO), polegającego na niepodaniu informacji zawartych w art. 14 ust. 1 i 2 RODO wszystkim osobom fizycznym, których dane osobowe spółka przetwarza, prowadzącym aktualnie lub w przeszłości jednoosobową działalność gospodarczą oraz osobom fizycznym, które zawiesiły wykonywanie tej działalności. Z decyzji wynika, że w ramach przeprowadzonej kontroli ustalono, iż:

1) w bazie danych systemu informatycznego spółka przetwarza dane osobowe osób fizycznych prowadzących działalność gospodarczą, które zostały pozyskane ze źródeł ogólnie dostępnych, w tym między innymi z CEIDG, z bazy REGON Głównego Urzędu Statystycznego;
2) w bazie danych znajdują się dane dotyczące ok. 3,59 mln osób fizycznych prowadzących aktualnie jednoosobową działalność gospodarczą oraz osób fizycznych, które zawiesiły tę działalność, oraz 2,33 mln osób fizycznych prowadzących w przeszłości działalność gospodarczą;
3) w bazie danych spółka przetwarza w szczególności dane adresowe (adres rejestrowy, adres do korespondencji, adres operacyjny) odnoszące się do osób fizycznych prowadzących działalność gospodarczą;
4) przed dniem rozpoczęcia obowiązywania RODO spółka wysłała informację o przetwarzaniu danych osobowych na wszystkie adresy poczty elektronicznej posiadane w bazie danych do przedsiębiorców prowadzących jednoosobową działalność gospodarczą;
5) spółka zamieściła także na swojej stronie internetowej informację o przetwarzaniu danych osobowych, odpowiadającą wymogom pełnej klauzuli informacyjnej z przepisu art. 14 ust. 1 i ust. 2 RODO;
6) spółka podjęła decyzję, aby nie realizować obowiązku informacyjnego poprzez wysłanie krótkich wiadomości tekstowych (SMS) wobec osób, których dane pozyskała ze źródeł publicznie dostępnych (w tym osób fizycznych prowadzących działalność gospodarczą), ponieważ nie posiada numerów telefonów w odniesieniu do każdej z tych osób, a także ze względu na wysokie koszty takiej akcji;
7) ze względu na wysokie koszty spółka nie zdecydowała się również na spełnienie tego obowiązku drogą tradycyjnej korespondencji wysłanej do osób, których dane przetwarza;

8) z wyjaśnień spółki wynika, że dane przez nią przetwarzane są danymi dostępnymi publicznie, zgromadzonymi w oficjalnych, publicznych rejestrach, zakres tych danych jest stosunkowo wąski, a ryzyko dla praw i wolności osób, których dane dotyczą, związane z ich przetwarzaniem – niskie;
9) spółka posiada łącznie 7 594 636 rekordów danych dotyczących osób fizycznych, w tym przedsiębiorców prowadzących jednoosobową działalność gospodarczą oraz osób będących wspólnikami lub członkami organów spółek, fundacji i stowarzyszeń. Spółka spełniła indywidualny obowiązek informacyjny wobec 682 439 osób, w stosunku do których posiada w ramach rekordu bazy danych adresy poczty elektronicznej;
10) w odniesieniu do 181 142 osób spółka dysponuje wyłącznie numerami telefonów komórkowych, a w odniesieniu do 6 490 226 osób dysponuje wyłącznie adresami korespondencyjnymi, z czego 2 924 443 rekordy dotyczą nieaktywnych działalności gospodarczych;
11) z wyjaśnień spółki wynika także, że gdyby miała wykonać obowiązek informacyjny ustanowiony w art. 14 ust. 1–2 RODO, indywidualnie wobec wszystkich osób fizycznych, których dane są przedmiotem postępowania, z wykorzystaniem poczty tradycyjnej, to koszt takiej operacji wyniósłby ponad 33 749 175,00 zł;
12) z wyjaśnień spółki wynika, że realizacja obowiązku informacyjnego w jego podstawowej formie (tj. indywidualnego kontaktu z każdą osobą, której dane dotyczą) powodowałaby po stronie spółki „niewspółmierny wysiłek", o którym mowa w art. 14 ust. 5 lit. b RODO, rozumiany jako obciążenie organizacyjne (tzn. konieczność oddelegowania pracowników i zasobów rzeczowych – komputerów, urządzeń biurowych – do realizacji wyłącznie tego zadania) oraz finansowe (tzn. koszt druku, przygotowania do wysyłki i nadania, w tym papieru, tonera, kopert, znaczków pocztowych, obsługi zwrotów korespondencji, ewentualnie wynagrodzenie podmiotów, którym Spółka mogłaby zlecić wykonanie tego zadania), które w krytyczny sposób zakłóciłyby funkcjonowanie spółki w stopniu, który mógłby wiązać się z koniecznością zakończenia prowadzenia działalności w Polsce;
13) spółka stosuje do przetwarzanych przez siebie danych osobowych wysokiej klasy zabezpieczenia techniczne. Spółka posiada wdrożone szczegółowe procedury i instrukcje dla pracowników zapewniające bezpieczeństwo przetwarzania danych.

Na podstawie powyższych ustaleń prezes UODO zadecydował o naruszeniu przepisów o przetwarzaniu danych osobowych i zdecydował o nałożeniu pieniężnej kary administracyjnej. Prezes UODO wziął pod uwagę między innymi, że:

1) nie został spełniony obowiązek informacyjny, wynikający z art. 14 ust. 1–3 RODO wobec osób fizycznych prowadzących aktualnie lub w przeszłości jednoosobową działalność gospodarczą;
2) stwierdzone w niniejszej sprawie naruszenie ma poważny charakter, dotyczy bowiem podstawowych praw i wolności osób, których dane spółka przetwarza;
3) naruszenie przez spółkę obowiązku podania podstawowych informacji o przetwarzaniu oraz pouczenia o przysługujących podmiotom danych prawach z tym związanych (wskazanych w art. 15–21 RODO), pociąga za sobą ryzyko odebrania im możliwości skorzystania z tych praw;
4) spółka podjęła świadomą decyzję (motywowaną chęcią uniknięcia dodatkowych nakładów finansowych) o niezrealizowaniu wobec osób fizycznych prowadzących aktualnie (w tym aktywnych, zawieszonych) lub w przeszłości jednoosobową działalność gospodarczą obowiązku;
5) brak spełnienia obowiązku informacyjnego prowadzi do uprzywilejowanej pozycji spółki w realizacji jej praw w stosunku do praw osób, których dane dotyczą i stanowią istotny element przedmiotu działalności spółki;
6) spółka pozyskuje dane ze wskazanych źródeł publicznych i stanowią one przedmiot jej wieloletniej działalności komercyjnej, zaś osoby, których te dane dotyczą, nie posiadają informacji o przetwarzaniu przez spółkę takich danych;
7) odpowiedzialność wobec osób, których dane dotyczą, spoczywa na spółce, a niewykonanie obowiązku informacyjnego z uwagi na koszty finansowe świadczy o obniżeniu wartości praw osób, których dane osobowe spółka przetwarza, w stosunku do wartości finansów spółki, której to argumentacji nie można uznać za zasadną w świetle wymogów RODO;
8) spółka pozyskuje środki finansowe w ramach prowadzonej działalności gospodarczej, której przedmiotem jest udostępnienie danych osobowych osób fizycznych jej klientom, jako odrębnym administratorom, w związku z produktami oferowanymi przez spółkę.

Od tej decyzji spółka złożyła skargę do wojewódzkiego sądu administracyjnego. Wojewódzki sąd administracyjny oddalił skargę w zakresie dotyczącym nakazu dopełnienia obowiązku informacyjnego wobec osób fizycznych prowadzących aktualnie działalność gospodarczą oraz osób fizycznych, które zawiesiły wykonywanie tej działalności, a którym informacje te nie zostały dotychczas podane, i tym samym uznał w tym zakresie zasadność decyzji prezesa UODO. Jednocześnie sąd uchylił decyzję prezesa UODO w części dotyczącej nakazu dopełnienia obowiązku informacyjnego wobec osób fizycznych prowadzących w przeszłości działalność gospodarczą. Prezes UODO ma ponownie przeprowadzić postępowanie administracyjne zgodnie ze wskazaniami sądu. Z wyroku sądu wynika, że zmieniła się liczba podmiotów danych dotkniętych naruszeniem. Liczba ta ma znaczenie dla wymierzenia kary administracyjnej oraz określenia jej wysokości. Należy mieć na uwadze, że wyrok nie jest prawomocny (stan na kwiecień 2020 r.).

WNIOSKI

1. Można przetwarzać dane osobowe ogólnodostępne w oparciu o określoną prawidłowo przez administratora podstawę prawną.
2. Przetwarzanie danych osobowych wymaga wypełnienia przez administratora obowiązków wymaganych przez przepisy prawa, w tym obowiązku informacyjnego wobec osób, których dane dotyczą.
3. Wysokie koszty dotyczące wypełnienia obowiązku informacyjnego nie uprawniają administratora do zwolnienia z wypełnienia obowiązku informacyjnego, w tym nie może on skorzystać ze zwolnienia przewidzianego przez ustawodawcę unijnego w art. 14 ust. 5 lit. b RODO dotyczącego możności niewypełnienia obowiązku informacyjnego, w sytuacji gdyby wymagało to „niewspółmiernie dużego wysiłku".

4.3. Urządzenia śledzące w odniesieniu do obowiązku informacyjnego – przypadek czeskiego przedsiębiorcy

Administrator zobowiązany jest udostępnić osobie, której dane dotyczą, informacje dotyczące przetwarzania danych osobowych, w tym informacje dotyczące tożsamości i danych kontaktowych administratora danych osobowych; celów przetwarzania danych osobowych i podstawę

prawną ich przetwarzania; okresu przechowywania danych osobowych (art. 13 RODO).

W praktyce może się zdarzyć, że przetwarzanie części danych osobowych sprowadza się do pozyskania danych. W szczególności sytuacja taka ma miejsce, gdy pozyskanie danych osobowych następuje w związku z zawarciem umowy między administratorem danych osobowych, świadczącym w ramach prowadzonej działalności gospodarczej określonego rodzaju usługi, a osobą, której te dane dotyczą, która decyduje się na skorzystanie ze świadczonych usług. W takim przypadku chęć zabezpieczenia roszczeń usługodawcy z tytułu zawartej umowy może uzasadniać potrzebę pozyskania danych osobowych usługobiorcy, które wprawdzie nie są konieczne do wykonania umowy zgodnie z jej treścią, jednak mogą okazać się niezbędne w przypadku dochodzenia przez usługodawcę wobec usługobiorcy roszczeń z tytułu zawartej umowy. W gruncie rzeczy zasady wykonywania obowiązku informacyjnego w takim przypadku są jasne – bowiem zgodnie z treścią art. 13 ust. 1 i 2 RODO administrator danych osobowych zobowiązany jest wykonać obowiązek informacyjny wobec osoby, której te dane dotyczą, w momencie pozyskiwania tych danych osobowych. Przedsiębiorca, który nie dopełni ciążącego na nim obowiązku informacyjnego wobec osoby, której dane przetwarza, naraża się co najmniej na pieniężną karę administracyjną, o czym przekonał się jeden z czeskich przedsiębiorców, prowadzący działalność gospodarczą związaną z wynajmem pojazdów silnikowych, na którego organ nadzorczy nałożył karę wysokości 30 tys. koron (niespełna 5 tys. zł).

WAŻNE

Administrator danych osobowych zobowiązany jest wykonać obowiązek informacyjny wobec osoby, której te dane dotyczą, w momencie pozyskiwania tych danych osobowych. Przedsiębiorca, który nie dopełni ciążącego na nim obowiązku informacyjnego, naraża się co najmniej na pieniężną karę administracyjną.

W 2018 r. w wyniku złożonej skargi czeski organ nadzorczy przeprowadził postępowanie kontrolne u jednego z przedsiębiorców świadczących usługi w zakresie wynajmu samochodów osobowych. Skarżą-

cy zarzucał przedsiębiorcy naruszenie przepisów RODO, polegające na zaniechaniu realizacji obowiązku informacyjnego wobec skarżącego o przetwarzaniu jego danych osobowych w związku z wyposażeniem wynajmowanego samochodu w lokalizator GPS. Jak zaznaczył skarżący, o fakcie zamontowania w wynajętym samochodzie urządzenia umożliwiającego monitorowanie lokalizacji pojazdu dowiedział się przypadkowo – w wyniku sporu z pracownikiem wypożyczalni.

Korzystając z komputera, pracownik wypożyczalni ustalił, że skarżący, poruszając się wynajętym samochodem po autostradzie w kierunku miejscowości Liberec, przekroczył dopuszczalną prędkość. Na podstawie tych danych pracownik wypożyczalni obciążył skarżącego (któremu przypisywał winę za powstanie pewnych usterek w samochodzie) karą umowną w wysokości 500 koron. Do skargi skarżący dołączył kopię umowy najmu samochodu oraz ogólnych warunków umowy, z których treści w żaden sposób nie można było wnioskować ani o wyposażeniu samochodu w lokalizator GPS, ani fakcie przetwarzania w związku z tym danych osobowych.

Jak wyjaśnił przedsiębiorca, dane pochodzące z zainstalowanych lokalizatorów GPS są udostępniane przede wszystkim czeskiej policji w wyniku połączenia się lokalizatora GPS z systemem. Ponadto przedsiębiorca zaznaczył, że dane z urządzeń lokalizacyjnych wykorzystywane są wyłącznie w ściśle określonych sytuacjach – na przykład w przypadku wystąpienia zdarzenia ubezpieczeniowego, naruszenia przepisów ruchu drogowego, naruszenia przepisów zawartej umowy najmu bądź jeżeli wynajęty samochód zostanie wykorzystany w celu popełnienia przestępstwa.

Pochylając się nad problematyką obowiązku informacyjnego dotyczącego przetwarzania danych osobowych pierwszoplanowym zadaniem jest ponad wszelką wątpliwość ustalenie, którym danym należy przypisywać przymiot danych osobowych. Zgodnie w przyjętą w rozporządzeniu definicją dane osobowe to informacje o zidentyfikowanej lub – co ważniejsze – możliwej do zidentyfikowania osobie fizycznej. Należy przyjąć, że możliwa do zidentyfikowania osoba fizyczna to w szczególności taka osoba, którą można pośrednio lub bezpośrednio zidentyfikować na podstawie danych o jej lokalizacji. Ponieważ stosowane przez przedsiębiorcę umowy najmu pojazdów zawierały imię i nazwisko na-

jemcy, jego adres, numer telefonu, serię i numer dowodu tożsamości oraz prawa jazdy, a wynajmowane pojazdy były wyposażone w lokalizator GPS umożliwiający wykonywanie połączeń zdalnych i przepływ informacji zarówno do administratora danych, jak i do osób trzecich (np. organów administracji publicznej), w omawianym przypadku według organu nadzorczego dochodziło do przetwarzania danych osobowych, w szczególności danych w postaci adresu IP oraz pozycji GPS pojazdu, które pozwalały na identyfikację konkretnej osoby, której te dane dotyczą. W związku z powyższym na administratorze danych osobowych ciążył obowiązek informacyjny wobec skarżącego dotyczący przetwarzania jego danych osobowych, w szczególności danych o jego lokalizacji w trakcie trwania umowy najmu. Przepisy dotyczące obowiązku informacyjnego administratora danych osobowych normują nie tylko zakres informacji, jakie administrator zobowiązany jest ujawnić osobie, której dane przetwarza, lecz również termin, w którym ujawnienie takich danych powinno nastąpić.

Administrator danych osobowych zobowiązany jest podać osobie, której dane osobowe zamierza przetwarzać, wszystkie przewidziane prawem informacje już w momencie pozyskiwania danych osobowych tej osoby (art. 13 ust. 1 i 2 RODO). Oznacza to, że przedsiębiorca nie może dokonywać oceny informacji ze względu na jakiekolwiek kryterium, od którego uzależni fakt i termin ujawnienia tych informacji swojemu klientowi. Tak więc jedyne informacje, których przedsiębiorca nie musi ujawniać w momencie pozyskiwania danych osobowych swojego klienta, to informacje, które nie są objęte obowiązkiem informacyjnym.

4.4. Informacja o stosowanym monitoringu na podstawie przykładu francuskiego pracodawcy

W dobie nieustannego rozwoju technologii teleinformatycznych wpisująca się w najnowsze standardy uczestniczenia w obrocie gospodarczym praktyka urzeczywistniania ochrony danych oraz zapewniania poufności informacji przetwarzanych w ramach szeroko pojmowanej działalności zawodowej może wywoływać przekonanie o tym, że najlepszym sposobem dostosowania się do aktualnej rzeczywistości gospodarczej oraz jej wymogów jest sięgnięcie po najnowsze rozwiązania technologiczne. Tymczasem okazuje się, że bezrefleksyjne wykonywanie obowiązków w zakresie ochrony danych może prowadzić do sytuacji, w której pryncypialny stosunek do jednego obowiązku może być

powodem poważnego naruszenia innego obowiązku. O tym, że konsekwencje stosowania norm prawnych w oderwaniu od systemu prawnego jako pewnej całości mogą być niezbyt przyjemne, przekonała się francuska spółka Uniontrad Company, prowadząca działalność gospodarczą polegającą na wykonywaniu przysięgłych i nieprzysięgłych tłumaczeń dokumentów.

We Francji, podobnie jak w Polsce, ze względu na szczególną rolę tłumaczeń przysięgłych w obrocie gospodarczym i prawnym, mocno podkreśla się potrzebę zapewnienia przez podmioty realizujące tłumaczenia przysięgłe zabezpieczenia dokumentów oraz nośników danych przed ich utratą, zniszczeniem lub zniekształceniem, a także przed nieuprawnionym dostępem osób trzecich. Pragnąc jak najlepiej zrealizować to zadanie, Uniontrad Company zdecydowała się zainstalować w swoim przedsiębiorstwie urządzenia do nadzoru wideo. W siedzibie spółki zainstalowano trzy kamery, z których jedną – w niedostępnym dla osób trzecich pomieszczeniu pracy tłumaczy. Kamera rejestrowała w trybie ciągłym obraz, na którym widoczne były stanowiska pracy sześciu tłumaczy oraz archiwum, w którym przechowywano dokumenty związane z tłumaczeniami, w tym tłumaczeniami przysięgłymi.

Na efekty podjętej przez spółkę decyzji nie trzeba było długo czekać. W krótkim czasie do organu nadzorczego wpłynęły cztery skargi, w których skarżący zarzucali przedsiębiorcy permanentne naruszanie przepisów RODO, w tym między innymi zaniechanie wykonania wobec nich obowiązku informacyjnego związanego z utrwalaniem ich wizerunku podczas wykonywania pracy. W wyniku przeprowadzonej przez CNIL kontroli stwierdzono także inne nieprawidłowości – na przykład w postaci przechowywania zarejestrowanych obrazów przez okres wykraczający poza okres niezbędny do zrealizowania celu, w jakim spółka przedmiotowe obrazy utrwalała. Organ nadzoru zobowiązał paryskiego przedsiębiorcę do zmodyfikowania stosowanego systemu monitoringu w ten sposób, aby system ten był proporcjonalny do celu, w jakim został wprowadzony w przedsiębiorstwie, jednakże spółka nie wcieliła w życie zaleceń rekomendowanych decyzji CNIL.

Na podstawie kolejnych skarg wniesionych do organu nadzoru w spółce przeprowadzona została kolejna kontrola zgodności stosowanych przez spółkę środków z RODO, w wyniku której Uniontrad Com-

pany została ukarana grzywną wysokości 20 tys. euro oraz karą w wysokości 200 euro za każdy dzień opóźnienia w dostosowaniu środków organizacyjnych i prawnych do zgodności z RODO. Warto na marginesie zaznaczyć, że paryskiej spółce groziła ponad trzykrotnie wyższa grzywna i pięciokrotnie wyższa kara za opóźnienie w wykonaniu decyzji CNIL, jednak ostatecznie organ nadzoru uwzględnił okoliczność, że spółka zdecydowała się na demontaż kamery w pomieszczeniu przeznaczonym do wykonywania pracy przez tłumaczy.

Należy zgodzić się ze stanowiskiem spółki, że norma wyrażona w art. 5 ust. 1 lit. f rozporządzenia RODO zobowiązywała spółkę do zapewnienia bezpieczeństwa przetwarzanych przez nią – w związku z prowadzoną działalnością – danych osobowych, znajdujących się między innymi w tłumaczeniach dokumentów, których przechowywanie przez określony czas było wymagane na podstawie odrębnych przepisów prawa. W celu zrealizowania przedmiotowego obowiązku spółka – jako administrator danych osobowych – objęła pomieszczenie, w którym znajdowały się nośniki danych osobowych podlegających ochronie ciągłym i nieprzerwanym monitoringiem. Jednocześnie spółka nie rozpoznała roli zasady minimalizacji danych, wyrażonej w art. 5 ust. 1 lit. c rozporządzenia RODO, zgodnie z którą dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których te dane są przetwarzane. Realizując zasadę ochrony danych osobowych kontrahentów i osób trzecich, spółka zaniedbała zasadę minimalizacji danych, związanych z przetwarzaniem danych osobowych swoich pracowników.

Z punktu widzenia spółki jako pracodawcy i administratora danych osobowych dotyczących różnych grup osób istotne jest to, że legalność praktyki instalowania monitoringu w pomieszczeniu biurowym, w którym świadczona jest praca, sama w sobie nie została zanegowana. W wydanej decyzji CNIL zaproponował nawet kilka rozwiązań integrujących potrzebę zapewnienia należytej ochrony danych osobowych osób trzecich oraz minimalizacji danych osobowych pracowników spółki, przetwarzanych w rezultacie stosowania środków, mających na celu ochronę innych danych osobowych osób trzecich. Wśród propozycji CNIL znalazł się postulat zmiany orientacji kamery, jej przesunięcie lub wdrożenie narzędzi umożliwiających anonimizację wizerunków pracowników – na przykład maskowanie dynamiczne.

Jednakże – jak zauważył organ nadzoru – wdrożenie w przedsiębiorstwie monitoringu musi pozostawać w zgodzie z zasadą proporcjonalności, zaś gromadzenie danych osobowych za pomocą urządzenia rejestrującego obraz musi być nieodzowne dla osiągnięcia zamierzonego celu. Ze względu na ilość danych osobowych przetwarzanych na podstawie monitoringu miejsca pracy oraz ze względu na zasadę minimalizacji danych pracodawca przed sięgnięciem po ten środek powinien rozważyć zastosowanie innych, mniej inwazyjnych rozwiązań. W przypadku zaś stwierdzenia, że nie umożliwiają one osiągnięcia zamierzonego celu, pracodawca powinien z najwyższą starannością przeanalizować aspekty związane z liczbą urządzeń, które są niezbędne w celu rejestrowania obrazu, lokalizacją każdego z nich, orientacją, okresem działania, charakterem pracy wykonywanej przez pracowników oraz innymi czynnikami, które umożliwiają ocenę adekwatności środka do celu, w którym pracodawca zamierza ów środek zastosować.

WAŻNE

Wdrożenie w przedsiębiorstwie monitoringu musi pozostawać w zgodzie z zasadą proporcjonalności, zaś gromadzenie danych osobowych za pomocą urządzenia rejestrującego obraz musi być nieodzowne dla osiągnięcia zamierzonego celu.

Problemy legalności i zasadności przetwarzania danych osobowych pracowników to niejedyne problemy związane z monitoringiem stanowiska pracy. Jak wynika z art. 12 ust. 1 RODO, administrator danych osobowych podejmuje odpowiednie środki w celu dostarczenia osobie, której te dane dotyczą, wszelkich informacji związanych z jej danymi osobowymi, w szczególności informacji o przetwarzaniu danych, sposobie ich przetwarzania oraz uprawnieniach i sposobach realizacji tych uprawnień przez osobę, której dane osobowe są przetwarzane. Ponadto administrator danych osobowych podejmuje odpowiednie środki w celu prowadzenia wszelkiej komunikacji dotyczącej praw przysługujących osobie, której dane są przetwarzane. Istotą przedmiotowego unormowania jest wprowadzenie w relacjach między administratorem danych osobowych a osobą, której te dane dotyczą, zasady transparentnego wykonywania obowiązków informacyjnych wobec osoby uprawnionej oraz

zasady przejrzystej komunikacji. Na mocy powyższych zasad komunikacja między administratorem danych osobowych a osobą, której dane dotyczą, powinna spełniać kryterium zwięzłości, przejrzystości i zrozumiałości, a także kryterium przystępności formy i języka, przy czym komunikacja może odbywać się zarówno tradycyjnymi kanałami komunikacyjnymi, jak i z wykorzystaniem kanałów komunikacji elektronicznej.

Jeżeli dane osobowe osoby, której te dane dotyczą, są zbierane od tej osoby, administrator, w momencie pozyskiwania tych danych, przekazuje osobie, której dane dotyczą, następujące informacje (art. 13 ust. 1 RODO):

- dane identyfikacyjne i kontaktowe administratora oraz, w stosownych przypadkach, dane identyfikacyjne i kontaktowe przedstawiciela administratora;
- dane kontaktowe inspektora ochrony danych, jeżeli osoba taka została ustanowiona;
- cele przetwarzania danych osobowych oraz ich podstawę prawną;
- prawnie uzasadnione interesy administratora danych lub osoby trzeciej, jeżeli przetwarzanie danych odbywa się na podstawie art. 6 ust. 1 lit. f RODO;
- dane odbiorcy lub kategorii odbiorców danych osobowych oraz – gdy ma to zastosowanie – informację o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej.

Oprócz informacji, o których mowa w art. 13 ust. 1 RODO, administrator, w momencie pozyskania danych osobowych, przekazuje osobie, której dane dotyczą, następujące dodatkowe informacje, niezbędne do zagwarantowania uczciwego i przejrzystego przetwarzania danych osobowych, tj.:

- okres przechowywania danych osobowych lub kryteria ustalenia tego okresu;
- informacje o prawie do żądania dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania;
- informacje o prawie sprzeciwu wobec przetwarzania;
- informacje o prawie przenoszenia danych;
- jeżeli podstawą przetwarzania jest zgoda – informacje o prawie do cofnięcia zgody na przetwarzanie;
- informacje o prawie do wniesienia skargi do organu nadzorczego;
- informację o tym, czy podanie danych osobowych jest konieczne – to znaczy, czy wynika z ustawy, umowy lub jest warunkiem

zawarcia umowy – i jakie są ewentualne konsekwencje ich niepodania, a także informacje o zautomatyzowanym podejmowaniu decyzji wobec osoby, której dane dotyczą, w tym o profilowaniu.

Wniosek, jaki należy wyciągnąć z analizy powyższych przepisów, jest prosty – objęcie stanowiska pracy pracownika monitoringiem jest przetwarzaniem danych osobowych, do którego stosuje się przepisy o ochronie danych osobowych, w tym obowiązek informacyjny. Co za tym idzie pracodawca bezwzględnie musi przekazać pracownikom informację o przetwarzaniu ich danych osobowych z monitoringu, przy czym sposób wykonania tego obowiązku nie może naruszać zasady przejrzystości. W praktyce oznacza to, że pracodawca musi poinformować pracownika w sposób zwięzły, przejrzysty, zrozumiały i łatwo dostępny o wprowadzeniu monitoringu, sposobie i celu przetwarzania danych z monitoringu oraz o prawach, jakie przysługują pracownikowi jako osobie, której dane dotyczą.

WAŻNE

Objęcie stanowiska pracy pracownika monitoringiem jest przetwarzaniem danych osobowych, do którego stosuje się przepisy o ochronie danych osobowych, w tym obowiązek informacyjny.

Warto w tym miejscu wspomnieć o fakcie, że zgodnie z brzmieniem art. 13 ust. 1 i 2 RODO obowiązek informacyjny powstaje w momencie pozyskania danych osobowych przez administratora od osoby, której te dane dotyczą. Jak podkreśliła CNIL, pracodawca, który nie dopełnia obowiązku informacyjnego wobec pracownika, którego dane osobowe przetwarza, nie może czuć się zwolniony z tego obowiązku przez sam fakt zaprzestania pozyskiwania danych osobowych z określonego źródła. Zatem w analizowanym przypadku obowiązek informacyjny w odniesieniu do przetworzonych danych osobowych nie wygasł z chwilą usunięcia źródła, z którego te dane pochodziły, a osoby, których dane dotyczyły, nadal mogły domagać się wypełnienia przez administratora przewidzianych w rozporządzeniu RODO obowiązków.

Z punktu widzenia przedsiębiorców, którzy już stosują bądź chcieliby w przyszłości zastosować monitoring stanowisk pracy, pomocne mogą być zaktualizowane na początku 2020 r. wytyczne dotyczące stosowania monitoringu wizyjnego wydane przez Europejską Radę Ochrony Danych Osobowych (EROD). Nowe wytyczne umożliwiają administratorom danych osobowych zebranych z monitoringu wizyjnego realizowanie obowiązku informacyjnego w sposób warstwowy. Zgodnie ze stanowiskiem EROD pierwszą warstwę może stanowić umieszczony w widocznym miejscu przed wejściem w obszar objęty monitoringiem znak graficzny (np. piktogram), opatrzony najważniejszymi informacjami o administratorze danych i celu przetwarzania danych osobowych. Natomiast drugą warstwę może stanowić pełna treść klauzuli informacyjnej o przetwarzaniu danych z monitoringu, dostępna fizycznie w przedsiębiorstwie administratora danych osobowych lub w wersji cyfrowej, dostępnej za pomocą kodu QR. Choć w ujęciu formalnym administrator danych osobowych nie ma obowiązku udostępniania pełnej treści klauzuli informacyjnej w więcej niż jednej formie, EROD zaleca przygotowanie zarówno wersji papierowej, jak i wersji zdigitalizowanej.

Podsumowując studium przypadku Uniontrad Company, można powiedzieć, że choć z punktu widzenia ochrony danych osobowych stosowanie najnowszych rozwiązań technologicznych nie zawsze jest najlepszym pomysłem, to całkowita rezygnacja z nowinek technicznych nie jest konieczna. Jednak aby ograniczyć ryzyko związane z wprowadzaniem nowych technologii do przedsiębiorstwa, warto uwzględnić to, że takie działanie wymaga znacznie szerszej i głębszej analizy prawnej niż tradycyjne rozwiązania, bo – jak pokazuje praktyka – ochrona danych osobowych jest obszarem, którego zaniedbanie może być kosztowne.

WZÓR. KLAUZULA INFORMACYJNA – MONITORING WIZYJNY

MONITORING WIZYJNY – KLAUZULA INFORMACYJNA

Zgodnie z art. 13 ust. 1 i ust. 2 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. („RODO") informujemy, że:

1. Na terenie przedsiębiorstwa (...), prowadzony jest wewnętrzny oraz zewnętrzny monitoring wizyjny, rejestrujący obraz za pomocą kamer przemysłowych;

2. Administratorem Pani/Pana danych osobowych jest (...), z którym można kontaktować się pod adresem e-mailowym: (...);
3. Administrator wyznaczył inspektora ochrony danych osobowych, z którym można kontaktować się od adresem e-mailowym: (...);
4. Twoje dane osobowe przetwarzane są w celu wynikającym z prawnie uzasadnionych interesów administratora (na podstawie przepisu art. 6 ust. 1 lit. f RODO), jakim jest zapewnienie bezpieczeństwa pracowników oraz współpracowników administratora, ochrony mienia administratora oraz zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić administratora na szkodę;
5. Twoje dane osobowe będą przechowywane do czasu ich nadpisania zależnego od pojemności dysku, jednak nie dłużej niż przez trzy miesiące. W przypadku, gdy nagranie stanowi dowód w postępowaniu prowadzonym na podstawie prawa lub gdy poweźmiemy wiadomość, że może stanowić dowód w takim postępowaniu, termin ten ulega przedłużeniu do czasu prawomocnego zakończenia postępowania;
6. Posiadasz prawo dostępu do treści swoich danych, prawo do żądania usunięcia danych, ograniczenia przetwarzania oraz prawo wniesienia sprzeciwu – z przyczyn związanych z Twoją szczególną sytuacją;
7. Masz prawo wniesienia skargi do organu nadzorczego, gdy uznasz, że przetwarzanie Twoich danych osobowych narusza przepisy prawa;
8. Administrator nie przetwarza Twoich danych osobowych w sposób, który wiązałoby się z podejmowaniem wyłącznie zautomatyzowanych decyzji co do Twojej osoby;
9. Twoje dane osobowe mogą być przekazywane podmiotom przetwarzającym je na nasze zlecenie, np. firmom obsługującym nasze systemy informatyczne lub udostępniającym nam narzędzia informatyczne oraz organom władzy publicznej w zakresie, w jakim są one uprawnione do ich otrzymywania;
10. Twoje dane osobowe nie będą przekazywane do państwa trzeciego/organizacji międzynarodowej.

4.5. Podsumowanie

Obowiązek informacyjny to jeden z kluczowych obowiązków związanych z przetwarzaniem danych osobowych. Nie ma gotowego szablonu obowiązku informacyjnego, który będzie pasował do wszystkich sytuacji. Treść obowiązku informacyjnego zależy od wielu kwestii, w szcze-

gólności od podstawy prawnej przetwarzania danych osobowych, celu przetwarzania danych, okresu przetwarzania danych osobowych, kręgu odbiorców danych osobowych czy obszaru przetwarzania danych osobowych. Informacje zawarte w klauzuli informacyjnej powinny zawsze być dostosowane do faktycznego przypadku.

Administrator zobowiązany jest do przekazania tych informacji osobie, której dane dotyczą, w momencie zbierania danych, a jeżeli danych nie uzyskuje się od osoby, której dane dotyczą, lecz z innego źródła – w rozsądnym terminie, zależnie od okoliczności. Udzielenie informacji nie jest jednak konieczne, jeżeli osoba, której dane dotyczą, dysponuje już tymi informacjami, jeżeli utrwalenie lub ujawnienie danych jest wyraźnie przewidziane prawem, lub jeżeli poinformowanie osoby, której dane dotyczą, okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku.

Rozdział 5.
Prawa osób, których dane dotyczą

Osobom, których dane są przetwarzane, przysługują prawa przewidziane w przepisach art. 15–22 RODO. Odpowiedzialnym za realizację tych praw jest administrator.

Ustawodawca unijny zwraca uwagę na prawa osób, których dane są przetwarzane. W związku z tym zadbano, aby osoby te miały większy dostęp do informacji o swoich danych i działaniach administratora. RODO zatem czyni administratora odpowiedzialnym za realizację praw osób, których dane dotyczą, a każdy administrator powinien wziąć to pod uwagę w trakcie wdrażania RODO.

Należy przypomnieć, że jedną z zasad przetwarzania danych osobowych jest zasada rozliczalności. Dotyczy ona zdolności administratora do wykazania, że przestrzega przepisów RODO, w tym między innymi realizuje prawa podmiotu danych.

WAŻNE

Zasadne jest więc stworzenie przez administratora stosownych procedur, zgodnie z którymi będzie postępował w razie zgłoszenia żądania (odnośnie danego prawa) przez podmiot danych.
Jedną z wdrożonych procedur powinna być procedura dotycząca nakazu potwierdzania tożsamości wnioskodawcy w przypadku istnienia wątpliwości w tym zakresie.

W wyniku zgłoszonego żądania przez osobę nieuprawnioną mogłoby dojść do udostępnienia danych lub wprowadzenia innego ryzyka dla ich bezpieczeństwa. Administrator powinien zatem wdrożyć rozwiązania mające na celu przeciwdziałanie ujawnieniu danych w wyniku złożenia żądania przez osobę nieuprawnioną właśnie na przykład poprzez stosowanie odpowiedniej procedury.

W interesie administratora powinno być również należyte dokumentowanie wpływających żądań i prowadzonej w związku z tym korespondencji. Takie dokumentowanie umożliwi administratorowi udowodnienie realizacji praw podmiotów danych w przypadku ewentualnej kontroli organu nadzorczego oraz zapewni dowody w przypadku ewentualnych sporów prowadzonych z podmiotami danych.

Co do zasady administrator nie odmawia podjęcia działań na żądanie osoby, której dane dotyczą, pragnącej wykonać prawa jej przysługujące, chyba że wykaże, iż nie jest w stanie zidentyfikować osoby, której dane dotyczą. Co więcej, zgodnie z przepisem art. 12 ust. 3 i 4 RODO administrator bez zbędnej zwłoki – a w każdym razie w terminie miesiąca od otrzymania żądania – powinien udzielić takiej osobie informacji o działaniach podjętych w związku z jej żądaniem. W razie potrzeby termin ten administrator może przedłużyć o kolejne 2 miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W terminie miesiąca od otrzymania żądania administrator jednak powinien poinformować osobę, której dane dotyczą, o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia.

Tabela. Prawa osób, których dane dotyczą

Prawa osób, których dane dotyczą	Opis
Dostęp do danych	Osoba, której dane są przetwarzane, jest uprawniona do uzyskania od administratora potwierdzenia, czy jej dane są przetwarzane. Jeżeli są, to osoba taka jest uprawniona do uzyskania dostępu do swoich danych oraz informacji o: 1) celach przetwarzania; 2) kategoriach danych osobowych; 3) odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych; 4) planowanym okresie przechowywania danych osobowych (w miarę możliwości), a gdy nie jest to możliwe, kryteria ustalania tego okresu; 5) prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;

	6) prawie wniesienia skargi do organu nadzorczego; 7) źródle informacji – jeżeli dane osobowe nie zostały zebrane od osoby, której one dotyczą, np. od podmiotu z grupy kapitałowej; 8) zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, oraz istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą: 9) odpowiednich zabezpieczeniach, o których mowa w art. 46 RODO, związanych z przekazaniem danych osobowych do państwa trzeciego lub organizacji międzynarodowej. Osoba, której dane dotyczą, korzystając z prawa dostępu do danych, może wedle swego uznania, choć w ramach katalogu zamkniętego, kształtować zakres żądanych informacji. Może więc żądać przekazania wszystkich informacji, kopii czy wglądu jedynie do wybranych informacji. **Ważne!** **Prawo dostępu nie powinno negatywnie wpływać na prawa lub wolności innych osób, w tym tajemnice handlowe lub własność intelektualną, w szczególności na prawa autorskie chroniące oprogramowanie. Względy te nie powinny jednak skutkować odmową udzielenia osobie, której dane dotyczą, jakichkolwiek informacji (motyw 63 RODO).**
Sprostowanie danych	Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania osoba taka ma także prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia. Ustawodawca unijny przewidział zatem dwa rodzaje sprostowań: poprawienie nieprawidłowych danych oraz uzupełnienie niekompletnych danych. **Ważne!** **Uzupełnienie danych osobowych nie może dotyczyć danych, które są nadmierne pod względem celu ich przetwarzania.**
Usunięcie danych, prawo do bycia zapomnianym	Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki dane te usunąć. Jest to konieczne, jeżeli zachodzi jedna z następujących okoliczności: 1) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetworzone; 2) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania; 3) osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 RODO wobec przetwarzania i nie występują nadrzędne, prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 RODO wobec przetwarzania; 4) dane osobowe były przetwarzane niezgodnie z prawem;

	5) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator; 6) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1 RODO. Prawo do żądania usunięcia danych osobowych nie ma zastosowania w zakresie, w jakim przetwarzanie jest niezbędne: 1) do korzystania z prawa do wolności wypowiedzi i informacji; 2) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi; 3) z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego zgodnie z art. 9 ust. 2 lit. h oraz lit. i RODO, a także art. 9 ust. 3 RODO; 4) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, o ile prawdopodobne jest, że prawo, o którym mowa w ust. 1, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania, lub 5) do ustalenia, dochodzenia lub obrony roszczeń.
Ograniczenie przetwarzania danych	Osoba, której dane dotyczą, ma prawo żądania od administratora ograniczenia ich przetwarzania w następujących przypadkach: 1) osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający administratorowi na sprawdzenie prawidłowości tych danych; 2) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania; 3) administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń; 4) osoba, której dane dotyczą, wniosła sprzeciw na mocy art. 21 ust. 1 wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą. Administrator może odmówić ograniczenia przetwarzania na przykład, jeśli okaże się, że wbrew stanowisku osoby, której dane dotyczą, jej dane są prawidłowe albo jeżeli osoba, której dane dotyczą, nie dowiedzie, że są one jej potrzebne do ustalenia, dochodzenia lub obrony roszczeń.
Przenoszenie danych	Osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe, jeżeli: 1) przetwarzanie odbywa się na podstawie zgody w myśl art. 6 ust. 1 lit. a RODO lub art. 9 ust. 2 lit. a RODO albo na podstawie umowy w myśl art. 6 ust. 1 lit. b RODO, oraz 2) przetwarzanie odbywa się w sposób zautomatyzowany.

Sprzeciw wobec przetwarzania danych	Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych opartego na: 1) art. 6 ust. 1 lit. e RODO – przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi, lub 2) art. 6 ust. 1 lit. f RODO – przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią. Po wniesieniu sprzeciwu administratorowi nie wolno już przetwarzać tych danych osobowych, chyba że wykaże on istnienie ważnych, prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia bądź obrony roszczeń. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw również wobec przetwarzania dotyczących jej danych osobowych: 1) na potrzeby marketingu bezpośredniego, w tym profilowania, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim; 2) do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 RODO, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.
Prawo do niepodlegania decyzjom opartym na zautomatyzowanym przetwarzaniu	Osoba, której dane dotyczą, ma uprawnienie, aby nie podlegać decyzji opartej wyłącznie na automatycznym przetwarzaniu, w tym również profilowaniu, jeżeli decyzja ta wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa. Jednak uprawnienie do niepodlegania decyzjom opartym na automatycznym przetwarzaniu nie będzie miało zastosowania, jeżeli decyzja: 1) jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem, 2) jest dozwolona prawem unijnym lub prawem krajowym, któremu podlega administrator i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, lub 3) opiera się na wyraźnej zgodzie osoby, której dane dotyczą.

WZÓR. ODPOWIEDŹ NA OTRZYMANE ŻĄDANIE

Miejscowość, dnia (...)

Nazwa/Imię i nazwisko
Adres
(administratora)

Imię i nazwisko
Adres
(osoby wnioskującej)

ODPOWIEDŹ NA WNIOSEK

(W przypadku spełnienia żądania)

W nawiązaniu do wniosku z żądaniem usunięcia danych osobowych z dnia (...), zgodnie z art. 17 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO) administrator danych osobowych informuje, iż żądanie zostało spełnione w terminie przewidzianym w art. 12 ust. 4 wyżej wymienionego rozporządzenia przez ich usunięcie.

LUB

(W przypadku odmowy spełnienia żądania)

W nawiązaniu do wniosku z żądaniem usunięcia danych osobowych z dnia (...), zgodnie z art. 17 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO) administrator danych osobowych informuje, iż żądanie zawarte we wniosku nie zostanie spełnione ze względu na istnienie przesłanki wyłączającej, tj.:
(należy przedstawić odpowiadający sytuacji powód)

* niezbędność przetwarzania do korzystania z prawa do wolności wypowiedzi i informacji;
* przetwarzanie danych jest niezbędne do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
* ze względu na interes publiczny w dziedzinie zdrowia publicznego;
* niezbędność przetwarzania danych osobowych do celów archiwalnych w interesie publicznym, do celów badań celów statystycznych;
* niezbędność przetwarzania do ustalenia, dochodzenia lub obrony roszczeń. Żądanie jest ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter.

(W przypadku odmowy spełnienia żądania)
Mając powyższe na uwadze, administrator danych osobowych informuje, iż przysługuje Panu/Pani prawo do wniesienia skargi do organu nadzorczego – prezesa Urzędu Ochrony Danych Osobowych.

5.1. Prawo do bycia zapomnianym

Przyjmuje się, że genezą prawa żądania do bycia zapomnianym była sprawa Mario Costa Gonzaleza (a dokładniej Google Spain SL i Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD) i Mario Costa Gonzálezowi, sygn. C-131/12). Osoba ta domagała się od hiszpańskiego odpowiednika UODO oraz hiszpańskiego oddziału Google usunięcia odnośnika do stron internetowych, na których umieszczone były jej dane osobowe. Hiszpan żądał usunięcia nieaktualnych informacji na jego temat, a dotyczących licytacji jego nieruchomości z uwagi na zadłużenie. Po wpisaniu jego imienia i nazwiska w wyszukiwarce internetowej była to jedna z pierwszych pojawiających się informacji.

Zainteresowany wskazywał, że spłacił już cały dług, obecnie nie ma już żadnych zaległości, a taka informacja wpływa negatywnie na jego dobre imię. Sprawa trafiła aż do Trybunału Sprawiedliwości Unii Europejskiej, który uznał, że Google jest administratorem danych osobowych Mario Costa Gonzaleza i nakazał usunięcie wszelkich linków odnoszących się do danych osobowych związanych z przedmiotowym zadłużeniem (choć najpewniej nie takiego efektu oczekiwał – w związku z jego

precedensowym wyrokiem, zarówno on, jak i jego dług zyskały swego rodzaju nieśmiertelność). Odcisnęła ona również swoje piętno na nowo tworzonym ogólnym rozporządzeniu o ochronie danych.

MOTYW 65 PREAMBUŁY RODO

Każda osoba fizyczna powinna mieć prawo żądania do sprostowania danych osobowych jej dotyczących oraz prawo do „bycia zapomnianym", jeżeli zatrzymywanie takich danych narusza niniejsze rozporządzenie, prawo Unii lub prawo państwa członkowskiego, któremu podlega administrator. Osoba, której dane dotyczą, powinna w szczególności mieć prawo do tego, by jej dane osobowe zostały usunięte i przestały być przetwarzane, jeżeli dane te nie są już niezbędne do celów, w których były zbierane lub w inny sposób przetwarzane, jeżeli osoba, której dane dotyczą, cofnęła zgodę lub jeżeli wniosła sprzeciw wobec przetwarzania danych osobowych jej dotyczących, lub jeżeli przetwarzanie jej danych osobowych nie jest z innego powodu zgodne z niniejszym rozporządzeniem.

Nie zawsze jednak administrator będzie zobowiązany do spełnienia żądania.

Zgodnie z art. 17 ust 3 RODO powyższe obowiązki są wyłączone w zakresie, w jakim przetwarzanie jest niezbędne:

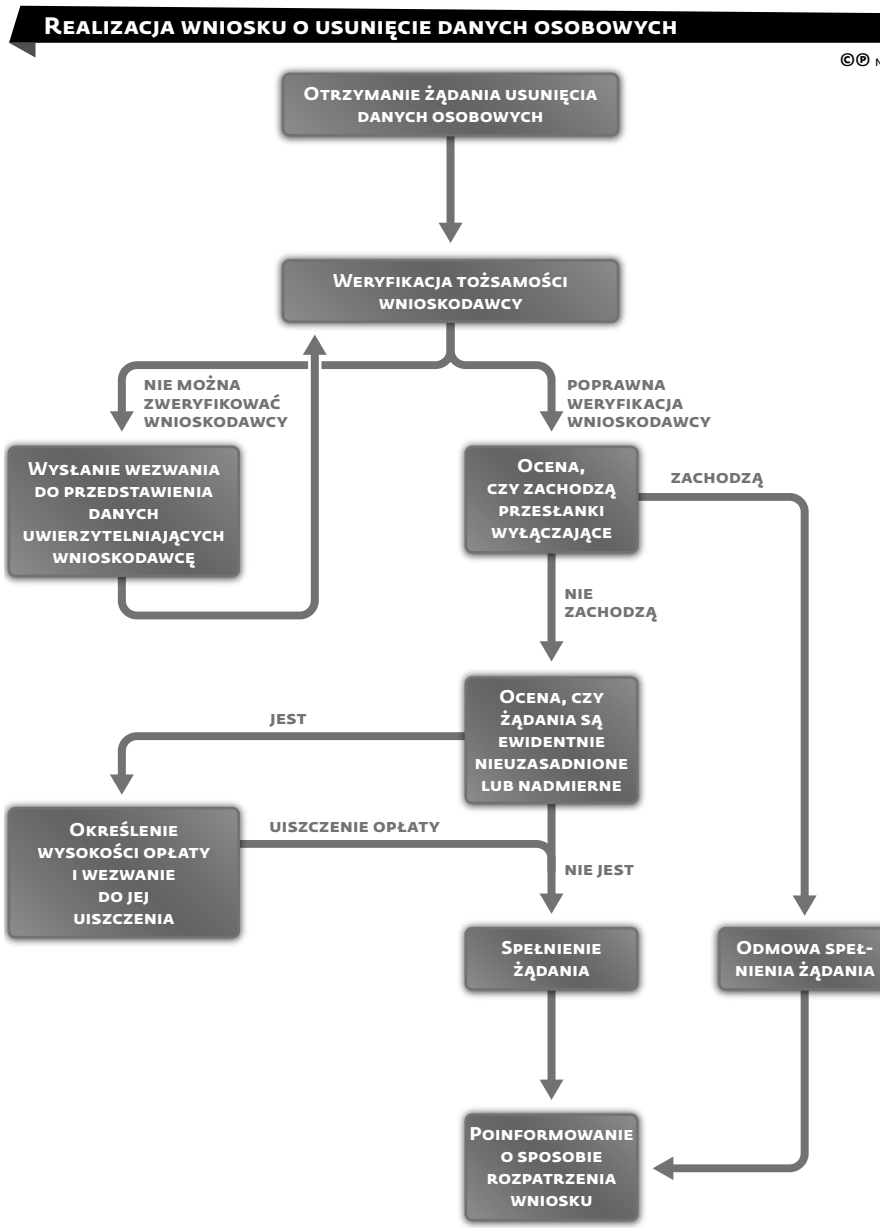
a) do korzystania z prawa do wolności wypowiedzi i informacji;
b) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy przepisów prawa, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
c) z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego zgodnie z art. 9 ust. 2 lit. h oraz lit. i i art. 9 ust. 3 RODO;
d) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1 RODO, o ile prawdopodobne jest, że prawo, o którym mowa w ust. 1, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania;
e) do ustalenia, dochodzenia lub obrony roszczeń.

Przykładowo więc administrator może odmówić usunięcia danych klienta, których przetwarzanie jest niezbędne do wywiązania się przez administratora z obowiązków wynikających z przepisów podatkowych. Administrator może odmówić również prawa do bycia zapomnianym osobie, która zakupiła w prowadzonym przez niego sklepie towar, ale za niego nie zapłaciła w całości. Administrator ma prawo dalej przetwarzać dane tego klienta mimo otrzymanego żądania, ponieważ jest mu to niezbędne w celu odzyskania długu.

W odniesieniu do art. 17 ust. 3 lit. b należy zwrócić również uwagę na wyrok Trybunału Sprawiedliwości w sprawie o sygn. akt C-398/15 (Manni), która dotyczyła obywatela Włoch domagającego się usunięcia z włoskiego rejestru spółek informacji o tym, że pełnił funkcję zarządzającego i likwidatora jednej ze spółek. W wyroku tym, mając na uwadze przeważający interes publiczny, który realizują rejestry spółek, Trybunał wprost odrzucił możliwość usunięcia bądź anonimizacji danych osobowych z rejestru handlowego, dopuszczając jedynie ograniczenie dostępu do nich osobom trzecim.

Administratorzy każdorazowo zobowiązani są do zweryfikowania, czy zachodzi przesłanka usunięcia danych osobowych (art. 17 ust. 1 lit. a–f RODO). Jeżeli tak, będą musieli usunąć dane osobowe objęte żądaniem. W każdym przypadku, zarówno przy spełnieniu żądania, jak i odmowie, należy poinformować osobę, która wniosła żądanie o rozstrzygnięciu jej żądania, w tym o przyczynach ewentualnej odmowy. W przypadku gdy administrator uzna, że żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, może on pobrać rozsądną opłatę, uwzględniając koszty administracyjne. W tej sytuacji administrator określa wysokość opłaty oraz wzywa osobę do uiszczenia opłaty. Za ewidentnie nieuzasadnione może być uznane żądanie, z którego treści wynika, że nie ma żadnego związku faktycznego pomiędzy wnioskodawcą a administratorem. Za nadmierne może być uznane żądanie wystosowywane częściej niż raz na 6 miesięcy, chyba że z faktycznego kontekstu sprawy może wynikać potrzeba ponowienia wniosku wcześniej.

Schemat. Realizacja wniosku o usunięcie danych osobowych



Wymagania nałożone na administratorów prawdopodobnie spowodowały, że zarówno oni, jak i podmioty przetwarzające dane na ich polecenie musiały zmodyfikować metody postępowania z danymi osobowymi. Z zawodowego doświadczenia autorów wynika, że najwięcej problemów przysporzyło administratorom zapewnienie sposobu na udzielanie szybkiej odpowiedzi na żądanie uprawnionego podmiotu (organizacyjnie i technicznie trudno sobie poradzić z dużą ilością żądań w tym samym czasie). Zdarzają się również podmioty, które postanowiły nie modernizować używanych przez siebie (często od wielu lat) systemów informatycznych, mimo że nie posiadały one opcji usuwania raz wprowadzonych do nich danych. Liczyły przy tym najprawdopodobniej (jak pokazują podane poniżej przykłady kar, było to myślenie życzeniowe), że po otrzymaniu żądania albo skłamią, że dane zostały usunięte, albo przemilczą żądanie, a sprawa nie będzie miała swojego dalszego ciągu. O ile w przypadku opóźnienia w odpowiedzi odpowiednie organy poszczególnych państw członkowskich potrafiły być wyrozumiałe dla administratorów, tak w przypadku nieudzielania odpowiedzi potrafiły karać z całą surowością.

5.1.1. Przypadek Delivery Hero Germany GmbH w Niemczech

W sierpniu 2019 r. Maja Smoltczyk, pełniąca urząd berlińskiego komisarza ds. ochrony danych i wolności informacji, nałożyła ponad 195 tys. euro kary na firmę dostarczającą pizzę (Delivery Hero Germany GmbH) za naruszenie obowiązków informacyjnych wobec klientów korzystających z jej usług. Decyzja jest ostateczna.

Według ustaleń berlińskiego inspektora ochrony danych Delivery Hero Germany GmbH nie usuwało kont byłych klientów mimo zgłaszania przez nich takich żądań. Bezpośrednią przyczyną nałożenia kary była skarga na nieusunięcie przez Delivery Hero kont 10 byłych klientów (konsumentów), którzy przestali korzystać z jej usług już w 2008 r. Ośmiu byłych klientów skarżyło się również na niechciane wiadomości e-mail. Delivery Hero Germany GmbH naruszył również niektóre przepisy wobec organu nadzorczego, tłumacząc się błędami technicznymi lub błędem pracownika.

Komisarz przypomniał, że każdy przedsiębiorca, który przetwarza dane osobowe, musi być w stanie technicznie i organizacyjnie przygotowany do bezzwłocznego zastosowania się do odpowiednich wniosków zainteresowanych osób. Wytłumaczenie przygotowane przez

ukaranego przedsiębiorcę nie może więc spotkać się z akceptacją organu. Podejmując decyzję o nałożeniu grzywny i jej wysokości, berlińscy inspektorzy wzięli pod uwagę zarówno przesłanki zaostrzające odpowiedzialność, takie jak liczba i czas występowania naruszeń, ich strukturalny charakter oraz brak reakcji ukaranego podmiotu na wskazówki przekazywane przez organ nadzorczy.

Za złagodzeniem kary przemawiało natomiast to, że Delivery Hero zostało przejęte 1 kwietnia 2019 r. przez holenderski koncern Takeway.com, a wszystkie naruszenia zasadniczo zostały popełnione przed tym przejęciem. Nowy właściciel zaakceptował wysokość grzywny i nie odwoływał się od orzeczenia. Organ nadzorczy postanowił dać szansę nowemu właścicielowi na usunięcie zaniedbań, co zostanie przez niego później poddane ponownej kontroli.

Co ciekawe, berliński komisarz ds. ochrony danych i wolności informacji już w marcu 2019 r. wymierzył innej firmie pierwszą grzywnę za naruszenie przepisów RODO. Karę w wysokości 50 tys. euro otrzymał działający na terenie kilku krajów europejskich (również w Polsce) internetowy bank N26. Fintech w celu zapobiegania praniu brudnych pieniędzy zbierał nazwiska byłych klientów, niezależnie od tego, czy klienta faktycznie podejrzewano o pranie pieniędzy. N26 również zaakceptował grzywnę wymierzoną przez organ oraz ogłosił wiele środków mających zaradzić poprzednim niedociągnięciom organizacyjnym, a tym samym poprawę ochronę danych swoich klientów.

Maja Smoltczyk – berliński komisarz ds. ochrony danych i wolności informacji: *W wielu firmach ochrona danych była przez długi czas zaniedbywana, chociaż jest to szczególnie ważne, podstawowe w erze cyfrowej, prawo. RODO powstało i działa właśnie przeciwko temu typowi naruszeniom. (...) Mam nadzieję, że te kary będą wywierać względem wszystkich przedsiębiorców efekt ostrzegawczy, tak by pamiętali, że każdy, kto pracuje z danymi osobowym, potrzebuje funkcjonującego zarządzania ochroną danych. Pomaga to nie tylko uniknąć grzywny, ale także wzmacnia zaufanie i satysfakcję klientów.*

5.1.2. Przypadek internetowego sprzedawcy na Łotwie

Państwowy inspektorat ds. danych Łotwy (DSI) rozpoczął postępowanie dotyczące skargi wobec sprzedawcy internetowego w związku z niezapewnieniem zgodności z prawami osób, których dane dotyczą,

zgodnie z art. 17 RODO – administrator nie odpowiedział na wniosek osoby, której dane dotyczą, oraz nie usunął jej danych osobowych bez zbędnej zwłoki.

W ramach postępowania DSI ustalił, że w 2018 r. skarżący kilkukrotnie zwracał się do sprzedawcy o usunięcie wszystkich jego danych osobowych, włącznie z numerem telefonu komórkowego skarżącego. Sprzedawca nie spełnił wniosku osoby, której dane dotyczą, w sprawie usunięcia danych i nadal przetwarzał rzeczone dane osobowe (włącznie z numerem telefonu skarżącego).

W dniu 26 sierpnia 2019 r. dyrektor DSI nałożył na sprzedawcę karę finansową w wysokości 7 tys. euro. Kara została nałożona na sprzedawcę, ponieważ nie wypełnił on obowiązku administratora polegającego na wykonaniu wniosku osoby, której dane dotyczą, oraz brakiem współpracy z DSI (sprzedawca nie przekazał DSI wnioskowanych informacji w określonym terminie ani nie zastosował się do zakazu wystosowanego przez DSI zgodnie z art. 58 ust. 2 lit. c oraz g RODO oraz art. 23 łotewskiej ustawy o przetwarzaniu danych osobowych).

Określając wysokość kary, dyrektor DSI wziął pod uwagę charakter, istotność oraz czas trwania naruszenia, stopień współpracy z organem nadzorczym, liczbę osób, których dane dotyczą, objętych naruszeniem oraz całkowity obrót roczny sprzedawcy w poprzednim roku fiskalnym (art. 83 ust. 5 lit. b oraz e RODO).

5.1.3. Przypadek BNP Paribas Personal Finance SA w Rumunii

Rumuński organ nadzoru ds. przetwarzania danych osobowych w wyniku skargi wszczął dochodzenie, w trakcie którego stwierdził, że BNP Paribas Personal Finance SA z siedzibą w Paryżu Oddział w Bukareszcie nie odpowiedział wnioskodawcy w miesięcznym terminie przewidzianym w art. 12 ust. 3 RODO, chociaż zażądał on usunięcia niektórych danych osobowych zgłoszonych w systemie ewidencji biura kredytowego. Bank został ukarany grzywną w wysokości 9508 lei, co odpowiada 2 tys. euro.

Bank po otrzymaniu wniosków od uprawnionych podmiotów odpowiadał na nie, jednak znacznie przekraczając przewidziany w art. 12 ust. 3 RODO termin jednego miesiąca od otrzymania wniosku. Na wysokość

kary wpływ miało to, że bank w uzgodnieniu z organem nadzoru dobrowolnie zastosował środek naprawczy, który polegał na przyjęciu na poziomie spółki środków dotyczących rozstrzygania wniosków osób, których dane dotyczą, tak aby możliwe było dotrzymanie przewidzianego prawem terminu.

5.2. Podsumowanie

Jak widać na przykładach zaprezentowanych w niniejszym rozdziale najgorsze, co może zrobić przedsiębiorca, to brak reakcji na przesłany przez uprawnionego wniosek z żądaniem usunięcia jego danych i brak współpracy z organami nadzoru. W przypadku gdy np. z przyczyn technicznych administrator nie jest w stanie niezwłocznie spełnić żądania usunięcia danych, powinien nawiązać kontakt z wnioskodawcą i poinformować go o tym, wskazując przewidywany czas spełnienia żądania. Bezwzględnie należy również odpowiadać na wezwania i realizować zalecenia organu nadzoru – postawa taka może bowiem spowodować rezygnację z nałożenia kary lub przynajmniej nałożenie jej w dolnych granicach. Każdy administrator może być również pewien, że działanie przeciwne – brak reakcji na wezwania organu nadzoru i niechęć do współpracy – odbiją się na wysokości sankcji nałożonej na administratora. Trzeba bowiem pamiętać, że głównym celem organu nadzoru nie jest realizacja celu fiskalnego i nakładanie kar w jak najwyższej wysokości i za najmniejsze przewiny, lecz zapewnienie poszanowania administratorów dla będących w ich posiadaniu danych osobowych i zapewnienie przestrzegania dotyczących tych danych przepisów. Jeśli cel ten uda się osiągnąć szybko i we współpracy z kontrolowanym administratorem, organ nie będzie zmuszony do sięgania po najbardziej rygorystyczne z posiadanych przez siebie uprawnień.

Rozdział 6.
Powierzenie przetwarzania danych

Przepisy RODO regulują kwestie powierzenia przetwarzania danych osobowych przez administratora. W treści ogólnego rozporządzenia o ochronie danych osobowych próżno jednak szukać definicji powierzenia przetwarzania danych osobowych. Chcąc najprościej wytłumaczyć, czym ono jest, należałoby wskazać, że do powierzenia przetwarzania danych dochodzi wówczas, gdy administrator zleca wybranemu podmiotowi dokonanie w swoim imieniu i na swoją rzecz określonych działań. W większości przypadków, gdy administrator nie jest przygotowany do realizacji danych działań, decyduje się na powierzenie przetwarzania danych osobowych profesjonaliście.

Należy jednak pamiętać, że jeżeli administrator powierzy komuś przetwarzanie danych osobowych, to nadal on decyduje o celu i sposobie przetwarzania tych danych i w dalszym ciągu ponosi odpowiedzialność za przetwarzanie zgodne z przepisami obowiązującego prawa. Podmiot przetwarzający jest natomiast zobowiązany do podejmowania zleconych działań i prawidłowego zabezpieczenia przetwarzania danych osobowych. Administrator w myśl art. 28 RODO ma obowiązek korzystać wyłącznie z usług podmiotów przetwarzających, które zapewniają gwarancję wdrożenia odpowiednich środków technicznych i organizacyjnych spełniających wymogi rozporządzenia i chroniących w odpowiedni sposób prawa osób, których dane dotyczą.

Zgodnie z treścią art. 28 ust. 3 RODO przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora. W dalszej części wspomnianego przepisu wskazano, że umowa powierzenia musi określać: przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa stron. Umowa powierzenia przetwarzania danych osobowych powinna być sporządzona w formie pisemnej (w tym w formie elektronicznej).

Na podstawie umowy powierzenia podmiot przetwarzający powinien zostać zobowiązany do:

a) przetwarzania danych wyłącznie na polecenia administratora;
b) zapewnienia, aby osoby upoważnione do przetwarzania zobowiązały się do zachowania tajemnicy;
c) podjęcia środków zapewniających bezpieczeństwo danych osobowych, zgodnie z art. 32 RODO;
d) pomagania administratorowi w wywiązaniu się z obowiązków dotyczących bezpieczeństwa danych osobowych (art. 32–36 RODO);
e) pomagania administratorowi poprzez odpowiednie środki techniczne i organizacyjne w wywiązaniu się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw, między innymi prawa dostępu do danych, sprostowania danych, usunięcia danych, ograniczenia przetwarzania danych, przenoszenia danych, sprzeciwu;
f) usunięcia lub zwrócenia administratorowi wszelkich danych osobowych oraz usunięcia wszelkich ich istniejących kopii, chyba że prawo unijne lub krajowe nakazują przechowywanie danych osobowych;
g) udostępnienia administratorowi wszelkich informacji niezbędnych do wykazania spełnienia obowiązków nałożonych na podmiot przetwarzający oraz umożliwienia administratorowi przeprowadzania audytów, w tym inspekcji, i przyczyniania się do nich.

Należy wskazać, że podmiot przetwarzający w celu wykonania określonych czynności w imieniu administratora może pod pewnymi warunkami powierzyć ich wykonanie innemu podmiotowi przetwarzającemu (podprocesorowi). W takiej sytuacji dochodzi do podpowierzenia. Aby jednak podmiot przetwarzający mógł skorzystać z takiej możliwości, musi uprzednio uzyskać zgodę administratora. Zgoda może być zarówno szczegółowa, jak i ogólna. Ważne jest natomiast, aby została udzielona pisemnie. Podmiot przetwarzający ma również obowiązek nałożenia na podprocesora takich samych obowiązków, jakie zostały nałożone na niego w umowie z administratorem. Ma to bardzo duże znaczenie z uwagi na to, że jeżeli podprocesor nie wywiąże się ze spoczywających na nim obowiązków w zakresie ochrony danych, to pełna odpowiedzialność wobec administratora za wypełnienie obowiązków podprocesora spoczywa na podmiocie przetwarzającym.

Odpowiedzialność administratora oraz podmiotu przetwarzającego określa natomiast art. 82 RODO. Zgodnie z treścią ust. 2 tego przepisu administrator uczestniczący w przetwarzaniu odpowiada za szkody spowodowane przetwarzaniem naruszającym przepisy RODO. Natomiast podmiot przetwarzający odpowiada za szkody spowodowane przetwarzaniem wyłącznie wtedy, gdy nie dopełnił obowiązków, które RODO nakłada bezpośrednio na podmioty przetwarzające, lub gdy działał poza zgodnymi z prawem instrukcjami administratora lub wbrew tym instrukcjom. Z kolei zgodnie z ust. 4, jeżeli w tym samym przetwarzaniu uczestniczy więcej niż jeden administrator lub podmiot przetwarzający albo uczestniczy w nim zarówno administrator, jak i podmiot przetwarzający i odpowiadają oni za szkodę spowodowaną przetwarzaniem, ponoszą wówczas odpowiedzialność solidarną za całą szkodę.

6.1. Naruszenie obowiązku zawarcia umowy powierzenia przetwarzania danych osobowych – przypadek burmistrza Aleksandrowa Kujawskiego

Brak zawarcia stosownej umowy powierzenia może pociągać za sobą poważne konsekwencje. Przekonał się o tym m.in. burmistrz Aleksandrowa Kujawskiego.

W dniach od 28 stycznia 2019 r. do 1 lutego 2019 r. u burmistrza Aleksandrowa Kujawskiego jako administratora danych przeprowadzona została kontrola zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych. Zakresem kontroli objęty został sposób przetwarzania danych osobowych w ramach procesu wysyłki korespondencji i prowadzenia Biuletynu Informacji Publicznej (BIP), a także sposób prowadzenia rejestru czynności przetwarzania oraz dokumentowania naruszeń ochrony danych osobowych.

W toku kontroli wykazano m.in., że burmistrz jako administrator danych udostępniał dane osobowe usługodawcy hostingowemu, na którego serwerach prowadzony był Biuletyn Informacji Publicznej Urzędu Miejskiego w Aleksandrowie Kujawskim, oraz podmiotowi zajmującemu się serwisowaniem strony BIP bez podstawy prawnej, tj. bez zawarcia umowy o powierzeniu przetwarzania danych osobowych. Tym samym burmistrz naruszył cytowany wcześniej art. 28 ust. 3 RODO. Niestety okazało się, że nie jest to jedyne naruszenie, którego dopuścił się burmistrz. Prezes UODO wskazał bowiem, że w przypadku udostęp-

nienia danych osobowych bez podstawy prawnej (bez uprzednio zawartej umowy powierzenia) następuje jednocześnie naruszenie zasad zgodności z prawem oraz poufności. Nie zawierając stosownej umowy, burmistrz doprowadził również do braku kontroli nad prawidłowością procesu przetwarzania danych zawartych w BIP i nie był w stanie wykazać, że następuje on przy spełnieniu wymogów wynikających z przepisów. Powyższe uchybienia doprowadziły jednocześnie do naruszenia zasady rozliczalności wynikającej z art. 5 ust. 2 RODO.

Organ wskazał ponadto, że burmistrz nie wdrożył odpowiednich procedur wewnętrznych dotyczących przeglądu zasobów opublikowanych w BIP pod kątem zapewnienia przetwarzania danych zgodnie z zasadą ograniczonego przechowywania, w wyniku czego na stronie BIP Urzędu Miejskiego w Aleksandrowie Kujawskim publikowane były dokumenty zawierające dane osobowe przez okres dłuższy, niż wynika to z przepisów prawa. W ten sposób burmistrz naruszył zasadę ograniczonego przechowywania danych określoną w art. 5 ust. 1 lit. e rozporządzenia.

Przeprowadzona kontrola ujawniła także nieprawidłowości polegające na niewdrożeniu odpowiednich środków technicznych i organizacyjnych, mających na celu ochronę praw lub wolności osób fizycznych w związku z przechowywaniem nagrania sesji Rady Miejskiej Aleksandrowa Kujawskiego wyłącznie na serwerach YouTube, bez wykonywania kopii nagrań sesji znajdujących się we własnych zasobach urzędu, oraz nieprzeprowadzeniu analizy ryzyka w związku z korzystaniem przez burmistrza z kanału YouTube (sesje Rady Miejskiej transmitowane były na stworzonym w tym celu kanale w serwie YouTube) w celu realizacji obowiązku prawnego wynikającego z art. 8 ust. 2 ustawy z 6 września 2001 r. o dostępie do informacji publicznej.

Burmistrz jako administrator danych, dokonując wyboru środków służących do transmisji w internecie oraz utrwalania ich za pomocą środków rejestrujących obraz i dźwięk, był odpowiedzialny za proces przetwarzania tych danych oraz realizację zasad przetwarzania wynikających z RODO. Zatem to na burmistrzu spoczywał obowiązek wdrożenia środków technicznych i organizacyjnych zapewniających odpowiedni poziom bezpieczeństwa danych. Z kolei wybór odpowiednich środków powinien być poprzedzony analizą ryzyka naruszenia praw i wolności osób fizycznych. Takiej analizy burmistrz Aleksandrowa Ku-

jawskiego jednak nie przeprowadził, czym naruszył art. 24 ust. 1 RODO i w konsekwencji nie wdrożył odpowiednich środków bezpieczeństwa, co skutkowało naruszeniem art. 32 rozporządzenia.

Jako ostatnie naruszenie organ wskazał braki w rejestrze czynności przetwarzania. Ujawniono, że w rejestrze brakuje informacji o odbiorcach danych, a także terminów usunięcia danych w odniesieniu do niektórych czynności przetwarzania. W tym zakresie, w ocenie organu, burmistrz dopuścił się po raz kolejny naruszenia zasady rozliczalności.

Biorąc pod uwagę charakter oraz liczbę naruszeń, prezes UODO nałożył na burmistrza karę pieniężną w wysokości 40 tys. zł. Była to pierwsza kara pieniężna nałożona na podmiot publiczny w związku z nieprzestrzeganiem przepisów RODO. Na uwagę zasługuje również wysokość nałożonej kary, która stanowi aż 40% maksymalnego wymiaru. Z pewnością kara nałożona na burmistrza ma w pewnym sensie wymiar prewencyjny. Pokazuje, że obowiązek przestrzegania przepisów RODO spoczywa nie tylko na podmiotach prywatnych, ale także na tych należących do sektora publicznego. Bez wątpienia jest to jasny sygnał, aby zweryfikować dotychczasowe procedury wewnętrzne i dostosować je do przepisów rozporządzenia. Jednocześnie w jasny sposób obrazuje, jak naruszenie jednego z obowiązków określonych w RODO (w tym przypadku niezawarcie umowy powierzenia) może przełożyć się na naruszenie wielu innych przepisów i w efekcie doprowadzić do nałożenia dotkliwej kary.

6.2. Podsumowanie

Proces powierzenia przez administratora danych do przetwarzania przez podmiot przetwarzający to jeden z najtrudniejszych do spełnienia wymogów prawnych. Nakłada on na administratora, jak i podmiot przetwarzający, wiele obowiązków, których wypełnienie powinno być w pełni rozliczalne zgodnie z art. 5 ust. 2 RODO.

Warto zatem zadbać, aby:
1) zgodnie z zasadą ochrony danych w fazie projektowania dokonać i udokumentować wybór podmiotu przetwarzającego,
2) zweryfikować zapisy umowy powierzenia przetwarzania danych lub stosowanego innego dokumentu prawnego,
3) ustalić zasady notyfikacji naruszeń ochrony danych,

4) ustalić zasady przeprowadzania audytów podczas trwania umowy,
5) ustalić zasady postępowania z danymi po rozwiązaniu umowy.

Prowadzenie przez administratora audytu u podmiotu przetwarzającego to dobra praktyka, która pozwoli na minimalizację ryzyka współpracy z nierzetelnym dostawcą usługi. Administrator nie musi sam przeprowadzać audytów, zgodnie z RODO może on skorzystać z usług profesjonalnych firm, które w jego imieniu przeprowadzą audyt oraz odpowiednio go udokumentują.

Rozdział 7.
Obowiązek wyznaczenia inspektora ochrony danych (IOD)

Inspektor ochrony danych osobowych (dalej: IOD) to podmiot, którego zadaniem jest stanie na straży przestrzegania przepisów o ochronie danych osobowych oraz wdrożenie w organizacji tych procedur, które w jak najpełniejszy sposób będą chronić dane osobowe. W zakresie niektórych przedsiębiorstw powołanie IOD jest obligatoryjne.

WAŻNE

Zaleca się administratorom udokumentowanie wewnętrznej procedury przeprowadzonej w celu ustalenia i uwzględnienia poszczególnych przesłanek istnienia konieczności lub jej braku w powołaniu inspektora ochrony danych osobowych.

Przepis art. 37 ust. 1 RODO przewiduje obowiązek wyznaczenia IOD dla danego podmiotu, gdy:

a) przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości,
b) główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę, lub
c) główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9, lub danych osobowych dotyczących wyroków skazujących i czynów zabronionych, o czym mowa w art. 10.

Można wskazać na następujące przykłady przetwarzania danych, będącego główną działalnością podmiotu, dokonywanego na dużą skalę:

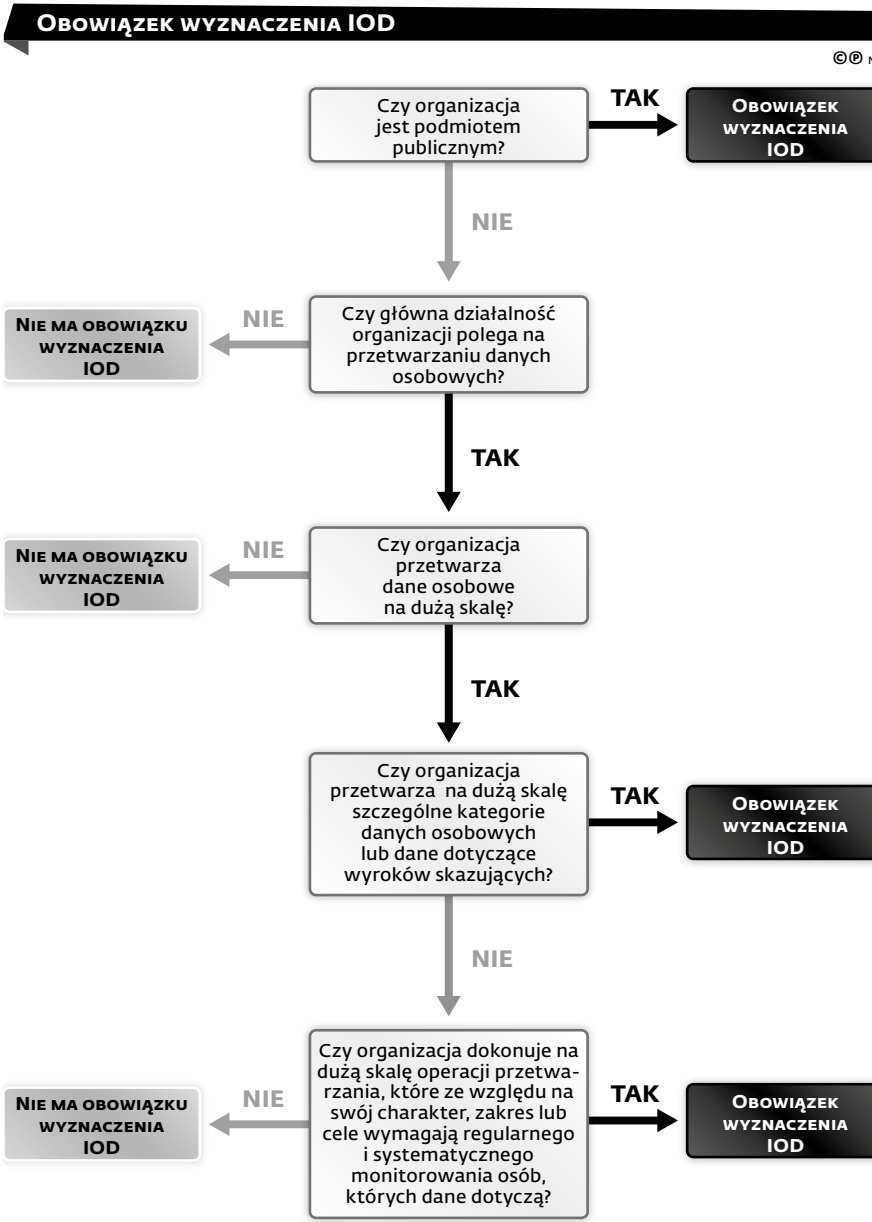
1) przetwarzanie danych pacjentów przez szpital w ramach prowadzonej działalności,
2) przetwarzanie danych klientów przez banki albo ubezpieczycieli w ramach prowadzonej działalności,
3) przetwarzanie danych (dotyczących treści, ruchu, lokalizacji) przez dostawców usług telefonicznych lub internetowych.

Do zadań inspektora należy przede wszystkim:

- informowanie podmiotów, które przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im,
- monitorowanie przestrzegania przepisów o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków,
- podejmowanie działań zwiększających świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty,
- udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO,
- współpraca z organem nadzorczym,
- pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

O wyborze IOD należy poinformować prezesa UODO. Prawidłowym i skutecznym sposobem zawiadomienia o wyznaczeniu jest zawiadomienie w postaci elektronicznej, opatrzone kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.

Schemat. Obowiązek wyznaczenia IOD



7.1. Naruszenie obowiązku wyznaczenia IOD

Przepisy RODO w określonych przypadkach wymagają, aby dany podmiot wyznaczył inspektora ochrony danych osobowych. W przypadku podmiotów, które są prawnie zobowiązane do wyznaczenia inspektora ochrony danych, istnieją następujące rozwiązania:

1) wyznaczenie zewnętrznego inspektora ochrony danych lub
2) wyznaczenie inspektora ochrony danych w przedsiębiorstwie (wewnętrznie).

Bez względu na to, który wariant zostaje wybrany, zadaniem zewnętrznego albo wewnętrznego inspektora ochrony danych jest zapewnienie, że ochrona danych jest przestrzegana i monitorowana w przedsiębiorstwie.

Naruszenie tego obowiązku może wiązać się ze sporą odpowiedzialnością. Przekonała się o tym niemiecka spółka Rapidata GmbH – dostawca internetu. Spółka pomimo wielokrotnych upomnień ze strony niemieckiego organu nadzoru nie wyznaczyła inspektora ochrony danych. Obowiązek wyznaczenia IOD zachodzi m.in., gdy główna działalność administratora polega na operacjach przetwarzania, które wymagają regularnego i systematycznego monitorowania podmiotów danych osobowych. Założenie, że ogólne rozporządzenie o ochronie danych dotyczy tylko dużych przedsiębiorstw, jest błędne. Nie ma minimalnej wielkości podmiotu w celu zaistnienia obowiązku wyznaczenia IOD. Nie stosując się więc do wezwań organu, wskazana spółka naruszyła postanowienia art. 37 RODO, wskutek czego niemiecki organ nadzoru nałożył karę pieniężną w wysokości 10 tys. euro. Przy wymiarze kary wzięto pod uwagę to, że Rapidata GmbH należy do kategorii mikroprzedsiębiorstw.

7.2. Podsumowanie

Obojętnie, czy w danej organizacji występuje obowiązek wyznaczenia IOD, czy jednak nie, trzeba pamiętać, że IOD dla administratora lub podmiotu przetwarzającego będzie stanowić zasadnicze wsparcie. IOD nie tylko będzie monitorował przetwarzanie danych osobowych w organizacji i przestrzeganie przepisów RODO, ale również przyczyniał się do ulepszania procesów przetwarzania danych osobowych. Zalecane jest powierzanie takiej funkcji specjaliście w tej dziedzinie.

Rozdział 8.
Dokumentacja administratora danych osobowych

Każdy administrator jest zobowiązany do wdrożenia odpowiednich środków technicznych i organizacyjnych, które będą zapewniać przetwarzanie zgodnie z RODO (art. 24 RODO). Odnosi się to w szczególności do realizacji zasad przez administratora: zasady zgodności z prawem, rzetelności, przejrzystości, ograniczenia celu, minimalizacji danych, prawidłowości, ograniczenia przechowywania, integralności, poufności i rozliczalności (por. rozdz. 2. Zasady przetwarzania danych osobowych).

Przepis ten odnosi się zatem również do wdrożenia odpowiednich polityk ochrony danych. Z brzmienia przepisu art. 24 ust. 2 RODO wynika, że wdrożenie polityk ochrony danych osobowych jest fakultatywne i zależne od stosowanej oceny administratora. Jednak należy mieć na uwadze, że wdrożenie takiej dokumentacji usystematyzuje przetwarzanie danych i ułatwi administratorowi chociażby wywiązanie się z obowiązku przetwarzania zgodnego z RODO.

Zgodnie natomiast z motywem 78 RODO, aby administrator mógł wykazać przestrzeganie RODO, powinien przyjąć wewnętrzne polityki i wdrożyć środki, które są zgodne w szczególności z zasadą uwzględniania ochrony danych w fazie projektowania oraz z zasadą domyślnej ochrony danych. Jak zostało wskazane, takie środki mogą polegać przede wszystkim na minimalizacji przetwarzania danych osobowych, jak najszybszej pseudonimizacji danych osobowych, przejrzystości co do funkcji i przetwarzania danych osobowych, umożliwieniu osobie, której dane dotyczą, monitorowania przetwarzania danych, umożliwieniu administratorowi tworzenia i doskonalenia zabezpieczeń.

PRZYKŁADOWE POLITYKI OCHRONY DANYCH OSOBOWYCH MOGĄ ZAWIERAĆ

1) omówienie zasad przetwarzania danych osobowych, podstaw przetwarzania danych przez administratora;
2) instrukcje w zakresie dotyczącym realizacji praw osób, których dane dotyczą;

3) informacje dotyczące stosowanych środków zabezpieczających;
4) wykaz budynków, pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe;
5) instrukcje dotyczące powierzenia przetwarzania danych osobowych;
6) wytyczne w zakresie upoważnienia do przetwarzania danych osobowych;
7) procedurę postępowania w przypadku naruszenia danych osobowych;
8) informacje o powołaniu inspektora ochrony danych osobowych albo braku obowiązku jego powołania;
9) informacje o odbiorcach danych osobowych;
10) wytyczne w zakresie przeprowadzania szkoleń z zakresu ochrony danych osobowych;
11) wytyczne w zakresie nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym;
12) wytyczne co do stosowania haseł do systemu informatycznego;
13) procedury rozpoczęcia, zawieszenia, zakończenia pracy użytkowników systemu informatycznego;
14) procedury tworzenia kopii zapasowych;
15) informacje dotyczące sposobu, miejsca i okresu przechowywania elektronicznych nośników informacji zawierających dane osobowe;
16) wytyczne dotyczące przeglądów i konserwacji systemu;
17) informacje o zabezpieczeniach systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego;
18) informacje o odnotowywaniu informacji o odbiorcach danych, którym dane zostały udostępnione, a także o dacie i zakresie udostępnienia;
19) procedurę usuwania danych;
20) politykę czystego biurka i ekranu;
21) politykę korzystania z sieci internet;
22) politykę korzystania z poczty elektronicznej.

W zależności od prowadzonej działalności przez administratora w organizacji może zaistnieć potrzeba przygotowania i wdrożenia innych procedur, mających również na celu bezpieczeństwo danych osobowych.

Abstrahując od polityk ochrony danych osobowych, należy wskazać, że z przepisów RODO wynika również obowiązek stosowania innej dokumentacji przy przetwarzaniu danych osobowych, w szczególności re-

jestru czynności przetwarzania oraz rejestru kategorii czynności przetwarzania (art. 30 RODO), rejestru naruszeń ochrony danych osobowych (art. 33 ust. 5 RODO).

8.1. Rejestr czynności przetwarzania

Każdy administrator powinien prowadzić rejestr czynności przetwarzania danych osobowych, za który odpowiada. Ze względu na to, że administrator ustala cele i sposoby przetwarzania danych, a także ponosi odpowiedzialność za ich przetwarzanie, ustawodawca unijny zobowiązał go do prowadzenia rejestru czynności przetwarzania.

W rejestrze tym zamieszcza się wszystkie następujące informacje:
1) imię i nazwisko lub nazwę oraz dane kontaktowe administratora i wszelkich współadministratorów, a także – gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych;
2) cele przetwarzania;
3) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
4) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich albo w organizacjach międzynarodowych;
5) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń;
6) planowane terminy usunięcia poszczególnych kategorii danych – jeżeli jest to możliwe;
7) ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO – jeżeli jest to możliwe.

Informacje te nie stanowią katalogu zamkniętego. Katalog ten podaje minimalne informacje, jakie ma posiadać prowadzony rejestr. Rejestr powinien mieć formę pisemną, w tym formę elektroniczną. Administrator powinien ująć w rejestrze co najmniej procesy przetwarzania danych i każdy proces uzupełnić o podane informacje.

Obowiązek prowadzenia rejestru czynności przetwarzania nie ma zastosowania do przedsiębiorcy lub podmiotu zatrudniającego mniej niż

250 osób, chyba że przetwarzanie, którego dokonują, może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą, nie ma charakteru sporadycznego lub obejmuje szczególne kategorie danych osobowych albo dane osobowe dotyczące wyroków skazujących i czynów zabronionych. Rekomendowane jest jednak w celach usystematyzowania przetwarzania danych osobowych prowadzenie takiego rejestru w każdym przedsiębiorstwie.

8.2. Rejestr kategorii czynności przetwarzania

Każdy podmiot przetwarzający powinien prowadzić rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora. Przypomnieć można, że podmiot przetwarzający dokonuje przetwarzania w imieniu administratora (por. rozdz. 6. Powierzenie przetwarzania danych).

W rejestrze kategorii czynności przetwarzania zamieszcza się następujące informacje:

1) imię i nazwisko lub nazwa oraz dane kontaktowe podmiotu przetwarzającego albo podmiotów przetwarzających, a także każdego administratora, w imieniu którego działa podmiot przetwarzający, a gdy ma to zastosowanie – przedstawiciela administratora lub podmiotu przetwarzającego oraz inspektora ochrony danych;
2) kategorie przetwarzań dokonywanych w imieniu każdego z administratorów;
3) o przekazaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń – gdy ma to zastosowanie;
4) ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO – jeżeli jest to możliwe.

Informacje te stanowią minimalny zakres, jaki ma posiadać prowadzony rejestr. Rejestr powinien mieć formę pisemną, w tym formę elektroniczną. Obowiązek prowadzenia rejestru kategorii czynności przetwarzania przez podmiot przetwarzający nie ma zastosowania do przedsiębiorcy lub podmiotu zatrudniającego mniej niż 250 osób, chyba że przetwarzanie, którego dokonują, może powodować ryzyko naruszeń

nia praw lub wolności osób, których dane dotyczą, nie ma charakteru sporadycznego lub obejmuje szczególne kategorie danych osobowych.

8.3. Podsumowanie

Dokumentacja dotycząca ochrony danych osobowych w praktyce ma przede wszystkim usystematyzować ochronę danych osobowych w danej organizacji i ułatwić osobom w organizacji prawidłowe operowanie na danych osobowych. Opracowana dokumentacja nie musi być obszerna, ważne, aby zawierała treści, z których będzie można korzystać w określonych przypadkach. Nie należy przygotowywać sztampowej dokumentacji niedostosowanej do organizacji, lecz należy opracować poszczególne treści zgodnie z prowadzoną działalnością, zakres danych osobowych, procesy przetwarzania czy analizy ryzyka. Tylko dostosowana dokumentacja będzie spełniać swoją rolę, w tym zasadę rozliczalności czy legalności przy przetwarzaniu danych.

Rozdział 9.
Podsumowanie – zalecenia

Prawie dwuletni okres obowiązywania RODO nie zlikwidował jeszcze wszystkich rozbieżności w zakresie realizowania obowiązków przewidzianych przepisami tego aktu prawnego. Wiele kwestii nadal nie było przedmiotem ostatecznych stanowisk organów nadzoru. Niezależnie od tego RODO obowiązuje i określa w swoisty sposób zasady i obowiązki dotyczące przetwarzania danych osobowych.

W 2019 r. prezes UODO nałożył kary finansowe za naruszenia przepisów o ochronie danych osobowych na ośmiu administratorów, w tym siedmiu z sektora prywatnego i jednego z sektora publicznego, na łączną kwotę ponad 4 mln zł. Najwyższą dotąd karę w Polsce, przekraczającą 2,8 mln zł, nałożono na spółkę Morele.net za niewystarczające zabezpieczenia danych osobowych.

Każdy podmiot, który przetwarza dane osobowe, jest zobowiązany do wdrożenia w ramach swojej organizacji rozwiązań zapewniających bezpieczne przetwarzanie danych osobowych. Jest zobowiązany na bieżąco monitorować przetwarzanie danych w organizacji i liczyć się z kolejnym ryzykiem oraz wdrażaniem nowych rozwiązań technicznych i organizacyjnych. Nie wystarczy raz wdrożyć RODO, lecz należy zrozumieć istotę ochrony danych i przepisów zawartych w RODO oraz prawidłowo je stosować cały czas w toku działania organizacji.

W niniejszym poradniku staraliśmy się zaakcentować, że RODO stanowi swoistą motywację do przeglądu przetwarzanych danych. Nie można bronić się przed wypełnianiem obowiązków informacyjnych, regulowaniem umów powierzenia przetwarzania danych osobowych czy też przed reagowaniem na incydenty. Każdy administrator powinien zadbać o zestaw procedur, prowadzenie rejestru czynności przetwarzania danych osobowych, stosowanie odpowiednich środków zabezpieczających, a także analizowanie ryzyka czy przeprowadzenie ocen skutków naruszeń.

Kancelaria Prawna ANSWER Wojciechowski i Partnerzy specjalizuje się w obsłudze przedsiębiorstw z branży nowoczesnych technologii, ze szczególnym naciskiem na ochronę danych osobowych, ochronę praw własności przemysłowej oraz odpowiedzialność podmiotów prowadzących handel elektroniczny.

Kamila Kozera,
partner/radca prawny

Bartosz Wojciechowski,
partner/radca prawny

Marcin Dratwiński,
radca prawny

Kamil Szczur,
aplikant radcowski

Michał Sobczak,
aplikant radcowski

Martyna Kośmicka,
aplikant radcowski

Elżbieta Białobrodzka-
-Skrzypiec,
prawnik

ISBN 978-83-66316-66-9