Ochrona Danych Osobowych wg RODO

Podstawy prawne ochrony danych osobowych:

- Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997r.
- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych
- Rozporządzenie Parlamentu Europy i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. L nr 119 z 04.05.2016 r., s.1dalej jako RODO

Hierarchia źródeł prawa

- **RODO**
- **Ustawa o ochronie danych osobowych – nowa**
- **Uregulowania sektorowe/branżowe**
- **Zatwierdzone kodeksy postępowania**

Prezesa Urzędu Ochrony Danych Osobowych (PUODO)

W polskich przepisach o ochronie danych osobowych znajdzie się także regulacja tego fragmentu zasad ochrony danych osobowych, który nie został uregulowany w RODO, czyli niektórych zasad przetwarzania m.in. danych kadrowych.

WSZYSTKIE TOCZĄCE SIĘ WCZEŚNIEJ OPERACJE PRZETWARZANIA DANYCH MUSZĄ BYĆ DOSTOSOWANE DO NOWYCH WYMOGÓW TAK, ABY 25 MAJA 2018 R. MÓC ZAPEWNIĆ ICH ZGODNOŚĆ Z RODO,

W nowym podejściu ochrona danych osobowych to ciągły proces.

Ochrona danych osobowych nie będzie sprowadzała się do wykonania kilku jasno określonych czynności, a raczej zaprojektowania całego systemu tej ochrony – i ustawiania procedur osobno pod wszystkie procesy, jakie dzieją się w organie i uwzględniają wykorzystanie danych osobowych.

RODO nie ma zastosowania do przetwarzania danych osobowych przez osobę fizyczną w ramach działalności czysto osobistej lub domowej, czyli bez związku z działalnością zawodową lub handlową. Działalność osobista lub domowa może między innymi polegać na korespondencji i przechowywaniu adresów, podtrzymywaniu więzi społecznych oraz działalności internetowej podejmowanej w ramach takiej działalności. Rozporządzenie ma jednak zastosowanie do administratorów lub podmiotów przetwarzających, którzy udostępniają środki przetwarzania danych osobowych na potrzeby takiej działalności osobistej lub domowej.

RODO nie ma zastosowania do danych osobowych osób zmarłych.

Państwa członkowskie mogą przyjąć przepisy o przetwarzaniu danych osobowych osób zmarłych

„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, 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;

„przetwarzanie” oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką *jak 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;*

Anonimizacja danych osobowych nie została zdefiniowana zarówno na gruncie dyrektywy 95/46/WE, ustawy o ochronie danych osobowych, jak i ogólnego rozporządzenia o ochronie danych osobowych. W związku z tym można założyć, że aktualne pozostaje stanowisko, zgodnie z którym **anonimizacja danych osobowych oznacza pozbawienie informacji cech danych osobowych**, a zatem możliwości identyfikacji na ich podstawie osoby fizycznej.

„administrator” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;

„podmiot przetwarzający” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora

„odbiorca” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią.

Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;

„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

„naruszenie ochrony danych osobowych” oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub winny sposób przetwarzanych

Zasady przetwarzania danych osobowych w RODO

- **Zasada 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 „zgodność z prawem, rzetelność i przejrzystość”** - przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą.
- **Zasada ograniczonego celu** - zbieranie 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 zpierwotnymi celami.

Zasada prawidłowości -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.

Zasada ograniczonego przechowywania – 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

Zasada integralności i poufności - 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 rozliczalności - Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie – art. 5 RODO

Zgodność przetwarzania z prawem art. 6

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

a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;

b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;

c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;

d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;

e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

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

Akapit pierwszy lit. f) nie ma zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań

Przetwarzanie szczególnych kategorii danych osobowych – art. 9

1. Zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.
2. Ust. 1 nie ma zastosowania, jeżeli spełniony jest jeden z poniższych warunków:

   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, o którym mowa w ust. 1;

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 osoób, 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 zgodnie z art. 89 ust. 1, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą

Obowiązek informacyjny

- Język – jasny prosty
- Forma – przejrzysta zrozumiała i łatwo dostępna,
- Sposób - pisemny, elektroniczny, ustny (po potwierdzeniu tożsamości osoby której dane dotyczą)

Administrator dokumentuje: (art. 33 ust. 5)

- wszelkie naruszenia ochrony danych osobowych;
- okoliczności naruszenia;
- skutki naruszenia;
- podjęte działania zaradcze.
- Organ nadzorczy na podstawie dokumentacji musi móc zweryfikowanie przestrzegania wymogów dotyczących zgłaszania naruszeń ochrony danych osobowych

Administrator dokumentuje: (art. 33 ust. 5)

- wszelkie naruszenia ochrony danych osobowych;
- okoliczności naruszenia;
- skutki naruszenia;
- podjęte działania zaradcze.
- Organ nadzorczy na podstawie dokumentacji musi móc zweryfikowanie przestrzegania wymogów dotyczących zgłaszania naruszeń ochrony danych osobowych

Incydenty mogą dotyczyć np.:

- ujawnianie informacji osobom nieupoważnionym;
- udostępnianie hasła i loginu innym użytkownikom;
- złamanie zasad polityki bezpieczeństwa informacji;
- uszkodzenie informacji, kradzież systemów (laptop, urządzenie przenośne);
- podejrzenie kradzieży danych.

Upoważnienie do przetwarzania danych powinno zostać wydane w formie pisemnej. W upoważnieniu takim powinna się znaleźć wzmianka o okresie, na jaki zostaje wydane, o zakresie danych, które mogą podlegać przetwarzaniu przez określoną osobę, a także o zakresie czynności podejmowanych przez nią w związku ze wspomnianymi danymi.

Odpowiedzialność za przestrzeganie przepisów niniejszej spoczywa na administratorze danych, co nie wyłącza odpowiedzialności podmiotu, który zawarł umowę, za przetwarzanie danych niezgodnie z tą umową.

Domyślna ochrona danych

- Art. 25 ust. 2 RODO Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągniecia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. [...]

Zabezpieczenie danych osobowych

Obowiązki ADO – art. 24 ust.1

- Wdrożenie odpowiednich środków technicznych i organizacyjnych w takim zakresie aby wykazać, że przetwarzanie odbywa się zgodnie z RODO uwzględniając:
- charakter, zakres, kontekst przetwarzania, cele przetwarzania,
- ryzyko naruszenia praw lub wolności osób fizycznych o rożnym prawdopodobieństwie i wadze zagrożenia.
- Środki w razie potrzeby są uaktualniane i poddawane przeglądom.

Zastosowane środki muszą być odpowiednie do zagrożenia i do kategorii danych oraz odzwierciedlać stan wiedzy w tej dziedzinie. Zapewnienie bezpieczeństwa danych to proces o charakterze ciągłym, który obejmuje analizę ryzyka powinien również uwzględniać zmienne okoliczności wpływające na poziom i charakter istniejących zagrożeń

Dokumentacja z RODO

- Polityki ochrony danych,
- Dokumentacja dotycząca przeglądów zastosowanych środków technicznych i organizacyjnych zabezpieczenia danych,
- Rejestry czynności Administratora oraz PROCESORÓW,
- Procedury postepowania w sprawie naruszeń ochrony danych, w tym rejestr naruszeń,
- Dokumentacja z dokonywanej analizy ryzyka,
- Dokumentacja dotycząca oceny skutków przetwarzania, • Dokumentacja Inspektora ochrony danych (IOD),
- Dokumentacja dotycząca zatwierdzonych Kodeksów Postepowania oraz dokumentacja dotycząca zatwierdzonego mechanizmu certyfikacji,
- Pozostała dokumentacja, którą wprowadził ADO i PROCESOR.

Rejestrowanie czynności przetwarzania – art. 30 :

- w celu zachowania zgodności z rodo administrator lub podmiot przetwarzający powinni prowadzić rejestry czynności przetwarzania, za które są odpowiedzialni.
- każdy administrator i każdy podmiot przetwarzający zobowiązani są współpracować z organem nadzorczym i na jego żądanie udostępniać mu rejestry w celu monitorowania operacji przetwarzania.

Rejestr czynności – PROCESOR w rejestrze podmiot przetwarzający zamieszcza:

• imię i nazwisko lub nazwę oraz dane kontaktowe podmiotu lub podmiotów przetwarzających oraz każdego administratora, w imieniu którego działa podmiot przetwarzający, a gdy ma to zastosowanie – przedstawiciela administratora lub podmiotu przetwarzającego oraz IOD;

• kategorie przetwarzanych dokonywanych w imieniu każdego administratora;

• gdy ma to zastosowanie – przekazania danych do państwa trzeciego lub organizacji międzynarodowych, w tym nazwa państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit 2 RODO, dokumentacja odpowiednich zabezpieczeń;

• jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (art. 32 ust. 1 RODO

Art. 9.Podmioty tworzące sektor finansów publicznych, Sektor finansów publicznych tworzą

1) organy władzy publicznej, w tym organy administracji rządowej, organy kontroli państwowej i ochrony prawa oraz sądy i trybunały;
2) jednostki samorządu terytorialnego oraz ich związki;

2a) związki metropolitalne;

3) jednostki budżetowe;

4) samorządowe zakłady budżetowe;

5) agencje wykonawcze;

6) instytucje gospodarki budżetowej;

7) państwowe fundusze celowe;

8)Zakład Ubezpieczeń Społecznych i zarządzane przez niego fundusze oraz Kasa Rolniczego Ubezpieczenia Społecznego i fundusze zarządzane przez Prezesa Kasy Rolniczego Ubezpieczenia Społecznego;

9) Narodowy Fundusz Zdrowia;

10) Samodzielne publiczne zakłady opieki zdrowotnej;

11) Uczelnie publiczne;

12) Polska Akademia Nauk i tworzone przez nią jednostki organizacyjne;
13) państwowe i samorządowe instytucje kultury;

14) inne państwowe lub samorządowe osoby prawne utworzone na podstawie odrębnych ustaw w celu wykonywania zadań publicznych, z wyłączeniem przedsiębiorstw, instytutów badawczych, banków i spółek prawa handlowego.

Inspektor ma mieć zagwarantowaną niezależność. Należy zatem wprowadzić rozwiązania (odpowiednie postanowienia wewnętrznych regulaminów organizacyjnych), które pozwolą na osiągniecie tego założenia, pamiętając o:

- odpowiednim usytuowaniu inspektora w strukturze organizacyjnej, tak, by był bezpośrednio podległy najwyższemu kierownictwu,
- zapewnieniu mu niezbędnych zasobów do wykonywania jego zadań,
- włączaniu inspektora we wszystkie procesy, gdzie przetwarzane są dane osobowe.

- 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 jakie mu przewidziano.
- Inspektor ochrony danych może być członkiem personelu administratora lub podmiotu przetwarzającego lub wykonywać zadania na podstawie umowy oświadczenie usług.
- Administrator lub podmiot przetwarzający publikują dane kontaktowe inspektora ochrony danych i zawiadamiają o nich organ nadzorczy.

- Osoby, których dane dotyczą, mogą kontaktować się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy niniejszego rozporządzenia.
- Inspektor ochrony danych może wykonywać inne zadania i obowiązki. Administrator lub podmiot przetwarzający zapewniają, by takie zadania i obowiązki nie powodowały konfliktu interesów.

Zadania inspektora ochrony danych

- 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
- 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

- udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 (Ocena skutków dla ochrony danych);
- współpraca z organem nadzorczym;
- pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach
- Inspektor nie ponosi odpowiedzialności w przypadku niezgodności z RODO. Z rozporządzenia wynika, że to administrator lub podmiot przetwarzający zobowiązany jest do zapewnienia i udowodnienia zgodności przetwarzania danych osobowych z przepisami prawa (artykuł 24(1)).
- Przetwarzanie danych zgodne z rozporządzeniem jest obowiązkiem administratora lub podmiotu przetwarzającego.

- W jednostkach, w których w dniu 24 maja 2018 r. funkcjonować będzie administrator bezpieczeństwa informacji stanie się on z mocy nowej ustawy inspektorem ochrony danych i pełnić będzie mógł swoją funkcje do dnia 1 września 2018 r., chyba że do tego dnia administrator zawiadomi Prezesa Urzędu o wyznaczeniu innej osoby na inspektora ochrony danych (art. 144 puodo).
- Administrator bezpieczeństwa informacji, która stała się, inspektorem ochrony danych, pełnić będzie swoją funkcję także po dniu 1 września 2018 r. jeżeli do tego dnia administrator złoży odpowiednie zawiadomienie do Prezesa Urzędu.

- Administrator, który do dnia wejścia w życie niniejszej ustawy nie powołał administratora bezpieczeństwa informacji, i który zgodnie z art. 37 RODO, ma obowiązek wyznaczenia inspektora ochrony danych, zobowiązany jest wyznaczyć inspektora ochrony danych oraz zawiadamia Prezesa Urzędu w terminie do dnia 31 lipca 2018 r.
- Ustawodawca zobligował administratora, który wyznaczył inspektora do zawiadomienia Prezesa Urzędu Ochrony Danych Osobowych o jego wyznaczeniu w terminie 14 dni od dnia wyznaczenia, wskazując imię, nazwisko, adres poczty elektronicznej lub numer telefonu inspektora. Te same dane należy niezwłocznie podać do publicznej wiadomości na swojej stronie internetowej po wyznaczaniu inspektora.

- Zawiadomienie o wyznaczeniu inspektora ochrony danych dokonywane będzie w drodze elektronicznej i winno zostać opatrzone kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.
- W przypadku wyznaczenia jednego inspektora dla kilku jednostek organizacyjnych w ramach danej jednostki samorządu terytorialnego, co jest dopuszczalne, należy wówczas uwzględnić struktury organizacyjne i wielkości danych jednostek w ten sposób, aby inspektor mógł prawidłowo wykonywać swoje liczne obowiązki, każdy z tych podmiotów dokonuje odrębnego zawiadomienia o ustanowieniu inspektora ochrony danych.