KRAJOWA IZBA DORADCÓW PODATKOWYCH

KRAJOWA RADA DORADCÓW PODATKOWYCH

INFORMATOR

Ochrona danych osobowych przez doradcę podatkowego po wejściu w życie RODO

Opracowany przez:

Komisję do spraw opracowania Kodeksu Postępowania Krajowej Izby Doradców Podatkowych w zakresie danych osobowych

Warszawa, dnia 20 kwietnia 2018 r.

KRAJOWA IZBA DORADCÓW PODATKOWYCH

ul. Bitwy Warszawskiej 1920 roku nr 3/310, 02-362 Warszawa, NIP 526-26-10-268

tel. (22) 578 50 00, fax (22) 578 50 09, biuro@kidp.pl, www.kidp.pl

1 Spis treści

2 Podstawa prawna

Niniejszy Informator sporządzono w oparciu o następujące akty prawne:

(i) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1), zwane dalej: **RODO**;

(ii) Projekt Ustawy o ochronie danych osobowych z dnia 5 kwietnia 2018 r. (Druk Sejmowy Sejmu VIII Kadencji nr 2410);

(iii) Projekt Ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679 z dnia 28 marca 2018 r.

(iv) Ustawę z dnia 5 lipca 1996 r. o doradztwie podatkowym (t.j. Dz. U. z 2018 r. poz. 377), zwaną dalej: **DorPodU**.

3 Zagadnienia wstępne

3.1 Wprowadzenie

RODO, a właściwie 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) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1) ustanawia na terenie całej Unii Europejskiej zasady oraz przepisy o ochronie danych osobowych osób fizycznych.

Jako rozporządzenie unijne RODO nie wymaga wdrożenia, ani implementacji, a jego postanowienia są stosowane w polskim porządku prawnym bezpośrednio. Oznacza to, że poza niewielkimi wyjątkami, postanowienia RODO będą źródłem podstawowych zasad oraz wymogów dotyczących ochrony danych osobowych w Polsce. Choć polski ustawodawca podjął już działania zmierzające do uchwalenia polskiej ustawy o ochronie danych osobowych[1] - polska ustawa będzie określała wyłącznie pewne detale, takie jak organ właściwy do nadzoru nad RODO, czy szczegółowe zasady prowadzenia kontroli w sprawie ochrony danych osobowych.

Postanowienia RODO zaczną obowiązywać wszystkich przedsiębiorców (w tym doradców podatkowych) od 25 maja 2018 r. Po tej dacie wszystkie podmioty przetwarzające dane w charakterze innym niż prywatny, czy rodzinny – będą zobligowani do zapewnienia przetwarzania danych osobowych na zasadach zgodnych z RODO.

3.2 Zakres zastosowania RODO

Postanowienia RODO wiążą i obowiązują każdego przedsiębiorcę, który prowadzi działalność na terytorium Unii Europejskiej, niezależnie od formy Jej prowadzenia. Co istotne, nie ma przy tym znaczenia, czyje dane podlegają przetwarzaniu (RODO ustala również standardy ochrony danych osobowych osób nieposiadających obywatelstwa kraju członkowskiego), ani gdzie dane są przechowywane.

[1] W dacie sporządzania niniejszego Informatora projekt Ustawy o ochronie danych osobowych był na etapie pierwszego czytania w Sejmie.

Zakres wyłączeń z zastosowania RODO jest stosunkowo niewielki. Zgodnie z art. 2 ust. 2 RODO Rozporządzenie nie ma zastosowania do przetwarzania danych osobowych:

(i) **w ramach działalności nieobjętej zakresem prawa Unii**;

(ii) przez państwa członkowskie w ramach wykonywania działań wchodzących w zakres tytułu V rozdział 2 TUE;

(iii) **przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze**;

(iv) przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom.

Z perspektywy podmiotu prywatnego najważniejsze pozostają wyłączenia, o których mowa w pkt. (i) i (iii) powyżej. Na ich mocy spod RODO wyłączona została działalność pozostająca bez związku z działalnością zawodową lub handlową[2], jak również sektory wyłączone spod jurysdykcji Unii Europejskiej[3].

W efekcie - doradcy podatkowi, przetwarzający dane osobowe w związku z prowadzoną działalnością zawodową będą zobligowani do wdrożenia i przetwarzania danych osobowych zgodnie z wymogami RODO. Co ważne – RODO będzie miało zastosowanie do przetwarzania przez doradców podatkowych danych osobowych **zarówno w sposób zautomatyzowany, jak i w sposób inny niż zautomatyzowany** [art. 2 ust. 2 RODO]. Oznacza to, że ochrona danych osobowych będzie musiała zostać zapewniona między innymi w ramach:

(i) przechowywania danych osobowych na serwerze kancelarii, w tym w przypadku korzystania z serwera zewnętrznego (chmury);

(ii) w ramach obiegu dokumentów w kancelarii;

(iii) w zakresie odbierania i wysyłania poczty elektronicznej, w tym wewnątrz kancelarii;

(iv) ochrony danych osobowych pracowników kancelarii, jak i danych osobowych pracowników Klientów;

[2] Np. ustalenie listy gości na przyjęcie, przechowywanie prywatnych numerów telefonu na komórce, etc.

[3] Takie jak bezpieczeństwo narodowe, czy obronność.

(v) przetwarzania danych osobowych w programie księgowym.

Dane osobowe podlegają ochronie bez względu na to, czy ostatecznie znajdą się w zbiorze danych osobowych. Oznacza to, że dane osobowe będą podlegały ochronie już od momentu ich zgromadzenia, niezależnie od tego, czy dane te będą przez doradcę wykorzystywane stale, czy incydentalnie.

RODO będzie chroniło dane osobowe osoby fizycznej niezależnie od tego, czy w danym przypadku będzie występowała jako konsument. Ochronie będą zatem podlegały również dane przedsiębiorców, czy przedstawicieli spółek, z którymi doradcy podatkowi współpracują wyłącznie na stopie zawodowej.

3.3 Czynności podlegające RODO

RODO będzie miało zastosowanie do czynności przetwarzania danych osobowych. Zawarta w art. 4 pkt 2 RODO definicja przetwarzania ma bardzo szeroki charakter i będzie oznaczała w zasadzie każdą operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych. Jak wspomniano powyżej, operacjami przetwarzania danych osobowych będą zarówno czynności zautomatyzowane (przy wykorzystaniu systemów informatycznych), jak i w inny sposób („na papierze" – w formie wydruków, akt, dokumentów, czy korespondencji papierowej).

RODO nie zawiera zamkniętego katalogu czynności składających się na przetwarzanie danych osobowych. Wskazuje jednak na stosunkowo szeroki katalog czynności takich jak: zbieranie danych, porządkowanie danych, przechowywanie danych, ich adaptowanie lub modyfikowanie, ale również - przeglądanie, wykorzystywanie (np. w toku pracy nad aktami sprawy, lub w ramach obsługi księgowej klienta), ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, usuwanie lub niszczenie.

UWAGA

Doradca podatkowy prowadzący księgi klienta może gromadzić i przechowywać dane osobowe pracowników/kontrahentów klienta nawet, gdy nie prowadzi obsługi płacowo-kadrowej. W takim przypadku gromadzenie i przechowywanie danych osobowych pracowników/kontrahentów klienta będzie przetwarzaniem danych osobowych.

3.4 Pojęcie danych osobowych

3.4.1 Definicja danych osobowych i podstawowe informacje

Definicja danych osobowych zawarta w art. 4 ust. 4 RODO jest bardzo szeroka. Zgodnie z RODO „dane osobowe" oznaczają **informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej** („osobie, której dane dotyczą"). Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować (której tożsamość znamy i którą możemy wskazać spośród innych osób), 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. Osobą możliwą do zidentyfikowania jest taka osoba, której tożsamości nie znamy, ale możemy poznać, korzystając z tych środków lub danych, które są dla nas dostępne.

W tym kontekście zakres danych osobowych jest bardzo szeroki i obejmie wszystkie informacje o charakterze osobowym, które mogą pomóc nam zidentyfikować daną osobę. Danymi osobowymi będą bowiem zarówno imię i nazwisko, czy PESEL osoby fizycznej, ale również:

(i) data urodzenia;
(ii) adres zamieszkania;
(iii) numer telefonu (w tym służbowy), czy adres e-mail (również służbowy);
(iv) płeć, kolor oczu, waga, wzrost lub inne dane biometryczne wskazujące na właściwości biologiczne danej osoby.

Choć RODO nie ma dotyczyć przetwarzania danych dotyczących osób prawnych, w tym danych o firmie i formie prawnej oraz danych kontaktowych osoby prawnej, o tyle nie można wykluczyć takich sytuacji, w których jednak dane o charakterze osobowym będą związane z danymi dotyczącymi osób prawnych. Przykładem tego mogą być dane osób fizycznych, w szczególności w przypadku, gdy w skład firmy wchodzi imię i nazwisko wspólnika, czy też w zakresie dotyczącym członków organów. O ile bowiem

osoby prawne nie będą posiadały danych osobowych, o tyle pracownicy, czy przedstawiciele osób prawnych – będą już takowe posiadali, i będą one podlegały ochronie.

W ramach danych osobowych RODO wyróżnia również tzw. dane wrażliwe, dotyczące szczególnych kategorii danych osobowych, takich jak ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby [art. 9 ust. 1 RODO]. Z perspektywy doradców podatkowych istotne znaczenie może mieć tu przetwarzanie danych w związku z obsługą kadrowo-płacową klientów (np. dane dotyczące stanu zdrowia pracowników, poznawane przy rozliczaniu zwolnień lekarskich), czy przynależność do związków zawodowych (przy obsłudze klienta, u którego działają związki zawodowe).

3.4.2 Dane osobowe przetwarzane przez doradcę podatkowego

Patrząc na powyższe należy wywnioskować, że doradca podatkowy w ramach prowadzonej działalności gospodarczej będzie przetwarzać dane osobowe:

(i) **w aspekcie zewnętrznym**, tj. związane ze świadczeniem usług doradztwa podatkowego; oraz

(ii) **w aspekcie wewnętrznym**, tj. w związku z obsługą swojej działalności gospodarczej, czy zawodowej.

W aspekcie zewnętrznym doradcy podatkowi będą przetwarzali dane ich klientów, jak również dane powierzone im przez klientów (np. dane pracowników rozliczanych przez doradcę podatkowego w ramach obsługi kadrowo-płacowej) niezbędne do wykonania usługi doradztwa podatkowego. Będą na nie składały się w szczególności: imię, nazwisko, adres, dane i informacje dotyczące poszczególnych spraw. Będą to dane zarówno samych klientów (lub przedstawicieli klientów, jeżeli klientem będzie osoba prawna – np. członkowie zarządu, czy reprezentanci), jak i innych osób, które będą przewijały się w toku postępowania (świadkowie, biegli, a nawet przedstawiciele organów).

W aspekcie wewnętrznym doradcy podatkowi będą przetwarzali dane swoich pracowników (np. imię i nazwisko, adres zamieszkania, PESEL, ale często również – stan rodzinny, numer telefonu i adres e-mail) i osób współdziałających przy prowadzeniu kancelarii (zleceniobiorców, stażystów, praktykantów, etc.).

3.5 Rodzaje podmiotów przetwarzających dane osobowe

Każdy podmiot, który profesjonalnie będzie przetwarzał dane osobowe, będzie traktowany jako:

(i) administrator danych; lub
(ii) podmiot przetwarzający (tzw. „procesor").

Administratorem danych może być podmiot funkcjonujący w dowolnej formie prawnej dającej mu zdolność do nabywania praw i zaciągania zobowiązań i związaną z tym możliwość ustalania celów i sposobów przetwarzania. Administratorem będzie więc osoba fizyczna (np. doradca podatkowy prowadzący kancelarię w ramach jednoosobowej działalności gospodarczej) lub prawna (np. spółka), organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych (innymi słowy – podejmuje decyzję o tym po co i jak wykorzystuje dane osobowe). Administratorem danych będzie między innymi:

(i) pracodawca w stosunku do danych osobowych swoich pracowników;
(ii) przedsiębiorca w stosunku do danych osobowych swoich klientów.

Podmiot przetwarzający dane osobowe nie decyduje o celach i środkach przetwarzania danych – działa na podstawie umowy z administratorem danych. Administrator danych może bowiem albo sam przetwarzać dane, albo skorzystać z usług zewnętrznego podmiotu, który te dane będzie przetwarzał w jego imieniu i na jego rzecz. Podmiot przetwarzający (procesor) może przetwarzać dane wyłącznie w zakresie i w celu przewidzianym w umowie.

Doradca podatkowy będzie więc z jednej strony administratorem danych, bo przetwarza dane swoich pracowników, współpracowników, kontrahentów czy klientów. Z drugiej natomiast strony będzie najczęściej procesorem (podmiotem przetwarzającym), bo będą mu powierzane dane z innych firm, współpracujących

z doradcą podatkowym, np. w zakresie obsługi kadrowo-płacowej. To klienci pozostaną tu administratorami danych, a doradcy podatkowemu powierzą dane czy to swoich pracowników, czy to dotyczące transakcji w celu realizacji odpowiednich usług.

Jak wspomniano, zgodnie z wymogami RODO administrator danych będzie mógł powierzyć innemu podmiotowi przetwarzanie danych w drodze umowy [art. 28 ust. 3 i 4 RODO], która powinna zostać zawarta na piśmie lub w formie elektronicznej [art. 28 ust. 9 RODO]. **Doradcy podatkowi będą zatem zobowiązani do zawarcia stosownych umów o powierzeniu przetwarzania danych osobowych ze wszystkimi klientami, którzy będą zlecać doradcy podatkowemu wykonywanie operacji na ich danych osobowych**. Będzie to dotyczyło w szczególności powierzenia doradcy podatkowemu obsługi księgowej, czy kadrowo-płacowej, które nierozerwalnie łączą się z przetwarzaniem danych osobowych pracowników lub kontrahentów klientów.

Co istotne, administratorem lub procesorem będzie zawsze podmiot operujący na danych osobowych, a nie jego pracownicy. Tym samym, podmiotem takim będzie:

(i) doradca podatkowy prowadzący kancelarię, a nie jej poszczególni pracownicy;
(ii) spółka partnerska zrzeszająca doradców podatkowych, a nie jej poszczególni partnerzy;
(iii) spółka z ograniczoną odpowiedzialnością będąca spółką doradztwa podatkowego, a nie jej pracownicy, czy nawet członkowie zarządu.

Oczywiście - w kancelarii dane osobowe faktycznie będą przetwarzane, czy wykorzystywane przez konkretne osoby – personel biurowy lub merytoryczny, zleceniobiorców, praktykantów, etc. Ciężar zapewnienia należytej ochrony danych osobowych w działalności będzie jednak spoczywał na administratorze lub procesorze, który będzie zobligowany do zapewnienia, by wszystkie osoby przetwarzające dane osobowe w strukturze organizacyjnej podmiotu posiadały odpowiednie upoważnienie do przetwarzania danych osobowych.

UWAGA!

Dla udowodnienia zapewnienia należytej ochrony danych osobowych doradca podatkowy będzie musiał również wykazać, że zatrudnione w kancelarii osobowy posiadają należytą wiedzę w zakresie zasad przetwarzania i ochrony danych osobowych. Taki obowiązek może zostać zrealizowany również poprzez zapewnienie pracownikom dostępu do szkoleń związanych z tematyką ochrony danych osobowych.

4 Zasady przetwarzania danych osobowych

4.1 Podstawy przetwarzania danych osobowych i zasada GDPR

RODO chroni podstawowe prawa i wolności osób fizycznych, w szczególności ich prawo do ochrony danych osobowych [art. 1 ust. 2 RODO]. W tym zakresie RODO wprowadza **generalną zasadę ochrony danych osobowych** [tzw. GDPR – (ang.) *general data protection rule*]. RODO przewiduje dwa reżimy dopuszczalności przetwarzania, w zależności od tego, czy poddane mają być temu przetwarzaniu dane zwykłe, czy też dane wrażliwe (szczególne kategorie danych) i zachowuje dotychczas obowiązujące zasady:

(i) ogólnego dopuszczenia przetwarzania danych zwykłych, gdy spełniona jest co najmniej jedna z przesłanek z art. 6 ust. 1 RODO (o których mowa poniżej), oraz

(ii) ogólnego zakazu przetwarzania danych wrażliwych, chyba że zachodzi którykolwiek z wyjątków pozwalających na takie przetwarzanie wskazanych w art. 9 ust. 2 RODO.

W motywie 40 RODO wskazano, że żeby przetwarzanie danych było zgodne z prawem, **powinno się odbywać na podstawie zgody osoby, której dane dotyczą, lub na innej uzasadnionej podstawie przewidzianej prawem albo w rozporządzeniu, albo w innym akcie prawnym Unii lub w prawie państwa członkowskiego**. Aby przetwarzanie danych osobowych było dopuszczalne, spełniona będzie musiała zostać chociaż jedna z przesłanek określona w art. 6 ust. 1 RODO, do których należą:

(i) **zgoda osoby**, której dane dotyczą, obejmująca przetwarzanie w jednym lub większej ilości celów;

(ii) **niezbędność do wykonania umowy**, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na wniosek tej osoby przed zawarciem umowy;

(iii) niezbędność do wypełnienia obowiązku prawnego ciążącego na administratorze;

(iv) niezbędność przetwarzania do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;

(v) niezbędność do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

(vi) **niezbędność przetwarzania do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią**, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

Przesłanki te mają charakter autonomiczny, co oznacza, że do wypełnienia przez administratora zasady legalności (i zarazem – dopuszczenia do przetwarzania przez niego danych) wystarczające będzie oparcie procesu przetwarzania danych osobowych wyłącznie na jednej z nich. Nie jest przy tym wykluczone równoległe występowanie w danym stanie faktycznym więcej niż jednej przesłanki legalizacyjnej.

4.1.1 Przetwarzanie danych niezbędnych do wykonania umowy

W pierwszej kolejności należy wskazać na niezbędność przetwarzania przez doradcę podatkowego danych osobowych w celu wykonania umowy łączącej go z klientem. Jest oczywiste, że dla prawidłowego wykonania przez doradcę podatkowego usługi (np. sporządzenia opinii prawno-podatkowej, reprezentacji klienta w postępowania) konieczne jest przetwarzania przez doradcę podatkowego pewnych kategorii danych osobowych. W takich przypadkach – **przetwarzanie danych osobowych przez doradcę podatkowego znajduje swoje uzasadnienie w umowie łączącej doradcę podatkowego z klientem**. Jedną z podstaw przetwarzania danych zwykłych jest bowiem niezbędność takiego przetwarzania do wykonania umowy z osobą, której dane dotyczą [art. 6 ust. 1 lit. b RODO). W tym obszarze doradca podatkowy nie będzie zatem musiał uzyskiwać odrębnej, wyraźnej zgody klienta na przetwarzanie danych osobowych. **Niemniej - zalecane jest, aby klient został poinformowany o tym, jakie jego dane osobowe oraz po co będą przetwarzane, jak również co do tego, że przetwarzanie danych w pewnym zakresie jest niezbędne dla prawidłowego wykonania usługi**.

UWAGA

Na podstawie art. 6 ust. 1 lit b RODO, czyli na podstawie umowy wykorzystywane mogą być wyłącznie dane niezbędne dla wykonania umowy (czyli tylko te dane, których doradca podatkowy potrzebuje, by prawidłowo wykonać usługę), a dane mogą być wykorzystywane tylko w celu wykonania umowy (czyli np. już nie w celach marketingowych).

4.1.2 Przetwarzanie w celu ochrony interesów administratora lub na podstawie przepisów prawa

W niektórych sytuacjach przetwarzanie danych osobowych będzie odbywało się w celu ochrony interesów doradcy podatkowego. W zakresie niezbędności przetwarzania danych osobowych celem realizacji prawnie uzasadnionych interesów doradcy podatkowego – będzie tu chodziło o wszystkie sytuacji, w których doradca podatkowy będzie potrzebował wykorzystania danych osobowych dla ochrony lub dochodzenia swoich praw. Jako przykład warto wskazać na **wykorzystanie danych osobowych celem dochodzenia roszczeń przez sądem od klienta, który uchyla się od płatności honorarium**. W takiej sytuacji doradca musi posłużyć się danymi klienta, by móc skutecznie dochodzić zapłaty przed sądem.

Dodatkowo, przetwarzanie danych osobowych będzie zgodne z prawem, gdy na takie przetwarzanie zezwalają szczególne przepisy prawa [art. 6 ust. 1 lit. c RODO]. Za przykład niech posłużą tu przepisy proceduralne, które wskazują konkretny zakres danych osobowych, jaki powinien zostać podany w związku z konkretnymi czynnościami procesowymi, jak art. 168 § 2 OP, wymagający wskazania w podaniu konkretnych danych osobowych strony. Jeżeli doradca podatkowy jako pełnomocnik będzie pełnił rolę administratora danych osobowych przetwarzanych w toku reprezentacji klienta – będzie wykorzystywał te dane na podstawie wyraźnego umocowania w przepisach postępowania.

4.1.3 Przetwarzanie na podstawie zgody

We wszystkich innych przypadkach, w których wykorzystanie danych osobowych nie będzie niezbędne dla wykonania usługi przez doradcę podatkowego, a doradca podatkowy nie wykaże istnienia istnej podstawy przetwarzania, przetwarzanie będzie musiało odbywać się na podstawie zgody. Będzie to miało zastosowanie np. **przy**

przetwarzaniu danych osobowych klientów dla celów marketingowych, takich jak wysyłka newsletteru o zmianach w przepisach podatkowych.

Na gruncie RODO zgoda 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 pkt 11 RODO]. W związku z tym zasadniczymi konstrukcyjnymi elementami zgody są jej dobrowolność, konkretność, świadomość i jednoznaczność.

Osoba, której dane dotyczą powinna być świadoma tego, że udziela zgody na przetwarzanie jej danych osobowych, do czego jej dane będą wykorzystywane i w jakim celu. **Informacja ta powinna zostać przekazana takiej osobie w sposób przejrzysty i zrozumiały, prostym językiem**.

Zgody nie można domniemywać – musi być wynikiem aktywnego działania osoby, której dane dotyczą. Milczenie, czy niepodjęcie żadnych działań (np. sprzeciwu) w żadnym razie nie powinny być traktowane jako zgoda. Co więcej – jeżeli osoba fizyczna będzie wyrażać zgodę w pisemnym oświadczeniu, które będzie dotyczyć także innych kwestii (np. w umowie, czy regulaminie), zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem, aby dana osoba od początku wiedziała i była w stanie z łatwością zauważyć, że podpisując umowę, czy akceptując regulamin – wyraża również zgodę na przetwarzanie jej danych osobowych.

4.2 Zasady przetwarzania danych osobowych

Oprócz wymogów co do konieczności istnienia podstawy prawnej przetwarzania, RODO wskazuje również na szereg zasad związanych z przetwarzaniem danych osobowych. Aby wykazać zgodność przetwarzania danych osobowych z RODO, dane osobowe muszą być:

(i) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą ("**zgodność z prawem, rzetelność i przejrzystość**");

(ii) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami ("**ograniczenie celu**");

(iii) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane ("**minimalizacja danych**");

(iv) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane ("**prawidłowość**");

(v) 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 na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą ("**ograniczenie przechowywania**");

(vi) 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**").

UWAGA!

Ciężar udowodnienia spełniania powyższych zasad ciąży na administratorze. To administrator jest odpowiedzialny za przestrzeganie zasad i musi być w stanie wykazać ich przestrzeganie (tzw. "rozliczalność") [art. 5 ust. 2 RODO].

Doradcy podatkowi, celem zapewnienia prawidłowości przetwarzania danych osobowych pod rządami RODO, będą zobligowani do przestrzegania każdej z tych zasad.

4.2.1 Zgodność z prawem

Zapewnienie realizacji zasady zgodności z prawem wymaga od doradcy podatkowego, aby dane osobowe przez niego przetwarzane były przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą. W efekcie:

(i) dla osób fizycznych powinno być zrozumiałe i przejrzyste, że dotyczące ich dane osobowe są zbierane, wykorzystywane i przetwarzane, jak również w jakim stopniu te dane osobowe są lub będą przetwarzane;

(ii) wszelkie informacje i wszelkie komunikaty związane z przetwarzaniem tych danych osobowych mają być zrozumiałe, łatwo dostępne i przejrzyście sformułowane;

(iii) osoby których dane dotyczą powinny być informowane o tożsamości administratora i celach przetwarzania oraz innych informacji mających zapewnić rzetelność i przejrzystość przetwarzania w stosunku do nich;

(iv) osobom których dane dotyczą należy zapewnić możliwość uzyskania informacji o przetwarzaniu ich danych;

(v) konkretne cele przetwarzania danych osobowych powinny być wyraźne, uzasadnione i sprecyzowane w momencie ich zbierania.

4.2.2 Zasada ograniczenia celu

Zgodnie z tą zasadą dane osobowe muszą być zbierane wyłącznie w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami. Tym samym, dane osobowe przetwarzane przez doradców podatkowych powinny być przetwarzane tylko w przypadkach, gdy celu przetwarzania nie można w rozsądny sposób osiągnąć innymi sposobami.

Na realizację tej zasady składa się wymóg konkretnego określenia celu przetwarzania (zbieranie danych nie jest dopuszczalne, jeżeli nie zostały określone cele, dla których mają być one zebrane), a także wykorzystania danych zgodnie z celem, dla realizacji którego zostały zebrane.

4.2.3 Zasada minimalizacji

RODO wprowadza tzw. zasadę minimalizacji danych osobowych. Zgodnie z nią, można przetwarzać wyłącznie takie dane osobowe, które są niezbędne do osiągnięcia celu przetwarzania danych. Przetwarzanie danych powinno więc zostać ograniczone do takich danych, bez których nie można osiągnąć celu przetwarzania danych.

Zasada ta wprowadza ilościowe ograniczenie zbierania i dalszego przetwarzania danych osobowych, co odróżnia ją od kolejnej z omawianych zasad, tj. zasady prawidłowości (poprawności) danych, która koncentruje się na ich jakości. W myśl omawianej zasady dane muszą być odpowiednie i stosowne do osiągnięcia celu ich zebrania, lecz zarazem nie mogą być nadmierne. Dane mogą być więc przetwarzane tylko w takim zakresie, który jest niezbędny dla osiągnięcia celu ich zebrania. Tym samym przetwarzanie danych w zakresie zbędnym dla osiągnięcia celu będzie oznaczało naruszenie przepisów rozporządzenia.

PRZYKŁAD

Jeżeli dane osobowe będą przetwarzane w związku ze świadczoną obsługą kadrowo-płacową, doradca podatkowy powinien przetwarzać wyłącznie dane niezbędne do prawidłowego rozliczenia kadr i płac klienta.

Do danych niezbędnych w tym przypadku nie należą kolor oczu i wzrost, które to dane są uwidocznione na „starych" dowodach osobistych.

4.2.4 Zasada ograniczenia czasu przetwarzania

Nowością na gruncie RODO jest wprowadzenie tzw. „prawa do bycia zapomnianym". Oznacza to, że **po wejściu w życie RODO, dane osobowe nie będą już mogły być przechowywane w nieskończoność**. Zgodnie z nią dane muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, **przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane**. Zgodnie z omawianą zasadą 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.

W efekcie, aby zapewnić realizację tej zasady i zapobiec przechowywaniu danych osobowych przez okres dłuższy, niż jest to niezbędne, doradca podatkowy powinien

ustalić termin ich usuwania lub okresowego przeglądu. RODO nie precyzuje jednak konkretnie tego okresu, wskazując po prostu, że dane powinny być usunięte, gdy nie będą już dłużej niezbędne do przechowywania danych. Sprawia to, że każdy doradca powinien indywidualnie określić czas przechowywania danych przed ich usunięciem – na tyle długi, na ile doradca znajduje uzasadnienie dla takiego okresu. Możliwe jest jednak wytypowanie kilku wspólnych dla wszystkich doradców minimalnych okresów przechowywania lub przetwarzania danych, np.:

(i) w zakresie dokumentów sporządzonych przez doradcę – powinny one być przechowywane przez okres nie krótszy niż 5 lat;

(ii) w zakresie zeznać, deklaracji, czy innych dokumentów w sprawach podatkowych – doradca podatkowy powinien przechowywać je co najmniej do upływu okresu przedawnienia danego zobowiązania podatkowego;

(iii) jeżeli przetwarzanie danych dokonywane jest w celu związanym z zatrudnieniem pracowników, doradca podatkowy powinien przetwarzać dane przez czas trwania zatrudnienia, a po jego ustaniu pracodawca jest zobowiązany przechowywać listy płac, karty wynagrodzeń albo inne dowody, na podstawie których następuje ustalenie podstawy wymiaru emerytury lub renty, przez okres 50 lat od dnia zakończenia u niego pracy przez pracownika.

4.3 Obowiązki informacyjne

RODO nakłada na administratorów obowiązek **zapewnienia osobom, których dane dotyczą – w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem - wszelkich informacji związanych z przetwarzaniem ich danych osobowych, oraz do zapewnienia należytej komunikacji w sprawie przetwarzania** [art. 12 ust. 1 RODO].

Informacji udziela się na piśmie lub w inny sposób, w tym w stosownych przypadkach - elektronicznie. Dopiero jeżeli osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie, o ile innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą [art. 12 ust. 1 RODO].

Obowiązek udzielania informacji dotyczącej przetwarzania danych osobowych dotyczy sytuacji, w której doradca podatkowy pozyskał dane osobowe[4]:

(i) bezpośrednio od osoby, od której pochodzą – np. od klienta, który podaje doradcy podatkowemu swoje dane osobowe przy zawieraniu umowy;

(ii) od innego podmiotu, niż osoba, której dane dotyczą – np. w sytuacji podania doradcy podatkowemu przez klienta danych innych osób zaangażowanych w sprawę lub postępowanie.

W tym zakresie RODO zobowiązuje przedsiębiorców do udzielenia osobom, których dane dotyczą informacji o:

(i) swojej tożsamości i danych kontaktowych;

(ii) danych kontaktowych inspektora ochrony danych – o ile został powołany;

(iii) celu przetwarzania danych osobowych, oraz podstawie prawnej przetwarzania;

(iv) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f RODO – informacji o prawnie uzasadnionych interesach realizowane przez administratora lub przez stronę trzecią;

(v) odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;

(vi) zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych.

(vii) okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, o kryteriach ustalania tego okresu;

[4] Na mocy art. 23 RODO poszczególne Państwa Członkowskie mogą zwolnić niektóre kategorie administratorów z niektórych obowiązków, w tym informacyjnych. W dacie sporządzania Informatora projekt polskich regulacji w tym względzie (Projekt Ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679) – nie przewidywał jednak (inaczej niż ma to miejsce w stosunku do adwokatów, czy radców prawnych) podobnego wyłączenia dla doradców podatkowych. Oznacza to, że o ile polskie przepisy nie zwolnią doradców podatkowych z obowiązków informacyjnych, będą oni zmuszeni do przestrzegania tych postanowień.

(viii) 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;

(ix) informacje o prawie wniesienia skargi do organu nadzorczego;

(x) 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;

(xi) zastosowaniu profilowania, czy zautomatyzowanego procesu podejmowania decyzji.

z o a o Aby uczynić zadość obowiązkom informacyjnym, **doradcy podatkowi będą zobligowani do przekazywania tych informacji klientom najpóźniej przy pozyskiwaniu tych danych**. Informacja powinna mieć zatem charakter uprzedni w stosunku do pozyskania i utrwalenia tych danych. Przepisy RODO **nie precyzują formy przekazania informacji, ani jej kształtu** (oprócz oczywiście wskazania na prostotę, przejrzystość i jasność przekazu). Informacja może zatem być skierowana na piśmie lub mailowo, indywidualnie do każdego klienta, lub na podstawie przygotowanego z góry szablonu.

PRZYKŁAD

Doradca podatkowy powinien przekazać informacje, o których mowa w art. 13 i RODO np.:

(i) przy podpisywaniu Umowy o świadczenie usług doradztwa podatkowego z klientem;

(ii) przy przyjmowaniu pełnomocnictwa;

(iii) przy pobieraniu od potencjalnego klienta namiarów kontaktowych za pośrednictwem formularza na stronie internetowej;

(iv) przy odpowiadaniu na zapytanie ofertowe.

W art. 14 RODO uregulowany jest drugi z obowiązków informacyjnych, który powstaje, jeżeli administrator pozyskuje dane z innego źródła niż od samego podmiotu tych danych. W przypadku gromadzenia danych osobowych niebezpośrednio od osób, których dane dotyczą, należy tym osobom dodatkowo przekazać informację o źródle danych, a więc o tym, skąd doradca podatkowy pozyskał ich dane osobowe.

Informacje, o których mowa w ust. 1 i 2, administrator podaje:

(i) **w rozsądnym terminie** po pozyskaniu danych osobowych - **najpóźniej w ciągu miesiąca** - mając na uwadze konkretne okoliczności przetwarzania danych osobowych;

(ii) jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą - najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą; lub

(iii) jeżeli planuje się ujawnić dane osobowe innemu odbiorcy - najpóźniej przy ich pierwszym ujawnieniu.

Dla doradców podatkowych będzie to dotyczyło również obowiązku informowania o przetwarzaniu danych osobowych np. pracowników klienta, których dane będą pozyskiwane w celu świadczenia na rzecz klienta usług kadrowo-płacowych, czy innych sytuacji, w których doradca podatkowy będzie świadczył usługi jako podmiot przetwarzający (procesor). Takie osoby będą musiały zostać poinformowani o tym fakcie w rozsądnym terminie, nie później niż w ciągu miesiąca.

> **PRZYKŁAD**
>
> Doradca podatkowy powinien podać takie dane np. w drodze ogólnej informacji pisemnej przekazanej klientowi do przekazania swoim pracownikom.

4.4 Prawo do bycia zapomnianym

Prawo do bycia zapomnianym jest jednym z nowych uprawnień przyznanych przez RODO osobom, których dane dotyczą. W zasadzie mamy do czynienia z dwoma uprawnieniami:

(i) do żądania usunięcia danych [art. 17 ust. 1 RODO]; oraz

(ii) do żądania bycia zapomnianym [art. 17 ust. 2 RODO].

Podstawowym uprawnieniem jest prawo do żądania usunięcia danych. Drugie z uprawnień, tj. prawo do bycia zapomnianym, przysługuje podmiotowi danych wyłącznie w przypadku skorzystania z prawa do usunięcia danych i wyłącznie w sytuacji, w której dotyczące go dane zostały upublicznione przez administratora (np. opublikowane na publicznie dostępnej stronie internetowej).

Osoba, której dane dotyczą, może żądać usunięcia jej danych przez administratora w następujących przypadkach:

(i) dane nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
(ii) cofnięcie zgody na przetwarzanie danych osobowych przez osobę, której dane dotyczą, przy jednoczesnym braku innej podstawy prawnej przetwarzania;
(iii) wniesienie sprzeciwu wobec przetwarzania przy jednoczesnym braku nadrzędnych prawnie uzasadnionych podstaw przetwarzania (art. 21 ust. 1 RODO) lub wniesienie sprzeciwu wobec przetwarzania danych na potrzeby marketingu bezpośredniego;
(iv) dane były przetwarzane niezgodnie z prawem;
(v) dane muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie UE lub państwa członkowskiego, któremu podlega administrator;
(vi) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego bezpośrednio dzieciom.

Jeżeli spełniona zostanie którakolwiek ze wskazanych powyżej przesłanek, zgodnie z art. 17 RODO osoba może się domagać od administratora niezwłocznego usunięcia dotyczących jej danych. Administrator ma w takim przypadku obowiązek:

(i) usunąć dane;
(ii) jeśli przekazał dane odbiorcom, ma obowiązek poinformować ich o usunięciu [art. 19 RODO];
(iii) jeżeli upublicznił dane podlegające usunięciu (w szczególności w Internecie), ma obowiązek domagać się od innych administratorów, którzy przetwarzają te dane, żeby oni też je usunęli, albo zaniechali ich wykorzystywania, przy czym administrator powinien w tym celu podjąć wyłącznie „rozsądne działania" uwzględniając między innymi środki techniczne;
(iv) na żądanie osoby ma obowiązek poinformować osobę, którym odbiorcom przekazał dane podlegające usunięciu.

UWAGA

Prawo do bycia zapomnianym nie przysługuje w stosunku do tych danych, które doradca podatkowy przetwarza w celach związanych z wykonywaniem zawodu. W pozostałych przypadkach, w szczególności w stosunku do danych osobowych przetwarzanych w celu związanym z zatrudnianie pracowników czy przy zbieraniu danych dla celów przesyłania klientom materiałów informacyjnych, prawo do bycia zapomnianym przysługuje na ogólnych zasadach.

5 Obowiązki doradcy podatkowego jako administratora danych osobowych

5.1 Zapewnienie bezpieczeństwa danych osobowych

Przepisy RODO przewidują dla administratorów szereg obowiązków, które będą musiały być spełnione celem zapewnienia należytej ochrony danych osobowych, wymagając od administratorów, by zapewnili **„odpowiednie" środki organizacyjne i techniczne służące ich należytej ochronie**. Tym samym **RODO nie wskazuje konkretnych rozwiązań, czy środków bezpieczeństwa danych osobowych, nakazując dostosowanie wdrażanych rozwiązań do skali ryzyka oraz specyfiki przetwarzania**.

Wdrażając odpowiednie środki techniczne i organizacyjne, administrator powinien brać pod uwagę **charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i różnej wadze zagrożenia**. Doradca podatkowy powinien zatem przy projektowaniu i wdrażaniu rozwiązań bezpieczeństwa bazować na kształtowaniu obowiązków, których zakres określany jest w każdym przypadku przez pryzmat oceny ryzyka (tzw. podejście oparte na ryzyku).

Dobór środków powinien uwzględniać:

(i) charakter, zakres, kontekst i cele przetwarzania;
(ii) ryzyko naruszenia praw lub wolności osób fizycznych w związku z przetwarzaniem;
(iii) stan wiedzy technicznej;
(iv) koszty wdrożenia poszczególnych rozwiązań.

RODO przewiduje dodatkowo, że każdy administrator powinien **uwzględniać ochronę danych już w fazie projektowania** (*privacy by design*) oraz w drodze realizacji **zasady domyślnej ochrony danych** (*privacy by default*). Oznacza to, że administratorzy mają obowiązek wdrażania odpowiednich środków technicznych i organizacyjnych już w momencie ustalania sposobów przetwarzania danych (czyli właśnie – **zaprojektowania odpowiednich procedur jeszcze przed rozpoczęciem**

przetwarzania, czy wejścia w życie RODO), a następnie - **utrzymywania tych środków w trakcie samego procesu przetwarzania, aby domyślnie były przetwarzane tylko te dane, które są niezbędne z punktu widzenia każdego konkretnego celu przetwarzania**. W szczególności takie rozwiązanie ma zapobiegać domyślnemu udostępnianiu danych nieograniczonemu kręgowi odbiorców.

Łatwo zauważyć, że obowiązki administratora w tym zakresie wymagają od niego postawy proaktywnej i prewencyjnej. Ochrona prywatności ma być bowiem zapewniona już na etapie tworzenia procedur, regulaminów, systemów, czy nawet strony internetowej kancelarii.

Celem przygotowania odpowiednich środków organizacyjnych i technicznych każdy doradca podatkowy powinien zatem:

(i) ustalić, jakie dane osobowe przetwarza, w jakim charakterze, po co, i na jakich zasadach;
(ii) określić związane z tym przetwarzaniem ryzyko naruszenia praw i wolności osób, których te dane osobowe dotyczą;
(iii) zaprojektować środki organizacyjne lub techniczne, które pozwolą na zaradzenie lub zminimalizowanie tego ryzyko – uwzględniając jednak istniejące możliwości techniczne i swoje możliwości finansowe.

RODO nie wskazuje konkretnych środków technicznych lub organizacyjnych, które należy zastosować, aby wykazać zgodność z określonymi w nim wymaganiami. Stąd, wybór środków bezpieczeństwa powinien być determinowany przez okoliczności i warunki przetwarzania danych oraz prawdopodobieństwo i powagę zdarzeń, które mogą doprowadzić do naruszenia praw i wolności osób, których dane są przetwarzane. Do rozwiązań i działań, które mogą być wykorzystane w celu minimalizacji ryzyka naruszenia praw i wolności osób, których dane dotyczą, w kontekście zapewnienia bezpieczeństwa przetwarzanych danych przed utratą poufności, zniszczeniem, nieuprawnioną modyfikacją lub brakiem dostępności, w art. 32 ust. 1 RODO zaliczono:

(i) pseudonimizację i szyfrowanie danych osobowych;
(ii) zarządzanie systemem w sposób zapewniający ciągłość poufności, integralności i dostępności przetwarzanych informacji;

(iii) zarządzanie systemem w sposób zapewniający zdolność do szybkiego przywrócenia dostępu do danych osobowych w razie wystąpienia incydentu fizycznego lub technicznego;

(iv) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Co jednak ważne - zgodnie z motywem 28 RODO, wskazane przykładowe środki techniczne i organizacyjne nie wykluczają zastosowania innych środków technicznych lub organizacyjnych, jeżeli byłyby one bardziej adekwatne do charakteru ryzyka (skutecznie minimalizowałyby ryzyko lub całkowicie je eliminowały).

Środki organizacyjne związane są z personelem dopuszczonym do przetwarzania danych osobowych. Składają się na nich wytyczne, regulaminy i procedury, określające zasady przetwarzania danych osobowych przez personel administratora. Będą nimi dla przykładu:

(i) polityka ochrony danych osobowych, określająca podstawowe zasady ochrony i przetwarzania danych osobowych w kancelarii doradcy podatkowego;

(ii) procedury ograniczające dostęp do danych osobowych osób niepowołanych, takie jak procedura czystego biurka i czystego pulpitu;

(iii) obowiązek nadawania upoważnień osobom dopuszczonym do przetwarzania danych osobowych i prowadzenie ewidencji takich upoważnień;

(iv) pouczenie pracowników o obowiązku zachowania w tajemnicy przetwarzanych danych osobowych oraz sposobów ich zabezpieczenia;

(v) obowiązek zapoznania osób upoważnionych do przetwarzania danych z przepisami o ochronie danych osobowych.

Środki techniczne można podzielić na:

(i) środki ochrony fizycznej,

(ii) środki dotyczące sprzętu infrastruktury informatycznej i telekomunikacyjnej oraz

(iii) środki w ramach stosowanych programów i baz danych.

W ramach środków ochrony fizycznej wymienia się najczęściej zabezpieczenia budynków i pomieszczeń, w których przetwarzane są dane osobowe. Wśród nich wymienia się też sposoby zabezpieczenia przechowywanych zbiorów danych w formie papierowej i w formie elektronicznej pod postacią kopii zapasowych lub archiwalnych zbiorów danych. Zastosowanie środków sprzętowych infrastruktury informatycznej i telekomunikacyjnej oraz środków ochrony programów i baz danych ma na celu przede wszystkim zabezpieczenie systemu informatycznego przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do tego systemu oraz przed utratą danych osobowych spowodowanych awarią zasilania. Warto wskazać w tym miejscu na:

(i) systemowe wymuszanie zmiany hasła dostępu do komputera lub oprogramowania;
(ii) oprogramowanie antywirusowe i firewall;
(iii) stosowanie zabezpieczeń fizycznych (zamków) w szafkach oraz szufladach, w których przetrzymywane są dane osobowe;
(iv) tworzenie kopii zapasowych danych;
(v) system kontroli dostępu do pomieszczeń.

5.2 Rejestrowanie czynności przetwarzania

Jednym z podstawowych obowiązków podmiotów przetwarzających dane, zarówno administratorów, jak i podmiotów przetwarzających (procesorów), jest obowiązek rejestrowania wszystkich czynności przetwarzania danych poprzez prowadzenie tzw. rejestru czynności przetwarzania danych (RCPD) [art. 30 RODO]. Aby zrozumieć, jak praktycznie podejść do RCPD, należy wyjść od tego, czym na gruncie RODO jest czynność przetwarzania danych.

Niestety, pojęcie to nie zostało zdefiniowane wprost w RODO, co może powodować trudności interpretacyjne co do tego, co należy rejestrować. Wszystkie dotychczasowe publikacje dotyczące tematu rejestrowania czynności przetwarzania danych zgodnie podkreślają, że **czynności przetwarzania to operacje wykonywane na danych, które łączy realizacja tego samego celu przetwarzania**. Należy zatem wyodrębniać czynności w **odniesieniu do wspólnych, związanych z tymi czynnościami określonych celów przetwarzania danych**. W praktyce tylko takie

podejście jest wykonalne i możliwe do zrealizowania. Pojęcie czynności może być tak wielopoziomowe, że nie kierując się grupowaniem czynności według realizowanych przez nie celów, można zidentyfikować od kilkuset do kilku tysięcy procesów, co byłoby nie do pogodzenia z wykonywaniem obowiązków doradcy podatkowego.

Stąd, rozsądnym podejściem będzie grupowanie czynności przetwarzania w rejestrze wedle celu, którego czynności dotyczą. Jako przykład można tu wskazać:

Przykładowe czynności przetwarzania danych:

(i) **administrowanie personelem i współpracownikami** – rekrutacja i selekcja personelu i pośredników (brokerów, niezależnych przedstawicieli itp.); administracja wynagrodzeń, dodatków, prowizji i płac; zastosowanie przepisów socjalnych;

(ii) **zarządzanie personelem i współpracownikami** – ocena i monitorowanie personelu i pośredników; planowanie szkoleń i kariery;

(iii) **organizacja pracy** – planowanie i monitorowanie zadań, nakładu pracy i wydajności;

(iv) **relacje z klientami** – zarządzanie klientami, zarządzanie zamówieniami, dostawy, fakturowanie usług; monitorowanie wypłacalności; spersonalizowany marketing i reklama; rejestracja klientów kancelarii;

(v) **relacje z dostawcami** – zarządzanie zamówieniami, płatności dla dostawców; poszukiwanie potencjalnych dostawców i ich ocena;

(vi) **kontakty z organami podatkowymi** – uczestnictwo w kontrolach i postępowaniach, sporządzanie niezbędnych pism, deklaracji, czy wniosków;

(vii) **obsługa klienta** – świadczenie usług doradztwa podatkowego, sporządzanie opinii, prowadzenie obsługi księgowej lub kadrowo-płacowej klienta.

Rejestr powinien być prowadzony w formie pisemnej lub elektronicznej. Doradcy podatkowi będą zobligowani do odnotowania w rejestrze:

(i) swojego imienia i nazwiska (nazwy) oraz danych kontaktowych;

(ii) celu przetwarzania (np. określone zgodnie z powyższymi przykładami);

(iii) opisu kategorii osób, których dane dotyczą, oraz kategorii danych osobowych, które podlegają przetwarzaniu (np. dane osobowe pracowników kancelarii, na które składają się: imię i nazwisko, adres zamieszkania, PESEL, informacje o stanie rodzinnym, etc.);

(iv) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione (np. pracownicy kancelarii obsługujący danego klienta, organy podatkowe, którym udostępnia się dane z deklaracji, etc.);

(v) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych (np. po upływie terminu przedawnienia właściwego zobowiązania podatkowego);

(vi) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa danych, dostosowanych do skali ryzyka.

RODO wskazuje, że obowiązek prowadzenia RCPD nie dotyczy przedsiębiorcy podmiotu zatrudniającego mniej niż 250 osób, chyba że przetwarzanie, którego dokonują, może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą, nie ma charakteru sporadycznego lub obejmuje szczególne kategorie danych osobowych, o których mowa w art. 9 ust. 1 RODO (tj. dane wrażliwe).

W konsekwencji zgodnie z art. 30 ust. 1 w zw. z art. 30 ust. 5 RODO przedsiębiorca (podmiot) prowadzi RCPD, jeżeli:

(i) zatrudnia 250 osób lub więcej;

(ii) dokonuje przetwarzania danych, które rodzi ryzyko naruszenia praw lub wolności osób, których dane dotyczą, i przetwarzanie to nie ma charakteru sporadycznego; lub

(iii) dokonuje, nawet sporadycznie, przetwarzania danych, które rodzi ryzyko naruszenia praw lub wolności osób, których dane dotyczą, i przetwarzanie to dotyczy danych szczególnych lub danych karnych.

W praktyce w większości przypadków obowiązek prowadzenia RCPD istnieje. **Za rekomendowane należy uznać prowadzenie rejestru czynności przetwarzania danych przez wszystkich doradców podatkowych niezależnie od stanu zatrudnienia**, uwzględniając, że:

(i) dane przetwarzane przez doradców podlegają szczególnej ochronie jako objęte tajemnicą zawodową, więc ich ujawnienie może prowadzić do naruszenia praw i wolności osób fizycznych;

(ii) RCPD stanowi dobry i przejrzysty sposób wykazania zgodności przetwarzania danych zgodnie z RODO - umożliwia rozliczalność, zapewnia mapowanie operacji przetwarzania danych i pozwala na identyfikację działań, jakie należy podjąć, aby właściwie przestrzegać zasad ochrony danych osobowych;

(iii) RCPD jest narzędziem kontroli nad własnymi danymi i informacjami stanowiącymi tajemnicę przedsiębiorstwa, co w dobie społeczeństwa informacyjnego i gospodarki informacyjnej musi przynieść korzyści.

Uzasadnia to przyjęcie, że doradcy podatkowi powinni zawsze prowadzić RCPD.

5.3 Inspektor ochrony danych

Inspektorzy Ochrony Danych (IOD) pod rządami RODO zastąpią dotychczasowych Administratorów Bezpieczeństwa Informacji. Powołanie IOD, z zastrzeżeniem kilku wyjątków, będzie nieobligatoryjne po wejściu w życie RODO.

Wyznaczenie IOD będzie jednak obligatoryjne, gdy:

(i) gdy dane są przetwarzane przez podmioty z sektora publicznego;

(ii) gdy 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;

(iii) gdy główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych lub danych osobowych dotyczących wyroków skazujących.

Uwzględniając powyższe, **doradcy podatkowi nie powinni zostać uznani za podmioty zobligowane do powołania IOD**. Nie mieszczą się bowiem w żadnej ze wskazanych powyżej przesłanek. W niektórych sytuacjach jego powołanie będzie jednak pożądane lub przydatne dla zapewnienia sprawności przetwarzania danych osobowych w kancelarii doradcy podatkowego.

Według RODO IOD ma być swoistym pośrednikiem pomiędzy zainteresowanymi stronami (np. organem ochrony danych osobowych, osobami, których dane dotyczą, albo jednostkami w ramach przedsiębiorstwa). **IOD nie odpowiada za zgodność organizacji z przepisami ochrony danych**. Odpowiedzialność za to ponosi zawsze kierownictwo jednostki (np. właściciel kancelarii) i nie może jej scedować na IOD. Inspektor ochrony danych, jak wynika z analizy postanowień RODO, pełni rolę konsultacyjno-uświadamiająco-doradczo-kontrolną.

Inspektor ochrony danych jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39 RODO. RODO pozostawia przy tym administratorom swobodę, w jaki sposób chcieliby oni współpracować z IOD. Funkcja IOD może być pełniona zarówno na podstawie umowy o pracę, jak i na podstawie umowy o świadczenie usług, w tym – jak się wydaje – na podstawie umowy z firmą świadczącą usługi IOD (outsourcing IOD). RODO przyznaje IOD wyjątkowo dużą niezależność. Administrator jest zobowiązany w szczególności zapewnić:

(i) by inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania tych zadań [art. 38 ust. 3 RODO];
(ii) niezależność IOD przy realizacji obowiązków.

Inspektor ochrony danych ma następujące zadania [art. 39 RODO]:

(i) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
(ii) 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;

(iii) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35;

(iv) współpraca z organem nadzorczym;

(v) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

5.4 Zgłaszanie naruszeń ochrony danych osobowych

RODO nakłada na podmioty przetwarzające dane osobowe obowiązek informowania o przejawach naruszenia ochrony danych osobowych. Za podobne incydenty należy uważać 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 pkt 12 RODO].

PRZYKŁADY
Kradzież danych z serwera kancelarii;
Przypadkowe przesłanie maila zawierającego dane osobowe do niewłaściwego klienta;
Wykasowanie zawartości serwera przez zwolnionego pracownika ostatniego dnia pracy;
Zagubienie akt sprawy Klienta.

Co do zasady, o wystąpieniu incydentu należy poinformować organ nadzorczy (w Polsce będzie nim Prezes Urzędu Ochrony Danych Osobowych). Informacja powinna zostać przekazania niezwłocznie, lecz nie później niż w ciągu 72 godzin od stwierdzenia naruszenia.

W pewnych przypadkach należy również informować o incydencie osoby, których dane dotyczą – będzie tak wtedy, gdy naruszenie może powodować wysokie ryzyko naruszenia praw i wolności osoby, której dane dotyczą. Jednocześnie - podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi [art. 33 ust. 2 RODO]. Jeżeli jednak będzie mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych – zgłoszenie nie będzie obligatoryjne.

W każdym jednak przypadku administrator będzie zobowiązany do prowadzenia specjalnego rejestru naruszeń, w którym będzie dokumentował wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania obowiązku prowadzenia rejestru i ewentualnego zgłaszania naruszeń [art. 33 ust. 5 RODO].

Dokumentacja powinna zatem uwzględniać wszystkie naruszenia ochrony danych osobowych: zarówno te, które zaistniały u administratora, jak i te, które zaistniały u podmiotu przetwarzającego. Na jej bowiem podstawie organ nadzorczy musi mieć również możliwość sprawdzenia, czy podmiot przetwarzający wykonuje swój obowiązek wynikający z przepisu art. 33 ust. 2 RODO.

W dokumentacji powinny być odnotowywane wszelkie naruszenia ochrony danych osobowych. Łącznie z tymi, których administrator nie zgłosił do organu nadzorczego z uwagi na małe prawdopodobieństwo, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osoby fizycznej. W ten sposób organ nadzorczy będzie miał możliwość weryfikacji, czy administrator podjął prawidłową decyzję o zaniechaniu zgłoszenia na podstawie art. 33 ust. 1 RODO.

5.5 Powierzenie przetwarzania

Wykonywanie zawodu doradcy podatkowego, zwłaszcza w zakresie usługowego prowadzenia ksiąg rachunkowych lub obsługi kadrowo-płacowej będzie nieodmiennie wiązało się z obowiązkiem powierzenia doradcy podatkowemu danych osobowych administratora. Z drugiej strony, w wielu sytuacjach – to doradca podatkowy będzie występował z pozycji podmiotu powierzającego dane osobowe podmiotowi trzeciemu.

PRZYKŁADY
Korzystanie z zewnętrznej poczty elektronicznej;
Korzystanie z serwera zewnętrznego (np. chmury);
Zlecanie podmiotowi zewnętrznemu niszczenia lub archiwizacji dokumentów.

RODO wymaga, aby w takich sytuacjach administrator zawarł z procesorem umowę w sprawie powierzenia przetwarzania danych osobowych, zgodną z art. 28 RODO.

Zawarcie takiej umowy przez doradcę podatkowego będzie wymagane w obu wariantach, tj.:

(i) gdy doradca będzie podmiotem przetwarzającym (procesorem), a któremu dane osobowe powierzy klient (administrator) – np. w przypadku świadczenia przez doradcę podatkowego usług obsługi kadrowo-płacowej pracowników klienta;
(ii) gdy doradca będzie administratorem powierzającym dane osobowe podmiotowi trzeciemu – np. w przypadku przechowywania danych kancelarii na serwerze zewnętrznym (w chmurze).

Umowa powierzenia przetwarzania powinna zawierać:

(i) przedmiot i czas powierzenia przetwarzania;
(ii) charakter i cel przetwarzania;
(iii) rodzaj powierzonych danych osobowych;
(iv) kategorie osób, których dane zostaną powierzone;
(v) związane z powierzeniem obowiązki i prawa administratora.

Dodatkowo, taka umowa powinna stanowić również, że podmiot przetwarzający [art. 28 ust. 3 RODO]:

(i) przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora;
(ii) zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
(iii) podejmuje wszelkie środki bezpieczeństwa związane z ochroną danych osobowych;
(iv) przestrzegania warunków korzystania z usług innego podmiotu przetwarzającego (tzw. podpowierzenie przetwarzania danych jest dopuszczalne wyłącznie za zgodą administratora danych);
(v) pomaga administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązków nałożonych na administratora na mocy RODO;

(vi) po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie;

(vii) 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.

Umowa powierzenia **może zostać zawarta w formie pisemnej oraz w formie elektronicznej**, pod warunkiem zapewnienia integralności i autentyczności dokumentu w postaci elektronicznej.

6 Kontrola i sankcje

Zgodnie z projektem Ustawy o ochronie danych osobowych[5] organem nadzorczym właściwym do kontroli postanowień RODO w Polsce ma stać się Prezes Urzędu Ochrony Danych Osobowych (PUODO). PUODO będzie również organem właściwym do prowadzenia postępowań i kontroli w sprawie naruszenia przepisów o ochronie danych osobowych.

W RODO brak jest przepisów zabraniających PUODO kontrolowania działalności doradców podatkowych. Niemniej, w Projekcie Ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679[6] przewiduje nowelizację DorPodU zakładającą wyłączenie wglądu PUODO w jakiekolwiek dane objęte tajemnicą zawodową doradcy podatkowego.

W pozostałym jednak zakresie – doradcy podatkowi powinni przygotować swoje regulacje wewnątrz kancelaryjne do wymogów RODO. Efekty kontroli mogą być bowiem dotkliwe. Na mocy RODO PUODO będzie uprawniony do nałożenia na doradcę podatkowych kar pieniężnych sięgających nawet **€ 10 000 000** lub **€ 20 000 000**, w zależności od rodzaju i skali naruszenia.

[5] W momencie przygotowywania Informatora projekt Ustawy o ochronie danych osobowych był na etapie pierwszego czytania w Sejmie.
[6] W momencie przygotowywania Informatora projekt znajdował się w fazie konsultacji przed Komitetem ds. Europejskich Rady Ministrów.