PARP

OCHRONA DANYCH OSOBOWYCH

– poradnik dla małych i średnich przedsiębiorców

enterprise europe network

Wsparcie dla biznesu w zasięgu ręki

Komisja Europejska

Ochrona danych osobowych

– poradnik dla małych i średnich przedsiębiorców

Warszawa 2017

Ochrona danych osobowych – poradnik dla małych i średnich przedsiębiorców

Autorzy:
Wojciech Dziomdziora – wstęp i rozdział 5
Bartosz Mendyk – rozdziały: 1, 2, 3 i 4
Sylwia Stefaniak, Halszka Suszek-Borowska, Olga Budziszewska – rozdział 6
Małgorzata Regulska-Cieślak – rozdział 7

Redakcja:
Paweł Sikorski

Niniejsza publikacja powstała we współpracy z Polską Izbą Informatyki i Telekomunikacji.

Niniejsza publikacja jest współfinansowana przez Komisję Europejską ze środków pochodzących z programu COSME na lata 2014–2020 oraz ze środków Ministerstwa Rozwoju w ramach programu pn. „Udział Polski w programie na rzecz konkurencyjności przedsiębiorstw oraz małych i średnich przedsiębiorstw (COSME) oraz w instrumentach finansowych programów UE wspierających konkurencyjność przedsiębiorstw w latach 2015–2021".

Publikacja jest dostępna w formie e-booka na stronach internetowych:
www.parp.gov.pl oraz www.een.org.pl

ISBN 978-83-7633-362-5

Wydawca:
Polska Agencja Rozwoju Przedsiębiorczości ul. Pańska 81/83
00-834 Warszawa
www.parp.gov.pl

Wydanie I
Nakład: 1 000 egzemplarzy

Skład, łamanie i korekta:
Pracownia C&C sp. z o.o.

SPIS TREŚCI

WSTĘP, CZYLI JAK PRZYGOTOWAĆ PRZEDSIĘBIORSTWO NA RODO?

Wojciech Dziomdziora

Potrzeba głębokiej reformy unijnego systemu ochrony danych osobowych była sygnalizowana w UE od wielu lat. Konieczność wprowadzenia kompleksowych zmian była determinowana wieloma czynnikami. Do najważniejszych z nich należy zaliczyć przestarzałość regulacji ochrony danych osobowych, które, jakby nie było, liczą sobie już ponad 20 lat. W ostatnich latach nasiliła się fala naruszeń prawa ochrony danych osobowych. W połączeniu z brakiem wyposażenia organów w realne środki prawne, uniemożliwiało to skuteczne egzekwowanie odpowiedzialności od podmiotów przetwarzających dane.

Mając na uwadze powyższe, Parlament Europejski i Rada przyjęły w kwietniu 2016 r. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)[1], zwane także w dalszej części publikacji **Rozporządzeniem** lub **RODO**. W polskim porządku prawnym będzie ono stosowane bezpośrednio od dnia 25 maja 2018 r., bez konieczności implementowania go ustawą. Przewiduje ono szereg kwestii, które krajowi ustawodawcy będą mogli doprecyzować, *vide* projekt polskiej ustawy o ochronie danych osobowych, zwanej w dalszej części publikacji również **Projektem** lub **nową UODO**.

Po wejściu w życie RODO przetwarzanie danych osobowych będzie odbywać się w nowym otoczeniu prawnym. W związku z tym, że wprowadzone zmiany niosą za sobą daleko idące konsekwencje prawne i biznesowe, już teraz warto, żeby przedsiębiorcy zwrócili uwagę na najważniejsze obszary, które będą wymagać audytu i przyjęcia szeregu zmian, w tym organizacyjnych i proceduralnych w ich firmach.

Celem niniejszego materiału jest jak najbardziej przystępne i syntetyczne objaśnienie zmian w dziedzinie ochrony danych osobowych, w taki sposób, aby nawet praktyk-amator posiadł podstawową wiedzę o tym, w jaki sposób przygotować się na wejście RODO. Tekst nie posiada waloru opinii prawnej.

We wstępie zostaną zasygnalizowane następujące kwestie:

- zgód na przetwarzanie danych osobowych,
- obowiązku informacyjnego,
- Inspektora Danych Osobowych,
- nowych praw podmiotów danych,
- rejestru czynności przetwarzania danych,
- zgłaszania naruszeń ochrony danych osobowych,
- powierzania przetwarzania danych,
- kodeksów i certyfikatów zgodności przetwarzania danych.

1. KLAUZULE ZGÓD

W świetle zmian wprowadzanych przez RODO, przedsiębiorcy (czyli administratorzy danych) w pierwszej kolejności powinni dokonać audytu zbiorów danych osobowych i podstaw prawnych stosowanych w ich organizacjach do przetwarzania danych.

Z uwagi na to, że jedną z najczęściej stosowanych podstaw przetwarzania danych jest zgoda osoby, której dane dotyczą (czyli podmiotu danych), RODO szczególnie odnośni się do kształtu zgody i jej założeń, które przechodzą ewolucje.

Zgodnie z RODO **zgoda** osoby, której dane dotyczą oznacza:

[1] Dz. Urz. UE, L 119, 4 maja 2016 r.

- dobrowolne,
- konkretne,
- świadome,
- jednoznaczne

okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych w formie ustnej, pisemnej lub elektronicznej. Może to polegać na zaznaczeniu okienka wyboru podczas przeglądania strony internetowej, na wyborze ustawień technicznych do korzystania z usług społeczeństwa informacyjnego lub też na innym oświadczeniu bądź zachowaniu, które w danym kontekście jasno wskazuje, że podmiot danych zaakceptował proponowane przetwarzanie jej danych osobowych. Milczenie, okienka domyślnie zaznaczone lub niepodjęcie działania nie powinny być traktowane jako wyrażenie zgody. Zgoda może zostać wyrażona w formie ustnej, pisemnej i elektronicznej.

Jeżeli przetwarzanie danych ma za podstawę zgodę w myśl Dyrektywy 95/46/WE w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, podmiot danych **nie musi ponownie wyrażać zgody**, **jeżeli pierwotny sposób jej wyrażenia odpowiada warunkom RODO**. Rozwiązanie to z pewnością będzie stanowić znaczne ułatwienie dla administratorów danych (przedsiębiorców).

Kwestią uregulowaną przez RODO jest również przetwarzanie danych osobowych dzieci w ramach świadczenia usług społeczeństwa informacyjnego np. korzystanie z portali społecznościowych czy kont e-mail. Zgodnie z RODO, w przypadku kiedy dochodzi do przetwarzania danych osobowych dziecka poniżej 16 roku życia, przetwarzanie takie jest zgodnie z prawem wyłącznie w sytuacji, w której rodzic lub opiekun prawny dziecka wyraził na to zgodę.

RODO pozostawia państwom członkowskim pewien poziom dyskrecji w określeniu granicy wiekowej, jednak nie może być ona niższa niż 13 lat. Zgodnie z Projektem, w Polsce granica ta będzie wynosić 13 lat.

RODO znosi również wymóg formy pisemnej w zakresie zgody na przetwarzanie danych wrażliwych[2].

1.1. REKOMENDACJE DLA MŚP

W związku ze zmianami w zakresie zgód należy rekomendować:

1. Przeprowadzenie audytu zbiorów danych przetwarzanych w ramach przedsiębiorstwa oraz podstaw prawnych, na podstawie których są przetwarzane dane osobowe.
2. Przeprowadzenie audytu wszystkich zgód zbieranych w przedsiębiorstwie pod kątem ich zgodności z RODO.
3. Ustalenie, czy zebrane już zgody spełniają wymogi RODO i tym samym, czy dalej stanowią legalną podstawę przetwarzania danych osobowych.
4. Ustalenie, czy w ramach działalności administratora danych (przedsiębiorstwa) dochodzi do przetwarzania danych osobowych osób poniżej 13 roku życia.
5. Jeżeli dochodzi do przetwarzania danych osobowych osób poniżej 13 roku życia, należy przygotować odpowiednią procedurę wyrażania zgody na przetwarzanie danych przez rodzica lub opiekuna prawnego oraz przygotować mechanizm weryfikacji wyrażenia tej zgody.
6. Przygotowanie mechanizmu umożliwiającego administratorowi danych wykazanie, że podmiot danych wyraził zgodę.

[2] Dane wrażliwe są to dane osobowe ujawniające w szczególności dane biometryczne, dane dotyczące zdrowia, seksualności, orientacji seksualnej podmiotu danych czy ujawniające przekonania religijne lub światopoglądowe.

2. OBOWIĄZEK INFORMACYJNY

Dla osób fizycznych przetwarzanie ich danych osobowych powinno być jasne, przejrzyste i rzetelne. Celem realizacji wymienionych przymiotów legalnego przetwarzania danych podmiot powinien posiadać wiedzę w przedmiocie tego, kto i po co przetwarza jego dane osobowe. Jednym z narzędzi zapewniających legalność przetwarzania jest **obowiązek informacyjny**, tj. zakres informacji, które administrator danych powinien przekazać podmiotowi danych w związku z przetwarzaniem jego danych osobowych.

Obecnie, zgodnie z art. 24 ust. 1 oraz art. 25 ust. 1 Ustawy o ochronie danych osobowych, administrator danych jest zobowiązany do poinformowania podmiotu o swoich danych identyfikujących, celu przetwarzania danych, kategorii ich odbiorców oraz o obowiązku lub dobrowolności podania danych.

Po 25 maja 2018 r. zakres obowiązku informacyjnego ulegnie znacznemu rozszerzeniu. Zgodnie z RODO administrator danych w przypadku pozyskiwania informacji od osoby, której one dotyczą, będzie zobowiązany do podania:

1) swojej tożsamości, pełnej nazwy i danych kontaktowych;
2) danych kontaktowych IOD (jeżeli został powołany);
3) celu i podstawy przetwarzania danych osobowych;
4) prawnie uzasadnionego interesu/-ów administratora danych (jeżeli takowy istnieje);
5) informacji o odbiorcach danych osobowych lub o kategoriach odbiorców;
6) informacji o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej;
7) okresu przechowywania danych;
8) informacji o prawach podmiotu (dostęp do danych, ich przenoszenie, sprzeciw, sprostowanie, usunięcie etc.);
9) informacji o prawie do cofnięcia zgody;
10) informacji o prawie do wniesienia skargi do organu nadzorczego;
11) informacji, czy podanie danych to wymóg ustawowy lub umowny lub warunek zawarcia umowy oraz konsekwencji niepodania danych;
12) informacji o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu (w tym o zasadach podejmowania, znaczeniach i konsekwencjach).

Jak widać, treść obowiązku informacyjnego jest dużo bardziej rozbudowana w RODO niż w obecnie obowiązujących przepisach i zawiera znacznie więcej informacji dla podmiotu danych. Jest to uzewnętrznienie jednego z założeń stojących za potrzebą nowelizacji przepisów ochrony danych osobowych, tj. zwiększenie uprawnień, świadomości i praw podmiotów danych w związku z przetwarzaniem ich danych osobowych.

2.1. REKOMENDACJE DLA MŚP

W związku ze zmianami w zakresie obowiązku informacyjnego należy rekomendować:

1. Analizę obowiązujących klauzul informacyjnych (papierowych i elektronicznych).
2. Przygotowanie nowych wzorów klauzul informacyjnych (rekomendujemy przygotowanie ich w porozumieniu z osobami odpowiedzialnymi za marketing w przedsiębiorstwie).

3. INSPEKTOR OCHRONY DANYCH

Regulacje RODO przewidują również zmiany w zakresie funkcji oraz wymogów związanych z osobą odpowiedzialną za ochronę danych i prawidłowy proces ich przetwarzania. Obecnie obowiązujące przepisy ochrony danych osobowych przewidują funkcję Administratora Bezpieczeństwa Informacji, dalej zwanego także **ABI**, którego powołanie jest fakultatywne.

Regulacje RODO wprowadzają instytucję Inspektora Ochrony Danych, dalej zwanego także **IOD** lub **inspektorem**, którego powołanie w określonych sytuacjach będzie obowiązkowe dla administratora danych. Dotyczy to sytuacji, w których:

a) przetwarzania dokonują organy lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania 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 oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa.

W odniesieniu do obowiązku powołania IOD, RODO posługuje się pojęciami nieostrymi, takimi jak „główna działalność", „duża skala", „systematycznie", których interpretacja zostanie najprawdopodobniej doprecyzowana przez praktykę. Wskazówką interpretacyjną wspomnianych pojęć są wytyczne Grupy Roboczej artykułu 29[3], dalej także **Grupa art. 29**, dotyczące IOD, które przedstawiają przykładowe sytuacje, w których powołanie IOD będzie obowiązkowe. Chodzi m.in. o działalność szpitali, marketing behawioralny czy przetwarzanie danych osobowych w związku z kartami na komunikacje publiczną[4].

RODO wymaga, aby IOD posiadał odpowiednie kwalifikacje zawodowe, chociaż RODO nie dookreśla ich dokładnie, a także wiedzę fachową na temat prawa i praktyk w dziedzinie ochrony danych, w tym specyficznych dla określonej branży, oraz umiejętności wypełnienia zadań stawianych mu przez RODO. Chodzi m.in. o nadzorowanie przetwarzania danych w przedsiębiorstwie, edukację w zakresie przetwarzania danych osobowych, przygotowywanie i opiniowanie dokumentacji dotyczącej przetwarzania danych.

IOD powinien podlegać jedynie najwyższemu kierownictwu przedsiębiorstwa (np. zarządowi). Nie musi być on pracownikiem administratora danych, funkcja ta może zostać powierzona osobie zewnętrznej na podstawie umowy o świadczenie usług (*outsourcing*).

W ramach swojej działalności IOD powinien być m.in. właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych w przedsiębiorstwie, wspierany przez administratora w wypełnianiu zadań, poprzez zapewnienie mu zasobów niezbędnych do wykonania tych zadań, np. powołania odpowiedniego zespołu wsparcia IOD oraz dostęp do danych osobowych i operacji przetwarzania, nie powinien również otrzymywać instrukcji od administratora danych.

3.1. REKOMENDACJE DLA MŚP

W związku ze zmianami w zakresie obowiązku powołania oraz funkcjonowania IOD należy rekomendować:

1. Przeanalizowanie działalności przedsiębiorstwa pod kątem obowiązku powołania IOD.
2. Rozważenie outsourcingu funkcji IOD.
3. Wybór odpowiedniej osoby na stanowisko IOD i umiejscowienie jej w strukturze.
4. Opracowanie procedury wyboru IOD.
5. Przygotowanie szkoleń lub webinarium z zakresu przetwarzania danych.
6. Opracowanie procedur działań IOD (m.in. zgłaszania naruszeń ochrony danych osobowych do organu nadzorczego lub kontaktu podmiotów danych z IOD).

---

[3] Jest to grupa, utworzona jeszcze na podstawie Dyrektywy, która składa się z organów nadzorczych danych osobowych państw Unii Europejskiej. Polskę reprezentuje GIODO. Grupa ta wydaje wytyczne, które stanowią uzupełnienie oraz objaśnienie zagadnień budzących wątpliwości.

[4] Wytyczne Grupy Roboczej z art. 29 dotyczące Inspektorów Ochrony Danych, wydane 13 grudnia 2016 r., są dostępne na http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

4. NOWE PRAWA PODMIOTÓW DANYCH

Jednym z głównych założeń RODO jest stworzenie mechanizmów dla podmiotów danych, w związku z którymi administratorzy danych zainteresowani wykorzystywaniem danych osobowych w ramach swojej działalności muszą liczyć się z silną kontrolą ze strony ich dysponentów. Idąc tym tropem, RODO znacznie rozszerza katalog praw przysługujących podmiotom danych w odniesieniu do przetwarzania ich danych osobowych.

Zgodnie z brzmieniem rozporządzenia, od 25 maja 2018 r. podmioty danych zostaną wyposażone w takie uprawnienia, jak:

- Prawo do bycia zapomnianym – podmiot danych ma prawo zażądać od administratora niezwłocznego usunięcia jego danych osobowych, jeżeli zajdzie jedna z enumeratywnie wymienionych okoliczności z art. 17 ust. 1 pkt. a-f RODO.
- Prawo do sprostowania danych – podmiot ma prawo żądać od administratora danych niezwłocznego sprostowania dotyczących jego danych osobowych, które są nieprawidłowe. Instytucja ta obecna jest już w polskich przepisach.
- Prawo do ograniczenia przetwarzania – osoba, której dane dotyczą, ma prawo żądania od administratora danych ograniczenia przetwarzania jej danych osobowych w przypadkach wymienionych w art. 18 ust. 1 pkt. a-d RODO.
- Prawo do przenoszenia danych – osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe. Przeniesienie danych jest możliwe, jeżeli przetwarzanie odbywa się na podstawie zgody lub wykonania umowy lub odbywa się w sposób zautomatyzowany (np. scoring kredytowy).
- Prawo do niepodlegania przez konkretną osobę fizyczną decyzjom wywołującym wobec niej skutki prawne lub podobnie wpływającym na nią w inny istotny sposób, a opartym na przetwarzaniu jej danych wyłącznie w sposób zautomatyzowany (za pomocą systemów informatycznych), w tym za pomocą profilowania danych. Przepis ten przewiduje również wyjątki od tej zasady, m.in. gdy takie przetwarzanie danych opiera się na wyraźnie udzielonej zgodzie przez osobę, której one dotyczą.

Co do zasady realizacja wspomnianych praw przysługujących podmiotowi danych powinna być bezpłatna. Jednak jeśli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, administrator może pobrać rozsądną opłatę. Administrator powinien zapewnić podmiotom danych możliwość skorzystania ze swoich praw również drogą elektroniczną, szczególnie kiedy przetwarzanie danych odbywa się elektronicznie. RODO nie przewiduje ograniczeń w częstotliwości korzystania przez podmiot danych z przysługujących mu praw. Administrator danych bez zbędnej zwłoki – a w każdym razie w terminie miesiąca od otrzymania żądania – powinien odnieść się do wniosku osoby, której dane dotyczą w zakresie realizacji przysługujących jej praw. Jeżeli administrator nie spełni żądania podmiotu danych, powinien podać tego przyczyny.

4.1. REKOMENDACJE DLA MŚP

W związku z rozszerzeniem katalogu praw przysługujących podmiotom danych należy rekomendować przygotowanie i implementowanie w przedsiębiorstwie wewnętrznych procedur umożliwiających podmiotowi danych realizację:

- Prawa do bycia zapomnianym;
- Prawa do sprostowania danych;
- Prawa do ograniczenia przetwarzania danych;
- Prawa do przeniesienia danych.

5. REJESTR CZYNNOŚCI

Celem ułatwienia administratorom wypełniania obowiązków związanych z przetwarzaniem danych osobowych, i jednoczesnym ograniczeniem biurokracji w tej materii, RODO wprowadza zupełnie nowe rozwiązanie, które zastąpi obowiązek rejestracji zbiorów danych – rejestr czynności przetwarzania danych osobowych. Obowiązek posiadania takiego rejestru spoczywa zarówno na administratorze danych, jak i na podmiocie, któremu powierzono przetwarzanie danych.

Zgodnie z RODO rejestr powinien zawierać:

- imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także, gdy ma to zastosowanie – dane przedstawiciela administratora oraz inspektora ochrony danych;
- cele przetwarzania – czy jest to np. cel marketingowy, realizacja zawartych umów;
- opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
- kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych – za odbiorców danych nie uznaje się organów publicznych, które występują w ramach konkretnego postępowania;
- przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej;
- planowane terminy usunięcia poszczególnych kategorii danych (jeżeli będzie to możliwe);
- ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, które mają zapewnić odpowiedni stopień bezpieczeństwa przetwarzanych danych, środki te mają uwzględniać m.in. stan wiedzy technicznej, koszty wdrażania, charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw i wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia (jeżeli będzie to możliwe).

Rejestr może być prowadzony w formie pisemnej lub elektronicznej. Administrator lub podmiot przetwarzający dane ma obowiązek udostępnić rejestr na każde żądanie organu nadzorczego. Organ nadzorczy dokonuje kontroli tych rejestrów w celu monitorowania operacji przetwarzania.

Obowiązek posiadania rejestru dotyczy podmiotów zatrudniających powyżej 250 osób, jednakowoż rekomendujemy implementowanie rejestru u każdego administratora danych, choćby dla celów ewentualnej kontroli przez organ nadzorczy.

5.1. REKOMENDACJE DLA MŚP

W związku z wprowadzeniem obowiązku posiadania rejestru czynności przetwarzania danych osobowych należy rekomendować:

1. Przeanalizowanie, czy administrator danych jest zobligowany do prowadzenia takiego rejestru.
2. Przygotowanie i implementowanie rejestru w przedsiębiorstwie.
3. Przygotowanie instrukcji do stosowania rejestru.
4. Przeszkolenie pracowników w zakresie stosowania rejestru.

6. ZGŁASZANIE NARUSZEŃ OCHRONY DANYCH

Wzorem polskiego prawa telekomunikacyjnego czy amerykańskich regulacji stanowych, RODO przewiduje obowiązek zgłaszania naruszeń ochrony danych osobowych do organu nadzorczego. O naruszeniu administrator powinien poinformować organ niezwłocznie, jednak nie później niż 72 godziny od wykrycia naruszenia. Zgłoszenie musi zawierać informacje wskazane w art. 33 ust. 3 pkt. 2-d RODO, czyli m.in. charakter naruszenia, wskazywać kategorię i przybliżoną liczbę osób, których dotyczy naruszenie, możliwe konsekwencje czy dane kontaktowe IOD.

Jeżeli naruszenie może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia o naruszeniu osobę, której dane dotyczą. Zawiadomienie powinno zawierać m.in. dane kontaktowe IOD lub opis możliwych konsekwencji naruszenia. Język, którym posługuje się administrator danych w relacji z podmiotem danych, powinien być jasny i prosty. Jeżeli jest to wykonalne, informacja odnośnie naruszenia może zostać przekazana za pomocą infografik, wyjaśniających podmiotowi danych charakter naruszenia.

6.1. REKOMENDACJE DLA MŚP

W związku z obowiązkiem zgłoszenia naruszeń ochrony danych osobowych nałożonego na administratora danych należy rekomendować:

1. Przygotowanie i implementowanie procedury zgłaszania naruszeń.
2. Przygotowanie i implementowanie procedury informowania podmiotu o naruszeniu.
3. Przygotowanie i implementowanie wzoru komunikatu o naruszeniu.

7. POWIERZENIE PRZETWARZANIA DANYCH

Z uwagi na nieprzerwanie rozwijający się segment usług outsourcingowych i coraz powszechniejsze korzystanie z tych usług przez administratorów danych, konieczne stało się bardziej precyzyjne uregulowanie współpracy pomiędzy administratorem danych osobowych a podmiotem, na rzecz którego dochodzi do powierzenia przetwarzania danych.

Obecnie powierzenie przetwarzania danych jest uregulowane dosyć oszczędnie w art. 31 Ustawy. Przepis wymaga, aby umowa o powierzenie przetwarzania danych określała jedynie cel i zakres danych podlegającym powierzeniu.

Po 25 maja 2018 r. zarówno treść umowy, jak i obowiązki związane z powierzeniem przetwarzania danych osobowych ulegną znacznemu rozszerzeniu.

Regulacje RODO uszczegóławiają obligatoryjne elementy umowy o powierzenie przetwarzania danych, która zgodnie z nowymi przepisami powinna zawierać:

a) przedmiot powierzenia;
b) czas powierzenia;
c) charakter powierzenia;
d) cel powierzenia;
e) rodzaj danych osobowych podlegających powierzeniu;
f) kategorie osób, których powierzane dane dotyczą;
g) obowiązki i prawa administratora (prawo dokonywania kontroli warunków przetwarzania danych osobowych/obowiązek cyklicznego sprawdzania merytorycznej poprawności powierzanych danych osobowych);
h) obowiązki procesora wynikające z art. 28 ust 3 pkt. a–h RODO (m.in. zobowiązanie do zachowania poufności w zakresie przetwarzanych danych, podjęcie środków bezpieczeństwa w stosunku do przetwarzanych danych, legalne korzystanie z usług innego podmiotu przetwarzającego).

Uregulowaniu podlega również kwestia korzystania z usług innych podmiotów przetwarzających w ramach tzw. podpowiedzenia przetwarzania danych. Podmiot przetwarzający nie może korzystać z usług innego przetwarzającego chyba, że administrator udzieli:

- **ogólnej pisemnej zgody na korzystanie z podwykonawców** – przetwarzający jest w tej sytuacji zobowiązany do informowania administratora o wszelkich dodaniach/zastąpieniach podmiotów przetwarzających, z których usług korzysta. Administrator musi mieć możliwość wyrażenia sprzeciwu wobec takich zmian;

- **szczegółowej pisemnej zgody na korzystanie z podwykonawców** – korzystanie z usług podwykonawcy przez podmiot przetwarzający wymaga każdorazowej zgody administratora danych.

7.1. REKOMENDACJE DLA MŚP

W związku ze zmianami dotyczącymi powierzenia przetwarzania danych należy rekomendować:

1. Przeanalizowanie obowiązujących umów pod kątem nowych wymogów dotyczących treści umów o powierzenie przetwarzania danych.
2. Renegocjowanie obowiązujących umów tak, aby ich treść odpowiadała wymogom RODO.
3. Przygotowanie nowych wzorów umów o powierzenie przetwarzania danych uwzględniających zmiany wynikające z RODO.

8. KODEKSY I CERTYFIKATY ZGODNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

Ochrona praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych wymaga wdrożenia odpowiednich środków technicznych i organizacyjnych, by zapewnić spełnienie wymogów niniejszego rozporządzenia. Aby móc wykazać realizację wymogów w zakresie zabezpieczeń przetwarzania danych osobowych, RODO wprowadza certyfikaty, niewystępujące dotychczas ani w polskim ani europejskim prawodawstwie.

Certyfikaty w zakresie danych osobowych będą przyznawane za pośrednictwem podmiotów certyfikujących, należących do sektora prywatnego. Podmioty takie będą posiadać zezwolenie organu nadzorczego i będą musiały odznaczać się wiedzą w zakresie przetwarzania danych osobowych oraz dawać rękojmię należytego wykonywania swoich obowiązków.

Podmioty certyfikujące, jeżeli stwierdzą, że stosowane przez administratora mechanizmy przetwarzania danych osobowych są zgodne z prawem, będą nadawały znak jakości lub oznaczenie ochrony danych osobowych, co będzie równoznacznie z zatwierdzeniem mechanizmu certyfikacji przetwarzania danych osobowych. Stosownie do art. 42 RODO stosowanie zatwierdzonego mechanizmu certyfikacji może być wykorzystane jako element stwierdzenia przestrzegania przepisów ochrony danych osobowych przez administratora danych.

Uzyskanie znaku jakości danych osobowych będzie więc bardzo korzystne dla administratorów danych osobowych. Znak jakości lub oznaczenie w zakresie ochrony danych osobowych będzie z pewnością wyróżnikiem podmiotów rzetelnie i uczciwie przetwarzających dane osobowe i będzie stanowiło pewnego rodzaju dowód staranności dla organu nadzorczego, np. w przypadku kontroli.

Przypomnijmy, że za niezgodne z prawem przetwarzanie danych osobowych RODO przewiduje dotkliwe sankcje w postaci kar pieniężnych do wysokości nawet 20 000 000 euro. Przy wymierzaniu sankcji państwowy organ ochrony danych osobowych bierze pod uwagę, czy administrator danych stosował mechanizmy certyfikacji ochrony danych osobowych, a zatem posiadanie takiego certyfikatu może być okolicznością łagodzącą przy określaniu wymiaru kary pieniężnej.

Przepisy RODO zachęcają przedsiębiorców do przygotowywania i stosowania branżowych kodeksów postępowania. Celem kodeksów jest pomoc we właściwym stosowaniu rozporządzenia RODO i równoczesne zapewnienie spełniania obowiązków wynikających z rozporządzenia przez administratora danych. Kodeksy powinny uwzględnić specyfikę różnych sektorów dokonujących przetwarzania oraz szczególnych potrzeb mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw. Stanowią one swoisty kontrakt zawierany pomiędzy regulatorem a określoną branżą, na podstawie którego sygnatariusze zobowiązują się do zachowania określonych wymogów w zakresie procesu przetwarzania danych.

W takich kodeksach można w szczególności określić obowiązki administratorów czy procesorów związane z ryzykiem naruszenia praw lub wolności osób fizycznych, jakie może powodować przetwarzanie przez nich danych.

Przepisy RODO dotyczące zarówno kodeksów, jak i certyfikacji są ogólne, wymagają doprecyzowania przez ustawodawcę krajowego. Projekt udostępniony przez Ministerstwo Cyfryzacji traktuje o zasadach certyfikacji przez polski organ nadzorczy. Jeżeli chodzi o regulacje dotyczące kodeksów postępowania, na dzień wydania niniejszego poradnika nie zostały one jeszcze opublikowane.

8.1. REKOMENDACJE DLA MŚP

W związku z uregulowaniem funkcjonowania certyfikatów i kodeksów postępowań należy rekomendować:

1. Przeanalizowanie dostępnych programów certyfikacyjnych i rozważenia uczestnictwa przedsiębiorstwa w programie.
2. Rozeznanie w planowanych kodeksach branżowych.
3. Rozważenie możliwości przygotowania sektorowego kodeksu postępowania.

9. PODSUMOWANIE

Od 25 maja 2018 r. omawiana dziedzina będzie w jednolity osób regulowana na szczeblu unijnym, co zapewni jednolitość regulacji w skali UE. Nie jest jednak przesądzone, że paneuropejskie rozporządzenie zapewni jednolitość wykładni i praktyki w stosowaniu go przez krajowe organy nadzorcze. Niemniej przetwarzanie danych osobowych odbywać się będzie w całkowicie nowym otoczeniu prawnym. Podkreślić należy również, że mamy tu do czynienia z niezbyt często spotykaną sytuacją, w której unijna regulacja oddziałuje wprost i bezpośrednio na prawa i obowiązki obywateli. Osobną kwestią jest zagadnienie czytania i stosowania nowego prawa z uwzględnieniem dotychczasowych regulacji i doświadczeń.

Niniejsze opracowanie poświęcone jest wybranym tematom – nowym wymogom, obowiązkom i obostrzeniom – a zamiarem autorów jest możliwie przystępnie i obrazowo przybliżyć wskazane zagadnienia. Wybrana forma i objętość materiału nie pozwalają ani na wyczerpanie tematu, ani na udzielenie odpowiedzi na wszystkie nurtujące pytania. Stąd w razie wątpliwości związanych ze zmianami koniecznymi do przygotowania przedsiębiorstwa na RODO, należy skontaktować się z prawnikami specjalizującymi się we wdrożeniu RODO oraz ochronie danych osobowych.

1. PRZEDMIOT OCHRONY – PODSTAWOWE POJĘCIA

Bartosz Mendyk

Prawidłowe wykonywanie obowiązków związanych z przetwarzaniem danych osobowych wymaga zrozumienia najważniejszych pojęć – definicji z tego obszaru. Na początku warto zaznaczyć, że RODO jest kolejnym krokiem w ewolucji systemu ochrony danych osobowych, dlatego większość użytych w nim definicji nie została przez Rozporządzenie wprowadzona, ale rozszerzona bądź doprecyzowana.

Pojęcia użyte w RODO mogą rodzić wiele pytań. Już sama kluczowa dla omawianego tematu definicja, czyli **dane osobowe**, wymaga szerszej i bardziej dogłębnej analizy. Jest to wynikiem tego, że na podstawie określonych kryteriów niektóre informacje w poszczególnych sytuacjach mogą zostać uznane za **dane osobowe**, a w innych sytuacjach tak się nie stanie. Celem niniejszej publikacji nie jest wyłącznie przedstawienie samej definicji, ale pokazanie odpowiednich mechanizmów, które pozwolą przedsiębiorcy samodzielnie rozpoznać, kiedy ma on do czynienia z danymi osobowymi, a kiedy nie.

Oprócz sygnalizowanego wcześniej pojęcia danych osobowych, w tym także **szczególnych kategorii danych**, kolejnymi definicjami, które zostaną omówione w niniejszym rozdziale, będzie **przetwarzanie danych osobowych** i **zbiory danych osobowych**. Te pojęcia także będą wymagały nieco dłuższego komentarza, chociaż są one w znacznej mierze zbieżne z tymi, które obowiązywały w ustawie z 1997 r. oraz z jej późniejszymi nowelizacjami.

W przepisach RODO zdefiniowano specjalne sposoby przetwarzania danych tj. **anonimizację** oraz **pseudonimizację**. Bardzo ważne jest również nowe pojęcie **profilowania** – ma ono szczególne znaczenie dla przedsiębiorców działających w sektorze IT i start-upów.

Przedsiębiorcy muszą również poznać **warunki pozyskiwania danych osobowych** i ich **przetwarzania**. Chodzi tutaj zarówno o **warunki ogólne** (dane zwykłe), jak i **przesłanki szczególne** (szczególne kategorie danych, wcześniej znane jako dane wrażliwe).

Dopiero zrozumienie tych wszystkich pojęć pozwoli skutecznie zarządzać danymi osobowymi i wdrożyć stosowne procedury zabezpieczające.

1.1. DANE OSOBOWE – DEFINICJA

Pojęcie danych osobowych zostało zawarte w RODO i jest ono zbieżne z uprzednio obowiązującym w polskiej ustawie. Zgodnie z treścią Rozporządzenia dane osobowe oznaczają „(…) informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, (…); możliwa do zidentyfikowania osoba fizyczna to 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”[1] (art. 4. ust 1 RODO).

Wskazując najważniejsze elementy definicji, należy wyróżnić:

1) „… informacje dotyczące…”

Należy to rozumieć bardzo szeroko. Informacją może być wygląd, imię i nazwisko, numer PESEL, kolor oczu, odciski palców, styl ubierania się, pozycja społeczna itd. Jednakże wymienione informacje będą mogły zostać uznane za dane osobowe dopiero wtedy, kiedy zostaną ze sobą powiązane w taki sposób, że dzięki nim będzie możliwa identyfikacja konkretnej osoby. Samo imię i nazwisko, numer identyfikacyjny czy piastowane stanowisko w miejscu zatrudnienia w oderwaniu od innych informacji **nie będzie** daną osobową.

[1] Aktualne będą tezy zawarte w D. Fleszar, *Zakres przetwarzania danych osobowych* w *działalności gospodarczej,* Wolters Kluwer Polska, 2008, s. 50.

2) „…zidentyfikowanej lub możliwej do zidentyfikowania..."

Oznacza to możliwość ustalenia czyjejś tożsamości w sposób niebudzący wątpliwości, czyli wykluczający jakiekolwiek przypuszczenia lub domniemania w tym zakresie. Rozporządzenie wskazuje, że „aby stwierdzić, czy dana osoba fizyczna jest możliwa do zidentyfikowania, należy wziąć pod uwagę wszelkie rozsądnie prawdopodobne sposoby (w tym wyodrębnienie wpisów dotyczących tej samej osoby), w stosunku do których istnieje uzasadnione prawdopodobieństwo, iż zostaną wykorzystane przez administratora lub inną osobę w celu bezpośredniego lub pośredniego zidentyfikowania osoby fizycznej. Aby stwierdzić, czy dany sposób może być z uzasadnionym prawdopodobieństwem wykorzystany do zidentyfikowania danej osoby, należy wziąć pod uwagę wszelkie obiektywne czynniki, takie jak koszt i czas potrzebne do jej zidentyfikowania, oraz uwzględnić technologię dostępną w momencie przetwarzania danych, jak i postęp technologiczny" (Motyw 26 RODO).

Informacji **nie uważa** się zatem za umożliwiającą określenie tożsamości osoby, jeżeli pomimo poniesionych kosztów, poświęconego czasu lub podjętych działań wykorzystanie tej informacji do zidentyfikowania osoby byłoby utrudnione. Klauzule generalne, czyli koszty, czas itd., zostaną doprecyzowane przez orzecznictwo sądowe.

Studium przypadku 1.

Numer rejestracyjny samochodu dla przedsiębiorcy niemającego dostępu do odpowiednich baz danych nie pozwoli na identyfikację właściciela pojazdu. Może najwyżej wskazać, że właściciel auta zarejestrował pojazd w określonej miejscowości. Tymczasem dla firmy detektywistycznej, która na podstawie numeru jest w stanie zidentyfikować właściciela za pomocą odpowiednich instrumentów, będzie on stanowić daną osobową.

Studium przypadku 2.

Danymi osobowymi **nie będą** pojedyncze informacje o dużym stopniu ogólności, np. nazwa ulicy i numer domu czy wysokość wynagrodzenia. Informacja ta będzie jednak stanowić daną osobową wówczas, gdy zostanie zestawiona z innymi dodatkowymi informacjami, które w konsekwencji można odnieść do konkretnej osoby.

3) „…osoby fizycznej…"

Ten fragment definicji oznacza, że przepisy regulujące kwestie ochrony danych osobowych dotyczą wyłącznie **pozostających przy życiu osób fizycznych**[2]. RODO nie ma zatem zastosowania do danych osobowych osób zmarłych, chociaż państwa członkowskie Unii Europejskiej mogą przyjąć odrębne przepisy dotyczące przetwarzania danych takich osób.

Tytułem uzupełnienia warto zauważyć, że ochrona ma zastosowanie do osób fizycznych – **niezależnie od ich obywatelstwa czy miejsca zamieszkania**.

Ponadto RODO **nie dotyczy** przetwarzania danych osobowych dotyczących osób prawnych, w szczególności przedsiębiorstw będących osobami prawnymi, w tym danych o firmie i formie prawnej oraz danych kontaktowych osoby prawnej (Motyw 14 RODO).

4) „…w celu bezpośredniego lub pośredniego zidentyfikowania osoby fizycznej…"

Pośrednia identyfikacja ma miejsce wtedy, kiedy do ustalenia tożsamości danej osoby zostają wykorzystane informacje zawarte w kilku zbiorach danych. Może to być np. lista zatrudnionych pracowników w przedsiębiorstwie X oraz lista kart ewidencjonujących czas pracy pracowników w tej firmie (Motyw 26 RODO).

Pośrednia możliwość zidentyfikowania jest związana również z **elektronicznym przetwarzaniem danych**. Osobom fizycznym mogą bowiem zostać przypisane identyfikatory internetowe – **takie jak adresy IP,**

[2] Aktualna pozostaje decyzja GIODO o sygn. DOLiS/DEC-520/12/35884.

identyfikatory plików cookie – generowane przez ich urządzenia, aplikacje i protokoły czy też inne identyfikatory, generowane na przykład przez etykiety RFID[3]. Może to skutkować zostawianiem „śladów", które, w szczególności w połączeniu z unikatowymi identyfikatorami i innymi informacjami uzyskiwanymi przez serwery, mogą być wykorzystywane do tworzenia profili i ich późniejszego uzupełniania lub modyfikowania oraz do identyfikowania konkretnych osób (Motyw 30 RODO).

Bezpośrednia identyfikacja wykorzystuje tylko jeden zbiór danych. Może to być np. teczka osobowa pracownika przedsiębiorstwa X.

1.1.1. POCZTA ELEKTRONICZNA

Adresy poczty elektronicznej (e-mail) w niektórych przypadkach są danymi osobowymi w rozumieniu RODO. Zazwyczaj bowiem są w nich umieszczone takie informacje jak:

- imię,
- nazwisko,
- dodatkowa informacja,

które w połączeniu pozwalają na identyfikację właściciela adresu poczty elektronicznej w sposób pośredni lub bezpośredni. Nie dzieje się tak jednak w każdym przypadku.

Studium przypadku 3.
Na liście subskrybentów newslettera sklepu internetowego są zarówno adresy e-mail, które stanowią dane osobowe (np. jan_stanislaw_kowalski@nazwafirmy.com.pl), jak i takie, które ich nie stanowią (np. flamaster@provider.eu). Mail kancelaria@bm.com.pl również nie będzie stanowił danej osobowej, bowiem nie wskazuje, kto w ramach prowadzonej działalności wykorzystuje skrzynkę pocztową.

1.1.2. ADRESY IP

Inną kwestią jest to, czy **adres IP** (z ang. *Internet Protocol Adddress*) stanowi daną osobową. Adres IP jest to numer porządkowy przypisany urządzeniu, które jest elementem sieci informatycznej. Sam numer nie pozwala w sposób bezpośredni zidentyfikować osoby fizycznej, która użytkuje urządzenie. Zakwalifikowanie adresu IP jako danej osobowej wiąże się z koniecznością posiadania dodatkowych informacji umożliwiających identyfikację osoby użytkującej urządzenie. Pojawia się także pytanie o to, czy adres IP ma charakter stały.

Jeżeli adres IP jest przyporządkowany do lokalnej sieci internetowej (z ang. *Local Area Network* – LAN), z której korzysta wielu współużytkowników, nie będzie daną osobową[4].

Adres IP będzie natomiast stanowić daną osobową, jeżeli:

- jest on na stałe przypisany do konkretnego urządzenia,
- urządzenie to jest przypisane konkretnemu użytkownikowi.

W powyższym przypadku jest bowiem możliwość identyfikacji konkretnej osoby fizycznej[5].

1.1.3. WIZERUNEK OSOBY FIZYCZNEJ

Szczególną kwestią, której nie można pominąć przy okazji rozważań na temat danych osobowych, jest **wizerunek osoby fizycznej**. Coraz więcej przedsiębiorców, zwłaszcza z branży usługowej (np. szkoły językowe lub szkoły aktywnego wypoczynku), prowadzi własne strony internetowe bądź tzw. *fun page* na portalach społecznościowych. Często umieszczają tam wizerunki ludzi korzystających z oferowanych przez nich usług.

---

[3] *Radio-frequency identification* – technologia przesyłania danych za pomocą fal radiowych.

[4] Aktualność zachowują również tezy wyrażone przez P. Barta, P. Litwiński w publikacji *Ustawa o ochronie danych osobowych. Komentarz*, 4 wydanie, s. 100–101.

[5] Wyrok Naczelnego Sądu Administracyjnego z 19 maja 2011 roku, sygn. (I OS K 1079/1021).

RODO precyzuje, że przetwarzanie fotografii nie powinno zawsze stanowić przetwarzania szczególnych kategorii danych osobowych, gdyż fotografie są objęte definicją „danych biometrycznych" tylko w takich przypadkach, w których są przetwarzane specjalnymi metodami technicznymi, umożliwiającymi jednoznaczną identyfikację osoby fizycznej lub potwierdzenie jej tożsamości (Motyw 51 RODO).

Wykorzystanie wizerunku oraz jego ochrona jest przewidziana w:

- RODO,
- Kodeksie cywilnym[6],
- Ustawie o prawie autorskim i prawach pokrewnych[7].

Wizerunek to wygląd człowieka bez względu na technikę jego utrwalenia, czyli:

- fotografia,
- rysunek,
- wycinanka,
- sylwetka,
- film,
- przekaz telewizyjny,
- przekaz wideo[8].

Zezwolenie na rozpowszechnianie wizerunku może być udzielone w dowolnej formie[9]. Bez zezwolenia osoby utrwalonej na zdjęciu jest dozwolone wykorzystanie wizerunku w dwóch wskazanych poniżej sytuacjach.

1. Chodzi o osobę powszechnie znaną, jeżeli wizerunek wykonano w związku z pełnieniem przez nią funkcji publicznych, w szczególności politycznych, społecznych, zawodowych[10]. Będzie to miało zastosowanie do polityków, sportowców, aktorów, dziennikarzy lub osoby powszechnie nieznanej, która urządza happening[11].
2. Chodzi o sytuację, w której osoba stanowi jedynie szczegół większej całości, czyli np. zgromadzenia publicznego, krajobrazu, imprezy masowej itd.

Osoba decydująca się na udział w zgromadzeniu publicznym wyraża **w sposób dorozumiany zgodę** na upublicznienie jej wizerunku[12].

Studium przypadku 4.
Na pierwszym planie plakatu szkoły językowej stoi trzech klientów, trzymając kciuki uniesione do góry. Ich twarze stanowią dane osobowe.

Studium przypadku 5.
Przedsiębiorca prowadzący szkołę prawa jazdy fotografuje w pełni wyposażoną salę wykładową. Na zdjęciu występuje jeden klient, który studiuje planszę dotyczącą pierwszeństwa na skrzyżowaniu. Na zdjęciu można rozpoznać klienta. Jednakże jego twarz jest szczegółem całości – zdjęcie ma bowiem pokazać wyposażoną salę do prowadzenia zajęć. W tym wypadku twarz klienta nie będzie stanowić danych osobowych.

6 Dz.U. 1964 nr 16 poz. 93. ze zm.
7 Dz.U. 1994 nr 24 poz. 83. ze zm.
8 Wyrok Sądu Apelacyjnego w Katowicach z dnia 28 maja 2015 roku o sygn. (I ACa 158/15).
9 Wyrok Sądu Apelacyjnego we Wrocławiu z dnia 27 czerwca 2014 roku o sygn. (I ACa 633/14).
10 W zakresie pojęcia osób publicznych zob. B. Banaszak, K. Wygoda, *Pojęcie Funkcji Publicznej jako przesłanka modyfikująca zakres ochrony danych osobowych*, [w:] *Ochrona danych osobowych, wczoraj, dziś, jutro*, Warszawa 2006,wyd. GIODO, 59 i n.
11 Wyrok Sądu Apelacyjnego w Poznaniu z dnia 2 września 2010 roku o sygn. (I ACa 620/10).
12 Wyrok Sądu Apelacyjnego w Łodzi z dnia 6 października 2014 roku o sygn. (I ACa 429/14).

1.2. SZCZEGÓLNE KATEGORIE DANYCH

W dotychczas obowiązującej ustawie mieliśmy do czynienia z danymi wrażliwymi, zwanymi także danymi sensytywnymi. Były one wyodrębnione na zasadzie wyjątku, czyli zostały enumeratywnie wyliczone, a ich lista była zamknięta. W RODO prawodawca europejski używa pojęcia **szczególna kategoria danych**. Będą to tylko i wyłącznie dane, które ustawodawca europejski bezpośrednio zakwalifikował do tej kategorii.

W art. 9 RODO wskazano, że szczególną kategorię danych tworzą informacje:

- ujawniające pochodzenie rasowe lub etniczne,
- ujawniające poglądy polityczne,
- ujawniające przekonania religijne lub światopoglądowe,
- ujawniające przynależność do związków zawodowych,
- dotyczące przetwarzania danych genetycznych,
- ujawniające dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej,
- ujawniające dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby.

W ustawie z 1997 roku wskazywano, że wrażliwymi danymi osobowymi są również dane o:

- przekonaniach filozoficznych,
- przynależności wyznaniowej,
- przynależności partyjnej,
- skazaniach,
- orzeczeniach o ukaraniu i mandatach karnych,
- innych orzeczeniach wydanych w postępowaniu sądowym lub administracyjnym,
- nałogach.

W RODO wyżej wskazane dane nie stanowią szczególnych kategorii danych. Do szczególnej kategorii danych zaliczono natomiast wspomniane wyżej:

- przekonania światopoglądowe,
- dane biometryczne,
- dane dotyczące zdrowia,
- dane genetyczne.

W ustawie o ochronie danych osobowych z 1997 r. dane te nie były wymienione lub były niedookreślone. Używane w obowiązującym dotychczas akcie prawnym określenie „kod genetyczny" odpowiada danym genetycznym w RODO. W Rozporządzeniu z danych genetycznych zostały też wyszczególnione **dane biometryczne**.

Co istotne, inaczej niż w wyżej wspomnianej ustawie, np. decyzje administracyjne **nie będą ujęte w tej kategorii.** To samo dotyczy orzeczeń w sprawach cywilnych lub gospodarczych.

RODO wskazuje również, że do szczególnych kategorii danych należą przekonania światopoglądowe, jednakże dopiero orzecznictwo sądowe doprecyzuje to pojęcie[13].

Przetwarzanie wyżej wymienionych kategorii danych co do zasady **jest zabronione**. Odstępstwa są możliwe **tylko** w sytuacjach, w których RODO tak stanowi. Przesłanki te zostaną wskazane na końcu rozdziału.

[13] Zob. Blog Dane Osobowe wpis pt. *Czym są dane osobowe wg RODO?* https://blog-daneosobowe.pl/czym-sa-dane-osobowe-wg-rodo/

Studium przypadku 6.
Przedsiębiorca rozważający wydzielenie pomieszczenia, w którym wolno palić papierosy, zbiera informacje, którzy z jego pracowników to osoby palące. Według przepisów RODO w takim przypadku **nie następuje** proces zbierania szczególnej kategorii danych. Dla przypomnienia – ustawa o ochronie danych osobowych z 1997 r. dane o nałogach uznaje za dane wrażliwe.

1.2.1. DANE GENETYCZNE, BIOMETRYCZNE ORAZ DANE DOTYCZĄCE ZDROWIA

Ze względu na ryzyko związane z przetwarzaniem szczególnych kategorii danych, RODO wyodrębniło te dane, które powinny być chronione w sposób szczególny. Zgodnie z art. 4 RODO są to:

- **dane genetyczne**, które należy definiować jako **dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej**, uzyskane z analizy próbki biologicznej danej osoby fizycznej, w szczególności z analizy chromosomów, kwasu dezoksyrybonukleinowego (DNA) lub kwasu rybonukleinowego (RNA) lub z analizy innych elementów umożliwiających pozyskanie równoważnych informacji;
- **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;
- **dane dotyczące zdrowia** oznaczają **dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej** – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia. Te ostatnie RODO definiuje szeroko, wskazując, że do tej kategorii należy zaliczyć:
- wszystkie dane o stanie zdrowia osoby, której dane dotyczą, ujawniające informacje o przeszłym, obecnym lub przyszłym stanie fizycznego lub psychicznego zdrowia osoby, której dane dotyczą; do danych takich należą informacje o danej osobie fizycznej zbierane podczas jej rejestracji do usług opieki zdrowotnej lub podczas świadczenia jej usług opieki zdrowotnej; numer, symbol lub oznaczenie przypisane danej osobie fizycznej w celu jednoznacznego zidentyfikowania tej osoby fizycznej do celów zdrowotnych;
- informacje pochodzące z badań laboratoryjnych lub lekarskich części ciała lub płynów ustrojowych, w tym danych genetycznych i próbek biologicznych oraz wszelkie informacje, na przykład o chorobie, niepełnosprawności, ryzyku choroby, historii medycznej, leczeniu klinicznym lub stanie fizjologicznym lub biomedycznym osoby, której dane dotyczą, niezależnie od ich źródła, którym może być na przykład lekarz lub inny pracownik służby zdrowia, szpital, urządzenie medyczne lub badanie diagnostyczne in vitro (Motyw 35 RODO).

Podsumowując, ustawodawca europejski **wskazuje, że dane dotyczące zdrowia stanowią szeroką definicję** i w przypadku wątpliwości przedsiębiorca powinien posłużyć się szeroką definicją.

1.3. DANE DOTYCZĄCE WYROKÓW SKAZUJĄCYCH I NARUSZEŃ PRAWA

RODO wyodrębnia kolejną kategorię danych – dane dotyczące wyroków skazujących i naruszeń prawa, które nie będą stanowiły szczególnej kategorii danych. Z jednej strony autorzy RODO wskazują, że podstawą ich przetwarzania będzie art. 6 i przetwarzanie tych danych będzie podlegało ogólnym zasadom, ale dopisano przepis, który zawiera istotne ograniczenie.

Artykuł 10 RODO wskazuje mianowicie, że ich przetwarzanie **będzie dopuszczalne wyłącznie pod nadzorem władz publicznych lub jeżeli prawo UE lub państwa członkowskiego będzie przewidywało taką możliwość.** Należy pamiętać, że dotyczy to wyłącznie wyroków skazujących i naruszeń prawa – jak sygnalizowano wcześniej, ograniczenia art. 10 nie będą obowiązywały np. w stosunku do decyzji administracyjnych czy orzeczeń sądów cywilnych.

1.4. PRZETWARZANIE DANYCH W ZBIORZE

Przedsiębiorca powinien przyjąć, że niezależnie od tego, czy dane osobowe są przetwarzane w zbiorze czy poza nim, podlegają przepisom Rozporządzenia.

1.4.1. ZBIÓR DANYCH OSOBOWYCH

Zbiór danych osobowych został zdefiniowany w RODO podobnie jak w dotychczasowej ustawie. Oznacza on „uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie" (art. 4 ust. 6 RODO).

Definicja zbioru składa się zatem z dwóch elementów, które należy doprecyzować.

1. **„…uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów…"**

Oznacza to konieczność zawarcia kryteriów umożliwiających odnalezienie danych osobowych w zestawie. Przyjmuje się, że mogą to być co najmniej dwa kryteria[14]:

a) osobowe (np. imię, nazwisko, data urodzenia, PESEL);
b) nieosobowe (np. data zamieszczenia danych w zbiorze)[15].

Z powyższego wynika, że tak jak w UODO, w **RODO istotna jest struktura zbioru,** czyli możliwość wyszukania według określonego klucza.

2. **„…niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie".**

Oznacza to, że niektóre kategorie danych mogą znajdować się np. w jednym skoroszycie, w drugim natomiast mogą znajdować się pozostałe kategorie danych związane z tymi pierwszymi.

Studium przypadku 7.
Rozproszony zbiór danych to np. zestaw informacji o pracownikach gromadzonych w związku z ich zatrudnieniem i świadczeniem przez nich pracy. Określone komórki organizacyjne pracodawcy, np. dział kadrowo-płacowy wykorzystują dane, które mogą być gromadzone w innym miejscu, np. w biurze obsługi. Istotne jest, aby istniało kryterium, na podstawie którego dział kadrowo-płacowy będzie mógł wyszukać dane.

Rozproszenie ma miejsce niezależne od tego, czy występuje w systemie informatycznym czy w formie papierowej.

Studium przypadku 8.
Proste etui na wizytówki, w które przedsiębiorca dowolnie wsuwa wizytówki swoich kontrahentów, nie będzie stanowić zbioru danych, bowiem nie ma tam kryteriów wyszukiwania. Natomiast książka na wizytówki, w której przedsiębiorca porządkuje je, np. według branż itp., będzie stanowić zbiór danych. W RODO istotne jest uporządkowanie według określonych kryteriów.

[14] Wyrok Naczelnego Sądu Administracyjnego z dnia 12 stycznia 2007 roku o sygn.(I OSK 218/06).

[15] Dlatego aktualne pozostają tezy komentarza J. Barta, P. Litwińskiego, Komentarz, 3. wydanie, Warszawa: C.H. Beck, 2015, który również zwraca uwagę, że „to bowiem struktura zbioru danych osobowych powinna zapewnić dostęp do danych zawartych w zbiorze."Ten sam autor zwraca jednak uwagę, że„nie można utożsamiać dostępności informacji w zbiorze z ich uporządkowaniem – o uporządkowaniu można bowiem mówić jedynie w znaczeniu posiadania przez zbiór odpowiedniej struktury, co nie oznacza jednak uporządkowania poszczególnych elementów, ale jedynie ich dostępność". por. P. Fajgielski, *Ochrona danych osobowych w telekomunikacji* – aspekty prawne, Lublin, wydawnictwo: „Lubelskie Towarzystwo Naukowe", 2003, s. 47.

1.4.2. PRZETWARZANIE DANYCH W ZBIORZE

Prawodawca unijny zdefiniował również pojęcie **przetwarzania danych** (art. 4 ust. 2 RODO). Oznacza ono operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany. Są to w szczególności:

- zbieranie,
- utrwalanie,
- organizowanie,
- porządkowanie,
- przechowywanie,
- adaptowanie lub modyfikowanie,
- pobieranie,
- przeglądanie,
- wykorzystywanie,
- ujawnianie poprzez przesłanie,
- rozpowszechnianie lub innego rodzaju udostępnianie,
- dopasowywanie lub łączenie,
- ograniczanie,
- usuwanie lub niszczenie.

Trudno znaleźć w prawie szerszą definicję. Należy uznać, że **faktycznie każda czynność, jakiej zostały poddane dane osobowe, będzie oznaczać ich przetwarzanie.**

Studium przypadku 9.
Przedsiębiorca zakupił nowe dyski twarde służące do przechowywania danych osobowych jego pracowników. Po przeniesieniu danych na nowe nośniki zniszczył te, na których do tej pory przechowywał dane. Niszczenie dotychczasowych nośników stanowi czynność przetwarzania danych.

Studium przypadku 10.
Przedsiębiorca postanowił zarchiwizować dane osobowe swoich pracowników. Oddanie dokumentów do archiwum zakładowego stanowi przetwarzanie danych osobowych.

1.4.3. PRZETWARZANIE DANYCH W DUŻEJ SKALI

Dotychczasowy obowiązek zawiadamiania organu nadzorczego (od 25 maja 2018 r. ma być to Urząd Ochrony Danych Osobowych) o przetwarzaniu danych osobowych **zostaje przez RODO zniesiony**. Europejski ustawodawca uznał, że tego typu działanie jest nie tylko niepotrzebne, ale przede wszystkim nieskuteczne. W RODO zostały uwypuklone **szczególne rodzaje** przetwarzania danych. Jednym z nich jest **przetwarzanie danych w dużej skali**. W przypadku dokonywania takiej czynności, na przedsiębiorcę zostały nałożone nowe obowiązki, takie jak np. poddanie przez administratora ocenie skutkom takiego przetwarzania. Obowiązek ten zostanie przedstawiony w kolejnym rozdziale.

RODO **nie definiuje**, czym jest duża skala przetwarzania. Grupa Art. 29 zauważa, że pojęcie „dużej skali" nie może być oparte na kryterium ilościowym, w każdej sytuacji należy to rozpoznawać indywidualnie. Można jednak założyć, że im bardziej działalność przedsiębiorcy jest związana z siecią internetową, np. prowadzi sklep internetowy, tym bardziej będzie prawdopodobne, że przetwarzanie odbywa się w dużej skali. Podobnie będzie w przypadku, kiedy usługa świadczona przez przedsiębiorcę polega na dostarczaniu tzw. inteligentnych urządzeń – aut, które same parkują lub liczników poboru ciepła, które sprawdzają, czy domownicy są w domu. We wszystkich tych przypadkach będzie można mówić o przetwarzaniu danych na dużą skalę.

1.4.4. ANONIMIZACJA I PSEUDONIMIZACJA

RODO definiuje, że przetwarzanie oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany. W takich przypadkach mają zastosowanie wszystkie zasady i procedury dotyczące ochrony danych, o których jest mowa w RODO. Z racji tego, że wspomnianych zasad i procedur jest dużo, Rozporządzenie stara się nakłonić administratorów danych do anonimizacji lub pseudonimizacji.

Techniki anonimizacji zostały doprecyzowane przez Grupę art. 29[16]. Wskazuje ona, że „zasady ochrony danych osobowych **nie powinny mieć zastosowania do informacji anonimowych**, czyli do takich, które nie wiążą się ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną, ani do danych osobowych zanonimizowanych w taki sposób, że osób, których te dane dotyczą, w ogóle nie można zidentyfikować lub już nie można zidentyfikować" (Motyw 26 RODO). Z powyższego można wysnuć wniosek, że jest to działanie **nieodwracalne** – po zanonimizowaniu danych w przyszłości nie będzie możliwe zidentyfikowanie określonej osoby na podstawie tych informacji. Na marginesie można zauważyć, że takie kategorie danych nie tworzą danych osobowych, a operacja na takich danych **nie stanowi** przetwarzania. Chociaż samo anonimizowanie danych jest przetwarzaniem.

Przykład: Zestaw danych w zbiorze przed anonimizacją

Lp.	Imię i nazwisko pracownika	Stanowisko	Wynagrodzenie brutto (w zł)	Wykształcenie
1.	Jan Kowalski	Naczelnik Biura Obsługi Klienta	5 530	wyższe mgr

Przykład: Zestaw danych w zbiorze po anonimizacji

Lp.	Imię i nazwisko pracownika	Stanowisko	Wynagrodzenie brutto (w zł)	Wykształcenie
1.		Naczelnik	5 530	wyższe

Innym działaniem jest **pseudonimizacja**. Jest to szczególny sposób przetwarzania danych, zbliżony do anonimizacji, z tą istotną różnicą, że proces ten **ma być odwracalny**. W RODO wyraźnie wskazano, że pseudonimizacja oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

Zaletą **pseudonimizacji** jest fakt, że **może ograniczyć ryzyko dla osób, których dane dotyczą oraz pomóc administratorom i podmiotom przetwarzającym wywiązać się z obowiązku ochrony danych** (Motyw 28 RODO).

Należy pamiętać, *że* pseudonimizacja odbywa się według określonego klucza, który musi być przechowywany osobno. Dane, które będą podlegać pseudonimizacji, cały czas **są danymi osobowymi** i należy *w* stosunku do nich stosować wszystkie zasady przetwarzania RODO[17].

[16] Grupa art. 29, w dokumencie nr 05/2014 wskazuje następujące możliwe techniki anonimizacji: dodawanie zakłóceń, permutacja, prywatność różnicowa, agregacja, k-anonimizacja, l-dywersyfikacja, t-bliskość.

[17] Por. Blog Dane osobowe – https://blog-daneosobowe.pl/, wpis pt. *Czym są dane osobowe wg RODO?,* dostępny pod linkiem: https://blog-daneosobowe.pl/czym-sa-dane-osbowe-wg-rodo/

1.4.5. PROFILOWANIE

Dokonywanie cyfrowych analiz i automatycznego przetwarzania danych staje się coraz bardziej powszechne. Już w 2001 r. Wojciech Wiewiórowski, ówczesny Generalny Inspektor Ochrony Danych Osobowych, zauważył, że profilowanie może odbywać się na dwa sposoby:

1) zbieranie z bardzo różnych źródeł pozyskanych legalnie danych i tworzenie na ich podstawie profilu osobowego klienta lub kandydata na klienta;
2) dołączanie do informacji, która dotyczy klienta, dodatkowych danych, statystycznie prawdziwych dla tego typu klientów. Omawiana sytuacja będzie miała miejsce wtedy, kiedy klient wykazuje np. cechę A, to na podstawie statystyki, administrator uznaje, że wykazuje też cechę B i cechę C. Te ostatnie nie są oczywiście informacjami potwierdzonymi, ale prawdopodobieństwo ich wystąpienia jest znaczne[18].

RODO w sposób szczegółowy reguluje zagadnienie profilowania i definiuje je jako **dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej** (art. 4 RODO). Oznacza to, że system komputerowy na podstawie określonych danych wysnuwa samodzielne wnioski.

W pełni zautomatyzowane profilowanie może stanowić zagrożenie dla konsumentów. Niebezpieczeństwo może polegać na podejmowaniu decyzji w oparciu o algorytm niekompletny lub popełniający błędy.

Prawodawca unijny, zdając sobie sprawę, że zakazanie profilowania nie będzie skuteczne, dopuścił je, ale na podmiot, który chce dokonywać profilowania, RODO nałożyło kilka obowiązków.

1. Przed rozpoczęciem profilowania należy poinformować, do czego będzie ono służyć oraz o konsekwencjach podejmowania decyzji na jego podstawie.
2. Klauzula informacyjna musi zawierać wyraźną informację, że dane osobowe będą podlegały profilowaniu. W praktyce zgoda na profilowanie będzie mogła być wyrażona poprzez odrębny „checkbox". Uwaga! Okienko nie może być domyślnie zaznaczone.
3. Należy poinformować, jakie dane są zbierane do profilowania oraz jakie konsekwencje wywołuje brak zgody na ich przetwarzanie.
4. Należy przeprowadzić ocenę skutków dla przetwarzania danych.
5. Należy wdrożyć środki techniczne i organizacyjne zapewniające w szczególności korektę powodujących nieprawidłowości w danych osobowych i maksymalne zmniejszenie ryzyka błędów.
6. Należy zabezpieczyć dane osobowe w sposób uwzględniający potencjalne ryzyko dla interesów i praw osoby.
7. System automatycznego podejmowania decyzji (czyli profilowania) musi być zaprojektowany tak, aby służyła ręczna korekta, tj. aby człowiek mógł zmienić rezultat decyzji wygenerowanej automatycznie. RODO wymusza, aby zabezpieczyć prawa do:
   a) wyrażenia własnego zdania,
   b) sprzeciwu,
   c) wyjaśnienia decyzji wynikającej z oceny podjętej automatycznie i zakwestionowania jej,
   d) interwencji człowieka.

Pomimo że coraz więcej systemów będzie dokonywać profilowania, RODO wyraźnie wskazuje, że powinny być do tego wykorzystywane profesjonalne algorytmy oraz żeby to czynnik ludzki był zawsze tym, który decyduje ostatecznie.

RODO wymienia przypadki, gdy podmiot profilujący dane powinien wykazać się szczególną ostrożnością. Są to przypadki:

- odrzucenia elektronicznego wniosku kredytowego,
- elektronicznej metody rekrutacji bez interwencji ludzkiej.

---

[18] Zob. Rozmowa z dr Wojciechem Rafałem Wiewiórowskim, *GIODO: trzeba informować klienta o tworzeniu jego profilu,* http://www.lex.pl/czytaj/-/artykul/giodo-trzeba-informowac-klienta-o-tworzeniu-jego-profilu (data dostępu: 12.12. 2017).

Dopuszczalne jest zatem profilowanie:

- efektów pracy,
- sytuacji ekonomicznej,
- zdrowia,
- osobistych preferencji lub zainteresowań,
- wiarygodności lub zachowania,
- lokalizacji lub przemieszczania się osoby,

ale trzeba spełnić wyżej wymienione wymogi (Motyw 71 RODO).

Ze względu na fakt, że skutki profilowania mogą dotyczyć praw osób, których dane są przetwarzane w sposób zautomatyzowany, w RODO zostały nałożone obowiązki prowadzenia profilowania w sposób:

- rzetelny,
- przejrzysty.

Dlatego poza wskazanymi wcześniej obowiązkami informacyjnymi, zapewnieniem interwencji ludzkiej (nie można poprzestać na zautomatyzowanym przetwarzaniu), prawa sprzeciwu itd., należy pamiętać, że system profilujący powinien działać w oparciu o możliwie najlepsze metody matematyczne i statystyczne; chodzi o to, żeby wyeliminować lub przynajmniej zminimalizować ryzyko popełnienia błędów.

Dla przedsiębiorców istotne znaczenie będą miały przesłanki legalizujące. Profilowanie będzie dozwolone wyłącznie wtedy, kiedy:

1) jest niezbędne do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem;
2) jest dozwolona prawem Unii lub prawem państwa członkowskiego;
3) opiera się na wyraźnej zgodzie osoby, której dane dotyczą (Motyw 71 RODO oraz art. 22 ust. 2 RODO).

W przypadku wykonywania czynności profilowania administrator **wdraża właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby**, której dane dotyczą, a **co najmniej prawa do uzyskania interwencji ludzkiej ze strony administratora do wyrażenia własnego stanowiska i do zakwestionowania tej decyzji** (art. 22 ust. 3 RODO).

1.5. WARUNKI OGÓLNE POZYSKIWANIA I PRZETWARZANIA DANYCH OSOBOWYCH

Poniżej zostaną wskazane zasady ogólne, przesłanki oraz szczególne przesłanki pozyskiwania i przetwarzania danych.

1.5.1. ZASADY OGÓLNE

Administrator danych osobowych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane przetwarza. RODO wskazuje, że przy przetwarzaniu należy uwzględnić poniższe zasady:

a) ma odbywać się zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą (**zasada legalności**);
b) dane mają być **zbierane w konkretnych, wyraźnych** i **prawnie uzasadnionych celach** i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane (…) za niezgodne z pierwotnymi celami (**zasada ograniczenia celu przetwarzania danych**);
c) ma być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (**zasada minimalizacji danych**);

Uwaga

Dotychczasowa praktyka wskazuje, że inspektorzy GIODO zwracają w trakcie kontroli szczególną uwagę na tę zasadę, która dotychczas często była opisywana jako **zasada ograniczenia ilościowego oraz czasowego**. Przedsiębiorca powinien zbierać tylko tyle danych, ile jest mu rzeczywiście koniecznie (minimalizm) oraz usuwać je, gdy tylko przestaną mu być potrzebne.

Studium przypadku 11.

Administrator danych z dużym prawdopodobieństwem naruszy zasadę minimalizmu, jeśli przy wejściu do swojej siedziby wydaje przepustkę, do której dołącza zdjęcia zrobione gościom, zbiera numery PESEL oraz numery dowodów osobistych. Trudno będzie mu udowodnić cel i adekwatność zbieranych danych osobowych.

d) zbierane dane mają być **prawidłowe i w razie potrzeby uaktualniane**; oznacza to również, że dane nieprawidłowe powinny być niezwłocznie usunięte lub sprostowane (**zasada prawidłowości danych**);
e) dane mają być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych z zastrzeżeniem, że zostaną wdrożone odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą (**zasada ograniczenia przechowywania**);
f) dane mają być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych (**zasada integralności i poufności**) (art. 5 ust. 1 RODO).

Ponadto szczególne znaczenie ma **zasada rozliczalności**. Przewiduje ona, że administrator danych jest odpowiedzialny za przestrzeganie przepisów o ochronie danych i że ma on wykazać, iż właściwie spełnił wymogi określone tymi przepisami. W praktyce będzie oznaczać, że zasada rozliczalności jest spełniona, jeśli:

- przedsiębiorca prawidłowo informuje o wszystkich prawach osoby fizyczne oraz zapewnia realizację tych praw;
- zbiera dane osobowe zgodnie z przepisami prawa; jeżeli odbywa się to na podstawie zgody, zgoda musi być wyrażona dobrowolnie, sformułowana możliwie prostym językiem oraz możliwa do cofnięcia w sposób równie prosty, jak została wyrażona;
- prowadzi wszelką wymaganą przepisami prawa dokumentację, czyli np. rejestr czynności przetwarzania, katalog wykazujący uzyskane zgody od podmiotów, których dane są przetwarzane itd.

1.6. PRZESŁANKI SZCZEGÓLNE DOPUSZCZALNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

RODO nakłada na administratora szereg nowych obowiązków związanych z podstawą przetwarzania. Nowe są informacje, które przedsiębiorca musi przedstawić osobie, której dane zamierza przetwarzać.

1.6.1. ZGODNOŚĆ PRZETWARZANIA Z PRAWEM – PODSTAWY PRZETWARZANIA

RODO określa niezależne i autonomiczne podstawy przetwarzania danych osobowych. Każda z powyższych przesłanek uzasadnia zbieranie danych w innej sytuacji i jest od siebie niezależna. Oznacza ona, że przetwarzanie jest zgodne z prawem, jeżeli został spełniony przynajmniej jeden z poniższych warunków. Dla przedsiębiorców znaczenie będą miały przesłanki (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;
c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze (chodzi np. o obowiązek przekazania danych osobowych organom ścigania);
d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej (jest to przesłanka, której przedsiębiorca co do zasady nie powinien wykorzystywać; będzie ona miała zastosowanie w nadzwyczajnych przypadkach, np. gdy przetworzenie danych będzie związane z uratowaniem życia lub zdrowia tej osoby).

Zgoda na przetwarzanie danych jest i będzie najczęściej stosowaną przesłanką przetwarzania danych osobowych w obrocie gospodarczym. Uważa się, że zgoda osoby, której dane dotyczą, **oznacza dobrowolne, konkretne, świadome** i **jednoznaczne okazanie woli**, którym osoba, której dane dotyczą, **w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych** (art. 4 ust. 11 RODO).

Może to polegać na zaznaczeniu okienka wyboru podczas przeglądania strony internetowej, na wyborze ustawień technicznych do korzystania z usług społeczeństwa informacyjnego lub też na innym oświadczeniu bądź zachowaniu, które w danym kontekście **jasno** wskazuje, że osoba, której dane dotyczą, zaakceptowała proponowane przetwarzanie jej danych osobowych.

Milczenie, okienka domyślnie zaznaczone lub niepodjęcie działania nie powinny zatem być traktowane jako wyrażenie zgody na przetwarzanie danych. Zgoda powinna dotyczyć wszystkich czynności przetwarzania dokonywanych w tym samym celu lub w tych samych celach. Jeżeli przetwarzanie służy różnym celom, potrzebna jest zgoda na **wszystkie te cele**. Jeżeli osoba, której dane dotyczą, **ma wyrazić zgodę w odpowiedzi na elektroniczne zapytanie, zapytanie takie musi być jasne, zwięzłe** i **nie zakłócać niepotrzebnie korzystania z usługi, której dotyczy** (Motyw 32 RODO).

Zgody nie uważa się za dobrowolną, jeżeli nie można jej wyrazić osobno na różne operacje przetwarzania danych osobowych, mimo że w danym przypadku byłoby to stosowne, lub jeżeli od zgody uzależnione jest wykonanie umowy – w tym świadczenie usługi – mimo że do jej wykonania zgoda nie jest niezbędna (Motyw 43 RODO).

Przykład 1. „Wyrażam zgodę na przetwarzanie wszelakich moich danych osobowych niezbędnych do realizacji umowy oraz na potrzeby prowadzonych w przyszłości kampanii marketingowych".

Przykład 2. „Administrator danych Sp. ABC z o. o. informuje, że wyrażenie zgody na przetwarzanie danych osobowych na potrzeby przyszłych kampanii marketingowych jest niezbędne dla należytego wykonania umowy".

Uwaga! Powyższe klauzule sprzeciwiają się przepisom prawa!

Przy pobieraniu zgód administrator powinien pamiętać o poniższych kwestiach.

1. Jeżeli administrator pobiera zgodę na przetwarzanie danych, to musi **być w stanie wykazać**, że osoba, której dane dotyczą, **wyraziła tę zgodę**. Oznacza to obowiązek archiwizowania zgód, przez co jest realizowana zasada rozliczalności.
2. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Osoba, której dane dotyczą, jest o tym informowana, zanim wyrazi zgodę. Wycofanie zgody musi być równie łatwe jak jej wyrażenie.
3. Zgoda musi być dobrowolna. Nie wolno uzależniać wykonania umowy, w tym świadczenie usługi, od wyrażenia zgody. Przedsiębiorca musi ustalić, czy zgoda jest niezbędna do wykonania tej umowy (art. 7 RODO).
4. Zgoda musi być wyraźnie określona; nie wolno przygotowywać domyślnie zaznaczonych checkboxów.

Należy pamiętać, że zgoda jest pobierana wtedy, kiedy nie zachodzi inna przesłanka legalizująca pobieranie danych. W sytuacji, gdy przepis prawa (np. kodeks pracy) daje podstawę do przetwarzania danych osobowych lub gdy przetworzenie jest niezbędne do zrealizowania umowy (np. wysyłka zakupionego towaru na adres klienta), **zgody się nie pobiera**.

Studium przypadku 12.
Kodeks pracy w artykule 22 [1] wskazuje, jakie dane osobowe pracodawca może pobrać od pracownika i kandydata do pracy. Oznacza to, że w takich sytuacjach nie jest potrzeba zgoda na zbieranie danych osobowych.

Studium przypadku 13.
Przedsiębiorca prowadzi mały sklep internetowy. Dla wysłania mailingu i reklamy musi zbierać zgodę na przetwarzanie danych osobowych.

RODO szczególną ochronę przyznaje dzieciom. Jest ona wynikiem uznania przez prawodawcę unijnego faktu, że mogą być one mniej świadome ryzyka, konsekwencji, zabezpieczeń i praw przysługujących im w związku z przetwarzaniem danych osobowych.

Dlatego tak ważne jest określenie, kim jest dziecko na potrzeby ochrony danych osobowych. RODO określiło ten wiek na 16 rok życia ze wskazaniem, że państwa członkowskie mogą zdecydować się na jego zmniejszenie. Na podstawie nowej polskiej ustawy o ochronie danych osobowych w **przypadku usług świadczonych drogą elektroniczną oferowanych bezpośrednio osobie, która nie ukończyła lat trzynastu i która przebywa na terytorium Rzeczpospolitej Polskiej, gdy podstawą przetwarzania danych osobowych jest zgoda tej osoby, przetwarzanie danych osobowych możliwe jest wyłącznie po uzyskaniu uprzedniej zgody jej przedstawiciela ustawowego albo po niezwłocznym potwierdzeniu przez przedstawiciela ustawowego zgody wyrażonej przez taką osobę**[19].

Z powyższego wynika, że osoby poniżej 13 roku życia nie mogą samodzielnie wyrazić zgody (wymagana jest uprzednia zgoda lub niezwłoczne potwierdzenie przez przedstawiciela ustawowego). Osoby powyżej 13 roku życia mogą samodzielnie wyrazić taką zgodę.

Gdy przedsiębiorca zbiera dane osobowe dzieci, powinien pamiętać, że zgody, obowiązki informacyjne itp. **powinny być sformułowane tak jasnym i prostym językiem, by dziecko mogło je bez trudu zrozumieć**.

[19] Należy pamiętać, że końcowy tekst i założenia ustawy mogą różnić się od projektu.

Uwaga
Przy redagowaniu treści zgody, która będzie pobierana od dzieci, warto wykorzystać współczynniki mglistości tekstu (np. współczynnik mglistości Gunninga). Są one dostępne również online. Takie narzędzia pomagają ustalić, czy język komunikacji z dzieckiem jest jasny i prosty oraz to, czy dziecko jest w stanie zrozumieć przekaz. W szczególnych przypadkach warto przemyśleć zasięgnięcia opinii polonisty.

Przedsiębiorcy, którzy świadczą usługi lub produkują towary, a istota usługi polega na zebraniu danych osobowych (w szczególności np. dostarczenie towaru pod podany adres lub wystawienie faktury itd.), **nie muszą** pobierać zgody. Zgoda z samej definicji oznacza, że jest dobrowolnym oświadczeniem woli. W przypadku części umów ich podanie jest niezbędne do realizacji umowy, a więc przedsiębiorcy nie powinni ich pobierać. Podstawą bowiem jest wskazana wcześniej **niezbędność do wykonania umowy**. Mogą to być umowy o dzieło, zlecenie lub sprzedaży, ale również dostawy, usługi i roboty budowlane.

Studium przypadku 14.
Właściciel restauracji lub firmy cateringowej oferuje usługę dostarczania swoich dań na wynos. Aby doręczyć je pod właściwy adres, zbiera dane osobowe klientów tj. imię i nazwisko (ewentualnie numer telefonu) oraz adres. Przetwarzanie następuje dla wykonania umowy.

Studium przypadku 15.
Tłumacz, wykonując usługę tłumaczenia aktu stanu cywilnego, dla zrealizowania usługi musi przetwarzać dane. Tłumaczenie następuje dla wykonania umowy.

Studium przypadku 16.
Przedsiębiorstwo organizujące szkolenie zawarło umowę, w ramach której musi przeszkolić pracowników, a następnie przeprowadzić egzamin oraz wystawić zaświadczenia dla poszczególnych pracowników. Wystawienie zaświadczenie następuję dla zrealizowania umowy.

1.6.2. PODSTAWY PRZETWARZANIA SZCZEGÓLNYCH KATEGORII DANYCH

RODO ustanawia ogólny zakaz przetwarzania szczególnych kategorii danych, wcześniej znanych jako dane wrażliwe. Ich przetwarzanie jest dozwolone wyłącznie wtedy, kiedy przepis RODO lub prawo państwa członkowskiego na to pozwala. Są to więc ściśle określone przypadki. Do najważniejszych przesłanek legalizujących należy:

a) 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;
b) 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;
c) 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;
d) 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;

e) przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;

f) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;

g) 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;

h) 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;

i) 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;

j) przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych (art. 9 RODO).

Uwagi

W RODO **zniesiono wymóg wyrażenia zgody na piśmie, który funkcjonował w UODO.** Zgoda może być wyrażona w elektroniczne formie, ale należy pamiętać, że zgodnie z zasadą rozliczalności trzeba będzie ją wykazać.

Gdy przetwarzanie będzie odbywać się na dużą skalę – niezależnie od tego, czy będą to dane zwykłe czy szczególna kategoria danych – obowiązkowe będzie powołanie Inspektora Ochrony Danych.

W przypadku przetwarzania na dużą skalę danych szczególnej kategorii, został nałożony obowiązek przeprowadzenia tzw. oceny skutków dla ochrony danych, o czym będzie mowa w następnym rozdziale.

Szczególne kategorie danych osobowych mogą być przetwarzane do celów profilaktyki zdrowotnej lub medycyny pracy (art. 9. 2 lit. h), **jeżeli są przetwarzane przez – lub na odpowiedzialność – pracownika podlegającego obowiązkowi zachowania tajemnicy zawodowej** na mocy prawa Unii Europejskiej lub prawa państwa członkowskiego lub przepisów ustanowionych przez właściwe organy krajowe **lub przez inną osobę również podlegającą obowiązkowi zachowania tajemnicy zawodowej na mocy prawa Unii lub prawa państwa członkowskiego**, lub przepisów ustanowionych przez właściwe organy krajowe.

Należy pamiętać, że Polska może w swojej ustawie zachować lub wprowadzić dalsze warunki, w tym ograniczenia w odniesieniu do przetwarzania danych genetycznych, danych biometrycznych lub danych dotyczących zdrowia.

1.7. OBOWIĄZKI INFORMACYJNE

1.7.1. DONIOSŁOŚĆ OBOWIĄZKU INFORMACYJNEGO

Prawodawca unijny szczególną wagę przykłada do realizacji praw przyznanych przez RODO. Będzie to możliwe tylko i wyłącznie wtedy, kiedy podmioty będą ich świadome, czyli **zostaną poinformowane o przysługujących im uprawnieniach wynikających z RODO**. Dlatego przy wdrażaniu wymogów Rozporządzenia szczególną uwagę należy zwrócić na ten element.

Dla większości przedsiębiorców to właśnie dopasowanie nowych klauz informacyjnych, w tym wskazanie nowych praw, a zwłaszcza opracowanie procedur ich wykonania, będzie stanowić najważniejszy element dostosowania się do wymagań RODO. Dlatego przedsiębiorcy powinni przeanalizować klauzule informacyjne, które wykorzystują obecnie i dostosować je do nowych wymogów.

Należy pamiętać, że obowiązki opisane w tym rozdziale powstają w trzech sytuacjach, czyli wtedy, kiedy:

1) dane pochodzą od osoby, której dotyczą;
2) dane nie pochodzą od osoby, której dotyczą;
3) administrator zmienia cel przetwarzania danych, tj. zebrane dane były niezbędne do realizacji umowy. Gdy w późniejszym okresie przedsiębiorca będzie chciał wykorzystać zebrane dane do marketingu, będzie musiał pobrać zgodę i dopełnić obowiązku informacyjnego.

1.7.2. FORMA SPEŁNIENIA OBOWIĄZKU INFORMACYJNEGO PRZEZ ADMINISTRATORA

RODO przewiduje trzy formy spełnienia tego obowiązku:

1) pisemną;
2) elektroniczną;
3) ustną.

Pierwsze dwie formy powinny być preferowane ze względu na zasadę rozliczalności, tj. stosując je, administrator danych będzie mógł udowodnić, np. na żądanie Prezesa Urzędu Ochrony Danych, że wypełnił spoczywające na nim obowiązki.

Dla ustawodawcy europejskiego istotne jest, aby informacje o przysługujących prawach w zakresie przetwarzania danych były przekazywane w **zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem** (art. 12 ust. 1 RODO). **Informacje te mogą być przekazywane w formie elektronicznej, na przykład za pomocą strony internetowej,** na której składane jest zamówienie on-line, lub innej zakładce, która wyświetla się w trakcie procesu zakupowego.

Gdy obowiązek informacyjny jest realizowany wobec dziecka, język powinien być jeszcze prostszy, aby dziecko było w stanie zrozumieć przekaz. Dlatego cytowanie dziecku aktów prawnych (lub np. zaleceń Gr. Art. 29) nie będzie można uznać za spełnienie obowiązków, gdyż język tam wykorzystywany jest abstrakcyjny i niezrozumiały dla dzieci, których zasób słownictwa jest ograniczony.

Obowiązek informacyjny **musi** być wypełniony bez względu na to, w jaki sposób dane zostały zebrane, czyli czy stało się to:

1) drogą pisemną;
2) telefonicznie;
3) w kontaktach bezpośrednich.

Nieistotny jest również sposób utrwalenia, czyli to, czy zbiór będzie miał postać papierową czy elektroniczną. Należy pamiętać, że **nie wolno** powyższego obowiązku poinformowania zastępować odesłaniem

np. do regulaminu konkursu, jeżeli osoba zainteresowana nie ma możliwości bezpośredniego zapoznania się nim.

W przypadku sporu to administrator będzie musiał udowadniać wypełnienie obowiązku informacyjnego, dlatego należy przyjąć, że zawsze będzie musiał spełniać obowiązek informacyjny[20]. **Spełnianie obowiązków informacyjnego** (art. 13 oraz 14 RODO) **jest wolne od opłat. Dopiero w sytuacji, gdy zainteresowany stara się nadużyć prawa przez regularne (ustawiczne) składanie wniosków, administrator danych może**:

a) pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań; albo
b) odmówić podjęcia działań w związku z żądaniem (art. 12 ust. 5 RODO).

1.7.3. INFORMACJE PODAWANE W PRZYPADKU ZBIERANIA DANYCH OD OSOBY, KTÓREJ DANE DOTYCZĄ

Obowiązek informacyjny określony został w art. 13 RODO. Wymienia on elementy, o jakich należy poinformować osobę, której dane dotyczą. Są to:

a) **tożsamość** i **dane kontaktowe administratora** oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela;
b) gdy ma to zastosowanie – **dane kontaktowe inspektora ochrony danych**;
c) **cele przetwarzania danych osobowych** oraz **podstawę prawną przetwarzania**;
d) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) – prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią;
e) **informacje o odbiorcach danych osobowych** lub o **kategoriach odbiorców**, jeżeli istnieją;
f) gdy ma to zastosowanie – **informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej** oraz o stwierdzeniu lub braku stwierdzenia przez Komisję Europejską odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46 (czyli przekazywanie z zastrzeżeniem odpowiednich zabezpieczeń), art. 47 (który wskazuje wiążące reguły korporacyjne lub art. 49 ust. 1 akapit drugi (czyli Wyjątki w szczególnych sytuacjach), wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych (art. 13 RODO).

Poza powyższymi informacjami, podczas pozyskiwania danych osobowych administrator podaje osobie, której dane dotyczą, następujące inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania:

a) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;

> Okresem tym będzie zrealizowanie umowy lub wycofanie zgody lub ustanie obowiązku przechowywania danych w związku z zatrudnieniem.

b) 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;
c) jeżeli przetwarzanie odbywa się na podstawie zgody lub zgody na przetwarzanie szczególnych kategorii danych – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;

[20] M. Krasińska, S. Mizerek (opr.), *ABC wybranych zagadnień z ustawy o ochronie danych osobowych* , Warszawa,„Wydawnictwo Sejmowe", 2011, s. 20.

d) informację o prawie wniesienia skargi do organu nadzorczego;
e) 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;
f) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu (art. 13 ust 2 lit. f).

Ponadto, przedsiębiorca powinien pamiętać, że RODO wskazuje, że **administrator musi podać wszelkie inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania**, uwzględniając konkretne okoliczności i kontekst przetwarzania danych osobowych.

Ostatecznie, jeśli administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem informuje on o tym zamiarze osobę, której dane dotyczą oraz udziela jej wszelkich innych stosownych informacji tj. o przysługujących prawach, nowym celu przetwarzania, podstawie przetwarzania itd.

Przykładowa klauzula informacyjna w przypadku zbierania danych od osoby, której dane dotyczą

Na podstawie przepisów Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, informuję, że:

1. Administratorem Pani/Pana danych osobowych jest Spółka XXX Sp. z o.o. z siedzibą w Krakowie (00-111), ul. 3 maja 2, lok. 43, zwana dalej Spółką.
2. Inspektorem ochrony danych (osobą odpowiedzialną za prawidłowość przetwarzanie danych) jest Jan Kowalski (kontakt do inspektora: iod@spolkaxxx.pl, tel. ……..).
3. Pani/Pana dane osobowe będą przetwarzane w celu marketingu produktów i usług Spółki i nie będą udostępniane innym odbiorcom. Podstawą prawną przetwarzania danych jest zgoda.
4. Dane osobowe będą przetwarzane do czasu cofnięcia zgody.
5. Dostęp do danych osobowych będzie przysługiwał wyłącznie upoważnionym pracowników działu marketingu.
6. Przysługują Pani/Panu żądanie dostępu do danych osobowych oraz poprawianie danych osobowych. Ponadto przysługuje Pani/Panu prawo usunięcia lub ograniczenia przetwarzania, prawo do wniesienia sprzeciwu wobec przetwarzania, a także prawo do przenoszenia danych.
7. Ponieważ podstawą przetwarzania danych jest wyrażona przez Panią/Pana zgoda, informujemy, że zgoda może być cofnięta w dowolnym momencie.
8. Przysługuje Pani/Panu skarga do organu nadzorczego Prezesa Urzędu Ochrony Danych Osobowych.

1.7.4. INFORMACJE PODAWANE W PRZYPADKU POZYSKIWANIA DANYCH OSOBOWYCH W SPOSÓB INNY NIŻ OD OSOBY, KTÓREJ DANE DOTYCZĄ

Zdarzają się sytuacje, gdy podmiot przetwarza dane osobowe, których nie pozyskał samodzielnie. W takich sytuacjach zastosowanie ma obowiązek poinformowania osoby o treściach wskazanych w RODO, który nieznacznie różni się od wskazanego powyżej.

Przykład
XXX Sp. z o.o produkuje i sprzedaje soki. W formularzu na stronie internetowej pobiera zgody na przetwarzanie danych w celach marketingowych. Następnie przekazuje dane osobowe do drugiej spółki (YYY. Sp. z o.o), która organizuje akcje marketingowe. YYY Sp. z o.o musi dopełnić obowiązków informacyjnych wskazanych w art. 14 RODO.

Jeśli administrator zbiera dane, których **nie pozyskał od osoby**, której dane dotyczą, ale z innego źródła, podaje osobie, której dane dotyczą:

a) swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela; niekoniecznie chodzi o pełnomocnika procesowego, ale o osobę, która zajmuje się ochroną danych w przedsiębiorstwie;
b) gdy ma to zastosowanie – dane kontaktowe inspektora ochrony danych (IOD);
c) cele przetwarzania, do których mają posłużyć dane osobowe oraz podstawę prawną przetwarzania;
d) kategorie odnośnych danych osobowych (dane osobowe zwykłe lub szczególne kategorie danych);
e) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
f) gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej.

Ponadto podczas pozyskiwania danych osobowych administrator powinien podać:

a) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
b) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) (tj. prawnie uzasadnionych celów) – prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią;
c) informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
d) jeżeli przetwarzanie odbywa się na podstawie zgody (art. 6 ust. 1 lit. a) lub zgody na przetwarzanie szczególnych kategorii danych (art. 9 ust. 2 lit. a) – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
e) informacje o prawie wniesienia skargi do organu nadzorczego;
f) źródło pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych; źródła dostępne publicznie to np. portale społecznościowe, w sytuacji gdy podmiot danych nie zastrzega prywatności postów, ograniczając ich zasięg dostępności;
g) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

W takiej sytuacji administrator informuje:

a) **w rozsądnym terminie** po pozyskaniu danych osobowych – **najpóźniej w ciągu miesiąca** – mając na uwadze konkretne okoliczności przetwarzania danych osobowych;
b) **jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą – najpóźniej przy pierwszej takiej komunikacji z osobą**, której dane dotyczą; lub
c) **jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu** (art.14 ust. 3 lit. c).

Przykładowa klauzula informacyjna w przypadku zebrania w sposób inny niż od osoby, której dane dotyczą

Na podstawie przepisów Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, informuję, że:

1. Administratorem Pani/Pana danych osobowych jest Spółka XXX Sp. z o.o. z siedzibą w Krakowie (00-111), ul. 3 maja 2, lok. 43, zwana dalej Spółką.
2. Inspektorem ochrony danych (osobą odpowiedzialną za prawidłowość przetwarzanie danych) jest Jan Kowalski (kontakt do inspektora: iod@spolkaxxx.pl, tel. .....).
3. Pani/Pana dane osobowe będą przetwarzane w celu marketingu produktów i usług Spółki i nie będą udostępniane innym odbiorcom. Podstawą prawną przetwarzania danych jest zgoda wyrażona przedsiębiorstwu YYY. Sp. z o.o.
4. Dane osobowe będą przetwarzane do czasu wycofania wyrażonej zgody.
5. Dostęp do danych osobowych będzie przysługiwał wyłącznie upoważnionym pracowników działu marketingu
6. Przysługują Pani/Panu żądanie dostępu do danych osobowych oraz poprawianie danych osobowych. Ponadto przysługuje Pani/Panu prawo usunięcia lub ograniczenia przetwarzania, prawo do wniesienia sprzeciwu wobec przetwarzania, a także prawo do przenoszenia danych.
7. Wykorzystywane dla celów marketingowym dane osobowe zostały pozyskane od podmiotu YYY. Sp. z o.o., który posiada zgody na wykorzystywanie danych osobowych, w tym przekazywanie ich podmiotom prowadzącym kampanie reklamowe.
8. Ponieważ podstawą przetwarzania danych jest wyrażona przez Panią/Pana zgoda, informujemy, że zgoda może być cofnięta w dowolnym momencie.
9. Przysługuje Pani/Panu skarga do organu nadzorczego Prezesa Urzędu Ochrony Danych Osobowych.

1.7.5. ZMIANA CELU PRZETWARZANIA DANYCH

W RODO decydujące znaczenie ma cel zbierania informacji. Dlatego, **jeżeli administrator planuje przetwarzać dane osobowe w celu innym niż cel, w których dane osobowe zostały zebrane, powinien on przed takim dalszym przetwarzaniem poinformować osobę, której dane dotyczą, o tym innym celu oraz dostarczyć jej innych niezbędnych informacji** (Motyw 61 RODO).

Powyższe obowiązki związane z obowiązkiem poinformowania, gdy dane nie pochodzą pod podmiotu danych lub poinformowaniem o zmianie celu, nie będą miały zastosowania, gdy wystąpią precyzyjnie określone przesłanki:

a) osoba, której dane dotyczą, dysponuje już tymi informacjami (art. 14 ust 5. lit. a);
b) udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku; w szczególności w przypadku przetwarzania do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem warunków i zabezpieczeń, o których mowa w art. 89 ust. 1, lub o ile obowiązek, o którym mowa w ust. 1 artykułu 14, może uniemożliwić lub poważnie utrudnić realizację celów takiego przetwarzania. W takich przypadkach administrator podejmuje odpowiednie środki, by chronić prawa i wolności oraz prawnie uzasadnione interesy osoby, której dane dotyczą, w tym udostępnia informacje publicznie (art. 14 ust. 5 lit. b);
c) pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator, przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą (art. 14 ust. 5 lit. c);

d) dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii lub w prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy (art. 14 ust. 5 lit. d).

Obszerność wskazanych regulacji dowodzi, że dla przedsiębiorców obowiązek informacyjny jest ważnym elementem systemu ochrony danych osobowych, a nawet jednym z filarów tego systemu. Ten aspekt działalności powinien być opracowany we współpracy Inspektora Ochrony Danych oraz pracowników zajmujących się obsługą klienta.

2. ZARZĄDZANIE BEZPIECZEŃSTWEM DANYCH OSOBOWYCH

Bartosz Mendyk

Prawidłowe zarządzanie systemem bezpieczeństwa danych osobowych w przedsiębiorstwie jest ściśle związane z podziałem kompetencji pomiędzy osobami odpowiedzialnymi za przetwarzanie danych osobowych. RODO, podobnie jak wcześniej Ustawa o ochronie danych osobowych, definiuje podmioty odpowiedzialne za prawidłowe zarządzanie danymi osobowymi, wskazując ich prawa oraz obowiązki w tym zakresie. Należyte zrozumienie podziału obowiązków pomiędzy Inspektorem Ochrony Danych (dalej: także **inspektorem** lub **IOD**) a administratorem danych pozwoli przedsiębiorcy wprowadzić odpowiednie procedury przetwarzania danych w przedsiębiorstwie.

Przepisy RODO, pomimo że same w sobie są obszerne, pozostawiają szerokie pole do interpretacji. Wskazana wcześniej Grupa art. 29 wydała wytyczne – interpretacje, które wskazują, jak należy rozumieć poszczególne obowiązki. Biorąc pod uwagę, że Prezes Urzędu Danych Osobowych oraz sądy będą wydawać decyzje oraz orzeczenia w oparciu o wytyczne Grupy art. 29, w dalszych częściach niniejszego rozdziału zostaną przedstawione jej zalecenia.

2.1. ADMINISTRATOR DANYCH

Pojęcie administratora jest jednym z najbardziej kluczowych w obszarze ochrony danych. Jest nim **osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych** (art. 4 ust. 7 RODO).

Studium przypadku 1.
Przy wejściu do siedziby przedsiębiorstwa X znajduje się portiernia obsługiwana przez pracowników zewnętrznej firmy ochroniarskiej, którzy prowadzą rejestr osób wchodzących do budynku. Jednakże to przedsiębiorstwo X jest administratorem danych osobowych, gdyż to ono, a nie przedsiębiorstwo ochroniarskie, decyduje o celach lub środkach zbierania danych.

Administratorem mogą być zatem zarówno podmioty publiczne, czyli organy państwa, samorządu terytorialnego oraz państwowe i samorządowe jednostki organizacyjne, jak również podmioty prywatne, czyli **przedsiębiorcy**. Według RODO przedsiębiorca to **osoba fizyczna lub prawna prowadząca działalność gospodarczą, niezależnie od formy prawnej, w tym spółki osobowe lub zrzeszenia prowadzące regularną działalność gospodarczą** (art. 4 ust. 18 RODO).

Chodzi zatem o:

- spółki jawne,
- spółki partnerskie,
- spółki komandytowe,
- spółki komandytowo-akcyjne,
- spółki z ograniczoną odpowiedzialnością,
- spółki akcyjne,
- osoby fizyczne prowadzące jednoosobową działalność,
- federacje branżowe, klastry i inne stowarzyszenia przedsiębiorców.

W ostatnim przypadku istotnym będzie fakt, że zarówno przedsiębiorcy zrzeszeni w klastrze, federacji czy stowarzyszeniu będą administratorami w zakresie danych przetwarzanych na potrzeby własnego przedsiębiorstwa, jak również będą nimi wskazane federacje itd. w zakresie, w jakim zbierają dane osobowe osób fizycznych. Jeżeli zatem klaster czy federacja zatrudnia własnych pracowników lub prowadzi akcje marketingowe poprzez wysyłkę mailingu, wówczas będzie administratorem danych.

Administratorami danych **nie będą organy** wcześniej wspomnianych podmiotów, czyli np.:

- zarząd i poszczególni członkowie zarządu,
- rada nadzorcza i członkowie rady nadzorczej,
- dyrektorzy departamentów,
- wspólnicy,
- partnerzy,
- komplementariusze, itd.

Studium przypadku 2.
W spółce A nastąpiło odwołanie prezesa, wymieniono radę nadzorczą oraz zakończono współpracę ze wspólnikiem. Fakty te nie mają żadnego znaczenia z punktu widzenia bycia administratorem danych osobowych – jest nim spółka A.

Uznanie podmiotu (np. przedsiębiorstwa) za administratora przesądza o tym, że **musi on wypełniać określone obowiązki**. Chodzi o:

1) **dbanie o zgodność przetwarzania danych z rozporządzeniem** RODO oraz o to, żeby administrator był w stanie wykazać, że tak postępuje, a więc zapewnia zasadę rozliczalności (art. 5 ust. 2);
2) **obowiązek informacyjny** wypełniany przy zbieraniu danych osobowych – administrator musi poinformować o fakcie zbierania danych osobę, której dane zbiera oraz wskazać kilka elementów, które zostały omówione w rozdziale wcześniejszym (art. 24 RODO);
3) **oszacowanie na podstawie obiektywnej oceny, czy z operacjami przetwarzania danych wiąże się ryzyko lub wysokie ryzyko naruszenia**; może to być przydatne przy opracowaniu oceny skutków dla ochrony danych, jeśli zajdzie taka konieczność. Ocena skutków dla ochrony danych zostanie opisana w dalszej części rozdziału (art. 24 RODO);
4) **zapewnienie bezpieczeństwa przetwarzania**, wynikające z obowiązku stosowania środków technicznych (np. szafy zamykane na klucz) i organizacyjnych (zasady wydawania pracownikom kluczy do pomieszczeń służbowych) zapewniających ochronę przetwarzanych danych osobowych (art. 32 i następne RODO);
5) **opracowanie rejestru czynności** przetwarzania, jeśli zajdzie przesłanka wskazana w RODO (art. 30 RODO);
6) **współpraca z organem nadzorczym**, np. poprzez zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu (art. 33 RODO);
7) **zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych** osobowych (art. 34 RODO).

Warto odnotować, że RODO **zniosło obowiązek rejestrowania zbiorów danych osobowych**. Obecnie to administrator danych wraz z inspektorem powinni zapewnić prawidłowość przetwarzania danych.

2.1.1. OGÓLNE OBOWIĄZKI ADMINISTRATORA

2.1.1.1. Obowiązek informacyjny

Podstawowym obowiązkiem, jaki RODO nakłada na administratora (np., przedsiębiorcę), jest **obowiązek informacyjny**. Niezależnie od przesłanki prawnej, na podstawie której są pozyskiwane dane osobowe, administrator **musi** poinformować osobę, od której zbiera dane, o wielu elementach (art. 13 RODO). Elementy te zostały przedstawione w rozdziale I.

2.1.1.2. Zapewnienie bezpieczeństwa przetwarzania

W odróżnieniu od obowiązującej dotychczas polskiej ustawy o ochronie danych osobowych i rozporządzenia[1], RODO **nie precyzuje** konkretnych norm, standardów czy działań, które powinni przedsięwziąć administratorzy w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych (np. określonej długości i siły hasła). Nakłada natomiast dosyć ogólnie sformułowany obowiązek ochrony praw osób i spełnianie wymogów rozporządzenia poprzez wdrożenie odpowiednich środków technicznych i organizacyjnych. Środki, o których mowa, muszą dotyczyć nie tylko samego przetwarzania danych, lecz także określania jego sposobów.

W tekście RODO prawodawca zamieszcza ich przykłady. Są to:

- **pseudonimizacja** (czyli odwracalna anonimizacja danych),
- **minimalizacja** (czyli pozyskiwanie tylko niezbędnych danych),
- **zapewnienie niezbędnych zabezpieczeń**.

Art. 25 obliguje administratora do takiego wdrożenia środków, które uwzględniają stan wiedzy technicznej, koszty ich wdrożenia, a także charakter, zakres, kontekst i cele przetwarzania. Ponadto środki, o których mowa, powinny być adekwatne do ryzyka naruszenia praw lub wolności o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.

2.1.1.3. Ocena skutków dla ochrony danych

Jak wcześniej wspomniano, RODO **zniosło obowiązek rejestrowania przez administratora zbiorów danych u Prezesa UODO**. Zdaniem unijnego ustawodawcy prowadziło to do nadmiernego obciążenia administracyjnego i finansowego, ale przede wszystkim nie zawsze przyczyniało się do poprawy ochrony danych osobowych. Jednakże w związku ze zniesieniem konieczności rejestrowania zbiorów danych, w przepisach RODO pojawił się nowy instrument – **ocena skutków dla ochrony danych** (ang. *Data Protection Impact Assessment* – DPIA). W tym aspekcie Grupa art. 29 również wydała swoje wytyczne[2]. Ocena skutków przetwarzania jest oszacowaniem prawdopodobieństwa i powagi naruszenia bezpieczeństwa danych osobowych, szczególnie w sytuacji, gdy są zbierane dane osobowe na dużą skalę oraz gdy są wprowadzane nowatorskie technologie, zwłaszcza te, które wykorzystują dane genetyczne bądź biometryczne lub inteligentny monitoring, który automatycznie może rozpoznawać twarze.

Przeprowadzenie oceny skutków dla ochrony danych jest zatem wymagane w szczególności w przypadku:

a) **systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu**, w tym profilowaniu, i jest podstawą

---

[1] Rozporządzenie w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, Dz. U. z 2004 r. Nr 100, poz. 1024.

[2] 4 kwietnia 2017 r. Grupa Robocza przyjęła projekt wytycznych w zakresie oceny skutków dla ochrony danych osobowych (WP 248).

decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;

b) **przetwarzania na dużą skalę szczególnych kategorii danych osobowych** lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa;

c) **systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.**

Mając na względzie szereg przepisów RODO (art. 35 ust. 1, art. 35 ust. 3 lit. a-c) oraz motywy 71, 75 oraz 91 preambuły RODO), Grupa art. 29 wskazała kryteria, które należy brać do oceny. Wskazała jednocześnie, że im więcej poniższych sytuacji nastąpi równocześnie, tym prawdopodobieństwo, że trzeba przeprowadzić ocenę, jest większe.

1. Ocena i *scoring*, w tym profilowanie i przewidywanie, w szczególności dotyczące takich aspektów podmiotu danych jak świadczenie pracy, sytuacja ekonomiczna, zdrowie, osobiste preferencje, zainteresowania, wiarygodność, zachowanie, lokalizacja czy poruszanie się.
2. Zautomatyzowane podejmowanie decyzji, w tym profilowanie, wywołujące skutki prawne lub wpływające na podmiot danych w podobny sposób.
3. Systematyczne monitorowanie mające na celu obserwowanie, monitorowanie lub kontrolowanie podmiotu danych, w tym systematyczne monitorowanie miejsc dostępnych publicznie. Chodzi tutaj np. o stosowanie monitoringu w hotelu, restauracji czy na stacji benzynowej w sytuacji, w której klient nie może wejść do obiektu lub skorzystać z usługi bez uprzedniego nagrania go przez monitoring wizyjny.
4. Przetwarzanie szczególnych kategorii danych.
5. Przetwarzane danych na dużą skalę.
6. Przetwarzanie danych osobowych podlegających łączeniu lub dopasowywaniu.
7. Przetwarzanie danych dotyczących wrażliwych podmiotów danych.
8. Wykorzystanie do przetwarzania danych innowacyjnych rozwiązań technicznych lub organizacyjnych, zwłaszcza w kontekście nowatorskich technologii wykorzystujących np. biometrię.
9. Transfer danych poza granice Unii Europejskiej, a zwłaszcza do USA.
10. Przetwarzanie danych samo w sobie utrudniające podmiotom danych wykonywanie przysługujących im praw lub korzystanie z usługi lub z umowy[3].

Wystąpienie dwóch lub więcej powyższych elementów powinno wiązać się z przeprowadzeniem oceny.

Zawartość oceny

Zgodnie z treścią art. 35 ust. 7 RODO ocena powinna zawierać co najmniej:

1. Systematyczny opis planowanych operacji przetwarzania danych i celów przetwarzania, czyli w jaki sposób oraz w jakim celu przedsiębiorca przetwarza dane osobowe pomiędzy poszczególnymi zbiorami.
2. Ocenę niezbędności i proporcjonalności przetwarzania w stosunku do celów, tj. wskazanie, czy określonego potencjalnie ryzykownego działania można uniknąć lub, jeśli nie ma takiej możliwości, jakie środki zastosowano, aby ryzyko zostało zminimalizowane.
3. Ocenę ryzyka naruszenia praw i wolności podmiotów danych, w szczególności, aby przedsiębiorca zdawał sobie sprawę z ryzyka, jakie niesie wykorzystywana technologia.
4. Środki planowane w celu zaradzenia ryzyku oraz wykazanie zgodności operacji przetwarzania danych z RODO.

RODO zakłada elastyczność struktury oraz formy dokonywanej oceny. Autorzy tego aktu prawnego nie chcieli, aby przeprowadzenie DPIA wymagało obowiązkowego wprowadzenia standardu ISO, itp. Przedsiębiorca oczywiście może je wprowadzić, ale nie jest ono niezbędne. Dlatego w RODO pozostawiono dowolność w formie, wskazując jedynie, jakie elementy powinny być zawarte.

RODO wskazuje również, kiedy **nie trzeba** dokonywać DPIA. Będą to wymienione dalej przypadki.

[3] Por. D. Nowak, *Ocena skutków dla ochrony danych* – projekt wytycznych Grupy Roboczej art. 29, http://traple.pl/blog/.

1. Charakter, zakres, kontekst i cele przetwarzania są bardzo podobne to przetwarzania, dla którego już została dokonana ocena. W takich przypadkach mogą być wykorzystane wyniki DPIA przeprowadzonej dla podobnego przetwarzania (art. 35 ust. 1).
2. Operacja przetwarzania ma podstawę prawną. Oceny skutków dla ochrony danych osobowych nie trzeba przeprowadzać wtedy, kiedy prawo UE lub państwa członkowskiego, któremu podlega administrator, reguluje już daną operację i jednocześnie oceny skutków dokonano w związku z przyjęciem tej regulacji. Taka redakcja artykułu uprawnia państwa członkowskie do podjęcia decyzji o konieczności dokonania oceny mimo spełnienia powyższych przesłanek (art. 35 ust. 10). W okresie kiedy powstawała niniejsza publikacja, nie została przeprowadzona przez ustawodawcę żadna ocena skutków.
3. Przetwarzanie jest uwzględnione w ustanowionym przez Prezesa Urzędu Danych Osobowych opcjonalnym wykazie Operacji przetwarzania niepodlegających wymogowi dokonania DPIA (art. 35 ust. 5).

Publikowanie oceny skutków przetwarzania danych zarówno częściowe, jak i całościowe, **nie jest wymagane** przepisami RODO i pozostaje ono jedynie w gestii administratora[4].

Uwagi

To administrator (np. przedsiębiorca) samodzielnie podejmuje decyzję o konieczności przeprowadzenia oceny.

Elementem zmniejszającym prawdopodobieństwo obowiązku przeprowadzenia DPIA jest również zmniejszenie kategorii zbieranych danych. W szczególności warto rozważyć np. ograniczenie monitoringu w zakładzie pracy.

2.1.1.4. Rejestrowanie czynności przetwarzania

Istotnym obowiązkiem, jaki został nałożony na administratorów, jest **rejestrowanie (ewidencjonowanie) czynności przetwarzania danych**. Polega ono na prowadzeniu dokumentacji, która zawiera wszystkie istotne z punktu widzenia przetwarzania informacje. Elementy składowe w większości już wcześniej musiały być uwzględnione w polityce bezpieczeństwa danych osobowych. Rejestr czynności przetwarzania opracowany przez inspektora ochrony danych powinien stanowić *vademecum* dla każdego pracownika w zakresie ochrony danych. Sporządza się go w wersji papierowej oraz wersji elektronicznej (art. 30 RODO).

W rejestrze czynności zamieszcza się następujące informacje:

a) **imię i nazwisko lub nazwę oraz dane kontaktowe administratora** oraz wszelkich współadministratorów, a także, gdy ma to zastosowanie, przedstawiciela administratora oraz inspektora ochrony danych;
b) **cele przetwarzania danych osobowych**, czyli np. marketing produktów i usług własnych, realizacja obowiązków zbierania danych nałożona przez przepisy prawa, np. przez kodeks pracy;
c) **opis kategorii osób, których dane dotyczą oraz kategorii danych osobowych**. Do kategorii osób będą należeli pracownicy, uczniowie, członkowie, klienci. Możliwe jest przetwarzanie dwóch kategorii danych, tj. danych zwykłych (np. imię, nazwisko, adres zamieszkania, data urodzenia), jak i danych szczególnie chronionych (np. stan zdrowia);
d) **kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione**, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych (definicja odbiorcy znajduje się w art. 4 pkt 9 RODO);

[4] W zakresie szczegółowej analizy por. również N. Kalinowska, P. Litwiński, *Ocena skutków dla ochrony danych i uprzednie konsultacje – nowe obowiązki podmiotów przetwarzających dane osobowe,* Monitor Prawniczy nr 13, 2017.

Rejestr czynności przetwarzania danych osobowych	
Nazwa administratora danych lub podmiotu przetwarzającego/przedstawiciela administratora lub podmiotu przetwarzającego	ABC Sp. z o.o lub Jan Kowalski prowadzący działalność gospodarczą jako:…
Współadministratorzy	(jeśli dotyczy)
Inspektor ochrony danych osobowych	Oznaczenie inspektora wraz z danymi kontaktowymi
Cel przetwarzania	Realizacja umów zawieranych z klientami, marketing produktów własnych, realizacja stosunku pracy na podstawie prawa pracy
Opis kategorii osób	Klienci, kontrahenci, pracownicy
Kategorie odbiorców	Przeszkoleni i upoważnieni pracownicy (ewentualnie: ewidencja osób upoważnionych stanowi załącznik do rejestru – w takim przypadku trzeba prowadzić ewidencję)
Kategorie danych osobowych	Dane zwykłe: imię, nazwisko, PESEL, adres, adres e-mail, dane wynikające z przepisów prawa
Informacje o przekazaniu do państwa trzeciego lub organizacji międzynarodowej	Nie dotyczy
Planowany termin usunięcia danych osobowych	Zrealizowanie umowy, przeprowadzenie akcji marketingowej, cofnięcie zgody
Opis technicznych i organizacyjnych środków bezpieczeństwa	Programy antywirusowe, hasło zmieniane co 3 miesiące, zabezpieczenia fizyczne i organizacyjne

Źródło: opracowanie własne

e) gdy ma to zastosowanie fakt **przekazania danych osobowych do państwa trzeciego**, czyli poza Unię Europejską. Komisja Europejska ma tu na myśli przede wszystkim Stany Zjednoczone Ameryki Północnej. Przekazywanie tam danych osobowych jest dozwolone, o ile kontrahenci z USA należą do programu *Privacy Shield*. Lista podmiotów uczestniczących jest dostępna pod linkiem https://www.privacyshield.gov/list. Za każdym razem, kiedy dane osobowe są przekazywane poza Unię Europejską, **trzeba to zaznaczyć** w rejestrze czynności przetwarzania;
f) jeżeli jest to możliwe, **planowane terminy usunięcia poszczególnych kategorii danych**;
g) **ogólny opis technicznych i organizacyjnych środków bezpieczeństwa**, o których jest mowa w art. 32 ust. 1.

RODO nie wymienia wymagań minimalnych w zakresie ochrony danych. Przedsiębiorca sam zatem powinien określić środki bezpieczeństwa. Chodzi tutaj o zabezpieczenie fizyczne, np. poprzez politykę kluczy, zabezpieczenie osobowe, np. poprzez przeszkolenie personelu czy zabezpieczenie informatyczne, np. poprzez posiadanie odpowiedniego oprogramowania antywirusowego.

Co istotne, wskazany obowiązek prowadzenia rejestru czynności przetwarzania co do zasady **ma zastosowanie do przedsiębiorców lub podmiotów zatrudniających więcej niż 250 osób**. Jednakże RODO przewiduje od tego wyjątki. Prowadzenie rejestru czynności będzie obowiązkowe również dla małego i średniego przedsiębiorcy gdy:

- przetwarzanie może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą,
- nie ma charakteru sporadycznego lub
- obejmuje szczególne kategorie danych osobowych (art. 30 ust. 5).

Sporadyczny charakter przetwarzania danych w tym kontekście oznacza, że przetwarzanie danych nie stanowi nieodłącznego elementu wykonywania przez przedsiębiorcę działalności. W związku z tym prowadzenie akcji marketingowych np. poprzez wysyłkę wiadomości e-mail wyklucza sporadyczność przetwarzania danych. Z kolei sklep stacjonarny sprzedający materiały budowlane, który nie wykorzystuje w swojej działalności platformy elektronicznej, najprawdopodobniej będzie przetwarzał dane osobowe jedynie sporadycznie.

Doprecyzowanie pojęć nastąpi w regulacjach resortowych lub kodeksach postępowania, które opracuje Prezes UODO. Do tego czasu przedsiębiorca, aby uzyskać odpowiedź na pytanie, powinien samodzielnie ocenić, czy przetwarzanie ma charakter sporadyczny. Pomocne w tej ocenie może być dokonanie wewnętrznego lub zewnętrznego audytu.

Studium przypadku 3.
Jeśli przedsiębiorca prowadzi przychodnię, to dla obsługi klientów musi przetworzyć dane osobowe, w tym dane dotyczące zdrowia. W takiej sytuacji występują łącznie co najmniej dwie przesłanki, tj. zbieranie danych nie ma charakteru sporadycznego oraz zbierane są dane dotyczące zdrowia. W takiej sytuacji przedsiębiorca musi opracować rejestr czynności przetwarzania.

2.1.1.5. Współpraca z organem nadzorczym

Kolejnym ważnym obowiązkiem każdego administratora jest współpraca z organem nadzorczym (art. 31 RODO). Będzie ona polegać na:

1) zgłaszaniu naruszeń ochrony danych osobowych;
2) uprzednich konsultacjach.

Obecnie w Polsce organem nadzorczym jest GIODO, niebawem będzie to **Prezes Urzędu Danych Osobowych**. To jemu będzie podlegać zdecydowana większość małych i średnich przedsiębiorstw. W nielicznych przypadkach będzie miała zastosowanie zasada *One stop shop*. Oznacza ona, że gdy przedsiębiorca prowadzi działalność transgraniczną (np. sprowadza auta z Niemiec do Polski), podlega jednemu organowi

nadzorczemu. Będzie to ten organ właściwy terytorialnie, gdzie znajduje się jego główna jednostka organizacyjna. Jest to miejsce, gdzie znajduje się **centralna administracja w Unii Europejskiej**, czyli miejsce, w którym siedzibę będzie miał zarząd spółki (por. Motyw 36 RODO). We wskazanej sytuacji, gdy siedziba zarządu przedsiębiorcy sprowadzającego auta będzie w Polsce, będzie on podlegał polskiemu organowi.

Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu

RODO zdefiniowało naruszenie ochrony danych osobowych jako naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych (art. 4 ust. 12 RODO).

Może ono skutkować powstaniem uszczerbku fizycznego, szkód majątkowych i niemajątkowych, takich jak np. utrata kontroli nad własnymi danymi osobowymi, sfałszowanie tożsamości, strata finansowa, nieuprawnione odwrócenie pseudonimizacji, naruszenie dobrego imienia, naruszenie poufności danych osobowych chronionych tajemnicą zawodową itd. Dlatego po stwierdzeniu naruszenia ochrony danych osobowych administrator ma obowiązek zgłosić je organowi nadzorczemu, czyli Prezesowi Urzędu Ochrony Danych, **w ciągu 72 godzin po stwierdzeniu naruszenia**. Jeżeli nie można dokonać zgłoszenia w terminie 72 godzin, zgłoszeniu powinno towarzyszyć wyjaśnienie przyczyn opóźnienia (Motyw 85 RODO).

Przedsiębiorca według swojej wiedzy samodzielnie powinien stwierdzić, czy naruszenie miało miejsce. Takie zgłoszenie musi co najmniej:

a) **opisywać charakter naruszenia ochrony danych osobowych**, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
b) **zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych** lub oznaczenie innego punktu kontaktowego[5], od którego można uzyskać więcej informacji na temat naruszenia;
c) **opisywać możliwe konsekwencje naruszenia ochrony danych osobowych**;
d) **opisywać środki zastosowane lub proponowane przez administratora** w celu zaradzenia na przyszłość naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach – planowane środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Na administratora nałożono obowiązek dokumentowania wszelkich naruszeń ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu na zweryfikowanie przestrzegania RODO. Forma i procedura takiego zgłaszania zostaną określone przez **organ nadzoru, czyli Prezesa Urzędu Danych Osobowych.**

W przypadku kontroli Prezesa UODO (np. w wyniku skargi), będzie on uwzględniał nie tylko same naruszenia, ale i fakt ich zgłoszeń lub zaniechanie tej czynności. Niedokonanie zgłoszenia może być elementem zwiększającym wysokość kary.

Uprzednie konsultacje

Artykuł 36 RODO wskazuje również, że jeśli ocena skutków dla ochrony danych wskaże, że przetwarzanie powodowałoby wysokie ryzyko naruszenia praw lub wolności osób fizycznych, w przypadku gdyby administrator nie zastosował środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania administrator ma obowiązek skonsultowania się z organem nadzorczym. Ma to miejsce wtedy, kiedy administrator uzna, że danego ryzyka nie da się zminimalizować środkami rozsądnymi z punktu widzenia

[5] Punkt kontaktowy nie oznacza pełnomocnika upoważnionego do reprezentowania spółki, a optymalny dla administratora sposób kontaktu z Prezesem Urzędu Danych Osobowych.

dostępnych technologii i kosztów wdrożenia. Konsultacje mają na celu pomoc przedsiębiorcy w sposobie znalezienia metody minimalizacji ryzyka.

2.1.1.6. Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych

Administrator powinien zawsze pamiętać, że nadrzędnym celem RODO jest ochrona praw osób, których dane dotyczą. Dlatego też rozporządzenie przewiduje, że jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą o takim naruszeniu.

Podobnie jak w przypadku obowiązku informacyjnego, również tutaj nadrzędnym obowiązkiem jest jasność przekazu. Chodzi o to, żeby podmiot danych osobowych mógł zrozumieć, że miało miejsce naruszenie jego danych oraz mieć świadomość potencjalnych konsekwencji, które wiążą się z tym faktem.

Takie zawiadomienie musi co najmniej:

a) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, który pozwoli uzyskać więcej informacji;
b) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
c) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach – środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Przykładowe zawiadomienie osoby o naruszeniu jej danych

Wczoraj w godzinach wieczornych przez przypadek został wysłany przez naszego pracownika e-mail z otwartą listą adresatów. Nasza spółka stara się wdrażać najwyższe standardy, dlatego przepraszamy za zaistniałą sytuację. Opisany błąd był spowodowany roztargnieniem pracownika. W stosunku do niego została wyciągnięta odpowiedzialność. Wszystkie osoby z Biura Obsługi Klienta zostaną przeszkolone w zakresie przestrzegania procedur bezpieczeństwa, aby na przyszłość sytuacja się nie powtórzyła.. W wyniku wysłania e-maila z otwartą listą adresatów mogą państwo otrzymywać SPAM. Inspektorem Ochrony Danych w naszej spółce jest Michał Kowalski, tel. 22 345 345, adres elektroniczny: iod@spolkaabc.pl.

Zawiadomienie **nie jest wymagane** w następujących przypadkach:

a) administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie. W szczególności chodzi o takie środki, jak pseudonimizacja oraz anonimizacja danych. Ich stosowanie powoduje, że nawet naruszenie danych nie spowoduje powstania dodatkowego obowiązku informacyjnego;
b) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;
c) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób (art. 34 RODO).

Ustawodawca unijny korzysta z pojęć niedookreślonych np. „niewspółmiernie dużego wysiłku". Ustalenie precyzyjne takich definicji będzie wymagało wydania decyzji przez Prezesa UODO oraz orzeczeń przez sądy. W chwili powstawania publikacji nie było możliwości wskazania, w jakich konkretnie sytuacjach nie wystąpi obowiązek zawiadamiania. Obowiązek rozstrzygnięcia leży zatem po stronie przedsiębiorcy. Zalecić można jedynie dokonanie takiego zawiadomienia w przypadku jakichkolwiek wątpliwości w tym zakresie.

2.2. PODMIOT PRZETWARZAJĄCY

Zgodnie z przepisami RODO podmiot przetwarzający oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe **w imieniu administratora**. Administrator powinien korzystać wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO. Podmiot przetwarzający nie może bez uprzedniej, szczegółowej i pisemnej zgody administratora podpowierzać wykonywania usług. W przypadku podpowierzenia, na podmiot przetwarzający drugiego stopnia (tj. ten, który przetwarza dane w wyniku umowy podpowierzenia), muszą być nałożone takie same obowiązki ochrony danych, jak w umowie między administratorem a podmiotem przetwarzającym.

Jeżeli przetwarzania dokonuje się na podstawie umowy, to powinna ona stanowić, że podmiot przetwarzający (art. 28 ust. 3 RODO):

a) **przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora** – co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej – chyba że obowiązek taki nakłada na niego prawo Unii Europejskiej lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający; w takim przypadku przed rozpoczęciem przetwarzania podmiot przetwarzający informuje administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny;
b) zapewnia, by osoby upoważnione do przetwarzania danych osobowych **zobowiązały się do zachowania tajemnicy** lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
c) podejmuje wszelkie środki wymagane w zakresie bezpieczeństwa przetwarzania (na mocy art. 32 RODO);
d) przestrzega warunków korzystania z usług innego podmiotu przetwarzającego, a więc w zakresie podpowierzenia;
e) biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III;
f) uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków administratora;

Studium przypadku 4.

Umowa kadrowo-płacowa powinna zawierać:

- **przedmiot**: przedmiotem umowy jest przetwarzanie danych osobowych pracowników administratora danych (np. przedsiębiorcy);
- **czas**: okres obowiązywania umowy świadczenia usług wynikających z umowy;
- **charakter**: przetwarzanie może mieć sporadyczny charakter, może również odbywać się w dużej skali, za pomocą systemów informatycznych oraz w formie papierowej;
- **cel**: realizacja *świadczonej* umowy;
- **rodzaj danych osobowych**: dane osobowe zawarte w zbiorze Pracownicy – dane zwykłe oraz szczególne kategorie danych;
- **kategorie osób, których dane dotyczą**: pracownicy administratora danych oraz podmiotu przetwarzającego;
- **obowiązki i prawa administratora**: w szczególności prawo dokonywania kontroli warunków przetwarzania danych osobowych;
- **obowiązki podmiotu przetwarzającego (w literaturze można spotkać również pojęcie procesora)**: wymienione powyżej (tj. zawarte w art. 28 ust. 3 pkt a)-h) RODO).

g) po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii Europejskiej lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych;
h) udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszym artykule oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.

2.3. INSPEKTOR OCHRONY DANYCH (IOD)

RODO nie zawiera definicji, kim jest inspektor ochrony danych. Poprzestaje wyłącznie na zadaniach, jakie ma on wypełniać oraz jego umiejscowieniu w strukturze przedsiębiorstwa. Należy więc przyjąć, że jest to osoba nadzorująca z upoważnienia administratora przestrzeganie stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych oraz wypełnianie przepisów RODO.

W zakresie wyznaczania inspektora ochrony danych, RODO nie przyznaje takiej dowolności administratorowi, jak dawała mu Ustawa o ochronie danych osobowych w kwestii wyznaczenia Administratora Bezpieczeństwa Informacji (ABI). Zgodnie z przepisami RODO, **jeśli administrator spełnia jedną z przesłanek powołania inspektora, to ma obowiązek go powołać**. Te przesłanki to:

1) przetwarzania danych dokonuje organ lub podmiot publiczny;
2) **główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania na dużą skalę, które, ze względu na swój charakter, zakres lub cele, wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą**.

Jest to podstawowa przesłanka powoływania inspektora ochrony danych. Sytuacje, w których powołanie inspektora będzie wymagane, zostaną szczegółowo doprecyzowane przez Prezesa UODO w drodze decyzji administracyjnych. Wydaje się jednak, że będzie to dotyczyć takich podmiotów, jak:

- agencje ochrony,
- kliniki i szpitale,
- hotele, które świadczą dodatkowe usługi SPA,
- właściciele aplikacji internetowych mających na celu zbieranie danych i analizowanie zachowania,
- właściciele urządzeń zaopatrzonych w inteligentne czytniki (np. spółdzielnia mieszkaniowa, która zainstalowała inteligentne czytniki w domach spółdzielców);

3) główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych albo danych osobowych dotyczących wyroków skazujących i naruszeń prawa (art. 37 ust. 1). W przeciwieństwie do poprzedniego punktu nie jest tu wymagana duża skala przetwarzania.

Administrator może zadecydować, czy inspektorem będzie **pracownik zatrudniony** w jego przedsiębiorstwie lub urzędzie czy też będzie nim **osoba z zewnątrz**.

Pierwszy przypadek wiąże się z przeszkoleniem pracownika w zakresie wymagań przepisów prawa, zwłaszcza RODO i przepisów sektorowych. Administrator **może powierzyć** inspektorowi wykonywanie także innych obowiązków służbowych, **jeżeli nie naruszy to prawidłowego wykonywania zadań z zakresu ochrony danych.** Powierzenie funkcji inspektora już zatrudnionemu pracownikowi może oznaczać konieczność zmiany struktury organizacyjnej – inspektor musi bowiem być podległy **bezpośrednio** pod kierownictwo jednostki np. pod prezesa przedsiębiorstwa.

W drugim przypadku administrator może powołać inspektora **poprzez zawarcie umowy sprawowania funkcji inspektora**, czyli skorzystanie z usług profesjonalisty mającego doświadczenie w pełnieniu swoich obowiązków. Jest to sytuacja najbardziej optymalna, jakkolwiek wiąże się z dodatkowymi kosztami.

Administrator **nie powołuje** inspektora w sytuacji, gdy przesłanki RODO do powołania inspektora nie zostały spełnione.

W sytuacji, w której przedsiębiorca ma wątpliwości, czy wyznaczać inspektora, powinien przeprowadzić wewnętrzny lub zewnętrzny audyt w celu zweryfikowania spełniania przesłanek RODO.

2.3.1. KWALIFIKACJE ORAZ KOMPETENCJE IOD

Minimalne wymagania stawiane w RODO inspektorom nie są wysokie. Artykuł 37 rozporządzenia nie wskazuje konkretnych kwalifikacji zawodowych. Inspektor powinien natomiast posiadać:

- **wiedzę fachową** na temat prawa i praktyk w dziedzinie ochrony danych; powyższe dotyczy nie tylko znajomości przepisów RODO, ale i przepisów sektorowych. W szczególnych gałęziach gospodarki, np. w przypadku spółek telekomunikacyjnych, przepisy sektorowe mogą mieć istotne znaczenie,
- **umiejętności wypełnienia zadań** opisanych w dalszej części publikacji.

Oznacza to, że wbrew opiniom, na które można się natknąć w internecie, inspektor **nie ma obowiązku** legitymować się wykształceniem wyższym, w szczególności wykształceniem prawniczym.

Przedsiębiorca, jako administrator, powinien jednak mieć na uwadze, że kwalifikacje inspektora muszą być współmierne do charakteru, skomplikowania i ilości danych przetwarzanych w ramach jednostki. Inne wymagania powinny być zatem postawione przed inspektorem w przedsiębiorstwie, w którym odbywają się złożone operacje przetwarzania danych osobowych, inne tam, gdzie jest przetwarzana duża ilości danych szczególnych kategorii, a jeszcze inne w firmie regularnie przekazującej dane do państw trzecich, czyli pozaunijnych.

2.3.2. ZADANIA INSPEKTORA OCHRONY DANYCH

Stanowisku inspektora ochrony danych przypisano następujące zadania:

a) **informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o spoczywających na nich obowiązkach** wynikających z RODO oraz z innych przepisów Unii Europejskiej lub przepisów krajowych, **i doradzanie im w tej sprawie**;

b) **monitorowanie przestrzegania** przepisów dotyczących danych osobowych, polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;

c) **udzielanie na żądanie zaleceń co do oceny skutków** dla ochrony danych oraz monitorowanie jej wykonania;

d) **współpraca z organem nadzorczym** tj. z Prezesem Urzędu Ochrony Danych Osobowych, czyli np. zgłaszanie naruszeń ochrony danych;

e) **pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami** oraz w **stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach** (art. 39 ust. 1).

2.3.3. PUBLIKOWANIE I ZAWIADOMIENIE O DANYCH KONTAKTOWYCH INSPEKTORA OCHRONY DANYCH

Podobnie jak w przypadku Ustawy o ochronie danych osobowych, w RODO został nałożony **obowiązek zgłaszania** przez administratora danych inspektora ochrony danych Prezesowi Urzędu Ochrony Danych Osobowych oraz **opublikowania danych kontaktowych do inspektora.** Takie działanie ma umożliwić zainteresowanym nawiązanie w łatwy sposób kontaktu z inspektorem.

W ramach dobrych praktyk można tu wskazać:

- adres korespondencyjny,
- telefon kontaktowy,

- dedykowany adres email,
- dedykowaną infolinię,
- formularz kontaktowy do inspektora na stronie internetowej organizacji.

Jak zostało wskazane we wstępie do niniejszej publikacji, polska ustawa będzie regulowała te kwestie, na które przyzwala RODO. Jedną z nich są elementy związane z rejestracją inspektora.

Zgodnie z art. 59 projektowanej nowej ustawy o ochronie danych osobowych (dalej: nowa UODO, administrator danych albo podmiot przetwarzający, który wyznaczył inspektora ochrony danych, zawiadamia Prezesa Urzędu o jego wyznaczeniu w terminie 14 dni od dnia, kiedy to miało miejsce. W zawiadomieniu należy wskazać:

- imię,
- nazwisko,
- adres poczty elektronicznej albo numer telefonu inspektora.

Nowa ustawa o ochronie danych będzie zawierać dodatkowe elementy zgłoszenia, takie jak adres swojej siedziby i pełną nazwę, a gdy administratorem lub podmiotem przetwarzającym jest osoba fizyczna (np. prowadząca jednoosobową działalność) – miejsce zamieszkania oraz imię i nazwisko.

Zgłoszenia będą odbywać się w formie elektronicznej. Prezes Urzędu prowadzi system teleinformatyczny umożliwiający przesyłanie zawiadomień w postaci elektronicznej.

Uwagi

Osoby wykonujące w dniu 24 maja 2018 r. funkcję administratora bezpieczeństwa informacji będą pełnić funkcję inspektora ochrony danych do dnia 1 września 2018 r. (art. 61 projektowanej ustawy).

Projekt ustawy zakłada, że zawiadomienie o zgłoszeniu inspektora będzie mogło być dokonane jedynie elektronicznie i opatrzone kwalifikowanym odpisem elektronicznym lub podpisem potwierdzonym profilem zaufanym ePUAP.

2.3.4. USYTUOWANIE INSPEKTORA W STRUKTURZE PRZEDSIĘBIORSTWA

Odpowiednio wysokie usytuowanie Administratora Bezpieczeństwa Informacji w hierarchii przedsiębiorstwa widoczne było już w UODO. W myśl jej przepisów, ABI musiał podlegać bezpośrednio pod kierownika jednostki. W nowym porządku prawnym sytuacja ta nie uległa zmianie.

W przepisach RODO przewidziano konieczność właściwego i niezwłocznego włączania inspektora ochrony danych we wszystkie sprawy dotyczące ochrony danych osobowych (art. 38 ust. 1).

Należy pamiętać, że takie włączenie inspektora oraz konsultowanie się z nim, zwłaszcza w początkowych fazach, wspomoże zapewnienie zgodności z RODO i uwzględnianie ochrony danych w fazie projektowania.

W związku z tym administrator powinien zapewnić między innymi:

- udział inspektora w spotkaniach przedstawicieli wyższego i średniego szczebla organizacji;
- uczestnictwo inspektora przy podejmowaniu decyzji dotyczących przetwarzania danych osobowych; niezbędne informacje powinny zostać udostępnione inspektorowi odpowiednio wcześniej, aby umożliwić zajęcie mu stanowiska;
- branie pod uwagę stanowiska inspektora przy podejmowaniu decyzji dotyczących przetwarzania danych osobowych;
- natychmiastowe konsultowanie się z inspektorem w przypadku stwierdzenia naruszenia albo innego zdarzenia związanego z danymi osobowymi.

2.3.5. WSPARCIE INSPEKTORA PRZEZ KADRĘ KIEROWNICZĄ

RODO wskazuje, że samo powołanie inspektora jest niewystarczające. Przepisy nakładają bowiem na administratora obowiązek wspierania inspektora ochrony danych w wypełnianiu przez niego zadań, zapewniając mu zasoby niezbędne do ich wykonania oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej (art. 38 RODO).

Grupa art. 29 wskazuje, że wsparcie inspektora ze strony kadry kierowniczej powinno uwzględnić poniższe aspekty.

1. Wymiar czasu pracy umożliwiający inspektorowi wykonywanie zadań. Jest to szczególnie istotne w przypadku wewnętrznych inspektorów zatrudnionych na tym stanowisku w niepełnym wymiarze czasowym albo w przypadku zewnętrznych inspektorów łączących obowiązki IOD z innymi zadaniami (np. prawnik reprezentujący spółkę w sprawach z prawa pracy i prawa handlowego jednocześnie pełni funkcję inspektora). Dobrą praktyką byłoby wskazanie czasu, który należy poświęcić na obowiązki IOD, oszacowanie czasu potrzebnego na wypełnienie tych obowiązków, ustalenie priorytetów IOD i stworzenie planu pracy inspektora.
2. Odpowiednie wsparcie finansowe, infrastrukturalne (tj. pomieszczenia, sprzęt, wyposażenie) i kadrowe, gdy to właściwe.
3. Oficjalne zakomunikowanie wszystkim pracownikom faktu wyznaczenia inspektora, tak aby wiedzieli o jego istnieniu oraz o pełnionych przez niego funkcjach.
4. Umożliwienie dostępu do innych działów organizacji, np. HR, działu prawnego, IT, ochrony itd., dzięki czemu IOD mogą uzyskać niezbędne wsparcie, wkład lub informacje z tych jednostek organizacyjnych.
5. Ciągłe szkolenie. IOD powinien mieć możliwość ciągłego aktualizowania wiedzy z zakresu ochrony danych osobowych. Celem powinno być zwiększanie wiedzy IOD i zachęcanie go do udziału w szkoleniach, warsztatach, forach poświęconych ochronie danych itd.
6. W zależności od rozmiaru i struktury organizacji przydatne może być powołanie zespołu inspektora ochrony danych, tj. IOD i jego pracowników. W przypadku powołania takiego zespołu, jego struktura, podział i zakres obowiązków powinny zostać jasno ustalone. Również w przypadku wyznaczenia IOD spoza organizacji, zespół pracowników podmiotu zewnętrznego powołany do wypełniania obowiązków związanych z ochroną danych osobowych może efektywnie wypełniać zadania IOD, gdy wyznaczona zostanie osoba odpowiedzialna za kontakt z klientem.

2.3.6. NIEZALEŻNOŚĆ INSPEKTORA

Przepisy RODO ustanawiają wysoki stopień niezależności inspektorów. W Motywie 97 zostało zapisane, że IOD – bez względu na to, czy są pracownikami administratora czy też są inspektorami zewnętrznymi – powinni być w stanie wykonywać swoje obowiązki i zadania w sposób niezależny, tj. nie otrzymywać instrukcji co do wykonywania swoich obowiązków.

Należy jednakże pamiętać, że w obszarze niezwiązanym z pełnieniem funkcji inspektora, IOD podlega zwykłej odpowiedzialności np. odpowiedzialności pracowniczej. Odwołanie inspektora może nastąpić, jeżeli doszło do złamania przez niego norm prawa karnego czy prawa pracy, czyli np. kradzieży pracowniczej, mobbingu lub każdego innego ciężkiego naruszenia obowiązków pracowniczych.

RODO nie wskazuje, w jakich sytuacjach i w jakim czasie inspektor może zostać odwołany i zastąpiony inną osobą[6].

Jeżeli przez zaniedbanie inspektora nastąpiło naruszenie danych osobowych, to taka sytuacja może stanowić przesłankę zwolnienia dyscyplinarnego IOD bądź wystąpienia przez administratora z roszczeniem odszkodowawczym.

[6] Powyższe przykłady w tabelach i tekst zostały opracowane na podstawie dyrektyw Grupa art. 29.

3. PRAWA OSÓB, KTÓRYCH DANE DOTYCZĄ, CZYLI INNE OBOWIĄZKI ADMINISTRATORA

Bartosz Mendyk

Portale internetowe, w tym portale społecznościowe, coraz częściej zamiast opłat za korzystanie z oferowanych przez nie usług, oczekują od użytkowników (klientów) udostępnienia danych osobowych oraz wyrażenia zgody na ich przetwarzanie. Staje się to szczególnie wartościowe wraz z rozwojem metod wykorzystujących przetwarzanie behawioralne (profilowanie), polegające na kojarzeniu tj. wiązaniu ze sobą tzw. danych surowych (z ang. *raw data),* czyli np. wieku, płci, wykształcenia, miejsca zamieszkania, wykonywanego zawodu, odwiedzanych stron internetowych itd., a następnie, dzięki specjalnym algorytmom, tworzenia profilu użytkownika (często potencjalnego klienta) np. w celu późniejszego ułatwienia czynności związanych z rekrutacją do pracy lub sporządzenia oferty handlowej.

Ze względu na powyższe prawodawca unijny rozbudował istniejące dotychczas regulacje mające służyć ochronie danych osobowych. Oprócz obowiązujących wcześniej praw, takich jak **dostęp do danych** i **prawo do sprostowania danych**, w treści RODO zostało także zawarte prawo do **ograniczenia przetwarzania**, **prawo do bycia zapomnianym (usunięcia danych)** czy **prawo do przenoszenia danych**. Przestrzeganie tych praw powinni uwzględnić wszyscy administratorzy (np. przedsiębiorcy) przetwarzający dane. Gdy przedsiębiorca dokonuje profilowania, powinien również wskazać prawo sprzeciwu.

3.1. PRAWO DOSTĘPU DO DANYCH OSOBOWYCH

Art. 15 ust. 1 RODO wskazuje, że osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora (np. przedsiębiorcy) informacji, czy przetwarza on jej dane osobowe, a jeżeli ma to miejsce – jest uprawniona do uzyskania dostępu do nich oraz do uzyskania informacji dotyczących:

- **celów przetwarzania**;
- **kategorii odnośnych danych osobowych**, czyli informacji o tym, czy dane trafiają do kategorii klientów, dostawców, pracowników administratora i ewentualnie podmiotu przetwarzającego (np. przedsiębiorcy);
- **odbiorców lub kategorii odbiorców**, którym dane osobowe zostały lub zostaną ujawnione; w szczególności chodzi o odbiorców w państwach trzecich oraz o organizacje międzynarodowe;
- **planowanego okresu przechowywania danych osobowych** lub kryteriów ustalania tego okresu;
- **prawa do żądania od administratora sprostowania**, usunięcia lub ograniczenia przetwarzania danych osobowych oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
- **prawa wniesienia skargi do organu nadzorczego**;
- **źródła dostarczającego dane osobowe**, jeżeli nie zostały one zebrane od osoby, której dane dotyczą;
- **zautomatyzowanego podejmowania decyzji**, w tym profilowania oraz istotnych informacji o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Prawo dostępu jest podstawowym i pryncypialnym prawem, a wszystkie pozostałe prawa wynikają właśnie z jego realizacji. Nieprawidłowe wypełnienie bądź niewypełnienie obowiązku w zakresie prawa dostępu do danych przez administratora (np. przedsiębiorcę), utrudni lub uniemożliwi wykonanie kolejnych praw. Dostęp do wymienionych wyżej kategorii informacji powinien zatem być skrupulatnie przestrzegany.

Prawo dostępu może stać się przedmiotem nadużyć ze strony osób, którym ono przysługuje. Może bowiem zaistnieć sytuacja, w której klienci danego przedsiębiorstwa będą celowo korzystać z przysługujących im uprawień w taki sposób, żeby wywołać określone negatywne konsekwencje w działalności firmy. Przykładowo – działając w porozumieniu wielu niezadowolonych klientów może kilka razy dziennie

wnioskować o dostęp do ich danych, co albo całkowicie uniemożliwi normalne funkcjonowanie przedsiębiorstwa lub przynajmniej bardzo je zakłóci.

Aby ograniczyć nadużycia w tym zakresie, art. 15 ust. 3 RODO precyzuje, że administrator (np. przedsiębiorca) jest zobowiązany do dostarczenia osobie, której dane dotyczą, **jednej nieodpłatnej kopii** danych osobowych podlegających przetwarzaniu. Jednak za każdą kolejną administrator **ma prawo pobrać opłatę** w rozsądnej wysokości. Wynika ona z kosztów administracyjnych związanych z dostarczeniem kopii danych osobowych. Po uiszczeniu stosownej opłaty przez wnioskodawcę nie ma możliwości odmówienia mu dostępu do danych, niezależnie od liczby dotychczasowych wniosków.

Studium przypadku 1.
Użytkowniczka jednego z portali społecznościowych wniosła do administratora o udostępnienie danych, które zostały na jej temat zebrane. W odpowiedzi dostała 800 stron maszynopisu. Gdyby regularnie wnosiła o udostępnienie katalogu zebranych danych, mogłaby poważnie utrudnić funkcjonowanie portalu.

Studium przypadku 2.
Jednoosobowy sklep internetowy, który otrzymywałby prośby od kilkudziesięciu klientów, byłby sparaliżowany przez składanie wniosków przez kilku klientów, którzy by w zmowie takie wnioski składali jednocześnie. Gdy właściciel zażąda zapłaty, a klienci ją uiszczą, to przedsiębiorca będzie musiał udostępniać to, o co w tym wypadku występuje.

W ustępie czwartym art. 15 znajduje się przepis, zgodnie z którym przekazanie kopii przetwarzanych danych osobowych nie może nastąpić, jeśli niekorzystnie wpływa to na prawa i wolności osób trzecich. Ów niekorzystny wpływ zostanie omówiony w dalszej części rozdziału – Prawo do przenoszenia danych.

Uwaga
Prawo dostępu do danych dotyczy wszystkich podmiotów, czyli klientów, kontrahentów oraz pracowników.

3.2. PRAWO DO SPROSTOWANIA DANYCH

Jedną z podstawowych zasad przetwarzania danych osobowych jest zasada prawdziwości (art. 16 RODO). Wynika z niej prawo do **sprostowania danych**, które przysługuje osobie zezwalającej na przetwarzanie jej danych. Uwzględniając cel przetwarzania danych, osoba, której dane dotyczą, ma prawo żądania uzupełnienia i aktualizacji niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia. W takiej sytuacji aktualizacja czy uzupełnienie nastąpi bez usuwania dotychczasowych danych zgromadzonych tylko na mocy tego właśnie oświadczenia.

Studium przypadku 3.
Przedsiębiorca na stronie internetowej zamieszcza formularz dotyczący zmiany danych. Klienci mogą go wypełnić oraz przesyłać poprawione dane, gdyby zmienili adres zamieszkania, nazwisko itd.

3.3. PRAWO DO OGRANICZENIA PRZETWARZANIA

Osoba, której dane dotyczą, wykonując swoje prawo dostępu, może nabrać przekonania, że np. przetwarzanie odbywa się niezgodnie z prawem. Powstaje więc sytuacja sporna – administrator (np. przedsiębiorca) zbiera dane osobowe, a osoba zainteresowana uważa, że nie ma on ku temu podstaw. Dlatego w rozporządzeniu przewidziano również rozwiązanie zabezpieczające, które zostało ujęte jako przysługujące prawo do ograniczenia przetwarzania.

Uwaga
W RODO nie zawarto definicji ograniczenia przetwarzania, a jedynie wskazano w nim przypadki, kiedy ono następuje. Jest to prawo podobne do prawa do bycia zapomnianym, z tą różnicą, że administrator, pomimo ograniczenia przetwarzania, może następnie przetwarzać te dane za zgodą osoby w sytuacjach określonych w art. 18 ust. 2, np. **ochrony własnych roszczeń** (proces sądowy o zniesławienie, naruszenie dóbr osobistych itd.). Jest to zatem prawo, które będzie wykorzystywane przy okazji pozwów sądowych lub skarg do organu nadzorczego, gdy klient, pracownik lub kontrahent uważa, że administrator nie ma podstaw do przetwarzania lub przetwarzane dane nie są prawdziwe.

RODO określa w art. 18 ust. 1 szereg sytuacji, w których osoba, której dane są przetwarzane, ma prawo żądać ograniczenia tej czynności. Dotyczy to następujących sytuacji:

- osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający administratorowi sprawdzić prawidłowość tych danych;

Studium przypadku 4.
Klient sklepu, czyli osoba, której dane dotyczą, zmienił nazwisko, o czym właściciel sklepu został poinformowany. Jednak, łamiąc zasadę prawdziwości danych, administrator nie zmienił danych. Dopóki administrator nie sprawdzi, czy dane klienta odpowiadają prawdzie, nie może ich przetwarzać np. do celów marketingowych. Okres aktualizacji będzie zależał od samego przedsiębiorcy.

- przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;

Studium przypadku 5.
Administrator portalu internetowego, który sprzedaje towary, gromadzi dane osobowe kupujących. Klient kwestionuje legalność przetrzymywania danych, bowiem nie wyraził zgody na wykorzystywanie ich do celów marketingowych, a regularnie dostaje newsletter z aktualną ofertą handlową. Jednocześnie chce nadal pozostać klientem tego sklepu. Do czasu wyjaśnienia zaistniałej sytuacji, klient ma prawo żądać ograniczenia przetwarzania jego danych – administrator nie ma prawa wysyłać mu newslettera z ofertą, ale nie przeszkadza to klientowi w robieniu zakupów w tym sklepie.

- administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub ochrony roszczeń;

- osoba, której dane dotyczą, skorzystała z prawa do sprzeciwu w związku z profilowaniem – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

W art. 18 ust. 2 wskazano konsekwencje ograniczenia przetwarzania danych osobowych. Zgodnie z tym przepisem, dane, które zostały objęte ograniczeniem, mogą być przetwarzane:

- wyłącznie za zgodą osoby, do której dane należą,
- w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej,
- z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego.

W celu ochrony interesu osoby udostępniającej swoje dane, RODO nakłada na administratora obowiązek, aby przed uchyleniem ograniczenia przetwarzania, poinformował ją o tym.

3.4. PRAWO DO USUNIĘCIA DANYCH (DO BYCIA ZAPOMNIANYM)

Postulaty wyodrębnienia prawa do bycia zapomnianym były formułowane od dawna, gdyż stale narastał problem przechowywania danych osobowych wbrew woli osób, których one dotyczą. Trybunał Sprawiedliwości UE (TSUE) dnia 13 maja 2014 r. uznał, że w pewnych sytuacjach nie może mieć to miejsca – stwierdził, że każdemu internaucie przysługuje prawo do bycia zapomnianym[1]. Orzeczenie nie nakazywało usuwania danych źródłowych ze stron internetowych, a wyłącznie odnośniki (linki) do nich, które indeksuje i publikuje wyszukiwarka. W tym kontekście ukształtowane przez TSUE prawo do bycia zapomnianym można uznać za niepełne. Na mocy tego wyroku odnosiło się ono bowiem **nie do danych zgromadzonych przez portal internetowy, a do operatora wyszukiwarki internetowej, który, zgodnie z rozumowaniem Trybunału, poprzez wyszukiwanie i publikowanie linków do portali internetowych gromadzi dane osobowe ich użytkowników**.

Podstawę materialną (tj. przepisem, na który podmioty danych mogą się powołać) prawa do bycia zapomnianym prawodawca unijny zawarł w art. 17 RODO, który w ust. 1 przesądza, że osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:

- dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
- osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie zgodnie z art. 6 ust. 1 lit. a) (tj. osoba, która wyraziła zgodę na przetwarzanie w określonym celu) lub art. 9 ust. 2 lit. a) (zgoda na przetwarzanie szczególnych danych osobowych), i nie ma innej podstawy prawnej przetwarzania;
- osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 (tj. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją...) wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 (tj. Jeżeli dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego) wobec przetwarzania;
- dane osobowe były przetwarzane niezgodnie z prawem;
- dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii Europejskiej lub prawie państwa członkowskiego, któremu podlega administrator;
- dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1 (tj. świadczonych dziecku) – jest tutaj mowa o osobie, która ze względu na wczesny

[1] Wyrok Trybunału (wielka izba) z dnia 13 maja 2014 r. Google Spain SL i Google Inc. przeciwkoAgencja Española de Protección de Datos (AEPD) i Mariowi Costesze Gonzálezowi, C 131/12, ECLI:EU:C:2014:317.

wiek udostępniła swoje dane osobowe, nie będąc świadomą skutków dla niej wynikających. Osoba, której dane dotyczą, powinna móc korzystać z tego prawa, mimo że już nie jest dzieckiem.

Studium przypadku 6.
Jan Kowalski w wyszukiwarce Google Search znajduje link do stron dziennika „La Vanguardia" z ogłoszeniem o licytacji nieruchomości za jego zaległości wobec zakładu ubezpieczeń społecznych. Jan Kowalski ma prawo uznać, że powyższa kwestia została rozwiązana już wiele lat temu i informacja o niej nie ma żadnego znaczenia. Administrator wyszukiwarki ma obowiązek spowodować, że zaprzestanie ona wyszukiwania linków dotyczących kłopotów Jana Kowalskiego z przeszłości[2]. Gdyby Jan Kowalski był znanym przedsiębiorcą, nie mógłby się powołać na prawo do bycia zapomnianym – bowiem ograniczeniem takiego prawa jest wolność wypowiedzi i informacji (art. 17 ust. 3 lit. a) RODO).

Studium przypadku 7.
Na portalu społecznościowym nastolatek zamieszcza zdjęcia, które potwierdzają jego beztroski tryb życia i zamiłowanie do alkoholu. W wieku 20 lat zauważył, że pracodawcy sprawdzają jego profil na portalu i nie może znaleźć żadnej pracy. Ma prawo zażądać usunięcia wskazanych informacji.

Powyższe oznacza, że prawo do bycia zapomnianym przez podmiot wnioskujący o usunięcie danych może być realizowane tylko częściowo, bowiem można usunąć jedynie określone kategorie danych (zdjęcia, tagi, numery telefonów).

Odrębnym przypadkiem jest usunięcie danych z kopii zapasowej; jest to utrudnione ze względu na ciągłość systemu. W takiej sytuacji należy poinformować, jaki jest czas przechowywania wspomnianych kopii i po upływie takiego czasu dane zostaną bezpowrotnie usunięte.

Ustęp drugi art. 17 nakłada na administratorów danych osobowych, o których mowa w ustępie 1, **obowiązek poinformowania innych administratorów posiadających te dane o żądaniu usunięcia wszelkich łączy do nich, kopii i replikacji**. Jednocześnie ten obowiązek powinien zostać zrealizowany przy użyciu „dostępnych dla administratora rozwiązań i kosztów realizacji". Można zatem wywnioskować, że w przypadku gdy administrator będzie zmuszony ponieść nadmiernie wysokie koszty lub nie będzie dysponował odpowiednimi środkami technicznymi, może odmówić wykonania obowiązku. Jego działania w kierunku zrealizowania swojej powinności muszą być zatem rozsądne.

Prawo do bycia zapomnianym ciężko będzie praktycznie zastosować z kilku względów:

1. Nie ma wskazanej jednoznacznej odpowiedzialności administratora danych osobowych za niedopełnienie obowiązków usunięcia danych oraz poinformowania innych administratorów o żądaniu usunięcia.
2. RODO nie wskazuje sposobu, w jaki administrator powinien poinformować inne podmioty będące administratorami danych osobowych.

3.4.1. WYŁĄCZENIE PRAWA DO BYCIA ZAPOMNIANYM W RODO

Istnieje zamknięty katalog okoliczności, które wyłączają prawo do bycia zapomnianym osobie, która udostępnia swoje dane. Należą do niego:

- korzystanie z prawa do wolności wypowiedzi i informacji – dotyczy to głównie działalności dziennikarskiej czy artystycznej;

[2] Taka była sentencja Trybunału Sprawiedliwości Unii Europejskiej z dnia 13 maja 2014 r. Google Spain SL i Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD) i Mario Costeja González. O sygn. C-131/12.

Studium przypadku 8.
Właściciel lokalnej gazety lub portalu informacyjnego nie musi usuwać danych o lokalnym radnym, który przyszedł na sesję w stanie nietrzeźwym, bowiem w ten sposób jest realizowana wolność wypowiedzi i informacji.

- wykonywanie prawnego obowiązku przetwarzania danych na mocy prawa UE lub państwa członkowskiego, któremu podlega administrator – jest to sytuacja, w której przedsiębiorca przetwarza dane osobowe w związku z ciążącym na nim obowiązkiem prawnym;

Studium przypadku 9.
Przedsiębiorca, nawet na wniosek pracownika, nie może usunąć jego danych po wygaśnięciu stosunku pracy, bowiem przepisy wymagają przechowywania ich przez 50 lat.
Studium przypadku 10.
Przedsiębiorca, który zorganizował akcję promocyjną – konkurs z nagrodami dla swoich klientów – jest zobowiązany przechowywać określone dane przez 5 lat od końca roku kalendarzowego, w którym odbywał się konkurs[3].

- wykonywanie zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
- **względy interesu publicznego w dziedzinie zdrowia publicznego** w związku z art. 9 ust.2 lit. h) oraz i), a także art. 9 ust. 3. To wyłączenie prawa do bycia zapomnianym dotyczy różnych danych związanych ze zdrowiem i zabezpieczeniem społecznym zatrudnionego, przetwarzanych przez lub na odpowiedzialność osoby (lub pracownika podmiotu administrującego), który podlega tajemnicy zawodowej. Dotyczy także danych, których przetwarzanie jest niezbędne ze względu na interes publiczny w dziedzinie zdrowia publicznego (np. ochrona przed poważnymi, transgranicznymi zagrożeniami zdrowotnymi czy zapewnienie wysokich standardów jakości opieki zdrowotnej i produktów leczniczych).

Studium przypadku 11.
Powiatowy Inspektor Sanitarny prowadzi rejestr osób uchylających się od szczepień. Rejestr ten jest prowadzony ze względu na zdrowie publiczne tj. zdrowie społeczeństwa jako całości. Osoby tam figurujące nie mogą wykorzystać prawa do bycia zapomnianym (usunięcia danych), aby usunąć informacje o sobie lub o swoich dzieciach.

- **ze względu na cele archiwalne w interesie publicznym, badania naukowe, historyczne, statystyczne – jeżeli prawdopodobne jest, że skorzystanie z prawa do bycia zapomnianym uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania.** Takiemu przetwarzaniu danych towarzyszyć musi wdrożenie środków technicznych i organizacyjnych służących zachowaniu zasady minimalizacji danych. Środki te mogą obejmować także pseudonimizację danych, jeśli pozwala ona realizować powyższe cele. Jeśli cele można realizować w drodze dalszego przetwarzania przy użyciu danych, które nie pozwalają na identyfikację osoby, należy je realizować w ten sposób.

[3] Zob. Ustawa z dnia 15 lutego 1992 r. o podatku dochodowym od osób prawnych Dz.U. 1992 nr 21 poz. 86, oraz Ustawa z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych Dz.U. 1991 nr 80 poz. 350.

Studium przypadku 12.
Lekarz dla celów naukowych zbiera zdjęcia pacjentów z owrzodzeniami twarzy. Realizacja prawa do bycia zapomnianym utrudni realizację celów przetwarzania, czyli badania naukowe.

- ustalanie, dochodzenie oraz ochronę roszczeń.

Po zrealizowanym wniosku o usunięcie danych, ze względu na zasadę rozliczalności, warto zachować wnioski o usunięcie danych. Mogą one być przydatne ze względów dowodowych, np. w sytuacji, w której podmiot zainteresowany stwierdzi, że nigdy nie składał takiego wniosku.

3.4.2. DANE OSOBOWE W REJESTRZE SPÓŁEK

Problematycznym aspektem prawa do bycia zapomnianym jest figurowanie osób w rejestrze spółek. Znalazł on nawet swój wyraz w postępowaniu przed TSUE, w kontekście sprawy *Camera di Commercio, Industria, Artiginato e Agricoltura di Lecce* przeciwko *Salvatore Manni* (C-398/15). Trybunał rozstrzygnął, czy dyrektywa 95/46/WE w sprawie ochrony danych osób fizycznych oraz dyrektywa 68/151/EWG w sprawie jawności dokumentów spółek nie kolidują ze sobą i czy dowolna osoba może bez ograniczenia czasowego uzyskać dostęp do danych dotyczących osób fizycznych figurujących w rejestrze spółki.

Zdaniem TSUE, jawność rejestru spółek służy zagwarantowaniu pewności prawa w stosunkach między spółkami a osobami trzecimi, a także ochronie interesów osób trzecich w stosunkach ze spółkami kapitałowymi. Nie jest zatem słuszne, aby osoba widniejąca w takim rejestrze mogła powoływać się na prawo ochrony danych osobowych.

Ze względu na zróżnicowanie terminów przedawnienia roszczeń w europejskich systemach prawnych oraz dużą liczbę praw i stosunków prawnych zawieranych między podmiotami gospodarczymi z różnych państw członkowskich, nie jest możliwe wykształcenie uniwersalnego terminu, po upływie którego następowałoby usunięcie danych osób fizycznych z rejestrów spółek. Można zatem dojść do wniosku, że **prawo do bycia zapomnianym nie jest absolutne**.

W szczególnych przypadkach stosowanie powyższego wyjątku może zostać ograniczone i to na życzenie każdego z państw członkowskich. W sytuacji, kiedy spółka została zlikwidowana odpowiednio wcześniej, a przeważające i uzasadnione względy dotyczące konkretnego przypadku osoby za tym przemawiają, dostęp do jej danych osobowych może zostać ograniczony wyłącznie do osób trzecich mających konkretny interes w ich pozyskaniu. Ocena tego ograniczenia powinna być przeprowadzana indywidualnie dla każdego przypadku.

3.4.3. PRAWO DO ZAPOMNIENIA A REPUTACJA PRZEDSIĘBIORCY

Ograniczeniem prawa do zapomnienia jest również reputacja przedsiębiorcy. Zagadnieniem tym zajmował się Europejski Trybunał Praw Człowieka w sprawie *Fuchsmann przeciwko Niemcom*[4]. W tej sprawie znany niemiecki przedsiębiorca działający w sektorze mediów został opisany przez znaną gazetę jako osoba, która ma przestępcze powiązania z kandydatem na burmistrza Nowego Jorku oraz rosyjską mafią poprzez swoje spółki nadawcze na Ukrainie. Raporty europejskich oraz amerykańskich organów ściągania potwierdzały tezy artykułu. Przedsiębiorca zwrócił się do gazety z wnioskiem o usunięcie danych. W skargach do sądów niemieckich zauważył, że naruszono jego prawo do dobrego imienia. Trybunał zauważył, że artykuł został napisany zgodnie ze sztuką dziennikarską, zaś dziennikarz zachował wymogi etyki zawodowej i orzekł, że Europejska Konwencja Praw Człowieka nie została naruszona. Artykuł nie zawierał również żadnych informacji na temat życia prywatnego skarżącego. Wniosek, jaki z tego należy wysnuć, jest taki, że przedsiębiorcy

[4] Wyrok Europejskiego Trybunału Praw Człowieka z 24.10.2017 r., skarga nr 71233/13.

związani z branżą medialną, którzy w gruncie rzeczy są osobami publicznymi (np. celebryci), powinni być przygotowani na krytykę, zaś ich działalność może być komentowana w środkach masowego przekazu.

3.5. PRAWO DO PRZENOSZENIA DANYCH

RODO zawiera także inne nowe przepisy, których nie było w poprzednio obowiązującej ustawie tj. **prawo do przenoszenia danych** (art. 20 RODO). Zawiera ono w sobie również prawo do **otrzymania danych**. Na początku należy bardzo wyraźnie podkreślić, że nie jest to przeniesienie w znaczeniu, które można znaleźć w słowniku języka polskiego, a raczej możliwość skopiowania metadanych i przekazanie ich do innego administratora.

Studium przypadku 13.
Mikroprzedsiębiorca, który prowadzi konto w jednym banku (konto prywatne, z którego opłaca przelewy biznesowe, do ZUS-u itp.), chce założyć rachunek w innym. Dotychczasowy bank powinien przekazać dane dotyczące zrealizowanych przelewów nowemu bankowi, tak aby przedsiębiorca mógł bez większych utrudnień i zakłóceń prowadzić swoją działalność.

Studium przypadku 14.
Mikroprzedsiębiorca chce przenieść historię swoich billingów do drugiego operatora komórkowego. Dane dotychczasowych rozmówców będą na jego wniosek przeniesione.

Należy pamiętać, że prawo do przenoszenia danych ma zastosowanie tylko wtedy, jeżeli przetwarzanie danych odbywa się w sposób **zautomatyzowany**, a w związku z tym **nie obejmuje zbiorów papierowych, a także nie wszystkie zbiory elektroniczne**.

Ze względu na ważkość prawa do przenoszenia danych, również w tym aspekcie Grupa art. 29 wydała swoje wytyczne[5]. Są one dosyć obszerne i regulują zagadnienie w sposób szczegółowy.

Prawo do przenoszenia danych realizuje dwa cele. Po pierwsze, jest kolejnym prawem zwiększającym kontrolę podmiotu danych. Po drugie, jak wynika to ze wskazanych powyżej przykładów, zwiększa ono konkurencyjność, poprzez ułatwienie zmiany usługodawcy. RODO wpisuje się więc w szerszą politykę Unii Europejskiej która jest nastawiona na wspieranie konkurencyjności, czyli realizację założeń strategii Jednolitego Rynku Cyfrowego.

Warto jednak przyjrzeć się nieco bliżej samej definicji prawa do przenoszenia danych. Wspomniany artykuł 20 RODO wskazuje, że **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:

a) przetwarzanie odbywa się na podstawie zgody lub zgody na przetwarzanie szczególnych kategorii danych lub na podstawie umowy na przetwarzanie danych osobowych lub szczególnych kategorii danych;
b) przetwarzanie odbywa się w sposób zautomatyzowany.

Definicję prawa do przenoszenia można podzielić na kilka mniejszych elementów.

Pierwszy element to **prawo do otrzymania** (czyli uzyskania) takich danych.

[5] GRUPA ROBOCZA ART. 29 DS. OCHRONY DANYCH, Wytyczne dotyczące prawa do przenoszenia danych przyjęte w dniu 13 grudnia 2016 r., ostatnio zmienione i przyjęte w dniu 5 kwietnia 2017 r., dokument o sygn. 16/EN WP 242 rew.01.

Studium przypadku 15.
Osoba, której dane dotyczą, może być zainteresowana uzyskaniem swojej dokumentacji medycznej od prywatnej kliniki, w której się leczyła, w celu skonsultowania dalszego leczenia u innego specjalisty lub całkiem bezcelowo. Administrator, w tym przypadku prywatna klinika, ma obowiązek wydać pacjentowi dane (np. na płycie CD lub na pamięci USB) oraz wstrzymać się od utrudniania przeniesienia danych innemu administratorowi, np. innej klinice. To ostatnie oznacza, że pacjent może żądać od dotychczasowego administratora (kliniki) bezpośredniego przekazania danych innej klinice, a administrator ma obowiązek spełnić to żądanie, o ile jest to technicznie możliwe.

Przekazanie powinno odbyć się w terminie nie dłuższym niż 3 miesiące za pośrednictwem internetu, lub na innym nośniku informacji.

Drugie uprawnienie wynikające z omawianego prawa dotyczy możliwości **żądania przeniesienia danych osobowych od jednego administratora danych do innego.** Realizacja tego prawa została ograniczona możliwościami technicznymi administratora.

Jak wspomniano, w RODO zostało użyte słowo „przeniesienie", które w języku polskim oznacza „zabrać coś lub kogoś i niosąc, umieścić gdzieś indziej"[6]. W tym przypadku jest ono rozumiane inaczej. Przeniesienie danych oznacza bowiem, że dotychczasowy administrator danych, także po ich przeniesieniu, może świadczyć usługi w oparciu o te dane. Nie ma on obowiązku ich usunięcia, chyba że osoba, której dane dotyczą, skorzysta z prawa do bycia zapomnianym. Przeniesienie danych nie ma wpływu na pierwotny okres przechowywania mający zastosowanie wobec przesłanych danych.

Poza zapewnieniem uprawnień konsumentom poprzez zapobieganie nadmiernemu związaniu się z administratorem (przedsiębiorcą), prawo do przenoszenia danych ma promować możliwości innowacji i wymiany danych osobowych między administratorami danych w bezpieczny sposób.

Prawo to zostało pomyślane przede wszystkim dla przedsiębiorstw komunikacyjnych i portali społecznościowych – zostało zaprojektowane, aby przenieść dane z jednego portalu społecznościowego na inny. Następnie w wyniku prac nad RODO jego zakres został rozszerzony. Ze względu na charakter informatyczny tego prawa, w Polskiej Izbie Informatyki i Telekomunikacji została powołana grupa robocza, która ma przygotować kodeks postępowania, a w nim zasady przenoszenia danych. Zespół składa się z przedstawicieli operatorów telekomunikacyjnych i firm informatycznych.

3.5.1. KONTROLA NAD PRZEKAZYWANYMI DANYMI

Przenoszenie danych może prowadzić do zagrożeń ich naruszenia. Administrator danych jest odpowiedzialny za podjęcie wszelkich środków bezpieczeństwa potrzebnych do zapewnienia, aby dane osobowe zostały bezpiecznie przesłane (np. z zastosowaniem szyfrowania na całej drodze przesyłu danych lub szyfrowania danych) do właściwego miejsca przeznaczenia przy użyciu silnych środków uwierzytelniających.

Ze względu na nawiązywaną współpracę administratora danych z podmiotem przetwarzającym dane, realizacja prawa przenoszenia danych powinna również być w sposób szczególny uwzględniona w umowie. Dlatego, zgodnie z artykułem 28 RODO, w treści umowy między administratorem danych a podmiotem przetwarzającym musi być uwzględniony obowiązek pomocy ze strony podmiotu przetwarzającego „administratorowi poprzez odpowiednie środki techniczne i organizacyjne, (…) [aby] wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw". W przypadku gdy część zbioru danych administratora zostanie przekazana podmiotowi przetwarzającemu, należy przydzielić w umowie każdemu z nich obowiązki dotyczące przetwarzania wniosków o przeniesienie danych od osób, których dane dotyczą.

[6] Zobacz definicję Słownika Języka Polskiego, dostępną online: https://sjp.pwn.pl/sjp/przeniesc;2510751.html

Studium przypadku 16.
W sytuacji, gdy osoba, która przekazała transakcje bankowe z historią swoich przelewów, chce, żeby bank przekazał jej dane przedsiębiorstwu pomagającemu w zarządzaniu budżetem, to przedsiębiorstwo to nie musi przetrzymywać danych, które są dla niego zbędne z punktu widzenia realizacji świadczonej usługi (przykład za Grupa art. 29).

Podmiot otrzymujący staje się nowym administratorem danych. Oznacza to, że musi on przestrzegać wszystkich obowiązków i umożliwiać realizację praw, jakie są gwarantowane przez RODO. W szczególności musi określić on **cel swojego przetwarzania danych**.

Uwaga
Przyjęte i zatrzymane dane powinny obejmować tylko te dane, które są niezbędne i istotne dla usługi świadczonej przez otrzymującego administratora danych.

Studium przypadku 17.
Przepisy prawa dotyczące zapobiegania prania brudnych pieniędzy i innych przestępstw finansowych mogą ograniczyć prawo do przeniesienia danych wobec podmiotów danych.

3.5.2. PODSTAWY PRZENOSZENIA DANYCH OSOBOWYCH

Zgodnie z art. 20 ust. 1 lit. a) RODO, aby dane uległy przeniesieniu, operacje przetwarzania muszą odbywać się:

- **na podstawie zgody osoby, której dane dotyczą** (w myśl artykułu 6 ust. 1 lit. a) lub w myśl artykułu 9 ust. 2 lit. a), gdy chodzi o szczególne kategorie danych osobowych);
- **na podstawie umowy**, której stroną jest osoba, której dane dotyczą, w myśl artykułu 6 ust. 1 lit. b).

Zgodnie z artykułem 20 RODO, aby dane mieściły się w zakresie prawa do przenoszenia danych, muszą być spełnione poniższe przesłanki.

1. **Powinny to być dane dotyczące osoby, która wnioskuje o ich przeniesienie**.

Dane zanonimizowane lub niedotyczące osoby nie zawierają się w tym warunku. Dane spseudonimizowane – ze względu na możliwość późniejszej identyfikacji – tak.

Przykład
Rejestry połączeń telefonicznych, wiadomości interpersonalnych lub VoIP w historii konta abonenta mogą zawierać dane osób trzecich zaangażowanych w połączenia przychodzące i wychodzące. Mimo że rejestry będą w związku z tym zawierały dane osobowe nie tylko abonenta, powinien on mieć możliwość otrzymania tych rejestrów w odpowiedzi na wniosek o przenoszenie danych, ponieważ rejestry dotyczą także jego. Administrator danych, do którego następnie przekazano rejestr, nie powinien ich przetwarzać w żadnym celu, który by negatywnie wpłynął na prawa i wolności stron trzecich (za Grupą art. 29).

Powyższe działanie dotyczy zarówno danych przekazanych np. przez określony formularz (adres pocztowy, nazwa użytkownika itd.), ale również z obserwacji jej działalności. Chodzi tutaj o historię wyszukiwania osoby, dane o ruchu i dane lokalizacyjne. Mogą również obejmować inne dane surowe, takie jak tętno monitorowane przez urządzenia noszone na ciele.

2. Nie może negatywnie wpływać na prawa i wolności innych.

Prawo do przeniesienia danych nie zostanie zrealizowane w sytuacji, w której przesyłanie danych od jednego administratora do innego uniemożliwia stronom trzecim realizację ich praw jako osób, których dane dotyczą, na mocy RODO (np. praw do informacji, dostępu, etc.).

Studium przypadku 18.
Rachunek bankowy osoby, której dane dotyczą, może zawierać dane osobowe dotyczące transakcji nie tylko posiadacza rachunku, ale również informacje dotyczące transakcji innych osób, jeżeli np. przesłały one pieniądze posiadaczowi rachunku. Jest mało prawdopodobne, by miał miejsce negatywny wpływ na prawa i wolności stron trzecich podczas przesyłania informacji dotyczących rachunku bankowego do posiadacza rachunku, gdy składany jest wniosek o przeniesienie – pod warunkiem, że w obu przykładach dane są wykorzystywane w tym samym celu (tj. adres kontaktowy używany tylko przez osobę, której dane dotyczą lub historia rachunku bankowego osoby, której dane dotyczą). (Za Grupą art. 29)

3. Informacje, które należy uprzednio przekazać osobie, której dane dotyczą.

W celu zapewnienia zgodności z nowym prawem do przenoszenia danych administratorzy danych muszą informować osoby, których dane dotyczą, o dostępności nowego prawa do przenoszenia danych.

Uwaga
Przekazując wymagane informacje, administratorzy danych muszą zapewnić, aby osoby, które udostępniają swoje dane, odróżniały prawo do przenoszenia danych od innych praw (za Grupą art. 29).

3.5.3. IDENTYFIKACJA OSOBY, KTÓREJ DANE DOTYCZĄ, PRZED USTOSUNKOWANIEM SIĘ DO WNIOSKU O PRZENIESIENIE DANYCH

RODO nie zawiera szczegółowych wymogów co do tego, w jaki sposób weryfikować tożsamość osoby, której dane dotyczą, gdy chce przenieść dane. W związku z art. 12 ust. 6 administrator, który ma uzasadnione wątpliwości co do tożsamości osoby, której dane dotyczą, może zażądać dodatkowych informacji niezbędnych do potwierdzenia jej tożsamości. Grupa art. 29 wskazuje, że jeśli osoba, której dane dotyczą, przekaże dodatkowe informacje umożliwiające jej identyfikację, administrator danych nie może odmówić realizacji wniosku o przeniesienie, jeżeli jest on prawidłowy.

Takie procedury weryfikacji osób zazwyczaj już w przedsiębiorstwach istnieją, dlatego dane osobowe wykorzystywane do rejestracji osoby, której dotyczy przetwarzanie, mogą być również wykorzystane jako dowód uwierzytelnienia osoby, której dane dotyczą, do celów przeniesienia.

Studium przypadku 19.
Nazwy użytkownika i hasła często są wykorzystywane, aby umożliwić osobom dostęp do ich danych na ich kontach e-mail, kontach na portalach społecznościowych oraz kontach używanych w różnych innych usługach, gdzie osoby zdecydowały się na używanie niektórych z nich bez ujawniania swojego pełnego imienia i nazwiska oraz tożsamości.

3.5.4. TERMIN PRZEWIDZIANY NA UDZIELENIE ODPOWIEDZI

Z treści art. 12 ust. 3 RODO wynika, że administrator danych udziela odpowiedzi osobie, której dane dotyczą, „bez zbędnej zwłoki" – a w każdym razie w terminie miesiąca od otrzymania żądania. Ten miesięczny okres

można przedłużyć do maksymalnie trzech miesięcy w przypadku skomplikowanych spraw, pod warunkiem, że w terminie miesiąca od otrzymania pierwotnego żądania poinformuje się osobę, której dane dotyczą, o przyczynach takiego opóźnienia.

3.5.5. ODMOWA UDZIELENIA ODPOWIEDZI NA WNIOSEK O PRZENIESIENIE DANYCH

Artykuł 12 RODO zakazuje administratorowi danych pobierania opłat za przekazanie danych osobowych, chyba że może on wykazać, że żądania są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter. Dodatkowo, jeżeli wnioskodawca podejmuje swoje działania nieprzerwanie pomimo wcześniejszego udzielenia odpowiedzi na wniosek, administrator może także odmówić spełnienia żądania. Ciężar dowiedzenia, że żądania są nieuzasadnione lub nadmierne, spoczywa na administratorze danych.

Grupa art. 29 wskazuje, że sytuacje nadmiernego lub nieuzasadnionego wnioskowania powinny dotyczyć niewielkiej liczby przypadków, w których administrator danych byłby w stanie uzasadnić swoją odmowę, nawet w odniesieniu do wielu wniosków o przeniesienie danych. Ponadto całkowity koszt procedur ustanowionych w celu udzielania odpowiedzi na wnioski o przeniesienie danych nie powinien być brany pod uwagę przy określaniu „nadmiernego charakteru" wniosku.

3.5.6. SPOSOBY I PRZESZKODY PRZEKAZYWANIA DANYCH PODLEGAJĄCYCH PRZENOSZENIU

Artykuł 20 ust. 1 RODO przewiduje, że osoby, których dane dotyczą, mają prawo do przesyłania danych do innego administratora bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe. Zaistniałe przeszkody można podzielić na **przeszkody prawne**, **techniczne** lub **finansowe.** Mogą być one tworzone przez administratora danych dla ograniczenia lub utrudnienia dostępu, przesyłania lub ponownego wykorzystania danych przez zainteresowaną osobę lub przez innego administratora danych.

Techniczna możliwość przesłania danych przez administratora danych innemu administratorowi, pod kontrolą osoby, której dane dotyczą, powinna być oceniana indywidualnie. Motyw 68 dalej wyjaśnia granice tego, co jest „technicznie możliwe", wskazując, że „nie powinno to nakładać na administratorów obowiązku prowadzenia lub wprowadzenia kompatybilnych technicznie systemów przetwarzania".

Grupa art. 29 oczekuje, że administratorzy danych będą przesyłać dane osobowe w interoperacyjnym formacie, pomimo faktu że RODO nie nakłada na pozostałe podmioty danych obowiązku wspierania tych formatów.

Uwaga
Osoba, której dane dotyczą, wnioskująca o dane sama jest odpowiedzialna za zabezpieczenie danych we własnym systemie. Wydaje się to oczywiste, ale poza świadomością samodzielnego zabezpieczenia swoich danych, podmioty nie zawsze wiedzą, przy użyciu jakich środków to uczynić. Dobrą praktyką będzie sytuacja, gdy administrator przekaże podmiotowi danych wskazówki w powyższej sprawie.

3.6. PRAWO SPRZECIWU W ZWIĄZKU Z PROFILOWANIEM

W II Rozdziale wskazano, że specjalnym rodzajem przetwarzania danych jest profilowanie, a więc zautomatyzowane podejmowanie decyzji dzięki wykorzystaniu matematycznej analizy. Pozwala ono na ocenę niektórych czynników osobowych człowieka i jego potencjału. Zostały tam też wyszczególnione obowiązki nałożone na administratora (np. przedsiębiorcę), czyli np. osobna zgoda na dokonywanie profilowania.

Autorzy RODO zdają sobie sprawę, że automatyczne decyzje mogą być obarczone błędem – system może niewłaściwie interpretować dane.

Studium przypadku 20.
Internauta przez pół roku śledzi ceny mieszkań w większych miastach. Nie musi to oznaczać, że szuka on najkorzystniejszej oferty na rynku, tylko np. pisze pracę licencjacką, w której porównuje koszty zakupu mieszkania. W związku z tym przekazywanie mu reklam przez deweloperów lub pośredników w handlu nieruchomościami wydaje się bezzasadne. Podobnie osoba, która np. wyszukuje w sieci informacje dotyczące działalności ugrupowań neonazistowskich, może robić to ze względu na prowadzone przez nią badania naukowe, a nie dlatego, że podziela poglądy takich organizacji.

O ile zatem profilowanie i dopasowywanie reklam niesie tylko ograniczone ryzyko dla ich odbiorcy (np. nieodpowiednio dopasowana oferta), to RODO wskazuje, że są określone przypadki, szczególnie istotne dla osoby, w których ma ona prawo do tego, aby to człowiek rozpatrzył jej decyzję. Są to sytuacje związane zwłaszcza ze sferą zawodową oraz pożyczkową. Profilowanie zostało już omówione w innym rozdziale niniejszej publikacji omawiającym podstawowe definicje i tam też są wskazane rekomendacje, w których przypadkach przedsiębiorca nie będzie mógł polegać wyłącznie na zautomatyzowanym podejmowaniu decyzji. Poniżej zostanie jedynie zaznaczony aspekt sprzeciwu.

Prawo do sprzeciwu wobec podejmowania zautomatyzowanych decyzji oznacza, że osoba nie wyraża zgody na profilowanie oraz ma prawo żądać, aby to człowiek podjął ostateczną decyzję.

Należy pamiętać, że zgodę na profilowanie należy uzyskać przed rozpoczęciem automatycznego przetwarzania danych. Sprzeciw ten w określonych sytuacjach może dotyczyć również profilowania dla celów naukowych, statystycznych lub historycznych (art. 89 ust. 1).

Prawo do sprzeciwu nie przysługuje wtedy, kiedy (art. 22 ust. 2):

1. Decyzja jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą a administratorem.
2. Decyzja taka jest dozwolona prawem Unii Europejskiej lub prawem państwa członkowskiego, któremu podlega administrator, jeżeli zapewnia ono środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą.
3. Decyzja opiera się na wyraźnej zgodzie osoby, której dane dotyczą.

4. PREZES URZĘDU OCHRONY DANYCH OSOBOWYCH ORAZ ODPOWIEDZIALNOŚĆ PRZEDSIĘBIORCY

Bartosz Mendyk

Od 25 maja 2018 r. instytucja Generalnego Inspektora Ochrony Danych Osobowych zostanie zniesiona, zaś w jej miejsce zostanie powołany Prezes Urzędu Ochrony Danych Osobowych (dalej także: UODO lub Urząd)[1]. Zmiany nie ograniczą się jednak wyłącznie do nazewnictwa. Prezes UODO zyska dużo nowych uprawnień, które są powiązane z odpowiedzialnością przedsiębiorcy.

Ze swojej strony przedsiębiorca będzie podlegał poniższym rodzajom odpowiedzialności.

1. **Odpowiedzialność administracyjna** – będzie to najważniejszy środek egzekwowania przestrzegania RODO. Prezes UODO będzie prowadził:
   - postępowania kontrolne,
   - postępowania w sprawie naruszenia przepisów o ochronie danych osobowych.

   Na podstawie wyników przeprowadzonych postępowań będzie mógł nakładać administracyjne kary pieniężne.
2. **Odpowiedzialność cywilna** – ten rodzaj odpowiedzialności jest związany z nowym roszczeniem przewidzianym w projekcie Ustawy[2], które jest wzorowane na postępowaniu o naruszenie dóbr osobistych.
3. **Odpowiedzialność karna** – w stosunku do obecnej ustawy została ograniczona do minimum – projekt ustawy wskazuje dwa rodzaje naruszeń prawa, za które przewiduje odpowiedzialność karną.

4.1. ZADANIA ORGANU NADZORCZEGO

Zadania Prezesa Urzędu, czyli organu nadzorczego, są wymienione zarówno w RODO, jak i w polskiej ustawie. Z punktu widzenia przedsiębiorców do najważniejszych jego zadań będzie należało:

1. Monitorowanie i egzekwowanie stosowania przepisów RODO.
2. Upowszechnianie w społeczeństwie wiedzy o ryzyku, przepisach, zabezpieczeniach i prawach związanych z przetwarzaniem danych osobowych oraz rozumienie tych zjawisk. Szczególna uwaga ma być poświęcona działaniom skierowanym do dzieci. Upowszechnianie wśród administratorów i podmiotów przetwarzających dane osobowe wiedzy o obowiązkach spoczywających na nich na mocy RODO.
3. Prowadzenie postępowań w sprawie stosowania RODO, w tym na podstawie informacji otrzymanych od innego organu nadzorczego lub innego organu publicznego.
4. Przyjmowanie standardowych klauzul umownych.
5. Ustanawianie i prowadzenie wykazów związanych z wymogiem dokonania oceny skutków dla ochrony danych.
6. Udzielanie zaleceń dotyczących operacji przetwarzania.
7. Zachęcanie do sporządzania kodeksów postępowania, wydawanie opinii na ich temat oraz zatwierdzanie tych kodeksów, w których znajdują się odpowiednie zabezpieczenia.
8. Zachęcanie do ustanawiania mechanizmów certyfikacji w dziedzinie ochrony danych oraz znaków jakości i oznaczeń z tej dziedziny, a także zatwierdzanie kryteriów certyfikacji.
9. Gdy ma to zastosowanie – dokonywanie okresowego przeglądu udzielonych certyfikacji.
10. Opracowywanie i publikowanie kryteriów akredytacji podmiotu monitorującego kodeksy postępowania oraz podmiotu certyfikującego.

---

[1] W rozdziale oparto się na projekcie ustawy z dnia 13 września 2017 r. Wszędzie w rozdziale, gdzie jest mowa o polskiej ustawie lub projekcie, autor ma na myśli wskazany projekt.

[2] Art. 78 i następne projektu ustawy.

11. Akredytowanie podmiotów monitorujących (czyli kontrolujących) kodeksy postępowania oraz podmiotów certyfikujących.
12. Wydawanie zezwoleń na klauzule umowne i przepisy.
13. Zatwierdzanie wiążących reguł korporacyjnych (art. 57 RODO).

RODO wskazuje ponadto, że Prezes Urzędu powinien ułatwiać wnoszenie skarg np. za pomocą takich środków, jak **gotowy formularz skargi**, który można wypełnić elektronicznie. Wnoszenie skarg jest uprawnieniem osób fizycznych, ale wpłynie to na przedsiębiorców (art. 57 ust. 2 RODO).

Przepisy RODO wskazują dodatkowo, że organ nadzorczy wypełnia zadania na rzecz osoby, której dane dotyczą, i – gdy ma to zastosowanie – inspektora ochrony danych **bezpłatnie** (art. 57 ust. 3 RODO).

RODO chroni również Urząd przed potencjalnym nadużyciem związanym ze składaniem wniosków w sposób oczywisty nieuzasadnionych lub nadmiernych, w szczególności ze względu na swą powtarzalność. W takich sytuacjach **organ nadzorczy może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych lub może odmówić podjęcia żądanych działań**.

Obowiązek wykazania, że żądanie jest w sposób oczywisty nieuzasadnione lub nadmierne, spoczywa na organie nadzorczym (art. 57 ust. 4 RODO).

4.2. UPRAWNIENIA

Prezesowi Urzędu RODO[3] przyznaje następujące typy uprawnień:

1) uprawnienia w zakresie prowadzonych postępowań;
2) uprawnienia naprawcze;
3) uprawnienia w zakresie wydawania zezwoleń;
4) uprawnienia doradcze.

Do uprawnień w zakresie **prowadzonych postępowań** należą:

a) nakazanie administratorowi i podmiotowi przetwarzającemu, a w stosownym przypadku przedstawicielowi administratora lub podmiotu przetwarzającego, dostarczenia wszelkich informacji potrzebnych organowi nadzorczemu do realizacji swoich zadań;
b) prowadzenie postępowań w formie audytów ochrony danych;
c) dokonywanie przeglądu udzielonych certyfikacji;
d) zawiadamianie administratora lub podmiotu przetwarzającego o podejrzeniu naruszenia niniejszego rozporządzenia;
e) uzyskiwanie od administratora i podmiotu przetwarzającego dostępu do wszelkich danych osobowych i wszelkich informacji niezbędnych organowi nadzorczemu do realizacji swoich zadań;
f) uzyskiwanie dostępu do wszystkich pomieszczeń administratora i podmiotu przetwarzającego, w tym do sprzętu i środków służących do przetwarzania danych, zgodnie z procedurami określonymi w prawie unijnym lub w prawie państwa członkowskiego.

Do uprawnień **naprawczych** będą należały:

a) wydawanie administratorowi lub podmiotowi przetwarzającemu ostrzeżeń dotyczących możliwości naruszenia przepisów niniejszego rozporządzenia poprzez planowane operacje przetwarzania;
b) udzielanie upomnień administratorowi lub podmiotowi przetwarzającemu w przypadku naruszenia przepisów niniejszego rozporządzenia przez operacje przetwarzania;
c) nakazanie administratorowi lub podmiotowi przetwarzającemu spełnienia żądania osoby, której dane dotyczą, wynikającego z praw przysługujących jej na mocy niniejszego rozporządzenia;
d) nakazanie administratorowi lub podmiotowi przetwarzającemu dostosowania operacji przetwarzania do przepisów niniejszego rozporządzenia, a w stosownych przypadkach wskazanie sposobu i terminu;

[3] Vide art. 57 RODO.

e) nakazanie administratorowi zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych;
f) wprowadzanie czasowego lub całkowitego ograniczenia przetwarzania, w tym zakazu przetwarzania;
g) nakazanie sprostowania lub usunięcia danych osobowych lub ograniczenia ich przetwarzania oraz nakazanie powiadomienia o tych czynnościach odbiorców, którym dane osobowe ujawniono;
h) cofnięcie certyfikacji lub nakazanie podmiotowi certyfikującemu cofnięcia udzielonej certyfikacji, lub nakazanie podmiotowi certyfikującemu nieudzielania certyfikacji, jeżeli jej wymogi nie są spełnione lub przestały być spełniane;
i) zastosowanie administracyjnej kary pieniężnej.

Do uprawnień w zakresie **wydawania zezwoleń** będą należały:
a) akredytowanie na mocy podmiotów certyfikujących;
b) udzielanie certyfikacji i zatwierdzanie kryteriów certyfikacji;
c) przyjmowanie standardowych klauzul ochrony danych;
d) zezwalanie na uzgodnienia administracyjne.

Do uprawnień **doradczych** będą należały:
a) udzielanie porad administratorowi zgodnie z procedurą uprzednich konsultacji;
b) wydawanie, z własnej inicjatywy lub na wniosek, opinii przeznaczonych dla parlamentu narodowego, rządu państwa członkowskiego lub – zgodnie z prawem państwa członkowskiego – innych instytucji i organów oraz ogółu społeczeństwa we wszelkich sprawach związanych z ochroną danych osobowych;
c) zezwalanie na przetwarzanie, jeżeli prawo państwa członkowskiego wymaga takiego uprzedniego zezwolenia;
d) opiniowanie i zatwierdzanie projektów kodeksów postępowania;
e) zezwalanie na klauzule umowne;
f) zatwierdzanie wiążących reguł korporacyjnych.

4.3. POSTĘPOWANIE KONTROLNE

Prezes Urzędu może prowadzić kontrole przestrzegania przepisów o ochronie danych osobowych. Będzie to jedno z najważniejszych jego zadań. Przepisy wskazują, że nie odbiega ono zasadniczo od postępowań kontrolnych prowadzonych przez GIODO. W nowej ustawie jest ono bardziej doprecyzowane, zaś niewątpliwie nowością będzie fakt, że będzie mogło być **niezapowiedziane**.

Postępowanie kontrolne będzie mogło być prowadzone zgodnie z zatwierdzonym przez Prezesa Urzędu planem kontroli bądź poza planem na podstawie uzyskanych przez Prezesa Urzędu informacji albo przeprowadzonych analiz. Jest to zbieżne z dotychczasową działalnością GIODO. Przykładowo przyjęty na 2017 r. plan kontroli sektorowych obejmował m. in. przychodnie i poradnie lekarskie oraz sklepy stosujące monitoring pozwalający na profilowanie klientów.

Kontrola może być przeprowadzona przez upoważnionego pracownika Urzędu, zwanego dalej **kontrolującym**. Jest to więc następca inspektora zatrudnionego obecnie w GIODO.

4.3.1. WYŁĄCZENIE KONTROLUJĄCEGO

Kontrolujący podlega wyłączeniu z postępowania kontrolnego na wniosek zainteresowanego, czyli kontrolowanego przedsiębiorcy, lub z urzędu, jeżeli wyniki kontroli mogłyby oddziaływać na jego prawa lub obowiązki, na prawa lub obowiązki jego małżonka albo osoby pozostającej z nim faktycznie we wspólnym pożyciu, krewnych i powinowatych do drugiego stopnia bądź osób związanych z nim z tytułu przysposobienia, opieki lub kurateli. Powody wyłączenia kontrolującego trwają także po ustaniu małżeństwa, przysposobienia, opieki lub kurateli. Kontrolujący może być wyłączony w każdym czasie, jeżeli zachodzą uzasadnione wątpliwości co do jego bezstronności (art. 67 projektu ustawy).

4.3.2. KONTROLA

Kontrolujący w przeprowadzaniu kontroli jest ograniczony **zakresem upoważnienia do przeprowadzenia kontroli**.

Upoważnienie do przeprowadzenia kontroli zawiera:

1) wskazanie podstawy prawnej przeprowadzenia kontroli;
2) oznaczenie organu kontroli;
3) imię i nazwisko, stanowisko służbowe osoby upoważnionej do przeprowadzenia kontroli oraz numer jej legitymacji służbowej, a w przypadku osób, o których mowa w art. 37 ust. 2, imiona i nazwiska tych osób oraz numer paszportu lub innego dokumentu potwierdzającego tożsamość;
4) określenie zakresu przedmiotowego kontroli, w tym okresu objętego kontrolą;
5) oznaczenie podmiotu objętego kontrolą, zwanego dalej **kontrolowanym**;
6) wskazanie daty rozpoczęcia i przewidywanego terminu zakończenia czynności kontrolnych;
7) podpis Prezesa Urzędu;
8) pouczenie podmiotu objętego kontrolą o jego prawach i obowiązkach;
9) datę i miejsce wystawienia imiennego upoważnienia.

Jeśli kontrolujący nie może okazać swojej legitymacji i upoważnienia ze względu na nieobecność kontrolowanego, to kontrolujący może okazać ją innemu pracownikowi kontrolowanego. Może także w tym wypadku okazać te dokumenty innej osobie[4] lub przywołanemu świadkowi, który powinien być funkcjonariuszem publicznym, a jednocześnie nie jest pracownikiem organu przeprowadzającego kontrolę.

W celu uzyskania informacji mogących stanowić dowód w sprawie naruszenia prawa przez administratora, kontrolujący ma prawo:

1) wstępu na grunt oraz do budynków, lokali lub innych pomieszczeń;
2) wglądu do wszelkich dokumentów i wszelkich informacji mających bezpośredni związek z przedmiotem kontroli;
3) przeprowadzania oględzin urządzeń, nośników oraz systemów informatycznych lub teleinformatycznych służących do przetwarzania danych;
4) żądać złożenia pisemnych lub ustnych wyjaśnień oraz wzywać i przesłuchiwać w charakterze świadka osoby w zakresie niezbędnym do ustalenia stanu faktycznego.

Kontrolowany przedsiębiorca zapewnia kontrolującemu oraz osobom upoważnionym do udziału w kontroli warunki i środki niezbędne do sprawnego przeprowadzenia kontroli, a w szczególności sporządza we własnym zakresie kopie lub wydruki dokumentów oraz informacji zgromadzonych na nośnikach, w urządzeniach lub w systemach informatycznych.

Kontrolowany dokonuje potwierdzenia za zgodność z oryginałem sporządzonych kopii lub wydruków. W przypadku odmowy potwierdzenia za zgodność z oryginałem potwierdza je kontrolujący, po czym czyni wzmiankę o odmowie potwierdzenia przez kontrolowanego w protokole kontroli.

W toku kontroli kontrolujący **może korzystać z pomocy funkcjonariuszy innych organów kontroli państwowej lub Policji**. Wykonują one czynności na polecenie kontrolującego. O taką pomoc kontrolujący wystąpi wtedy, kiedy kontrolowany intencjonalnie uniemożliwia przeprowadzenie kontroli np. przez ograniczenie dostępu do pomieszczeń.

W uzasadnionych przypadkach przebieg kontroli lub poszczególne czynności w jej toku, po uprzednim poinformowaniu kontrolowanego, mogą być utrwalane przy pomocy urządzeń rejestrujących obraz

[4] Projekt ustawy odwołuje się do art. 97 Kodeksu cywilnego, który wskazuje, że osobę czynną w lokalu przedsiębiorstwa przeznaczonym do obsługiwania publiczności poczytuje się w razie wątpliwości za umocowaną do dokonywania czynności prawnych, które zazwyczaj bywają dokonywane z osobami korzystającymi z usług tego przedsiębiorstwa. Przepis ten odnosi się do osób na kasie, portierni i innym stanowisku przeznaczonym do obsługi klientów przedsiębiorstwa, odbiorów przesyłek pocztowych itp.

lub dźwięk. Informatyczne nośniki danych w rozumieniu przepisów o informatyzacji działalności podmiotów realizujących zadania publiczne, na których zarejestrowano przebieg kontroli lub poszczególne czynności w jej toku, stanowią załącznik do protokołu z kontroli.

Kontrolujący może przesłuchać pracownika kontrolowanego w charakterze świadka. Przed rozpoczęciem przesłuchania kontrolujący obowiązany jest uprzedzić świadka o odpowiedzialności karnej za zeznanie nieprawdy lub zatajenie prawdy oraz informuje go o przysługujących mu uprawnieniach. Osoba może odmówić udzielenia informacji lub współdziałania w toku kontroli tylko wtedy, gdy naraziłoby to **ją lub jej małżonka, wstępnych, zstępnych, rodzeństwo oraz powinowatych w tej samej linii lub stopniu, jak również osoby pozostające w stosunku przysposobienia, opieki lub kurateli, a także osobę pozostającą we wspólnym pożyciu, na odpowiedzialność karną**. Prawo odmowy udzielenia informacji lub współdziałania w toku kontroli trwa po ustaniu małżeństwa lub rozwiązaniu stosunku przysposobienia, opieki lub kurateli.

4.3.3. PROTOKOŁY Z KONTROLI

Kontrolujący ustala stan faktyczny na podstawie dowodów zebranych w toku kontroli, a w szczególności **dokumentów, przedmiotów, oględzin oraz ustnych lub pisemnych wyjaśnień i oświadczeń.**

Przebieg przeprowadzonej kontroli kontrolujący przedstawia w protokole kontroli, który powinien zawierać:

1) wskazanie nazwy albo imienia i nazwiska oraz adresu kontrolowanego;
2) imię i nazwisko osoby reprezentującej podmiot kontrolowany oraz nazwę organu reprezentującego ten podmiot;
3) imię i nazwisko, stanowisko służbowe, numer legitymacji służbowej oraz numer upoważnienia kontrolującego, a w przypadku osób, o których mowa w art. 37 ust. 2 (kontrolerów z innych krajów UE), imię i nazwisko, numer paszportu albo innego dokumentu potwierdzającego tożsamość oraz numer upoważnienia;
4) datę rozpoczęcia i zakończenia czynności kontrolnych;
5) określenie przedmiotu i zakresu kontroli;
6) opis stanu faktycznego ustalonego w toku kontroli oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych;
7) wyszczególnienie załączników;
8) omówienie dokonanych w protokole poprawek, skreśleń i uzupełnień;
9) informację o pouczeniu kontrolowanego o prawie zgłaszania zastrzeżeń do protokołu oraz o prawie odmowy podpisania protokołu;
10) datę i miejsce podpisania protokołu przez kontrolującego i kontrolowanego.

Protokół kontroli podpisują kontrolujący i kontrolowany. Przed podpisaniem protokołu kontrolowany może, w terminie 7 dni od przedstawienia mu go do podpisu, złożyć na piśmie zastrzeżenia do tego protokołu. W razie zgłoszenia zastrzeżeń, kontrolujący dokonuje ich analizy i w razie potrzeby podejmuje dodatkowe czynności kontrolne, a w przypadku stwierdzenia zasadności zastrzeżeń, zmienia lub uzupełnia odpowiednią część protokołu w formie aneksu do protokołu. W razie nieuwzględnienia zastrzeżeń w całości lub w części kontrolujący informuje o tym kontrolowanego na piśmie. O odmowie podpisania protokołu kontrolujący czyni wzmiankę w protokole.

Protokół w postaci papierowej sporządza się w dwóch egzemplarzach, z których jeden pozostawia się kontrolowanemu, a w przypadku protokołu sporządzonego w postaci elektronicznej, doręcza się go kontrolowanemu.

Postępowanie kontrolne nie może trwać dłużej niż miesiąc od dnia podjęcia czynności kontrolnych.

4.3.4. WYNIKI KONTROLI

Na podstawie ustaleń kontroli kontrolujący może żądać wszczęcia postępowania dyscyplinarnego lub innego przewidzianego prawem postępowania[5] przeciwko osobom winnym uchybień i poinformowania kontrolującego, w określonym terminie, o wynikach tego postępowania i podjętych działaniach. W razie stwierdzenia, że działanie lub zaniechanie kierownika jednostki organizacyjnej, jej pracownika lub innej osoby fizycznej będącej administratorem danych lub podmiotem przetwarzającym, wyczerpuje znamiona przestępstwa określonego w ustawie, Prezes Urzędu kieruje do organu powołanego do ścigania przestępstw zawiadomienie o popełnieniu przestępstwa, dołączając dowody dokumentujące podejrzenie.

> Przykładem postępowania dyscyplinarnego będzie postępowanie związane z naruszeniem obowiązków pracowniczych. Zostało ono przewidziane w kodeksie pracy. Inne przewidziane prawem postępowanie dotyczy np. sytuacji, gdy przepisy RODO naruszył radca prawny. W tym przypadku kontrolujący będzie czekał na ustalenia rzecznika dyscyplinarnego lub Okręgowego Sądu Dyscyplinarnego Okręgowej Izby Radców Prawnych.

W szczególnych przypadkach Prezes Urzędu kieruje do Policji lub Prokuratury zawiadomienie o popełnieniu przestępstwa, dołączając dowody dokumentujące podejrzenie.

4.4. POSTĘPOWANIE W SPRAWIE NARUSZENIA PRZEPISÓW O OCHRONIE DANYCH OSOBOWYCH

Kolejnym zadaniem, jakie zostało postawione przed Prezesem UODO, jest prowadzenie postępowań w sprawie naruszenia przepisów o ochronie danych osobowych (art. 44 i następne projektu ustawy).

Postępowanie będzie postępowaniem **jednoinstancyjnym**. Oznacza to, że **od decyzji nie będzie przysługiwać odwołanie do organu wyższej instancji**, a wyłącznie **skarga** do Wojewódzkiego Sądu Administracyjnego.

W sytuacji gdy Prezes Urzędu uzna, że mogło dojść do naruszenia przepisów o ochronie danych osobowych, obowiązany jest do niezwłocznego wszczęcia postępowania. Do przekonania takiego może dojść w trakcie kontroli lub w wyniku skargi od podmiotu danych osobowych. Stroną będzie więc administrator danych, wobec którego istnieje podejrzenie, że naruszył dane osobowe. Różnicą w stosunku do odpowiedzialności cywilnej jest to, że w postępowaniu cywilnym podmiot danych osobowych np. klient sklepu samodzielnie może wnieść powództwo, natomiast w omawianym postępowaniu to Prezes Urzędu wszczyna postępowanie.

Organizacja społeczna (w szczególności NGO, które zajmują się ochroną danych osobowych) może występować z żądaniem:

1) wszczęcia postępowania,
2) dopuszczenia jej do udziału w postępowaniu, jeżeli jest to uzasadnione celami statutowymi tej organizacji i gdy przemawia za tym interes osoby, której prawa zostały naruszone.

W przypadku naruszenia przepisów o ochronie danych osobowych Prezes Urzędu, w drodze decyzji administracyjnej podejmuje rozstrzygnięcia zgodnie ze swoimi uprawnieniami, które zostały określone w art. 58 RODO.

---

[5] Inne przewidziane prawem postępowanie dotyczy np. sytuacji, gdy naruszenie RODO jednocześnie jest naruszeniem np. tajemnicy zawodowej. W takiej sytuacji kontrolujący ma prawo oczekiwać informacji, jak zakończyło się postępowanie w korporacji zawodowej (np. okręgowej izbie radców prawnych, gdy naruszycielem okazał się radca prawny).

4.4.1. TAJEMNICE PRZEDSIĘBIORSTWA

Ogólna zasada wyrażona w przepisach stanowi, że Prezes Urzędu ma prawo dostępu do wszelkich informacji, w tym danych osobowych, niezbędnych Prezesowi Urzędu do realizacji zadań. Wyjątek przewidziany przez ustawę wskazuje na **ograniczenie ze względu na tajemnice ustawowo chronione**, czyli np. tajemnicę adwokacką, dziennikarską, lekarską czy informację niejawną[6]. W takich przypadkach wykonywanie prawa dostępu do informacji jest możliwe na zasadach określonych w przepisach regulujących dostęp do tajemnic ustawowo chronionych[7].

Istotną **nowością** jest możliwość zastrzeżenia informacji, dokumentów lub ich części jako **tajemnicy przedsiębiorstwa**[8]. Rozwiązanie to jest wzorowane na art. 9 Prawa telekomunikacyjnego, gdy przedsiębiorca telekomunikacyjny mógł zastrzec przed Prezesem Urzędu Komunikacji Elektronicznej dokumenty lub ich części zawierające tajemnicę przedsiębiorstwa (art. 49 projektu ustawy).

Ponieważ każde prawo może być przedmiotem nadużycia, Prezes Urzędu może **uchylić** zastrzeżenie tajemnicy w drodze decyzji administracyjnej, jeżeli uzna, że informacje, dokumenty lub ich części nie spełniają przesłanek do objęcia ich tajemnicą przedsiębiorstwa. Jest to odrębna decyzja administracyjna, wobec czego również od niej przysługuje skarga do sądu administracyjnego.

Ponadto środkiem ograniczającym wgląd do dokumentów, czyli jawność dla podmiotów trzecich, jest możliwość wydania przez Prezesa Urzędu na wniosek zainteresowanego przedsiębiorcy lub z urzędu, czyli z własnej inicjatywy, postanowienia ograniczającego prawo do wglądu, jeżeli udostępnienie tego materiału groziłoby ujawnieniem tajemnicy przedsiębiorstwa lub innych tajemnic podlegających ochronie na podstawie odrębnych przepisów.

Dla skorzystania z tego prawa przedsiębiorca będzie zobowiązany złożyć **wniosek o ograniczenie prawa wglądu do materiału dowodowego.** Składa się go do Prezesa Urzędu wraz z uzasadnieniem oraz wersją dokumentu niezawierającą informacji objętych ograniczeniem ze stosowną adnotacją (art. 50 ust 2).

Przedsiębiorca składa do Prezesa materiał dowodowy wraz z wnioskiem o ograniczenie dostępu.

Jeśli złożony wniosek nie będzie spełniał wymagań określonych powyżej, Prezes Urzędu **wzywa** wnioskodawcę **do jego uzupełnienia w wyznaczonym terminie.** W przypadku nieprzedłożenia w wyznaczonym terminie uzupełnionej wersji dokumentu, wniosek pozostawia się bez rozpoznania (art. 50 ust 3).

---

[6] W szczególności tajemnice zawodowe zawarto np. w ustawie z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty (Dz.U.08.136.857 z późniejszymi zmianami), ustawie z dnia 26 stycznia 1984 r. Prawo prasowe (Dz. U. 84.5.24 z późniejszymi zmianami), ustawie z dnia 26 maja 1982 r. Prawo o adwokaturze (Dz.U.09.146.1188 z późniejszymi zmianami), itd. Przykładowy przepis regulujący tajemnice: Art. 6. 1. (prawa o adwokaturze) Adwokat obowiązany jest zachować w tajemnicy wszystko, o czym dowiedział się w związku z udzielaniem pomocy prawnej.

[7] Przykładem może być Prawo Prasowe: art. 15 ust. 2. Dziennikarz ma obowiązek zachowania w tajemnicy: danych umożliwiających identyfikację autora materiału prasowego, listu do redakcji lub innego materiału o tym charakterze, jak również innych osób udzielających informacji opublikowanych albo przekazanych do opublikowania, jeżeli osoby te zastrzegły nieujawnianie powyższych danych, Ustawa z dnia 26 stycznia 1984 r. Prawo prasowe, Ustawa z dnia 26 stycznia 1984 r.

[8] Zastrzeżenia dokonuje się, poza wszystkim, przez np. oznaczenie dokumentów jako posiadające walor tajemnicy przedsiębiorstwa. Są to więc np. dane obrazujące wielkość produkcji i sprzedaży, a także źródła zaopatrzenia i zbytu. Tajemnica przedsiębiorstwa została zdefiniowana w art. 11 pkt 4 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. 2003 r. Nr 153 poz. 1503, z późn. zm.). W związku z ustawą, aby informacja stanowiła tajemnicę przedsiębiorstwa, musi spełniać trzy warunki: 1. Posiadać charakter techniczny, technologiczny, organizacyjny przedsiębiorstwa lub posiadać wartość gospodarczą; 2. Nie została ujawniona do wiadomości publicznej; 3. Podjęto w stosunku do niej niezbędne działania w celu zachowania poufności.

4.4.2. NAKAZ OGRANICZENIA PRZETWARZANIA DANYCH OSOBOWYCH

W ramach postępowania w sprawie o naruszenie przepisów wyodrębniono możliwość wydania przez Prezesa UODO postanowienia nakazującego ograniczenie przetwarzania danych. Jest to swoiste postępowanie zabezpieczające. Nakaz zostanie wydany w sytuacji, gdy w toku postępowania zostanie uprawdopodobnione przez Prezesa UODO, że przetwarzanie danych osobowych przez przedsiębiorcę narusza przepisy o ochronie danych osobowych, a dalsze ich przetwarzanie może spowodować poważne i trudne do usunięcia skutki. Przedsiębiorca będzie musiał natychmiast zastosować się do takiego postanowienia.

Studium przypadku 1.
Administrator danych – przedsiębiorca świadczący usługi medyczne – wyjątkowo źle przetwarza dane osobowe w swoim przedsiębiorstwie. Na wysypiskach śmieci znajdywane są dane osobowe o stanie zdrowia klientów, a system internetowy jest niezabezpieczony. W tej sytuacji w trakcie postępowania w sprawie naruszenia przepisów Prezes Urzędu postanowieniem nakazuje wstrzymanie przetwarzania danych do czasu wydania decyzji.

4.4.3. NASTĘPSTWA POSTĘPOWANIA

Jeżeli postępowanie kończy się pozytywnie dla przedsiębiorcy, tj. kontrolujący nie stwierdzi naruszenia przepisów przez administratora, Prezes UODO umarza sprawę, jeżeli toczy się ona przed tym urzędem. Oznacza to, że sprawa jest zakończona i żadne konsekwencje przedsiębiorcy nie grożą.

W przypadku gdy waga naruszenia przepisów o ochronie danych osobowych jest znikoma, a strona zaprzestała naruszenia, Prezes UODO może w drodze decyzji administracyjnej udzielić upomnienia. Jest to środek bardziej o charakterze wychowawczym niż *stricte* karnym.

W przypadku naruszenia przepisów o ochronie danych osobowych Prezes Urzędu, w drodze decyzji podejmuje rozstrzygnięcia:

1) uwzględnienie żądań zawartych w skardze osoby, której dane dotyczą;
2) dostosowanie operacji przetwarzania danych osobowych do przepisów rozporządzenia 2016/679, ze wskazaniem, jeżeli to jest właściwe, sposobu i terminu dostosowania;
3) zawiadomienie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych;
4) wprowadzenie czasowego lub całkowitego ograniczenia przetwarzania danych osobowych lub zakazu przetwarzania;
5) sprostowanie lub usunięcie danych osobowych;
6) powiadomienie odbiorców, którym dane osobowe zostały ujawnione, o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych;
7) zawieszenie przepływu danych do odbiorców w państwie trzecim lub do organizacji międzynarodowej.

Niezależnie od powyższych rozstrzygnięć, w drodze decyzji Prezes Urzędu może **nałożyć administracyjną karę pieniężną.** Nakładanie administracyjnych kar pieniężnych zostało opisane w dalszej części niniejszego rozdziału.

Dla zwiększenia skuteczności decyzji wskazano, że **podlegają one natychmiastowemu wykonaniu**. Wniesienie przez stronę skargi do sądu administracyjnego powoduje wstrzymanie wykonania decyzji **jedynie w zakresie dotyczącym administracyjnej kary pieniężnej**. Oznacza to, że pozostałe elementy, czyli np. powiadomienie odbiorców o ograniczeniu przetwarzania danych, pomimo skargi podlegają natychmiastowemu wykonaniu.

4.5. ADMINISTRACYJNE KARY PIENIĘŻNE

Prezes UODO, w drodze decyzji, **może nałożyć na podmioty niebędące organami publicznymi administracyjne kary pieniężne** na podstawie i na warunkach określonych w RODO (art. 58 ust. 2 lit. i). To RODO zatem decyduje o ogólnych warunkach i wysokości kar pieniężnych.

1. Prezes Urzędu zapewni, aby nakładane kary **były w każdym indywidualnym przypadku skuteczne, proporcjonalne i odstraszające.**
2. Administracyjne kary pieniężne nakłada się zależnie od okoliczności każdego indywidualnego przypadku. **Decydując, czy nałożyć administracyjną karę pieniężną oraz ustalając jej wysokość, zwraca się w każdym indywidualnym przypadku należytą uwagę na:**
   a) charakter, wagę i czas trwania naruszenia przy uwzględnieniu charakteru, zakresu lub celu danego przetwarzania, liczby poszkodowanych osób, których dane dotyczą, oraz rozmiaru poniesionej przez nie szkody;
   b) umyślny lub nieumyślny charakter naruszenia;
   c) działania podjęte przez administratora lub podmiot przetwarzający w celu zminimalizowania szkody poniesionej przez osoby, których dane dotyczą;
   d) stopień odpowiedzialności administratora lub podmiotu przetwarzającego z uwzględnieniem środków technicznych i organizacyjnych wdrożonych przez nich (…);
   e) wszelkie stosowne wcześniejsze naruszenia ze strony administratora lub podmiotu przetwarzającego;
   f) stopień współpracy z organem nadzorczym w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych negatywnych skutków;
   g) kategorie danych osobowych, których dotyczyło naruszenie;
   h) sposób, w jaki organ nadzorczy dowiedział się o naruszeniu, w szczególności, czy i w jakim zakresie administrator lub podmiot przetwarzający zgłosili naruszenie;
   i) jeżeli wobec administratora lub podmiotu przetwarzającego, których sprawa dotyczy, zostały wcześniej zastosowane w tej samej sprawie środki, (…) – przestrzeganie tych środków;
   j) stosowanie zatwierdzonych kodeksów postępowania (…) lub zatwierdzonych mechanizmów certyfikacji (…) oraz
   k) wszelkie inne obciążające lub łagodzące czynniki mające zastosowanie do okoliczności sprawy, takie jak osiągnięte bezpośrednio lub pośrednio w związku z naruszeniem korzyści finansowe lub uniknięte straty.

W art. 83 ust. 3 RODO wskazuje, że jeżeli administrator lub podmiot przetwarzający **narusza umyślnie lub nieumyślnie w ramach tych samych lub powiązanych operacji przetwarzania kilka przepisów niniejszego rozporządzenia**, całkowita wysokość administracyjnej kary pieniężnej nie przekracza wysokości kary za najpoważniejsze naruszenie.

Naruszenia przez administratora lub podmiot przetwarzający obowiązków wynikających z RODO[9] podlegają administracyjnej karze pieniężnej w wysokości do 10 000 000 EUR, a w przypadku przedsiębiorstwa – w wysokości do 2% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa, czyli Prezes Urzędu obowiązany jest do wybrania kwoty wyższej.

[9] RODO wskazuje na następujące obowiązki: warunki wyrażenia zgody przez dziecko w przypadku usług społeczeństwa informacyjnego (art. 8), przetwarzanie niewymagające identyfikacji, uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych. Ponadto dotyczy współadministratorów, przedstawicieli administratorów lub podmiotów przetwarzających niemających jednostki organizacyjnej w Unii, podmiotów przetwarzających, przetwarzanie z upoważnienia administratora lub podmiotu przetwarzającego, rejestrowanie czynności przetwarzania, współpraca z organem nadzorczym, dot. bezpieczeństwa danych osobowych, w zakresie oceny skutków dla ochrony danych i uprzednich konsultacji, (vide art. 25 –39 oraz przepisy dot. certyfikacji oraz podmiotu certyfikującego 42 i 43 RODO.

W art. 83 ust. 5 RODO jest mowa o najpoważniejszych rodzajach naruszeń, za które przewidziano najwyższy rodzaj kary w wysokości do 20 000 000 EUR, a w przypadku przedsiębiorstwa – w wysokości do 4% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa, czyli mniej korzystna dla przedsiębiorcy. Do tych przewinień należy:

a) nieprzestrzeganie podstawowych zasad przetwarzania, w tym warunków zgody;
b) nieprzestrzeganie praw osób, których dane dotyczą;
c) nieprzestrzeganie regulacji związanych z przekazywaniem danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej;
d) nieprzestrzeganie nakazu tymczasowego lub ostatecznego ograniczenia przetwarzania lub zawieszenia przepływu danych orzeczonego przez organ nadzorczy lub niezapewnienie dostępu skutkującego naruszeniem.

Równowartość wyrażonych w euro kwot, o których mowa powyżej, oblicza się w złotych według średniego kursu euro ogłoszonego przez Narodowy Bank Polski w tabeli kursów na dzień 28 stycznia każdego roku, a w przypadku, gdy w danym roku Narodowy Bank Polski nie ogłasza średniego kursu euro w dniu 28 stycznia – według średniego kursu euro ogłoszonego w najbliższej po tej dacie tabeli kursów Narodowego Banku Polskiego.

Karę pieniężną uiszcza się w terminie 14 dni od dnia upływu terminu na wniesienie skargi do sądu administracyjnego albo od dnia uprawomocnienia się orzeczenia sądu administracyjnego. W razie upływu terminu **kara pieniężna podlega ściągnięciu w trybie przepisów o postępowaniu egzekucyjnym w administracji** (art. 85 Projektu ustawy)[10].

Prezes Urzędu może na wniosek podmiotu ukaranego odroczyć uiszczenie kary pieniężnej albo rozłożyć ją **na raty** ze względu na ważny interes wnioskodawcy. Do wniosku o odroczenie albo rozłożenie na raty kary pieniężnej dołącza się uzasadnienie. W przypadku odroczenia uiszczenia kary pieniężnej albo rozłożenia jej na raty, Prezes Urzędu nalicza od nieuiszczonej kwoty odsetki w stosunku rocznym, których wysokość wynosi 50% stawki odsetek za zwłokę, ogłaszanej na podstawie art. 56 § 3 ustawy z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa (Dz. U. z 2012 r. poz. 749, z późn. zm.), od dnia następującego po dniu złożenia wniosku.

W przypadku rozłożenia na raty kary pieniężnej, odsetki, o których mowa w art. 87 ust. 3 Projektu Ustawy, są naliczane odrębnie dla każdej raty. Odsetki są naliczane za okres od dnia upływu odroczonego terminu płatności kary pieniężnej albo terminu zapłaty poszczególnych rat.

Prezes Urzędu może uchylić odroczenie uiszczenia kary pieniężnej albo rozłożenie jej na raty, jeżeli ujawniły się nowe lub uprzednio nieznane okoliczności istotne dla rozstrzygnięcia lub jeżeli rata nie została uiszczona w terminie.

Rozstrzygnięcie Prezesa Urzędu w przedmiocie odroczenia uiszczenia kary pieniężnej albo rozłożenia jej na raty następuje w drodze postanowienia, na które nie przysługuje skarga do sądu administracyjnego.

Przepisów art. 189f (art. 189f § 1: Organ administracji publicznej, w drodze decyzji, odstępuje od nałożenia administracyjnej kary pieniężnej i poprzestaje na pouczeniu) i art.189k (art. 189k § 1: Organ administracji publicznej, który nałożył administracyjną karę pieniężną, na wniosek strony, w przypadkach uzasadnionych ważnym interesem publicznym lub ważnym interesem strony, może udzielić ulg w wykonaniu administracyjnej kary pieniężnej) Kodeksu postępowania administracyjnego **nie stosuje się**.

4.6. ODPOWIEDZIALNOŚĆ CYWILNA

Autorzy polskiej ustawy przewidują nowy rodzaj postępowania sądowego, który jest zbliżony do naruszenia dóbr osobistych. Sprawy cywilne będą rozstrzygane przez sądy okręgowe. Dlatego więc niezależnie od prawa do żądania wszczęcia postępowania przez organ nadzorczy, każda osoba, której prawa przysługujące

[10] Ustawa z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji. Dz.U. 1966 nr 24 poz. 151.

na mocy przepisów o ochronie danych osobowych zostały naruszone, może żądać, ażeby ten, kto dopuścił się naruszenia, dopełnił czynności potrzebnych do **usunięcia jego skutków**.

Studium przypadku 2.
Podmiot danych może żądać usunięcia danych, które mogą naruszać dobra osobiste. Podmiot danych może żądać usunięcia danych osobowych z baz danych administratora.

Wystąpienie z powyższym roszczeniem nie wyłącza możliwości wystąpienia z innymi roszczeniami z tytułu naruszenia przepisów o ochronie danych osobowych np. **roszczeniem odszkodowawczym**.

Sprawy dotyczące roszczeń z tytułu naruszenia ochrony danych osobowych rozstrzygane są przez sąd okręgowy w trybie postępowania cywilnego. Zanim wytoczone zostanie powództwo, sąd w przeciągu 3 dni rozpoznaje wniosek osoby, która dochodzi swoich praw z tytułu naruszenia ochrony danych osobowych.

Dotyczy on spraw:

1) o zabezpieczenie dowodów oraz o zabezpieczenie związanych z nimi roszczeń;
2) o zobowiązanie naruszającego prawa przysługujące na mocy przepisów o ochronie danych osobowych do udzielenia informacji i udostępnienia określonej przez sąd dokumentacji mającej znaczenie dla roszczeń;
3) o zobowiązanie innej niż naruszający osoby do udzielenia informacji, które mają znaczenie dla roszczeń.

Sąd, dopuszczając dowód lub rozpoznając wnioski, zapewnia zachowanie tajemnicy przedsiębiorcy i innych tajemnic ustawowo chronionych.

Od powyższych obowiązków może uchylić się ten, kto według przepisów Kodeksu postępowania cywilnego mógłby jako świadek odmówić zeznań lub odpowiedzi na zadane mu pytanie (a więc małżonkowie stron, ich wstępni, zstępni i rodzeństwo oraz powinowaci w tej samej linii lub stopniu, jak również osób pozostających ze stronami w stosunku przysposobienia). W uzasadnionych przypadkach sąd może uzależnić wydanie postanowienia o zabezpieczeniu dowodów od złożenia kaucji. Zażalenia na postanowienia sądu w sprawach sąd rozpoznaje w terminie 7 dni.

4.7. PRZEPISY KARNE

Prawodawca europejski oraz polski jednomyślnie uważają, że przepisy i odpowiedzialność karna powinna być ograniczona do minimum. Dlatego w projekcie nowej ustawy wskazano dwa czyny zabronione.

Pierwsze z nich to **wykroczenie**[11], które polega na udaremnieniu lub utrudnianiu kontrolującemu prowadzenia kontroli przestrzegania przepisów o ochronie danych osobowych i które podlega **grzywnie.** To przypadek, kiedy przedsiębiorca np. nie wpuszcza kontrolującego do pomieszczeń, w których przetrzymuje katalogi swoich klientów.

Przestępstwem orzekanym w trybie kodeksu postępowania karnego, które jest zagrożone grzywną, ograniczeniem wolności albo pozbawieniem wolności do roku jest czyn polegający na przetwarzaniu bez podstawy prawnej szczególnych kategorii danych osobowych.

4.8. AKREDYTACJA I CERTYFIKACJA

Jak wspomniano na początku tego rozdziału, do zadań Prezesa UODO należy również certyfikacja podmiotów prywatnych.

[11] Oznacza to, że orzekanie w sprawach następuje w trybie przepisów ustawy z dnia 24 sierpnia 2001 r. – Kodeks postępowania w sprawach o wykroczenia.

Uwaga: Prezes Urzędu prowadzi publicznie dostępny wykaz administratorów i podmiotów przetwarzających, którym udzielono certyfikacji.

Certyfikowane podmioty będą udzielały innym podmiotom, a zwłaszcza przedsiębiorcom, akredytacji.

Akredytacja będzie poświadczać bezpieczeństwo danych klienta u przedsiębiorcy, co z pewnością będzie stanowiło duży atut. Zwiększenie zaufania do administratora danych pozwoli na wzrost zainteresowania świadczonymi usługami.

Uzyskanie certyfikatu lub akredytacji będzie przyznawało uprawnienie do posługiwania się znakiem jakości i oznaczeń graficznych w zakresie ochrony danych osobowych, mających świadczyć o zgodności z RODO operacji przetwarzania prowadzonych przez administratorów i podmioty przetwarzające.

Studium przypadku 3.
Tak jak na towarach znajdują się oznaczenia np. wolny od glutenu czy *fair trade,* tak na stronach internetowych, recepcji itp. przedsiębiorca będzie mógł używać oznaczeń graficznych, które będą informowały, że w odpowiedni i sprawdzony sposób chroni on dane osobowe swoich klientów.

Uwagi
Prezes Urzędu udziela certyfikatu przedsiębiorcy, który odpłatnie nadaje akredytacje innym przedsiębiorcom. Jest to więc instytucja zbliżona do przyznawania standardu certyfikacji ISO.

Uzyskanie takiego certyfikatu/akredytacji będzie całkowicie dobrowolne.

Certyfikacja nie wpływa na spoczywający na administratorze lub podmiocie przetwarzającym obowiązek przestrzegania RODO i pozostaje bez uszczerbku dla zadań i uprawnień organów nadzorczych.

5. CHMUROWE PRZETWARZANIE DANYCH OSOBOWYCH W ŚWIETLE RODO

Wojciech Dziomdziora

5.1. CHARAKTERYSTYKA USŁUG CHMUROWYCH

Korzystanie z informatycznych rozwiązań chmurowych jest powszechne. Dotyka ono niemal całej aktywności w sieci zarówno prywatnej, jak i w coraz większym zakresie zawodowej. Dzięki rozwiązaniom chmurowym można korzystać z poczty elektronicznej, serwisów społecznościowych, aplikacji biurowych oraz wielu innych usług, zaczynając od usług bankowych, zaś na rozrywkowych kończąc. Często nawet nie uświadamiamy sobie, że narzędzie, które wykorzystujemy to „chmura".

Pisząc o prawnych aspektach przetwarzania danych osobowych w chmurze, nie da się niestety uniknąć choćby podstawowych określeń technicznych.

Przetwarzanie w chmurze można zasadniczo opisać jako szczególny rodzaj outsourcingu usług IT. Celem usług chmurowych jest zapewnienie zasobów informatycznych, czyli zarówno oprogramowania, jak i sprzętu na żądanie użytkowników. Przetwarzanie danych jest realizowane poza strukturami przedsiębiorcy korzystającego z usług chmurowych.

Warto wskazać kilka cech charakterystycznych dla rozwiązań chmurowych[1], istotnych dla dalszych rozważań:

1. Rozwiązania chmurowe znacznie ograniczają początkowe inwestycje kapitałowe, gdyż użytkownik potrzebuje jedynie sprzętu zdolnego do komunikacji z Internetem spełniającego oczywiście odpowiednie wymogi obliczeniowe, jednakże zazwyczaj niezbyt wyśrubowane.
2. Opłaty po stronie użytkowników mają najczęściej charakter wydatków operacyjnych, przy czym bardzo często model płatności jest oparty na tym, że użytkownicy płacą tylko za to, z czego faktycznie korzystają.
3. Usługi chmurowe wykazują zazwyczaj daleko idącą skalowalność, co pozwala użytkownikom na dużą elastyczność w prowadzonej działalności.
4. Dostawcy usług chmurowych często przenoszą dane i aplikacje użytkowników (np. między różnymi komputerami lub między różnymi centrami przetwarzania danych) w celu optymalnego wykorzystania własnej infrastruktury oraz zachowania wysokiej jakości świadczonych usług. W konsekwencji użytkownik nie musi znać dokładnej lokalizacji danych lub procesów ani wiedzieć, który sprzęt w danym momencie faktycznie obsługuje tego użytkownika.
5. Korzystanie z usług chmurowych pozwala na dostęp do danych i aplikacji kiedykolwiek i gdziekolwiek jest to potrzebne oraz za pomocą wielu urządzeń – komputerów, tabletów, smartfonów i innych.

5.2. RODZAJE CHMUR PUBLICZNYCH

Istnieje kilka rodzajów chmur obliczeniowych: prywatna, publiczna, hybrydowa oraz wspólna.

Usługi **chmury publicznej** co do zasady są dostępne dla każdego. Najczęściej są one dostarczane w całości przez jednego dostawcę. Z racji powszechności i często daleko idącej standaryzacji, taka chmura charakteryzuje się wysoką dostępnością zarówno pod kątem stawianych wymogów technicznych dla sprzętu korzystającego, jak i z uwagi na koszty. Zasadniczo użytkownicy nie mają (lub mają daleko ograniczoną)

[1] Zawarta w tym rozdziale charakterystyka chmury obliczeniowej powstała w oparciu o Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Wykorzystanie potencjału chmury obliczeniowej w Europie"; Bruksela, dnia 27.9.2012 r.; COM(2012) 529 final; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:PL:PDF; (odczyt w dniu 27.03.2017 r.)

kontroli nad lokalizacją infrastruktury czy naturą dostarczanych im procesów informatycznych. Wydaje się, że taki rodzaj chmury obliczeniowej jest najbardziej rozpowszechniony wśród małych i średnich przedsiębiorców, głównie z uwagi na koszty oraz prostotę użytkowania, a także rosnące zaufanie do tego rodzaju usług.

Kolejnym rodzajem jest **chmura prywatna**, zwana także wewnętrzną. To infrastruktura teleinformatyczna zbudowana na potrzeby jednego podmiotu. Wymaga ona znacznych nakładów inwestycyjnych oraz ponoszenia kosztów związanych z utrzymaniem i rozwojem. Z uwagi na koszty jest ona najczęściej wybierana przez duże podmioty prowadzące rozproszoną działalność, czyli np. korporacje międzynarodowe, którym zależy na podwyższonym bezpieczeństwie przetwarzania danych. Powyższe rozwiązanie daje bowiem większą kontrolę zarówno w odniesieniu do dostępu, lokalizacji, jak sposobów zabezpieczeń danych.

Chmura hybrydowa łączy systemy chmury publicznej i prywatnej. W chmurze hybrydowej dane są zarządzane i przetwarzane zarówno wewnętrznie, jak i przez dostawców zewnętrznych. Pozwala to na korzystanie z wysokowydajnych i ekonomicznie efektywnych usług chmury publicznej przy jednoczesnym przetwarzaniu danych szczególnie dla użytkownika wrażliwych na własnej infrastrukturze.

Czasem wyróżnia się również **chmurę wspólną**, tj. taką, która ma wszystkie cechy chmury prywatnej, jednakże służy grupie podmiotów prowadzących podobną działalność i dlatego mających podobne wymagania techniczne, w szczególności co do bezpieczeństwa przetwarzania danych. Taka chmura może służyć przykładowo grupie banków, podmiotów leczniczych czy administracji publicznej. Pozwala ona na osiągnięcie specyficznych dla danej branży celów biznesowych przy jednoczesnym obniżeniu kosztów.

Warto wskazać podstawowe modele, w jakich są świadczone usługi chmurowe. Należą do nich:

1. Infrastruktura jako usługa (ang. Infrastructure as a Service – IaaS);
2. Platforma jako usługa (ang. Platform as a Service – PaaS);
3. Oprogramowanie jako usługa (ang. Software as a Service – SaaS).

W modelu IaaS usługodawca udostępnia, obsługuje i serwisuje wyłącznie infrastrukturę teleinformatyczną, w szczególności serwery, dyski twarde, łącza telekomunikacyjne. Kwestie związane z oprogramowaniem, bazami danych i systemami operacyjnymi pozostają po stronie usługobiorcy.

W modelu PaaS dostawca dostarcza to, co w modelu IaaS oraz dodatkowo zapewnia platformę informatyczną, na którą składa się przykładowo system operacyjny lub zestaw narzędzi informatycznych, umożliwiającą uruchamianie lub tworzenie zewnętrznego, w tym własnego oprogramowania.

Najdalej idący model przetwarzania w chmurze (SaaS) zakłada świadczenie usług w zakresie udostępniania infrastruktury, systemu operacyjnego oraz gotowych aplikacji.

5.3. WYMAGANIA RODO

Jedną z podstawowych zasad ustanowionych w RODO jest zasada odpowiedzialności administratora danych za przestrzeganie przepisów RODO. Jest on obowiązany do podejmowania odpowiednich działań w celu zapewnienia bezpieczeństwa danych osobowych. Realizacja tego obowiązku spoczywa na administratorze bez względu na środki użyte do przetwarzania danych osobowych, a więc także w przypadku, kiedy wykorzystuje on usługi chmurowe. Jednakże RODO stawia szczególne wyzwania dla korzystania z chmury obliczeniowej.

RODO wymaga, aby zarówno administrator danych osobowych, jak i podmiot przetwarzający dane, a także dalsi przetwarzający, znali miejsce przetwarzania danych. Związane jest to z zagadnieniami jurysdykcji oraz właściwej ochrony prawnej danych. Wydaje się zatem, że wystarczy, aby administrator, powierzając dane podmiotowi przetwarzającemu, tj. dostawcy usług chmurowych, wymagał od niego podania informacji o krajach, na terytorium których będą przetwarzane dane. Jest to istotne z tego powodu, że RODO ogranicza możliwość przekazywania danych do państw trzecich, poza EOG (Europejski Obszar Gospodarczy – tj. państwa członkowskie UE, Norwegia, Islandia i Lichtenstein). Tymczasem przy świadczeniu usług chmurowych

bardzo często zdarza się, że używane są serwery rozsiane po całym świecie lub serwery czy inne urządzenia zlokalizowane są co prawda w Europie, ale zarządzane są zdalnie przez podmioty spoza UE. W takich przypadkach przekazywanie danych musi być zgodne z przepisami RODO.

RODO wymaga, aby zarówno administrator danych osobowych, jak i podmiot przetwarzający dane, szacowali ryzyko właściwe do przetwarzania danych oraz wdrażali minimalizujące je środki. Powinny one zapewnić odpowiedni poziom bezpieczeństwa, uwzględniać stan wiedzy technicznej oraz koszty ich wdrożenia w stosunku do ryzyka i charakteru danych osobowych podlegających ochronie. Dane osobowe muszą być chronione przed ich przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, zmodyfikowaniem, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem do danych osobowych. Co prawda, jak wyżej powiedziono, obowiązek stosowania właściwych środków ochrony spoczywa zarówno na administratorze, jak i na podmiocie przetwarzającym, to administrator powinien dokonać analizy, czy podmiot przetwarzający dane, z którego usług zamierza skorzystać, daje rękojmie stosowania odpowiednich zabezpieczeń. RODO w motywie 81 mówi, że „administrator powinien, powierzając podmiotowi przetwarzającemu czynności przetwarzania, korzystać z usług wyłącznie podmiotów przetwarzających, które zapewniają wystarczające gwarancje – w szczególności jeżeli chodzi o wiedzę fachową, wiarygodność i zasoby – wdrożenia środków technicznych i organizacyjnych odpowiadających wymogom niniejszego rozporządzenia, w tym wymogom bezpieczeństwa przetwarzania". Treść ta zasadniczo jest następnie powtórzona w art. 28 ust.1 RODO.

Wspomniana analiza powinna być oparta na informacjach przekazywanych przez podmiot przetwarzający dane. Warto przykładowo poszukać odpowiedzi na następujące pytania:

1) czy podmiot przetwarzający dane, z którego usług chmurowych zamierzam skorzystać, stosuje zatwierdzony kodeks postępowania lub zatwierdzony mechanizm certyfikacji?;
2) czy podmiot ten stosuje międzynarodowe normy, np. normę ISO/IEC 27001, standaryzującą systemy zarządzania bezpieczeństwem informacji?;
3) czy z usług chmurowych tego podmiotu korzystają jednostki sektora publicznego lub uznane podmioty gospodarcze, czyli jaka jest jego lista referencji?;
4) czy podmiot ten ma odpowiednią rynkową renomę?;
5) czy na gruncie kontraktowym podmiot ten zobowiązuje się do pokrycia części lub całości szkód, jakie zostaną wywołane wskutek naruszenia przepisów o ochronie danych osobowych?

Trzeba wyraźnie podkreślić, że nie ma systemów w 100% pewnych i takich, które nie mogą ulec awarii lub zorganizowanemu cyberatakowi. Jednakże korzystanie z renomowanych, sprawdzonych usługodawców znacznie zwiększa pewność dobrego zabezpieczenia danych i tym samym przestrzegania prawa.

Powierzenie przetwarzania danych, co jest warunkiem koniecznym skorzystania z usług chmurowych dla przetwarzania danych, wymaga zawarcia umowy pomiędzy administratorem danych a podmiotem przetwarzającym. Na mocy postanowień art. 28 ust. 3 RODO umowa ta musi regulować co najmniej następujące kwestie:

1) przedmiot i czas trwania przetwarzania danych osobowych;
2) charakter i cel przetwarzania;
3) rodzaj danych osobowych;
4) kategorie osób, których dane dotyczą;
5) obowiązki i prawa administratora.

Ponadto w umowie podmiot przetwarzający musi zobowiązać się do:

1) przetwarzania danych osobowych wyłącznie na udokumentowane polecenie administratora – co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej – chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający; w takim przypadku przed rozpoczęciem przetwarzania podmiot przetwarzający informuje administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny;

2) zapewnienia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
3) podjęcia wszelkich środków wymaganych na mocy art. 32 RODO;
4) przestrzegania warunków korzystania z usług innego podmiotu przetwarzającego;
5) biorąc pod uwagę charakter przetwarzania, w miarę możliwości do pomagania administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w RODO, takich jak prawo do dostępu do własnych danych, żądania sprostowania i usuwania danych, ograniczenia przetwarzania danych, przenoszenia danych, prawa do sprzeciwu wobec zautomatyzowanego przetwarzania danych, w tym profilowania (prawa te szczegółowo określone zostały w rozdziale III RODO);
6) uwzględniając charakter przetwarzania oraz dostępne mu informacje, do pomagania administratorowi wywiązywania się z obowiązków:
   a) wdrożenia odpowiednich środków technicznych i organizacyjnych, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku (obowiązek szczegółowo określony w art. 32 RODO);
   b) zgłoszenia organowi nadzorczemu przypadku naruszenia ochrony danych osobowych (obowiązek szczegółowo określony w art. 33 RODO);
   c) zawiadomienia osoby, której dane stały się przedmiotem naruszenia ochrony danych osobowych mogącego powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych (obowiązek szczegółowo określony w art. 34 RODO);
   d) dokonania oceny skutków planowanych operacji przetwarzania dla ochronny danych osobowych (obowiązek szczegółowo określony w art. 35 RODO);
   e) przeprowadzenia ewentualnych konsultacji z organem nadzorczym w sprawie przetwarzania danych (obowiązek szczegółowo określony w art. 36 RODO);
7) po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usuwania lub zwracania mu wszelkich danych osobowych oraz usuwania wszelkich ich istniejących kopii, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych;
8) udostępniania administratorowi wszelkich informacji niezbędnych do wykazania spełnienia obowiązków określonych powyżej oraz umożliwiania administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzania audytów, w tym inspekcji, i przyczyniania się do nich.

Należy również pamiętać, że w przypadku typowych usług chmurowych podmiot świadczący tego rodzaju usługi zazwyczaj korzysta z podwykonawców. A zatem w takiej sytuacji dochodzi do dalszego powierzenia przetwarzania danych. Zgodnie z art. 28 ust. 2 RODO podmiot przetwarzający morze korzystać z usług innego podmiotu przetwarzającego jedynie za uprzednią szczegółową lub ogólną pisemną zgodą administratora. W przypadku ogólnej pisemnej zgody podmiot przetwarzający ma obowiązek poinformować administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian. Wspomniana wcześniej zgoda w praktyce obrotu wyrażana jest najczęściej w umowie zawieranej między administratorem a podmiotem przetwarzającym. „Dalszy" podmiot przetwarzający jest obowiązany do wypełniania tych samych obowiązków, które wypełnia podstawowy podmiot przetwarzający.

Warto zwrócić uwagę, że zarówno Komisja Europejska i krajowy organ nadzorczy będą mogły określić tzw. standardowe klauzule umowne dotyczące kwestii, o których była wyżej mowa. Należy przypuszczać, że klauzule takie zostaną przyjęte, tym bardziej, że obowiązywały także przed wejściem w życie RODO. W praktyce renomowane podmioty oferujące usługi chmurowe i przetwarzające dane obecnie chętnie posługują się, a zapewne tak samo będzie również pod reżimem RODO, standardowymi klauzulami umownymi. Stosowanie tych klauzul zapewnia bowiem zgodność z przepisami o ochronie danych osobowych.

5.4. PODSUMOWANIE

RODO pozwala na przetwarzanie danych osobowych w chmurze publicznej. Wiąże się to z koniecznością dokonania wyboru dostawcy. Dostawca ten musi być podmiotem wiarygodnym, zapewniającym przestrzeganie przepisów RODO oraz posiadającym odpowiednią renomę. Konieczne jest również zawarcie umowy o powierzeniu przetwarzania danych. Umowa musi zawierać co najmniej postanowienia wskazane w RODO. Zawierając umowę, można opierać się na standardowych klauzulach umownych, jeżeli zostaną one określone przez Komisję Europejską lub krajowy organ nadzorczy.

6. ZABEZPIECZANIE I ANALIZOWANIE RYZYK PRZETWARZANIA DANYCH OSOBOWYCH

Sylwia Stefaniak, Halszka Suszek-Borowska, Olga Budziszewska

Jesteśmy świadkami czwartej rewolucji technologicznej, która wpływa na wiele aspektów naszego życia. Z jednej strony wiemy, że przynosi nam wiele korzyści, ale z drugiej strony coraz więcej osób wyraża swoje wątpliwości co do swojego bezpieczeństwa czy ochrony tożsamości w sieci. Jeśli zatem zdajemy sobie sprawę z zalet nowych technologii, ważne jest również, aby mieć pełny obraz tego, co te technologie ze sobą niosą. Musimy sobie zawsze postawić pytanie, co ja mogę zrobić, żeby móc wpłynąć na swoje bezpieczeństwo i bezpieczeństwo moich danych, które przechowuję w Internecie? Oprócz zabezpieczeń technicznych, określonych zachowań oraz zdrowego rozsądku, pojawiają się także nowe przepisy chroniące prawa osób prywatnych. Takie właśnie zadanie ma RODO, które wymaga od nas myślenia o przetwarzaniu danych osobowych jako procesie.

Wdrożenie RODO obejmuje szeregów procesów – od inwentaryzacji danych poprzez zarządzanie nimi, aż do zapewnienia odpowiedniej ochrony na opracowanym systemie raportowania. Organizacje, które wdrożyły System Zarządzania Bezpieczeństwem Informacji ISO 27001, mają już znaczną część pracy wykonaną. Te, które takiego systemu nie posiadają, powinny go potraktować jako najlepszą praktykę we wrażaniu RODO. Dlaczego? Wiele wymagań zawartych w RODO ma bezpośrednie odzwierciedlenie w ISO 27001.

Certyfikacja ISO 27001 jest potwierdzeniem, że organizacja wdrożyła System Zarządzania Bezpieczeństwem Informacji – system, który jest wspierany przez kierownictwo, ma odzwierciedlenie w kulturze i strategii firmy, oraz podlega stałemu monitoringowi, audytowi i doskonaleniu. Dla art. 32 ust. 1 RODO, który porusza kwestie bezpieczeństwa przetwarzania danych, ma to kluczowe znaczenie. Przepis ten nakłada na administratora i przetwarzającego dane obowiązek wdrożenia„odpowiednich środków technicznych i organizacyjnych, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku (…)".

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

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

Proszę zwrócić uwagę, że cztery powyższe kroki są całkowicie niezależne od tego, jaka technologia informatyczna jest wykorzystywana w firmie. To tylko po raz kolejny wskazuje, że wdrożenie RODO nie jest problemem technologicznym. Skoro przestrzeganie przepisów Rozporządzenia jest obowiązkiem firmy, jego wymagania są niezależne od technologii, zaś o skuteczności wdrożenia będzie decydowało wdrożenie w firmie odpowiednich procesów związanych z wymaganiami rozporządzenia, to warto zadać sobie pytanie, kto jest za to wszystko odpowiedzialny. A także, czy możemy się tą odpowiedzialnością z kimś podzielić lub ograniczyć ryzyko.

6.1. SYSTEM ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

W celu omówienia Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), warto omówić certyfikację ISO/IEC 27001:2013. Ta norma to standard bezpieczeństwa, który formalnie określa SZBI. W formalnej

specyfikacji norma opisuje obszary wymagań, które definiują sposób wdrażania, monitorowania, utrzymania i ciągłego doskonalenia bezpieczeństwa. Norma ta opisuje również zestaw najlepszych praktyk, które obejmują wymagania dotyczące dokumentacji, podziału odpowiedzialności, dostępności, kontroli dostępu, bezpieczeństwa, audytu oraz środki naprawcze i zapobiegawcze.

6.1.1. NAJWAŻNIEJSZE OBSZARY BEZPIECZEŃSTWA INFORMACJI, CZYLI WSPÓLNY MIANOWNIK DLA RODO I ISO 27001:2013

Wśród środków zapewniania bezpieczeństwa RODO wymienia:

a) pseudonimizację i szyfrowanie danych osobowych,
b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,
d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Porównując RODO z ISO 27001:2013, znajdujemy bezpośrednie odniesienie do tych środków.

Szyfrowanie danych jest jednym ze 114 zabezpieczeń wskazanych w załączniku A do Normy ISO 27001:2013. Każde z tych zabezpieczeń ma zmniejszyć ryzyko związane z przetwarzaniem informacji. Warto przy tym podkreślić, że ryzyko nie wiąże się jedynie z utratą informacji – bezpieczeństwo to także dostępność, poufność, integralność informacji i, co istotne z punktu widzenia RODO, autentyczność danych osobowych. Szyfrowanie danych jest zatem mechanizmem ochrony, który powinien być wdrożony na podstawie rzetelnej analizy ryzyka, tzn. takiej, która pozwala ocenić poziom wymaganej ochrony, a zarazem dostępność i integralność danych osobowych. Łatwo bowiem sobie wyobrazić sytuację, gdy dane osobowe są tak„chronione", że stają się niedostępne dla administratora danych osobowych, który ma prawo i obowiązek ich przetwarzania. Co to znaczy? Że nadmierne szyfrowanie i ich zabezpieczanie też może być szkodliwe. Wyobraźmy sobie sytuację, w której klucze szyfrujące ma jedna osoba w organizacji – a w pewnym momencie ją zmieni. W takiej sytuacji nie można mówić o bezpieczeństwie danych osobowych – zarówno pod kątem ISO 27001:2013, jak i RODO.

Analiza ryzyka to fundament procesu przygotowania do wdrożenia ISO 27001:2013. Na podstawie szczegółowej analizy zagrożeń i podatności administrator ma zapewnić poufność, integralność i dostępność informacji. Art. 32 RODO zobowiązuje wdrożenie środków bezpieczeństwa „uwzględniających 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". Każdy, kto ma za sobą analizę ryzyka w organizacji, dobrze wie, jak czasochłonny i wymagający jest to proces. Ci, którzy wdrożyli ISO 27001:2013, ogromną część pracy w tym zakresie mają za sobą.

Ciągłość działania polega na przygotowaniu planu na wypadek wystąpienia sytuacji, które mogą stanowić zagrożenie dla dalszego sprawnego funkcjonowania organizacji. Ostatnie ataki ransomware (WannaCry, Petya) pokazały, jak ważny jest ten obszar zapewnienia bezpieczeństwa. W tym przypadku ISO 27001:2013 znacznie rozszerza wymagania RODO – poza danymi osobowymi ważne jest szybkie przywrócenie dostępności, integralności, poufności wszystkich kluczowych zasobów informacyjnych. Era gospodarki cyfrowej nie idzie na kompromis; stawką są setki tysięcy, miliony strat każdego dnia braku dostępu do zasobów informacyjnych, a od połowy 2018 r. – także konsekwencje związane z sankcjami RODO.

Monitorowanie, audyt i doskonalenie to codzienność organizacji, które wdrożyły i certyfikowały ISO 27001:2013. W kontekście RODO, odnowienie certyfikacji jest niejako dowodem, że organizacja wykazała **należytą staranność** w zapewnianiu bezpieczeństwa danych osobowych. W przypadku wystąpienia incydentu może to być istotny argument za zmniejszeniem kar, które zgodnie z RODO mają znacząco wpłynąć na motywację firm i organizacji do zwiększenia poziomu bezpieczeństwa danych osobowych. Niemniej

oprócz SZBI, należy jeszcze pamiętać o pozostałych formach zabezpieczenia informacji, a mianowicie o *privacy by design* oraz *privacy by default*.

6.2. *PRIVACY BY DESIGN* I *PRIVACY BY DEFAULT*

RODO nie daje nam instrukcji tego, w jaki sposób należy postępować w przypadku procedur i zabezpieczania danych osobowych. Podobnie jest z zasadą **privacy by design**, o której musimy pamiętać już w trakcie projektowania wszystkich procesów, ale która nie została zdefiniowana w tym akcie prawnym. Obszar tego typu ochrony zależy od celu przetwarzania informacji, jego charakteru i sposobu. Pomocny w tym przypadku jest artykuł 25 RODO, który mówi, że „uwzględniając 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 wynikające z przetwarzania, administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą".

Najważniejszą informacją wynikającą z tej zasady jest wprowadzenie wszelkich sposobów zabezpieczania danych już **w trakcie planowania procesu**. Przykładowo przedsiębiorca, który będzie chciał wdrożyć w swojej organizacji chmurę obliczeniową, będzie musiał już na początku planowania procesu wdrożenia przeanalizować, czy dana infrastruktura, rozwiązanie czy dostawca są godni zaufania, jakie środki bezpieczeństwa będą wprowadzone, czy administrator ma kontrolę nad swoimi danymi, czy ma odpowiednie zapisy umowne z podwykonawcami (oczywiście zgodne z RODO), ale przede wszystkim – jakie operacje zamierza wykonywać przy zastosowaniu danego rozwiązania. Warto też zaznaczyć, że istotne jest rozważenie, czy w swojej infrastrukturze administrator jest w stanie zapewnić takie same lub wyższe środki bezpieczeństwa niż dostawca chmury obliczeniowej. Z kolei na podstawie takiej analizy powinien dokonać wyboru adekwatnego rozwiązania.

Następnie administrator powinien ustalić, jakie przesłanki będą pozwalały mu na przetwarzanie danych, czy posiada odpowiednie zgody, w jaki sposób je zbiera, czy osoba fizyczna jest odpowiednio poinformowana o celu przetwarzania (obowiązek informacyjny), stosowanych zabezpieczeniach, itd. Warto zaznaczyć, że w procesie przetwarzania należy uwzględnić jedynie takie dane osobowe, które są niezbędne w osiągnięciu celu ich przetwarzania. Jak to określić? Należy odpowiedzieć na pytania, które powiedzą nam, ile danych osobowych zbieramy, w jakim zakresie (liczba typów danych), w jakim okresie (czasowość) oraz kto i na jakiej zasadzie ma do nich dostęp.

Privacy by design nie jest pojęciem nowym, funkcjonuje na rynku już od dłuższego czasu, niemniej jednym z bardziej istotnych dla przedsiębiorcy wiarygodnych źródeł informacji w tym zakresie może być interpretacja, która powstała w wyniku prac Międzynarodowej Konferencji Rzeczników Ochrony Danych i Prywatności z 2010 r. Zgodnie z nią ochrona prywatności w fazie projektowania powinna się opierać na siedmiu zasadach:

1. Podejście proaktywne, nie reaktywne i zaradcze, nie naprawcze.
2. Prywatność jako ustawienie domyślne.
3. Prywatność włączona w projekt.
4. Pełna funkcjonalność: suma dodatnia, nie suma zerowa.
5. Ochrona od początku do końca cyklu życia informacji.
6) Widoczność i przejrzystość.
7. Poszanowanie dla prywatności użytkowników[1].

[1] 32. Międzynarodowa Konferencja Rzeczników Ochrony Danych i Prywatności, Jerozolima, 27 – 29 października 2010 r., Rezolucja w Sprawie Prywatności w Fazie Projektowania. Źródło: http://www.giodo.gov.pl/plik/id_p/2104/j/pl (dostęp dnia 28.11.2017 r.).

Każdy przedsiębiorca powinien również, oprócz **zaplanowania** procesu pod względem bezpieczeństwa przetwarzania, dopilnować, czy ten proces jest **realizowany**. Podobnie jak w przypadku corocznych audytów norm ISO omówionych w podrozdziale dotyczącym Systemu Zarządzania Bezpieczeństwem Informacji, warto się zastanowić, czy zasadne byłoby wprowadzenie regularnego sprawdzania funkcjonowania zasady *privacy by design* oraz wymogów wprowadzonych na etapie projektowania, np. kontrolowania posiadanych zgód i ich zasadności, wprowadzonych systemów informatycznych, odpowiedniego informowania osób fizycznych o procesach, w jakich ich dane uczestniczą. Dobrą praktyką byłoby również porównanie z „nowościami rynkowymi", np. systemów informatycznych, ponieważ rozwiązania przyjęte podczas etapu projektowania po roku jego funkcjonowania niekoniecznie mogą okazać się najlepsze.

Praktykowanie *privacy by design* jest jedną z bardziej wartościowych zmian wprowadzonych przez RODO. Jak każda analiza, wiąże się ona oczywiście ze swego rodzaju ryzykiem – głównie z tego powodu, że nie zostało jeszcze wypracowane modelowe egzekwowanie prawa przez sądy, regulatora, ani też nie znamy wzorcowych „dobrych praktyk rynkowych". Niemniej wprowadzenie jakiejkolwiek polityki i zasad prywatności do każdego procesu przetwarzania danych osobowych działa na korzyść zarówno administratora w budowaniu jego wiarygodności, jak i prawa do prywatności osób fizycznych.

Oprócz *privacy by design* administrator danych osobowych powinien pamiętać również o **privacy by default**. Działanie to powstało w oparciu o ten sam artykuł 25 RODO, ale nie dotyczy całego projektowania procesu, tylko zapewnienia takich domyślnych ustawień systemu informatycznego, które zapewnią adekwatną do celu przetwarzania ochronę danych osobowych już w momencie rozpoczęcia korzystania z usługi, czyli włączenia systemu informatycznego, aplikacji itd. Rozszerzenie lub zmniejszenie tych ustawień może nastąpić dopiero po uzyskaniu takiej informacji od właściciela danych osobowych, który w tym przypadku jest użytkownikiem takiego systemu. Twórcy lub właściciele systemów informatycznych nie mogą sami zmieniać tych spośród domyślnych ustawień, które mogą ingerować w prywatność osoby fizycznej.

6.3. SZACOWANIE RYZYKA NARUSZEŃ DANYCH OSOBOWYCH

Dane przetwarzane przez organizacje są cennymi aktywami, a na rynku osiągają dużą wartość handlową. Jak wynika z treści RODO, wraz z wejściem w życie tego dokumentu, większość organizacji będzie zobowiązana do szacowania ryzyka, jakie wiąże się z przetwarzaniem danych. Każda organizacja, która dane przetwarza, musi liczyć się z tym, że jest narażona na wpływ czynników zewnętrznych oraz wewnętrznych, które mogą spowodować naruszenie bezpieczeństwa. W konsekwencji może to prowadzić do niezgodnego z prawem nieuprawnionego dostępu do danych, a także utracenia czy choćby zmodyfikowania przetwarzanych danych.

Stan, w którym zachodzi możliwość niezrealizowania założeń organizacji w wyniku zajścia określonych zdarzeń, nazywamy **ryzykiem.** Zarządzanie ryzykiem to proces identyfikacji, oceny, postępowania i kontroli potencjalnych zdarzeń lub sytuacji, dostarczający racjonalnego zapewnienia, że cele organizacji zostaną zrealizowane.

Obowiązek analizy ryzyka wynika z przepisów prawa. W Rozporządzeniu Rady Ministrów z 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności § 20 ust. 1 (dalej: KRI) czytamy, że podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali System Zarządzania Bezpieczeństwem Informacji[2]. System ma zapewniać poufność, dostępność

[2] Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Dz. U. 2012 poz. 526, Paragraf 20 ust. 1.

i integralność informacji z uwzględnieniem takich atrybutów jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

§ 20 ust. 2 pkt. 3 KRI wskazuje, że zarządzanie bezpieczeństwem informacji jest realizowane w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań: przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko stosownie do wyników przeprowadzonej analizy[3]. Oprócz podstawy prawnej administrator danych powinien odpowiedzieć na kilka pytań. Przede wszystkim: jakie dane będzie chronić i w jaki sposób zamierza to robić? Jakie środki bezpieczeństwa powinien przedsięwziąć oraz jakie mogą być konsekwencje naruszenia przyjętych zasad ochrony danych? Odpowiedzi na te pytania powinno przynieść szacowanie ryzyka naruszeń danych osobowych.

6.3.1. PROCES ZARZĄDZANIA RYZYKIEM – ETAPY SZACOWANIA RYZYKA

Odpowiednim podejściem do zarządzania ryzykiem jest traktowanie go jako jednego z procesów organizacji, a nie pojedynczego etapu w ramach realizowanego wdrożenia określonej polityki. O skutecznym zarządzaniu ryzykiem w organizacji można mówić tylko i wyłączenie w sytuacji, gdy są podejmowane działania związane z ciągłym monitorowaniem i analizą ryzyk oraz z reagowaniem na zmieniające się warunki otoczenia w kontekście identyfikacji nowych zagrożeń. Proces zarządzania ryzykiem można podzielić na kilka etapów. Pierwszym z nich jest **wyznaczenie kontekstu strategicznego**, w którym należy opracować metodykę zarządzania ryzykiem oraz określić jej odpowiedzialność w tym zakresie. Szczególnie ważne jest uwzględnienie roli kierownictwa na etapie określenia kryteriów akceptacji ryzyka.

Kolejnym etapem jest **identyfikacja ryzyka**. Polega ona na określeniu przyczyn niepożądanych incydentów. Obejmuje identyfikowanie aktywów, zagrożeń, podatności i potencjalnych następstw zidentyfikowanych incydentów.

Następny etap to **określenie zagrożeń dla zidentyfikowanych aktywów**. Zagrożenia mogą występować zarówno w wyniku działań celowych, jak i przypadkowych, a przyczynić się do nich może podatność, którą także należy identyfikować. Dobrym przykładem identyfikowanej podatności może być brak szkoleń z zakresu bezpieczeństwa.

Kolejnym krokiem jest **wykonanie estymacji ryzyka**. Analiza odbywa się w kontekście istniejących zabezpieczeń oraz prawdopodobieństwa wystąpienia incydentów. Podczas szacowania ryzyka należy wziąć pod uwagę odpowiednie statystyki oraz możliwość wystąpienia zagrożeń. W przypadku zagrożeń spowodowanych celowym działaniem są to motywy oraz możliwości, zaś w przypadku zagrożeń spowodowanych przypadkowym działaniem – czynniki środowiskowe, czynniki wpływające na błędy ludzkie oraz nieprawidłowe działanie urządzeń. Analizując skutki wystąpienia ryzyka, należy rozważyć zarówno konsekwencje bezpośrednie, takie jak koszt wymiany lub naprawy utraconych aktywów, jak i trudne do oszacowania konsekwencje pośrednie, do których można zaliczyć: utratę wizerunku oraz koszty utraconych możliwości.

Ostatnim etapem szacowania ryzyka jest **dokonanie jego oceny.** W tym kroku powinno się porównać wyznaczone poziomy ryzyka z ustalonymi kryteriami oraz nadać priorytety poszczególnym ryzykom. Chodzi tu o przyporządkowanie ryzyk do danej grupy. W zależności od przyjętej metodyki, zazwyczaj ryzyka są dzielone na niskie, średnie i wysokie. Wynikiem tego etapu powinna być lista ryzyk wytypowanych do podjęcia działań redukujących ich wartość do akceptowalnego poziomu.

Aby zminimalizować ryzyko, powinniśmy określić prawdopodobieństwo wystąpienia określonych zagrożeń, skutki ich wystąpienia oraz istotność dla analizowanego obszaru. Rzetelna analiza ryzyka pozwoli przygotować praktyczną politykę bezpieczeństwa, a zastosowanie odpowiednich środków z pewnością zminimalizuje zagrożenie dla danych, które przetwarza organizacja. O ile jednak nie mamy gotowych odpowiedzi,

[3] Tamże, paragraf 20 ust. 2 pkt. 3.

warto również posilać się dobrymi praktykami rynku, np. grupą norm ISO 27000, mówiących o Systemie Zarządzania Bezpieczeństwem Informacji.

Jak ISO 27001 może pomóc w procesie wdrożenia RODO?

Kilka przykładów, jak normy ISO 27001, 27017, 27018 i 22301 adresują wymagania RODO:

ISO		RODO	
27001	Polityka bezpieczeństwa	Art. 24, ust 2	Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora **odpowiednich polityk ochrony danych**.
	Kontrola dostępu	Art. 5, ust. 1 f)	Dane osobowe muszą być (...)przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed **niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą**, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność").
	Zarządzanie ciągłością działania	Art. 32 ust. 2	Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności **ryzyko** wiążące się 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.
	Zarządzanie incydentami związanymi z bezpieczeństwem informacji	Motyw 49	Przetwarzanie danych osobowych w zakresie bezwzględnie niezbędnym i proporcjonalnym do zapewnienia bezpieczeństwa sieci i informacji (...) oraz bezpieczeństwa związanych z nimi usług oferowanych lub udostępnianych poprzez te sieci i systemy przez organy publiczne, zespoły reagowania na zagrożenia komputerowe, zespoły reagowania na **komputerowe incydenty naruszające bezpieczeństwo**, dostawców sieci i usług łączności elektronicznej oraz dostawców technologii i usług w zakresie bezpieczeństwa jest prawnie uzasadnionym interesem administratora, którego sprawa dotyczy.

ISO		RODO	
27017	Współdzielona odpowiedzialność (klient i dostawca) w środowisku chmurowym	Artykuł 82	1. 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. 2. Każdy administrator uczestniczący w przetwarzaniu odpowiada za szkody spowodowane przetwarzaniem naruszającym niniejsze rozporządzenie. **Podmiot przetwarzający odpowiada za szkody spowodowane przetwarzaniem wyłącznie, gdy nie dopełnił obowiązków, które niniejsze rozporządzenie nakłada bezpośrednio na podmioty przetwarzające**, lub gdy działał poza zgodnymi z prawem instrukcjami administratora lub wbrew tym instrukcjom.
	Usuwanie zasobów i usług klienta z chmury	Motyw 81	Po zakończeniu przetwarzania w imieniu administratora podmiot przetwarzający powinien – zgodnie z decyzją administratora – zwrócić lub usunąć dane osobowe, chyba że prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający, nakładają obowiązek przechowywania danych osobowych.
27018	Administrator wie, co dzieje się z jego danymi. Przestrzeganie tej normy zapewnia przejrzystość zasad zwrotu, **przesyłania i usuwania danych osobowych przechowywanych w centrach danych.** Administrator jest nie tylko informowany, **gdzie** znajdują się dane, ale także są wskazane firmy, które współpracują z przetwarzającym i mają dostęp do tych danych.	Sekcja 3	Art. 16: Sprostowanie i usuwanie danych; Art. 17: Prawo do usunięcia danych; Art. 18: Prawo do ograniczenia przetwarzania; Art. 19 Obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania; Art. 20 Prawo do przenoszenia danych.
	Administrator jest również informowany o przypadkach dostępu osób nieupoważnionych do danych osobowych oraz obiektów i sprzętu używanego do przetwarzania danych, jeżeli skutkują one utratą, ujawnieniem lub modyfikacją tych danych.	Art. 33 ust. 1	W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

ISO		RODO	
	Zgodność z normą ISO 27018 zapewnia różne istotne **środki ochrony**. Standard narzuca pewne ograniczenia dotyczące postępowania z danymi osobowymi, w tym ograniczenia ich przesyłania w sieciach publicznych i przechowywania na nośnikach przenośnych, a także odpowiednie procesy odzyskiwania i przywracania danych. Norma ta wymaga ponadto podpisania zobowiązania do zachowania **poufności** przez wszystkie osoby, które zajmują się przetwarzaniem danych osobowych.	Motyw 39	Dane osobowe powinny być przetwarzane w sposób zapewniający im odpowiednie **bezpieczeństwo** i odpowiednią **poufność**, w tym ochronę przed nieuprawnionym dostępem do nich i do sprzętu służącego ich przetwarzaniu oraz przed nieuprawnionym korzystaniem z tych danych i z tego sprzętu.
22301	Polityka zarządzania ciągłością działania definiująca cele kierownictwa. Proces zarządzania ciągłością funkcjonowania organizacji zapewniający systemowe podejście.	Art. 5, ust. 1 f)	Dane osobowe muszą być (...)przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed **niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą**, zniszczeniem lub uszkodzeniem za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność").
	Strategia zarządzania ciągłością działania jako odpowiedź na istniejące ryzyka. Analiza działalności przez pryzmat ryzyka	Motyw 90	W takim przypadku administrator powinien przed przetwarzaniem dokonać oceny skutków dla ochrony danych, aby ocenić konkretne prawdopodobieństwo i powagę wysokiego ryzyka, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz źródła ryzyka. Ocena skutków powinna w szczególności obejmować planowane środki, zabezpieczenia i mechanizmy mające minimalizować to ryzyko, zapewniać ochronę danych osobowych oraz wykazać przestrzeganie niniejszego rozporządzenia.
	Testowanie, zarządzanie i przegląd środków ochrony zarówno technicznych, jak i organizacyjnych (przede wszystkim planów awaryjnych).	Art. 32 ust. 2	Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności **ryzyko** wiążące się 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.

ISO		RODO	
22301	Budowa świadomości pracowników i podmiotów współpracujących.	Art. 39 ust. 1b)	Inspektor ochrony danych ma następujące zadania: (...) monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, **działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania** oraz powiązane z tym audyty.
	Opracowanie i wdrożenie środków ochrony wynikające ze realizacji strategii.	Art. 39 ust. 2	Inspektor ochrony danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

Źródło: opracowanie własne

Jak widać, odpowiedzi na wymagania, które stawia przed nami RODO, można znaleźć w innych aktach normatywnych, które funkcjonują na rynku. Mogą one niekiedy stanowić wzór postępowania w zagadnieniach, z którymi administrator danych osobowych będzie musiał się zmierzyć. Ten rezultat jednak w dużej mierze będzie zależał od wykonania analizy ryzyka i tego, jak zaimplementuje konkretne procedury.

6.4. PODSUMOWANIE

RODO jest istotną zmianą prawa dotyczącego prywatności i bezpieczeństwa danych osobowych w Unii Europejskiej. Niedostosowanie procesów do nowych wymagań prawnych jest obciążone znaczącymi konsekwencjami finansowymi. RODO wymaga, aby organizacje szanowały i chroniły dane osobowe – niezależnie od tego, gdzie są one wysyłane, przetwarzane lub przechowywane. Z powyższych informacji wynika, że sposób zabezpieczania danych jest procesem ciągłym – nie jest to czynność, którą wykonamy, a następnie możemy o niej zapomnieć. Monitorowanie tego, co się dzieje z danymi, w jaki sposób i w jakim celu są przetwarzane, powinno być dokumentowane w całych procesach, w których zapewniona jest podstawowa i domyślna prywatność. Oczywiście na te działania ma z kolei wpływ szacowanie ryzyka i wynik tych analiz. O ile będziemy wiedzieć, w jakim celu przetwarzamy dane i w jakich ilościach mamy je zbierać do realizacji danego celu, taka analiza i wprowadzenie zabezpieczeń nie powinno być skomplikowane. Najważniejszy jest rozsądek i rzetelność w przeprowadzaniu procesów przetwarzania danych osób fizycznych. Należy pamiętać, że brak dochowania należytej staranności w tym zakresie, oprócz skutków finansowych związanych z karami administracyjnymi, rodzi dodatkowo skutki prawne (pozwy cywilne), a także wizerunkowe (utrata zaufania do firmy).

7. OCHRONA DANYCH OSOBOWYCH PRACOWNIKÓW PO WEJŚCIU W ŻYCIE RODO

Małgorzata Regulska-Cieślak

Kwestia związana z pozyskiwaniem danych osobowych w polskim porządku prawnym jest rozproszona w ponad 130 aktach prawnych. Dlatego, poza uchwaleniem nowej ustawy o ochronie danych osobowych (dalej także: nowa UODO), konieczne jest dokonanie licznych zmian w innych ustawach. Zdecydowano się dokonać tego w projekcie ustawy – Przepisy wprowadzające ustawę o ochronie danych osobowych. Można od razu zaznaczyć, że na gruncie prawa pracy zmiany będą rzeczywiście rewolucyjne.

7.1. DANE OSOBOWE PRACOWNIKÓW DO 24 MAJA 2018 R.

7.1.1. JAKICH DANYCH OSOBOWYCH MOŻE ŻĄDAĆ PRACODAWCA?

Definicja danych osobowych została omówiona w pierwszym rozdziale niniejszej publikacji. Zgodnie z Kodeksem pracy, w jego obecnym brzmieniu, dane osobowe dzieli się na dane, które pracodawca może pobrać od **kandydatów** do pracy oraz od osób już **zatrudnionych**.

Zasadniczo tylko art. 22 [1] Kodeksu pracy reguluje wprost kwestię danych osobowych kandydatów do pracy i pracowników.

Przepis art. 22 [1] § 1 stanowi, że pracodawca ma prawo żądać od osoby ubiegającej się o zatrudnienie, czyli **kandydata**, podania danych osobowych obejmujących:

„1) imię (imiona) i nazwisko,
2) imiona rodziców,
3) datę urodzenia,
4) miejsce zamieszkania (adres do korespondencji),
5) wykształcenie,
6) przebieg dotychczasowego zatrudnienia".

Z kolei art. 22 [1] § 2 Kodeksu pracy statuuje, że pracodawca – niezależnie od danych osobowych, które może pobrać od kandydata na podstawie art. 22 [1] § 1 Kodeksu pracy – ma prawo żądać od **pracownika** podania także:

1) innych danych osobowych pracownika, a także imion i nazwisk oraz dat urodzenia dzieci pracownika, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy,
2) numeru PESEL pracownika nadanego przez Rządowe Centrum Informatyczne Powszechnego Elektronicznego Systemu Ewidencji Ludności (RCI PESEL).

O stan cywilny pracodawca pytać **nie może**.

Udostępnienie pracodawcy danych osobowych następuje w formie **oświadczenia** osoby, której one dotyczą. Pracodawca ma prawo żądać udokumentowania tych danych osobowych, np. w formie świadectw pracy, aktów urodzenia dzieci, dyplomów ukończenia szkół, kursów itd.

Pracodawca może również żądać podania innych danych osobowych niż określone powyżej, jeżeli obowiązek ich podania wynika z odrębnych przepisów.

7.1.2. UJAWNIANIE DANYCH PRACOWNIKÓW

Co do ujawniania na zewnątrz zakładu pracy nazwisk pracowników wypowiedział się Sąd Najwyższy w wyroku z 19 listopada 2003 r.[1], w uzasadnieniu którego stwierdził, że: „(...) najistotniejszym składnikiem zakładu pracy (przedsiębiorstwa) są ludzie, a funkcjonowanie zakładu wiąże się nierozłącznie z kontaktami zewnętrznymi – z kontrahentami, klientami (...). Dlatego pracodawca nie może być pozbawiony możliwości ujawniania nazwisk pracowników, zajmujących określone stanowiska w ramach instytucji. Przeciwne stanowisko prowadziłoby do sparaliżowania lub poważnego ograniczenia możliwości działania pracodawcy, bez żadnego rozsądnego uzasadnienia w ochronie interesów i praw pracownika. (...) Imiona i nazwiska pracowników widnieją na drzwiach w zakładach pracy, umieszcza się je na pieczątkach imiennych, pismach sporządzanych w związku z pracą, prezentuje w informatorach o instytucjach i przedsiębiorstwach, co oznacza, że zgodnie z powszechną praktyką są one zasadniczo jawne".

GIODO również uważa, że **wolno** zamieścić na stronie internetowej firmy dane służbowe pracownika, takie jak jego imię i nazwisko, służbowy adres e-mail czy służbowy numer telefonu, które są ściśle związane z życiem zawodowym pracownika i z wykonywaniem przez niego obowiązków służbowych. Ze względu na to dane te mogą być wykorzystywane przez pracodawcę **bez zgody** osoby, której one dotyczą.

Studium przypadku 1.
Na stronie internetowej firmy X, w zakładce pn. Kontakt, widnieją następujące dane: Jan Kowalski, Asystent Zarządu, tel. (0-11) 123 45 67, e-mail: jan.kowalski@firmax.com.pl. Aby legalnie ujawnić takie dane pracownika, pracodawca nie potrzebuje uzyskać na to jego zgody, gdyż są to dane związane z wykonywaniem obowiązków służbowych. Innych danych dotyczących, np. daty urodzenia, wykształcenia, miejsca zamieszkania czy też telefonu prywatnego pracodawca nie może ujawnić.

7.1.3. INNE DANE PRACOWNICZE

Przepis art. 22 [1] § 5 Kodeksu pracy stanowi, iż w zakresie nieuregulowanym w tym artykule do danych osobowych, o których mowa w tych przepisach, stosuje się przepisy odrębne, a zatem m.in. przepisy ustawy o ochronie danych osobowych. Zgodnie zaś z art. 23 ust. 1 pkt 1 UODO przetwarzanie danych jest dopuszczalne tylko wtedy, kiedy osoba, której dane dotyczą, wyrazi na to **zgodę**, chyba że chodzi o usunięcie dotyczących jej danych.

Zgodnie z wyrokiem Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 27 listopada 2008 r.[2] „W zakresie innych danych pracowniczych, niż wymienione w art. 22 [1] § 1-4 k.p., zastosowanie mają przepisy ustawy o ochronie danych osobowych. Wypływa z tego następujący wniosek: pracodawca żąda jedynie tych danych, które wymaga od pracownika prawo pracy i pracodawca może żądać od pracownika także danych, które wymagane są przez inne przepisy prawa".

Innych danych osobowych, np. zaświadczenie o stanie zdrowia, pracodawca **nie może** pobrać i przetwarzać, chyba że wynika to z odrębnych przepisów. „W sytuacji gdy przepisy prawa pracy formułują ograniczenia, a nawet zakaz zatrudniania osób przy określonych rodzajach prac (dotyczy to w szczególności kobiet w ciąży), pozyskania informacji, które są niezbędne do wypełnienia tego obowiązku, nie można uznać za naruszenie art. 22 [1] k.p."[3].

Zgodnie z art. 22 [1] § 4 Kodeksu pracy pracodawca może żądać podania innych danych osobowych niż określone powyżej, jeżeli obowiązek ich podania wynika z odrębnych przepisów. Takim odrębnym przepisem jest przykładowo art. 8 ust. 1 ustawy z dnia 4 marca 1994 r. o zakładowym funduszu świadczeń socjalnych,

[1] I PK 590/02, OSNP 2004/20/351.
[2] Sygnatura akt. II SA/Wa 903/08.
[3] Baran Krzysztof W. (red.), *Kodeks pracy. Komentarz,* wyd. III. Opublikowano: WK 2016

który nie wprost, ale jednak zezwala na przetwarzanie danych osobowych niezbędnych do ustalenia prawa do świadczeń socjalnych przydzielanych ze środków funduszu.

Prawo żądania informacji, które dotykają sfery osobistej, przewidują niektóre pragmatyki pracownicze. Przykładowo art. 6 ust. 1 pkt 2 ustawy z dnia 21 listopada 2008 r. o pracownikach samorządowych wymaga od wszystkich zatrudnionych w samorządzie korzystania z pełni praw publicznych, zaś od zatrudnionych na podstawie wyboru lub powołania – dodatkowo niekaralności za umyślne przestępstwo ścigane z oskarżenia publicznego lub umyślne przestępstwo skarbowe (art. 6 ust. 2 wyżej cytowanej ustawy). Wówczas, na podstawie art. 6 ust. 1 pkt 10 ustawy o Krajowym Rejestrze Karnym, pracodawcom przysługuje prawo do uzyskania informacji o osobach, których dane osobowe zostały zgromadzone w rejestrze, ale tylko w zakresie niezbędnym do zatrudnienia pracownika, co do którego z przepisów ustawy wynika wymóg niekaralności, korzystania z pełni praw publicznych, a także ustalenia uprawnienia do zajmowania określonego stanowiska, wykonywania określonego zawodu lub prowadzenia określonej działalności gospodarczej.

Podstawą do przetwarzania przez pracodawcę danych osobowych tak kandydatów do pracy, jak i pracowników są przepisy prawa pracy, w tym Kodeksu pracy oraz wydane na jego podstawie akty wykonawcze, zwłaszcza rozporządzenie w sprawie zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika, które wskazuje, jakie informacje mogą być żądane (np. w zakresie wykształcenia), ale i inne przepisy. W myśl bowiem § 6 tego rozporządzenia celem prowadzenia akt osobowych pracowników jest gromadzenie dokumentów dotyczących ubiegania się o zatrudnienie, nawiązania stosunku pracy i przebiegu zatrudnienia (również na podstawie umów cywilnoprawnych) oraz dokumentów związanych z ustaniem zatrudnienia. GIODO w decyzji z 8 sierpnia 2014 r.[4] wskazuje, że po ustaniu stosunku pracy dalsze przetwarzanie danych osobowych pracownika, zgromadzonych w aktach osobowych, odbywa się w celach archiwalnych na podstawie przepisów ustawy z 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach[5].

7.1.4. JAKICH DANYCH OSOBOWYCH PRACODAWCA NIE MOŻE PRZETWARZAĆ?

Pracodawcy nie wolno przetwarzać m.in.:

- **danych biometrycznych**, takich jak linie papilarne, obraz tęczówki oka czy kod DNA. Wynika to z decyzji GIODO z 15 grudnia 2009 r. (DIS/DEC-1261/46988/09) oraz z wyroku NSA z 6 września 2011 r. (I OSK 1476/10), o którym mowa poniżej;
- **danych pozyskiwanych wskutek monitoringu komputerów**, o którym pracownik nie wie. Dane mogą być przetwarzane jedynie wtedy, kiedy pracownik wie o monitoringu i się na niego godzi, a sam monitoring jest zgodny z przepisami, w tym przepisami o ochronie danych osobowych. Wynika to z wyroku WSA w Warszawie z 6 czerwca 2012 r. (II SA/Wa 453/12), z wyroku NSA z 13 lutego 2014 r. (I OSK 2436/12) oraz z licznych wypowiedzi GIODO;
- **danych o przynależności związkowej** – pozyskiwanie informacji o korzystaniu przez pracownika z ochrony związkowej jest dopuszczalne jedynie w toku konsultacji ze związkami zawodowymi w razie zamiaru wypowiedzenia/rozwiązania umowy o pracę z konkretnym pracownikiem. Wynika to z decyzji GIODO z 15 lutego 2013 r. (DOLiS/DEC-181/13/10107) oraz z wyroku SN z 24 czerwca 2013 r. (II PK 341/12);
- **danych o przyczynach wypowiedzenia umowy o pracę** – o naruszeniu zasady poufności i nieudostępniania danych osobom nieupoważnionym stanowi wyrok SA w Gdańsku z 12 czerwca 2013 r. (III APa 16/13). Tylko upoważnieni do przetwarzania danych osobowych pracownicy pracodawcy mogą zapoznać się z przyczynami wypowiedzenia umowy o pracę konkretnego pracownika;

[4] DOLiS/DEC-789/14/61757.

[5] Dz. U. z 2016 r. poz. 1506.

- **danych byłego pracownika umieszczonych w miejscu publicznie dostępnym** – stanowi to naruszenie zakazu udostępniania danych osobom nieupoważnionym. Wynika to z decyzji GIODO z 5 lutego 2015 r. (DOLiS/DEC 76/15/8797).

Pracodawca **nie ma** podstawy prawnej do żądania przekazania kopii dowodu osobistego. „Stanowisko GIODO w tej sprawie jest niezmienne – kserowanie przez pracodawcę dowodu osobistego kandydata do pracy narusza ustawę o ochronie danych osobowych, jeżeli prowadzi do pozyskania szerszego zakresu danych osobowych niż ten, do którego pracodawca jest uprawniony"[6].

Warto również zwrócić uwagę na żądanie przez pracodawcę podania przez kandydata do pracy innych danych osobowych niż te wymienione w art. 22 [1] § 1 Kodeksu pracy. Może chodzić np. o przedstawienie referencji. W tym zakresie GIODO wypowiada się negatywnie – żądanie przedstawienia referencji przez kandydata do pracy prowadzi do naruszenia prawa, w tym ustawy o ochronie danych osobowych[7].

Jeśli pracodawca chce użyć zdjęcia (wizerunku) pracownika, **musi otrzymać jego zgodę**. Zdaniem GIODO zdjęcie nie mieści się w katalogu informacji wskazanych w 22 [1] § 1 Kodeksu pracy, dlatego posłużenie się wizerunkiem pracownika wymaga jego zgody. Dodatkowo jest chronione przepisami Kodeksu cywilnego.

GIODO **pozwala** na ujawnianie danych osobowych pracownika typu imię i nazwisko oraz stanowisko na identyfikatorze, jeśli obowiązek jego noszenia wynika z wewnętrznych uregulowań wydanych przez pracodawcę. Chodzi np. o regulamin pracy wydany na podstawie art. 104 § 1 Kodeksu pracy. W opinii GIODO pracodawca ma także prawo przetwarzać dane osobowe pracownika w celach związanych z przeprowadzeniem obligatoryjnych badań okresowych mających na celu stwierdzenie, czy zachodzą przeciwwskazania zdrowotne do pracy na zajmowanym przez pracownika stanowisku[8].

7.1.5. DOPUSZCZALNOŚĆ PRZETWARZANIA DANYCH

W myśl art. 23 ust. 1 pkt 1 ustawy o ochronie danych osobowych przetwarzanie danych **jest dopuszczalne** tylko w enumeratywnie wymienionych w tym przepisie przypadkach, czyli wtedy, kiedy:

1) osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych,
2) jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa,
3) jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą,
4) jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego,
5) jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

Natomiast art. 27 ust. 1 UODO wyraźnie **zakazuje** przetwarzania danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym, przy czym przetwarzanie powyższych danych jest dopuszczalne w dziesięciu wymienionych sytuacjach, między innymi wówczas, gdy przetwarzanie jest

---

[6] Pismo Generalnego Inspektora Ochrony Danych Osobowych z dnia 5 lipca 2012 r., Rzeczpospolita. PiP 2012/161/4, LEX nr 154330.

[7] Pismo Generalnego Inspektora Ochrony Danych Osobowych z dnia 5 lipca 2012 r., Rzeczpospolita PiP 2010/267/6, LEX nr 41948.

[8] Decyzja GIODO z 22 maja 2012 r., DOLiS/DEC-458/12/31754.

niezbędne do wykonania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych jest określony w ustawie (art. 27 ust. 2 pkt 6 ww. ustawy).

W tym miejscu warto przytoczyć wyrok Naczelnego Sądu Administracyjnego w Warszawie z dnia 6 września 2011 r.[9] Zgodnie z tym orzeczeniem „wyrażona na życzenie pracodawcy pisemna zgoda pracownika na pobranie i przetworzenie jego danych osobowych (chodziło o pobranie danych biometrycznych i ich wykorzystanie do kontroli czasu pracy pracowników zatrudnionych w urzędzie skarbowym) narusza prawa pracownika i swobodę wyrażenia przez niego woli. Za tak sformułowanym stanowiskiem przemawia zależność pracownika od pracodawcy. Generalnie więc brak równowagi w relacji pracodawca-pracownik stawia pod znakiem zapytania dobrowolność w wyrażeniu zgody na pobieranie i przetworzenie danych osobowych (biometrycznych). Z tego względu ustawodawca ograniczył przepisem art. 22 [1] ustawy z dnia 26 marca 1974 r. - Kodeks pracy (Dz. U. z 1998 r. Nr 21, poz. 94 ze zm.) katalog danych, których pracodawca może żądać od pracownika. Jak wynika z utrwalonego orzecznictwa Naczelnego Sądu Administracyjnego, z którym skład orzekający w tej sprawie się identyfikuje, uznanie faktu wyrażenia przez pracownika zgody na przetwarzanie jego danych (art. 23 ust. 1 pkt 1 ustawy o ochronie danych osobowych) za okoliczność legalizującą pobranie od pracownika innych danych niż wskazane w art. 22 [1] Kodeksu pracy stanowiłoby naruszenie tego przepisu Kodeksu pracy (porównaj wyrok NSA z dnia 1 grudnia 2009 r. sygn. akt I OSK 249/09 - publikowany ONSA i WSA 2011/2/39)".

Zatem rozszerzenie katalogu danych określonych w art. 22 [1] Kodeksu pracy nie może zatem nastąpić przez zastosowanie przepisów ogólnych, tj. art. 23 ust. 1 pkt 1 ustawy o ochronie danych osobowych.

7.1.6. PRZETWARZANIE DANYCH BEZ ZGODY

Jeśli pracodawca żąda od pracowników jedynie danych osobowych, których wymagają przepisy, **nie potrzebuje** zgody tych osób na ich przetwarzanie. Zgodnie z art. 23 ust. 1 pkt 2-5 ustawy o ochronie danych osobowych pracodawcy mają prawo przetwarzać dane osobowe pracowników i współpracowników bez ich zgody, gdy jest to niezbędne:

- dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa,
- do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą,
- do wykonania określonych prawem zadań realizowanych dla dobra publicznego,
- dla wypełnienia prawnie usprawiedliwionych celów (zwłaszcza marketing bezpośredni własnych produktów lub usług pracodawcy oraz dochodzenie roszczeń tytułu prowadzonej działalności gospodarczej) realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

W decyzji z 5 lutego 2002 r. GIODO stwierdził, że „każda z przesłanek wymienionych w art. 23 ust. 1 ustawy ma charakter autonomiczny i niezależny, a spełnienie choćby jednej z nich, daje podstawę do przetwarzania danych osobowych"[10].

Pracodawca potrzebuje do przetwarzania danych zgody kandydatów do pracy w procesie rekrutacji. Jednak **nie dotyczy** to danych, których pracodawca może od nich żądać na podstawie Kodeksu pracy. Pracodawca nie musi zatem uzyskiwać zgody:

- **kandydata do pracy** – jeśli żąda podania wyłącznie następujących danych: imię (imiona) i nazwisko, imiona rodziców, data urodzenia, miejsce zamieszkania (adres do korespondencji), wykształcenie oraz przebieg dotychczasowego zatrudnienia oraz
- **pracownika** – gdy oprócz danych wymienionych powyżej, poprosi o inne dane osobowe pracownika, w tym nr PESEL, a także imiona i nazwiska oraz daty urodzenia jego dzieci, jeżeli podanie takich danych

[9] Sygnatura akt. I OSK 1476/10.
[10] GI-DEC-DS-23/02.

jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy.

Warto jednak zapoznać się z decyzją GIODO z 23 stycznia 2015 r.[11], w której GIODO podkreślił, że „(...) jeśli osoba ubiegająca się o zatrudnienie podaje w dokumentach rekrutacyjnych więcej informacji, niż wynika to z wymienionych przepisów prawa, wówczas podstawą prawną do ich przetwarzania przez potencjalnego pracodawcę jest zgoda tej osoby (czyli podstawa prawna art. 23 ust. 1 pkt 1 ustawy). Taka zgoda jest także wymagana, jeśli dane miałyby być przetwarzane nie tylko w celu rekrutacji, ale także np. w celach marketingowych".

Pracownik może w każdej chwili **wycofać zgodę** na przetwarzanie swoich danych. Sama zgoda ma być oświadczeniem woli, z którego ma jasno wynikać, że dana osoba przystała na przetwarzanie swoich danych i w jakim celu. Nie można jej domniemywać ani dorozumiewać z oświadczenia o innej treści (art. 7 pkt 5 ustawy o ochronie danych osobowych). GIODO uważa, że przy jej udzielaniu powinna być zagwarantowana opcjonalność, tj. osoba składająca oświadczenie powinna mieć możliwość wyrażenia zgody na określone działania albo jej niewyrażenia. Taki sam pogląd wyraził Naczelny Sąd Administracyjny w wyroku z 4 kwietnia 2003 r. (II SA 2135/02). Z kolei w wyroku z 25 listopada 2008 r. (I OSK 1743/07) sąd ten uznał, że jeżeli zgoda ma być wyrażona na wymaganym formularzu, formularz musi zawierać dokładne pouczenie o skutkach wyrażenia zgody, a ogólnikowe pouczenie przez odesłanie do ustawy o ochronie danych osobowych, takim pouczeniem nie jest.

7.1.7. OBOWIĄZKI PRACODAWCY

Na pracodawcy jako administratorze danych spoczywają pewne obowiązki względem pracowników i współpracowników.

W pierwszej kolejności pracodawca ma prawny obowiązek **zabezpieczyć** dane osobowe kandydatów do pracy i pracowników przed uszkodzeniem lub zniszczeniem oraz dostępem osób nieuprawnionych.

W celu wykonywania swoich obowiązków może powołać administratora bezpieczeństwa informacji (ABI). Dla administratora (pracodawcy) jest to o tyle wygodne, że w takim wypadku to ABI zapewnia przestrzeganie przepisów o ochronie danych osobowych.

Pracodawca nie musi także zgłaszać zbiorów danych do rejestracji w GIODO – robi to za niego administrator bezpieczeństwa informacji.

Ustawa wymaga, aby funkcję ABI sprawowała osoba, która łącznie spełnia następujące warunki:

1) ma pełną zdolność do czynności prawnych oraz korzysta z pełni praw publicznych,
2) posiada odpowiednią wiedzę w zakresie ochrony danych osobowych,
3) nie była karana za umyślne przestępstwo.

Sprawdzenie, czy kandydat spełnia te warunki, leży po stronie administratora (pracodawcy).

ABI musi podlegać bezpośrednio kierownikowi jednostki organizacyjnej lub osobie fizycznej będącej administratorem danych oraz musi mieć zapewnione środki i organizacyjną odrębność niezbędne do niezależnego wykonywania zadań z zakresu ochrony danych osobowych.

Powołanie ABI należy zgłosić GIODO w terminie 30 dni od dnia jego powołania. Na tej podstawie GIODO wpisuje ABI do rejestru ABI (art. 46b UODO).

Pracownik musi zostać **poinformowany** o tym, że jego dane są przetwarzane i w jakim celu jest to robione. Ustawa o ochronie danych osobowych nie precyzuje formy, w jakiej należy przekazać takie informacje. W związku z tym każda forma poinformowania, tj. ustna, telefoniczna, elektroniczna, pisemna (klauzula w dokumentach i formularzach), jest dopuszczalna. Za niepoinformowanie pracowników lub współpracowników o przysługujących im prawach wynikających z ustawy o ochronie danych osobowych grozi grzywna, kara ograniczenia wolności lub jej pozbawienia do roku (art. 54 ustawy o ochronie danych osobowych).

[11] DOLiS/DEC 41/15/5125.

Administratorzy danych osobowych są zwolnieni z obowiązków informacyjnych, gdy przepis innej ustawy niż UODO zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania oraz jeśli osoba, której dane dotyczą, otrzymała wcześniej informacje wymagane tą ustawą.

Ustawa o ochronie danych osobowych rozróżnia dwa rodzaje obowiązku informacyjnego w sytuacji, kiedy administrator danych zbiera je:

- w sposób bezpośredni od danej osoby (art. 24 UODO) oraz
- w postaci pośredniej, czyli np. od firmy rekrutacyjnej (art. 25 UODO).

Jeśli chodzi o bezpośredni sposób pozyskiwania danych pracownika należy poinformować o:

- **adresie** siedziby pracodawcy i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna – miejscu zamieszkania oraz imieniu i nazwisku,
- **celu zbierania danych**, a w szczególności o znanych pracodawcy w czasie udzielania informacji lub przewidywanych odbiorcach lub kategorii odbiorców danych,
- **prawie dostępu** pracownika do treści danych oraz ich **poprawiania**,
- **dobrowolności** albo **obowiązku** podania danych, a jeżeli taki obowiązek istnieje, pracodawca musi wskazać jego podstawy prawną.

Jeśli chodzi o pośredni sposób pozyskiwania danych, pracownika należy poinformować o:

- **adresie** siedziby pracodawcy i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna – miejscu zamieszkania oraz imieniu i nazwisku,
- **celu i zakresie** zbierania danych, a w szczególności pracodawca musi przekazać informacje o odbiorcach lub kategoriach odbiorców danych,
- **źródle danych**,
- **prawie dostępu** pracownika do treści danych oraz ich **poprawiania**,
- prawie wniesienia, w przypadkach wymienionych w art. 23 ust. 1 pkt 4 i 5 ustawy o ochronie danych osobowych, pisemnego, umotywowanego **żądania zaprzestania przetwarzania danych** ze względu na szczególną sytuację oraz prawo wniesienia sprzeciwu wobec przetwarzania danych w przypadkach wymienionych w art. 23 ust. 1 pkt 4 i 5 ustawy o ochronie danych osobowych, gdy administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania danych osobowych innemu administratorowi danych osobowych.

W dalszej kolejności należy stwierdzić, że pracodawca:

- jako administrator danych osobowych jest zobligowany do dołożenia szczególnej staranności w celu ochrony interesów osób, których dane dotyczą (art. 26 ust. 1 ustawy o ochronie danych osobowych),
- musi zapewnić, aby dane te były zbierane i przetwarzane zgodnie z prawem i celami, a także przechowywane jedynie tak długo, jak to jest konieczne (art. 26 ust. 1 ustawy o ochronie danych osobowych),
- jest zobowiązany zapewnić pracownikowi wgląd w jego dokumentację, udzielać wyjaśnień i zapewnić możliwość dokonywania modyfikacji (art. 32-35 ustawy o ochronie danych osobowych),
- powinien także zastosować środki techniczne i organizacyjne, które zablokują do nich dostęp osobom nieupoważnionym (art. 36 ust. 1 ustawy o ochronie danych osobowych),
- musi mieć pełną kontrolę nad procesem przetwarzania danych, czyli jakie dane zostały zgromadzone, przez kogo zostały wprowadzone do zbioru oraz komu są udostępnianie (art. 38 ustawy o ochronie danych osobowych).

Za niewłaściwe zabezpieczenie przetwarzanych danych osobowych przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, pracodawcy grozi grzywna, kara ograniczenia wolności albo pozbawienia wolności do roku. Natomiast za ich udostępnienie lub umożliwienie dostępu do nich osobom

nieupoważnionym grozi grzywna, kara ograniczenia wolności albo pozbawienia wolności do lat 2 lub roku – gdy pracodawca działał nieumyślnie.

Art. 37 UODO przewiduje, że do przetwarzania danych osobowych mogą być dopuszczone **wyłącznie** osoby posiadające upoważnienie nadane przez administratora danych. Przepis ten nie przewiduje żadnych wyłączeń, dlatego pracodawca powinien na piśmie upoważnić swojego pracownika (np. kadrową, księgową) do przetwarzania danych osobowych innych swoich pracowników.

Pracodawca ma obowiązek prowadzenia **ewidencji** osób upoważnionych do przetwarzania danych, o której mowa w art. 39 UODO. Ewidencja ta powinna zawierać imiona i nazwiska wszystkich osób upoważnionych przez administratora do wykorzystywania danych osobowych, daty nadania i ustania oraz zakres upoważnień do przetwarzania danych oraz identyfikatory odnośnie tych osób, które dopuszczone zostały do przetwarzania danych w systemach informatycznych.

Pracodawca może **powierzyć** przetwarzanie danych innemu podmiotowi w drodze umowy zawartej na piśmie (art. 31 ust. 1 UODO). Dotyczy to np. outsourcingu kadrowo-płacowego. W treści tej umowy pracodawca musi umieścić cel i zakres, w jakich dane mogą być przetwarzane przez podmiot, który przejmuje to zadanie od niego. Zdaniem GIODO powierzenie to nie wymaga zgody osoby, której dane dotyczą, ani jej informowania (decyzja z 11 września 2015 r., DIS/DEC-749/15/83430). Zgodnie z art. 7 pkt 6 ustawy o ochronie danych osobowych podmiot, któremu powierzono przetwarzanie danych osobowych, nie jest traktowany jako odrębny „odbiorca" danych.

7.2. ZMIANA PRZEPISÓW OD 25 MAJA 2018 R.

Na kwestię przetwarzania danych osobowych pracowników w RODO zostało poświęconych kilka osobnych przepisów. Między innymi w związku z ich treścią opracowano projekt zmian do Kodeksu pracy.

RODO pozostawiło w tym zakresie polskiemu ustawodawcy pewną dozę swobody. Może on bowiem zawrzeć bardziej szczegółowe przepisy mające zapewnić ochronę praw i wolności w przypadku przetwarzania danych osobowych pracowników w związku z zatrudnieniem w szczególności do celów rekrutacji, wykonania umowy o pracę, w tym wykonania obowiązków określonych przepisami lub porozumieniami zbiorowymi, zarządzania, planowania i organizacji pracy, równości i różnorodności w miejscu pracy, bezpieczeństwa i higieny pracy, ochrony własności pracodawcy lub klienta oraz do celów indywidualnego lub zbiorowego wykonywania praw i korzystania ze świadczeń związanych z zatrudnieniem, a także do celów zakończenia stosunku pracy.

Jeśli chodzi o zatrudnienie, to zmiany dotyczą przede wszystkim Kodeksu pracy, ale także ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe.

7.2.1. ZMIANY W KODEKSIE PRACY

Przepisy, które obecnie zawierają jedynie możliwość żądania określonych danych osobowych w stosunkach pracy, na skutek RODO zostają zmienione na **obowiązek** pobierania tych danych. Zmodyfikowany będzie katalog danych osobowych pobieranych od osoby ubiegającej się o zatrudnienie oraz pracownika. Przepisy zawierają również unormowanie zasad wyrażenia zgody przez osobę ubiegającą się o zatrudnienie lub pracownika na pobranie określonych danych osobowych przez pracodawcę (w przypadku pracownika chodzi np. o dane biometryczne). Nowością jest określenie przez ustawodawcę negatywnego katalogu danych, których pozyskanie nie może nastąpić nawet za zgodą osoby ubiegającej się o zatrudnienie lub pracownika.

Również to, o co od wielu lat zabiegali pracodawcy, ma szansę zostać unormowane po wejściu w życie RODO. Chodzi np. o monitoring pracowników. W projekcie zmian do Kodeksu pracy uregulowano bowiem instytucję monitoringu jako szczególną formę przetwarzania danych osobowych pracowników.

Wprowadzono także podstawę prawną (chodzi o zmianę w zakresie art. 229) do pozyskiwania i przechowywania przez pracodawcę skierowań na badania lekarskie oraz orzeczeń lekarskich wydawanych w wyniku tego skierowania, jeżeli osoba przyjmowana do pracy u innego pracodawcy posiada aktualne orzeczenie lekarskie stwierdzające brak przeciwskazań do pracy na danym stanowisku.

W kodeksie pracy zmiany dotyczą **5 artykułów**, w tym zostaną dodane **trzy nowe** przepisy.

1) Zamiana art. 22 [1] Kodeksu pracy

Przepis art. 22 [1] w § 1 normuje, jakie dane osobowe mogą być żądane od kandydatów do pracy. Zgodnie z projektem pracodawca będzie mógł żądać podania od osoby ubiegającej się o zatrudnienie danych osobowych obejmujących:

1) mię (imiona) i nazwisko;
2) datę urodzenia;
3) adres do korespondencji;
4) adres poczty elektronicznej albo numer telefonu;
5) wykształcenie;
6) przebieg dotychczasowego zatrudnienia.

Nowością jest zatem możliwość żądania adresu e-mail albo numeru telefonu. W praktyce w CV kandydaci sami podawali te dane. Jednocześnie z listy danych, których można żądać, zniknęły imiona rodziców kandydata.

Natomiast § 2 art. 22 [1] dotyczy już pracownika. Pracodawca będzie mógł żądać od pracownika podania danych osobowych obejmujących:

1) adres zamieszkania;
2) numer PESEL, a w przypadku jego braku – rodzaj i numer dokumentu potwierdzającego tożsamość;
3) inne dane osobowe pracownika, a także dane osobowe dzieci pracownika i innych członków jego najbliższej rodziny, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy.

W przypadku pracowników wprowadzono możliwość żądania – w przypadku braku numeru PESEL – danych o rodzaju i numerze innego dokumentu potwierdzającego tożsamość pracownika.

W dalszej kolejności zmianie ulegnie § 3 art. 22 [1], którego projekt stanowi, że „Udostępnienie pracodawcy danych osobowych następuje w formie oświadczenia osoby, której one dotyczą. Pracodawca żąda udokumentowania danych osobowych osób, o których mowa w § 1 i 2, **jeżeli uzna za konieczne ich potwierdzenie**". Zmieniła się ostatnia, podkreślona część tego przepisu.

Zmienione zostanie brzmienie następnego paragrafu art. 22 [1] § 4. Zgodnie z brzmieniem § 4 przetwarzanie danych osobowych, o których mowa w § 1–3, będzie możliwe tylko w zakresie niezbędnym do realizacji stosunku pracy. Zatem działy HR nie będą mogły robić żadnych statystyk na inne potrzeby niż wynikające wprost ze stosunku pracy, np. jaki profil kandydatów najchętniej aplikuje do pracy u danego pracodawcy.

Dosyć istotną zmianę wprowadza nowy § 5 art. 22 [1]. Zgodnie z nim przetwarzanie danych osobowych, uzyskanych na podstawie § 1 pkt 3 i 4 po nawiązaniu stosunku pracy, jest możliwe tylko w przypadku, gdy pracownik wyrazi na to zgodę, o której mowa w art. 22 [2] § 1. Zatem adres e-mail oraz prywatny numer telefonu pobrany od kandydata do pracy pracodawca będzie mógł przetwarzać po jego zatrudnieniu tylko za zgodą tego pracownika.

2) Nowy przepis art. 22 [2] Kodeksu pracy

Po art. 22 [1] w projekcie ustawy nowelizującej Kodeks pracy znajdują się aż trzy nowe artykuły – art. 22 [2]-22 [4]. Nowy art. 22 [2] składa się z 6 paragrafów.

Przepis § 1 ma otrzymać następujące brzmienie:

„§ 1. Przetwarzanie przez pracodawcę innych danych osobowych niż wymienione w art. 22 [1] § 1 i 2 jest dopuszczalne tylko wtedy, gdy dotyczą one stosunku pracy i osoba ubiegająca się o zatrudnienie lub pracownik wyrazi na to zgodę w oświadczeniu złożonym w postaci papierowej lub elektronicznej".

Oznacza to, że dane osobowe inne niż:

1) imię (imiona) i nazwisko;
2) data urodzenia;
3) adres do korespondencji;
4) adres poczty elektronicznej albo numer telefonu;
5) wykształcenie;
6) przebieg dotychczasowego zatrudnienia;
7) adres zamieszkania;
8) numer PESEL, a w przypadku jego braku – rodzaj i numer dokumentu potwierdzającego tożsamość;
9) dane osobowe pracownika, a także dane osobowe dzieci pracownika i innych członków jego najbliższej rodziny konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy,

będą mogły być przetwarzane przez pracodawcę tylko za zgodą pracownika wyrażoną w formie elektronicznej (np. podane w mailu z informacją o wyrażonej zgodzie na ich przetwarzanie) lub pisemnej.

Przepis art. 22 [2] Kodeksu pracy w § 2 reguluje kwestię danych biometrycznych. Według obecnego projektu brzmi on następująco: „§ 2. Przetwarzanie przez pracodawcę danych biometrycznych obejmuje tylko dane osobowe pracownika, jeśli dotyczą one stosunku pracy i pracownik wyrazi na to zgodę w oświadczeniu złożonym w postaci papierowej lub elektronicznej".

Definicja **danych biometrycznych** jest zawarta w RODO w art. 4. Zgodnie z RODO, dane biometryczne to dane osobowe wynikające ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, taką jak wizerunek twarzy lub dane daktyloskopijne. Co do zasady, przetwarzanie takich danych będzie zabronione, jednakże RODO zawiera wyjątki od tej zasady, w tym m.in. wyraźną i dobrowolną zgodę podmiotu, którego dane dotyczą.

Możliwe będzie np. pobranie odcisku palca, który zastąpi często dziś stosowaną kartę magnetyczną uprawniającą do wejścia na teren zakładu pracy i który jednocześnie pozwoli na kontrolę czasu pracy. Będzie to możliwe, ale za **zgodą pracownika**. Zgoda ta nie może być dorozumiana – ma być wyrażona w formie pisemnej lub elektronicznej. Dane biometryczne nie mogą być pobierane od kandydata do pracy. Nie ma bowiem uzasadnienia, dla pozyskiwania danych biometrycznych od osób ubiegających się o zatrudnienie. Przepisy odrębne mogą również zobowiązywać do gromadzenia np. danych biometrycznych, a wówczas wyłączona będzie konieczność pozyskania zgody na ich gromadzenie.

Przepis art. 22 [2] § 3 statuuje kwestię zgody pracownika na przetwarzanie innych danych osobowych niż wskazane w art. 22 [1] Kodeksu pracy oraz danych biometrycznych, wprowadzając normę ochronną: „§ 3. Brak zgody, o której mowa w § 1 i 2, nie może być podstawą niekorzystnego traktowania osoby ubiegającej się o zatrudnienie lub pracownika, a także nie może powodować wobec nich jakichkolwiek negatywnych konsekwencji, zwłaszcza nie może stanowić przyczyny uzasadniającej odmowę zatrudnienia, wypowiedzenia stosunku pracy lub jego rozwiązania bez wypowiedzenia przez pracodawcę".

Paragraf ten nie wymaga szerszego komentarza – wprowadza on po prostu ochronę stosunku pracy z powodu odmowy wyrażenia zgody na udostępnienie i przetwarzanie danych osobowych innych niż wymienione w art. 22 [1] § 1 i 2 Kodeksu pracy.

Kolejny paragraf art. 22 [2] brzmi następująco: „§ 4. Przetwarzanie, o którym mowa w § 1 i 2, dotyczy danych osobowych udostępnianych na wniosek pracodawcy lub danych osobowych przekazanych pracodawcy z inicjatywy osoby ubiegającej się o zatrudnienie lub pracownika".

Oznacza to, że dane osobowe pracownika mają być udostępniane na wniosek pracodawcy lub z inicjatywy osoby, której dotyczą. Nie mogą być pozyskane od osób trzecich. Wyobraźmy sobie grupę kapitałową. W spółce matce pracownik ma umowę o pracę i pracuje na 1/2 etatu. Spółka córka chce go zatrudnić na drugą połowę etatu. Dane osobowe tego pracownika musi pozyskać od niego bezpośrednio, a nie od spółki matki.

Kolejnym paragrafem w nowym art. 22 [2] jest paragraf 5. Ustawodawca wprowadza w nim katalog danych, które nie mogą być przetwarzane nawet za zgodą osoby, której dane dotyczą. Ich gromadzenie możliwe będzie więc wyłącznie w przypadkach, gdy jest to konieczne dla wypełnienia obowiązku wynikającego z przepisu prawa. Chodzi o następujące dane osobowe:

1) o nałogach;
2) o stanie zdrowia;
3) o życiu seksualnym lub orientacji seksualnej.

Ponadto jest konieczne zapewnienie szczególnych warunków technicznych gromadzenia danych biometrycznych, które zawierać będzie rozporządzenie wydane przez ministra właściwego do spraw informatyzacji. Dlatego też Minister właściwy do spraw informatyzacji określi, w drodze rozporządzenia, sposób gromadzenia danych biometrycznych, uwzględniając zapewnienie ochrony przetwarzanych danych biometrycznych odpowiedniej do zagrożeń. Stanowi o tym ostatni – 6 paragraf art. 22 [2].

3) Nowy przepis art. 22 [3] Kodeksu pracy

Kolejnym nowym artykułem jest art. 22 [3] o treści następującej:

„§ 1 Pracodawca żąda podania danych osobowych:

1) innych niż określone w art. 22 [1] § 1 i 2,
2) wskazanych w art. 22 [2] § 2 i 5

– jeżeli obowiązek ich podania wynika z odrębnych przepisów lub gdy jest to niezbędne do wypełniania obowiązku pracodawcy nałożonego przepisem prawa.

§ 2. Przetwarzanie danych osobowych, o których mowa w § 1, jest możliwe tylko w zakresie niezbędnym do realizacji tego obowiązku".

Chodzi np. o karalność kandydatów do pracy – będzie możliwe pozyskanie takich danych tylko wtedy, kiedy w stosunku do określonej grupy zawodowej pozwala na to odrębny przepis.

4) Nowy przepis art. 22 [4] Kodeksu pracy

W kolejnym nowym przepisie ustawodawca wyszedł naprzeciw oczekiwaniom pracodawców i uregulował instytucję monitoringu. Korzystając z możliwości wprowadzenia przez państwo członkowskie przepisów szczególnych dotyczących przetwarzania danych osobowych w zatrudnieniu (art. 88 RODO), w przepisach prawa pracy wprowadzona została instytucja „monitoringu" jako szczególna forma przetwarzania danych osobowych pracowników.

Treść nowego art. 22 [4] Kodeksu pracy jest następująca:

§ 1. Dla zapewnienia bezpieczeństwa pracowników lub ochrony mienia lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę, pracodawca podejmuje decyzję o wprowadzeniu szczególnego nadzoru nad miejscem pracy lub terenem wokół zakładu pracy w postaci środków technicznych umożliwiających rejestrację obrazu (monitoring), jeżeli uzna to za koniczne. Monitoring nie może stanowić środka kontroli wykonywania pracy przez pracownika.

§ 2. Monitoring nie obejmuje pomieszczeń, które nie są przeznaczone do wykonywania pracy, w szczególności pomieszczeń sanitarnych, szatni, stołówek lub palarni.
§ 3. Dane osobowe uzyskane w wyniku zastosowania monitoringu pracodawca przetwarza wyłącznie do celów, dla których zostały zebrane i przechowuje przez okres niezbędny dla realizacji tych celów.
§ 4. Pracodawca informuje pracowników o wprowadzeniu monitoringu, w sposób przyjęty u danego pracodawcy nie później niż 14 dni przed uruchomieniem monitoringu. Pracodawca przed dopuszczeniem pracownika do pracy informuje go o stosowaniu monitoringu."

Z treści nowego art. 22 [4] Kodeksu pracy wynika, że wyłączną przesłanką wprowadzenia monitoringu jest bezpieczeństwo pracowników lub ochrona mienia lub zachowanie w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę. Wystarczy spełnienie jednej z nich, aby można było wprowadzić monitoring. Monitoring nie będzie obejmował wszystkich pomieszczeń. Kwestie związane z monitoringiem należy unormować np. w regulaminie pracy, a gdy nie ma obowiązku wydania go, to w obwieszczeniu albo w innej formie zwyczajowo przyjętej w danym zakładzie pracy. Pracownik musi wiedzieć o wprowadzeniu monitoringu z 14-dniowym wyprzedzeniem.

5) Nowa treść art. 229 Kodeksu pracy

Trudno jest obecnie pisać o zmianach w zakresie art. 229 Kodeksu pracy, gdyż ustawodawca na obecnym etapie legislacyjnym pomylił jednostki redakcyjne tego przepisu. Niemniej poniżej przedstawiono brzmienie zmian w ich, jak się wydaje, właściwej postaci.

W art. 229 dotyczącym badań lekarskich:
a) § 1 [1] pkt 2 otrzymuje brzmienie:
„2) przyjmowane do pracy u innego pracodawcy na dane stanowisko w ciągu 30 dni po rozwiązaniu lub wygaśnięciu poprzedniego stosunku pracy, **jeżeli posiadają aktualne orzeczenie lekarskie stwierdzające brak przeciwwskazań do pracy w warunkach pracy opisanych w skierowaniu na badania lekarskie i pracodawca ten stwierdzi, że warunki te odpowiadają warunkom występującym na danym stanowisku pracy, z wyłączeniem osób przyjmowanych do wykonywania prac szczególnie niebezpiecznych**".

Obecnie pracownik ma przedstawić to orzeczenie lekarskie pracodawcy. Nastąpiła zmiana jednego wyrazu – czasownik „przedstawić" zamieniono na „posiadać" oraz spójnika (z „a" na „i").

Dalsze zmiany art. 229 Kodeksu pracy dają pracodawcy prawo do żądania aktualnego orzeczeń lekarskich od konkretnych kategorii pracowników oraz skierowań na badania będące podstawą wydania takiego orzeczenia i przechowywania ich.
b) po § 1[2] dodaje się § 1[3] w brzmieniu:
„§ 1[3]. Pracodawca żąda od osoby, o której mowa w § 1 [1] pkt 2 oraz w § 1 [2], aktualnego orzeczenia lekarskiego stwierdzającego brak przeciwwskazań do pracy na danym stanowisku oraz skierowania na badania będące podstawą wydania tego orzeczenia."

Zgodnie z tą zmianą pracodawca żąda od osoby przyjmowanej, w ciągu 30 dni po rozwiązaniu lub wygaśnięciu poprzedniego stosunku pracy, do pracy na dane stanowisko, a także od osoby, która aktualnie pozostaje w stosunku pracy z innym pracodawcą, orzeczenia lekarskiego stwierdzającego brak przeciwwskazań do pracy na danym stanowisku oraz skierowania na badania będące podstawą wydania tego orzeczenia.
c) § 7 otrzymuje brzmienie:
„§ 7. Pracodawca przechowuje orzeczenia wydane na podstawie badań lekarskich, o których mowa w § 1, 2 i 5, orzeczenia i skierowania uzyskane na podstawie § 1[3] oraz skierowania, o których mowa w § 4a."

Do Kodeksu pracy wprowadzono zmianę polegającą na dodaniu podstawy prawnej do przechowywania przez pracodawcę konkretnych skierowań i orzeczeń lekarskich. Ponieważ w projekcie zmian dodano § 1[3] to również i określone tym paragrafem orzeczenia lekarskie i skierowania na badania pozyskiwane

od konkretnej kategorii pracowników będzie można przechowywać. Nadto pracodawca ma podstawę prawną do przechowywani skierowań wystawionych przez niego na badania wstępne, okresowe i kontrolne.
d) po § 7 dodaje się § 7[1] w brzmieniu:
„§ 7[1]. W przypadku stwierdzenia, że warunki określone w skierowaniu, o którym mowa w § 1[3], nie odpowiadają warunkom występującym na danym stanowisku pracy, pracodawca zwraca osobie przyjmowanej do pracy to skierowanie oraz orzeczenie lekarskie wydane w wyniku tego skierowania".

Pracodawca nie ma podstawy prawnej do przechowywania u siebie skierowania oraz orzeczenia lekarskiego od osoby przyjmowanej w ciągu 30 dni po rozwiązaniu lub wygaśnięciu poprzedniego stosunku pracy, do pracy na dane stanowisko, a także od osoby, która aktualnie pozostaje w stosunku pracy z innym pracodawcą, jeżeli nie odpowiadają one potrzebom pracodawcy na danym stanowisku pracy.

7.3. ZMIANY W PRAWIE BANKOWYM

RODO spowodowało istotną zmianę dla pracowników i kandydatów do pracy w banku. Otóż do ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe wprowadzono art. 13c o brzmieniu następującym:
„1. W przypadku pracownika i osoby ubiegającej się o zatrudnienie na stanowisku umożliwiającym dostęp do danych dotyczących banku lub klientów banku, bank może żądać od pracownika i tej osoby przedłożenia informacji dotyczących karalności, w tym informacji czy ich dane osobowe są zgromadzone w Krajowym Rejestrze Karnym.
2. Bank ma prawo żądać od pracownika danych biometrycznych, w szczególności w postaci odcisków palców, głosu, obrazu rogówki i sieci żył palców, jeżeli podanie takich danych jest konieczne ze względu na kontrolę dostępu do informacji przetwarzanych przez bank i pomieszczeń.
3. Bank ma prawo przechowywania informacji i danych, o których mowa w ust. 1 i 2, wyłącznie przez okres zatrudnienia pracownika.
4. Przepis ust. 1 i 3 stosuje się odpowiednio do osoby ubiegającej się o zatrudnienie u przedsiębiorcy lub przedsiębiorcy zagranicznego, o których mowa w art. 6a ust. 1."

Jak czytamy w uzasadnieniu do projektu ustawy Przepisy wprowadzające ustawę o ochronie danych osobowych: „W związku ze szczególnym charakterem działalności jaką prowadzą banki i powszechnym korzystaniem z usług finansowych świadczonych przez banki, pożądanym jest zapewnienie adekwatnej ochrony informacji powierzanych podmiotom świadczącym tego typu usługi.

Proponuje się zatem wprowadzenie do przepisów Prawa bankowego postanowień, które dawałyby bankom podstawę prawną do pozyskiwania i przetwarzania danych o niekaralności pracowników zatrudnianych na określonych stanowiskach. Należy wskazać, że w obecnym stanie prawnym przepisy prawa pracy nie dają pracodawcom instrumentów, aby politykę bezpieczeństwa informacji poufnych wdrażać już na etapie doboru pracowników. Mając na uwadze, że osoby zatrudnione przez banki mają bezpośredni dostęp do danych objętych ochroną, zasadnym jest zachowanie szczególnej ostrożności przy doborze kadry. Intencją regulacji jest zminimalizowanie ryzyka zatrudnienia osoby, która mogłaby mieć zamiar wykorzystania przedmiotowego dostępu w celach nieuczciwych.

Ponadto, w celu zapobieżenia przed dostępem nieuprawnionych osób do informacji przetwarzanych przez bank i pomieszczeń, regulacje w art. 13c stwarzają możliwość żądania od pracownika danych biometrycznych, co pozwoli na kontrolę dostępu do ww. informacji. Należy jednocześnie zwrócić uwagę, że umożliwienie instytucjom finansowym korzystania z nowoczesnych rozwiązań w zakresie identyfikacji pracowników stanowi istotną przesłankę w związku rozwojem nowoczesnych form komunikacji oraz stosowanych zabezpieczeń. Uwzględniając, że banki mogą, w drodze umowy agencyjnej, powierzyć wykonywanie określonych czynności objętych działalnością banku przedsiębiorcom krajowym lub zagranicznym, przewidziano również możliwość żądania informacji dotyczącej niekaralności od osób ubiegających się o zatrudnienie (a także pracowników) u tych przedsiębiorców (art. 13c ust. 4)".

O AUTORACH

Wojciech Dziomdziora

Radca prawny, *counsel* w kancelarii Domański Zakrzewski Palinka. Jest specjalistą w zakresie prawa telekomunikacji i nowych technologii, prawa autorskiego, mediów, rynków regulowanych, ochrony informacji oraz prawa ochrony konkurencji i konsumentów. Doradza wiodącym firmom medialnym, informatycznym, telekomunikacyjnym i innym. Wspiera przedsiębiorców, szczególnie z branży mediów, telekomunikacji, IT i gospodarki elektronicznej w procesach regulacyjnych (reprezentacja przed UKE, KRRiT, UOKiK) oraz legislacyjnych. W latach 2006–2007 był członkiem KRRiT. Wcześniej pracował w TVN, w MKiDN, gdzie był dyrektorem Departamentu Prawnego oraz w Kancelarii Prezesa Rady Ministrów. Jest pełnomocnikiem Zarządu Polskiej Izby Informatyki i Telekomunikacji ds. ochrony danych osobowych i zarządzania informacją. Jest arbitrem Komisji Prawa Autorskiego. Członek Rady Konsultacyjnej Polskiej Izby Komunikacji Elektronicznej. Członek Okręgowej Izby Radców Prawnych w Warszawie.

Bartosz Mendyk

Doktor nauk prawnych, absolwent Wydziału Prawa i Administracji UW. Opublikował kilkadziesiąt prac dotyczących bezpieczeństwa informacji w prasie popularnej oraz naukowej. Współpracuje z kilkunastoma instytutami i podmiotami prywatnymi w zakresie doradztwa. Prowadzi szkolenia z obszaru ochrony danych osobowych.

Sylwia Stefaniak

Paralegal w dziale Corporate, External & Legal Affairs w firmie Microsoft. Jest odpowiedzialna za koordynację lokalnych wymagań prawnych w krajach z Europy Centralnej i Wschodniej (Polska, Węgry, Rumunia, Bułgaria, Mongolia) w kontekście wdrożenia usług chmury obliczeniowej. Doświadczenie zawodowe zdobywała we współpracy z uczelniami wyższymi oraz ze szkoleniowymi centrami Microsoft. Większość prowadzonych przez nią projektów dotyczyło dostarczania usług chmury obliczeniowej, w tym we wdrażaniu lokalnych wymagań prawnych. Zaowocowało to zdobyciem doświadczenia przy prowadzeniu projektów badawczych, szkoleniowych oraz testów bezpieczeństwa.

Halszka Suszek-Borowska

Prawnik i psycholog śledczy. Od 7 lat związana z branżą informatyczną. Doświadczenie zawodowe zdobywała w Polsko-Japońskiej Akademii Technik Komputerowych. Większość prowadzonych przez nią działań skupiało się na rozwiązaniach prawnych w szkolnictwie wyższym oraz prowadzeniu projektów badawczych w dziedzinie informatyki. Dodatkowo od prawie trzech lat prowadzi tam wykłady Prawo w biznesie. W firmie Microsoft prowadzi i rozwija projekt House of Cloud. Ma on na celu utrzymanie jednolitej bazy wiedzy zawierającej informacje pozwalające na szybką odpowiedź na pytania klientów dotyczące polskich wymagań prawnych i organizacyjnych związanych z wdrożeniem usług chmury publicznej, a także podnoszenie naszej wiedzy dotyczącej tych zagadnień.

Olga Budziszewska

Absolwentka kryminologii na Uniwersytecie Warszawskim oraz Zarządzania Bezpieczeństwem Informacji w Instytucie Organizacji i Zarzadzania w Przemyśle, Certyficate Information System Manager. Od 12 lat związana z cyberbezpieczeństwem i zarządzaniem bezpieczeństwem informacji. Od 4 lat pracuje w Microsoft, wspierając wdrożenia projektów w chmurze obliczeniowej Microsoft Azure. Jako Cybersecurity Assurance Manager pomaga jednostkom samorządu terytorialnego oraz organizacjom edukacyjnym w bezpiecznej transformacji cyfrowej.

Małgorzata Regulska-Cieślak

Radca prawny, obecnie prowadzi indywidualną praktykę zawodową w Warszawie. Jest współautorką publikacji książkowych pt. „Kadry i płace w instytucjach kultury" (2012 r.), „Wzory dokumentów w instytucjach kultury" (2013 r.), „Kadry i płace w instytucjach kultury" (2016 r.) oraz autorką publikacją „Związki zawodowe w zakładzie pracy" (2013 r.). Doświadczenie zawodowe zdobyła, pracując w kancelariach prawnych, największych spółkach kapitałowych w Polsce oraz świadcząc wszechstronną pomoc prawną osobom fizycznym, korporacjom oraz instytucjom kultury. Na co dzień uczestniczy w sporach sądowych z zakresu prawa pracy, sporządza opinie z zakresu prawa pracy oraz projekty wewnątrzzakładowych aktów prawa pracy. Artykuły autorstwa Małgorzaty Regulskiej-Cieślak ukazały się w Gazecie Małych i Średnich Przedsiębiorstw, w Prawie Spółek, w Biuletynie Euro Info oraz innych czasopismach. Od września 2016 r. aktywnie prowadzi blog www.umowyzpracownikiem.pl dotyczący wszelkich umów zawieranych z pracownikami w ramach stosunku pracy.

enterprise europe network

Wsparcie dla biznesu w zasięgu ręki

Sieć Enterprise Europe Network funkcjonuje od 1 stycznia 2008 r. Została powołana w ramach Programu Ramowego na rzecz Konkurencji i Innowacji (CIP), a w perspektywie finansowej Unii Europejskiej na lata 2014-2020 funkcjonuje w ramach Programu na rzecz konkurencyjności przedsiębiorstw oraz małych i średnich przedsiębiorstw (COSME) oraz Horyzont 2020.

Sieć oferuje małym i średnim przedsiębiorstwom (MŚP) kompleksowe usługi, które mają im pomóc w pełni rozwinąć ich potencjał i zdolności innowacyjne oraz wesprzeć w pozyskaniu nowych partnerów biznesowych. Enterprise Europe Network jest także pośrednikiem umożliwiającym instytucjom Unii Europejskiej pełniejszą orientację w potrzebach małych i średnich przedsiębiorstw.

Na całym świecie działa około 600 ośrodków Enterprise Europe Network oferujących bezpłatne wsparcie dla przedsiębiorców w postaci kompleksowych usług informacyjnych, szkoleń i doradztwa z zakresu prawa i polityk Unii Europejskiej, prowadzenia działalności gospodarczej w Polsce i za granicą, zamówień publicznych, ochrony danych osobowych, udziału w programach ramowych UE itd.

Ośrodki Enterprise Europe Network są afiliowane przy rozmaitych organizacjach wspierających rozwój gospodarczy, takich jak izby przemysłowo-handlowe, agencje rozwoju regionalnego czy centra wspierania przedsiębiorczości. Źródłem finansowania działalności ośrodków Sieci są środki unijne oraz fundusze pochodzące z budżetu państwa.

Największa na świecie sieć wspierająca MŚP w internacjonalizacji. Ponad 60 państw, 600 organizacji, 3000 ekspertów.

Powiązanie międzynarodowego doświadczenia ze znajomością lokalnych rynków. 30 ośrodków w Polsce, co najmniej 1 w każdym województwie, współpraca regionalnych ekspertów z ogólnoświatową siecią wspierającą MŚP.

Wsparcie w rozwoju biznesu dzięki zindywidualizowanej pomocy, dostępowi do finansowania i nowym partnerom biznesowym.

Zasada „zawsze właściwych drzwi”, która w praktyce oznacza nieodsyłanie przedsiębiorcy bez udzielenia mu niezbędnych informacji.

Ośrodek Enterprise Europe Network
Polska Agencja Rozwoju Przedsiębiorczości
ul. Pańska 81/83
00-834 Warszawa

e-mail: coordinator_cpbsn@parp.gov.pl
www.een.org.pl
tel. + 48 22 432 71 02, faks + 48 22 432 70 46
czynny w godz. 8:30–16:30

Polska Agencja Rozwoju Przedsiębiorczości (PARP) jest agencją rządową, która została powołana w 2000 r. do wspierania rozwoju mikro, małych i średnich przedsiębiorstw. Przez 16 lat działalności Agencja wypracowała wiele form wsparcia, które obejmują finansowanie przedsiębiorstw, usługi rozwojowe, działalność edukacyjną i informacyjną oraz działania na rzecz budowy kultury przedsiębiorczości i innowacyjności w Polsce. Obszary działalności PARP rozwijają się wraz z rozwojem gospodarczym i wyłanianiem się nowych trendów w przedsiębiorczości i innowacyjności. Tym samym PARP na przestrzeni lat stała się prekursorką w tworzeniu wielu nowych obszarów wsparcia i opracowywaniu zróżnicowanych sposobów udzielania pomocy (finansowanie, edukacja, promocja). Stymulowaniu przedsiębiorczości, innowacyjności i konkurencyjności polskich przedsiębiorców służą nowe instrumenty perspektywy finansowej Unii Europejskiej 2014–2020. PARP jest zaangażowana w realizację trzech programów operacyjnych współfinansowanych ze środków europejskich: Inteligentny Rozwój, Polska Wschodnia, Wiedza Edukacja Rozwój.

Aktywność PARP koncentruje się na pięciu obszarach:

- rozwoju przedsiębiorstw i przedsiębiorczości, przez wspieranie rozwoju nowych pomysłów i modeli biznesowych,
- innowacyjności przedsiębiorstw, przez inicjowanie i kompleksowe wspieranie aktywności przedsiębiorstw w tym obszarze,
- ekspansji międzynarodowej przedsiębiorstw, przez wsparcie przedsiębiorców sektora MSP we wchodzeniu na zagraniczne rynki,
- współpracy wśród przedsiębiorstw i otoczenia biznesu, a więc wsparciu budowania powiązań między nimi,
- tworzenia przyjaznej i innowacyjnej administracji, przez pomoc w kreowaniu polityki innowacyjnej państwa oraz rozwijanie i promowanie takich rozwiązań w sektorze publicznym.

PARP

www.parp.gov.pl

Polska Agencja Rozwoju Przedsiębiorczości
ul. Pańska 81/83
00-834 Warszawa
telefon: 22 432 80 80
fax: 22 432 86 20
e-mail: info@parp.gov.pl

Informatorium PARP
e-mail: biuro@parp.gov.pl
telefon: 22 432 89 91-93

ISBN 978-83-7633-362-5