Opracowanie dotyczące zasad ochrony danych osobowych
po zmianach wprowadzanych przez rozporządzenie RODO

W chwili obecnej kwestie związane z ochroną danych osobowych reguluje ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2016 r. poz. 922 z późn. zm.). Jednocześnie z dniem 25 maja br. regulacje dotyczące ochrony danych osobowych ulegną znaczącej zmianie zacznie być bowiem stosowane rozporządzenie Parlamentu Europejskiego 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. UE z 2016 r. L 119, s. 1) czyli RODO. Ostateczny kształt nowych regulacji nie jest do końca ustalony, ciągle trwają m.in. prace nad projektem nowej ustawy o ochronie danych osobowych mającej zapewnić skuteczne stosowanie w Polsce unijnego rozporządzenia 2016/679 (RODO). Z kolei szczegółowy zakres obowiązków i wymogów do spełnienia zależał będzie każdorazowo od tego jak prowadzona jest dana działalność gospodarcza i w jaki sposób przetwarzane są dane osobowe.
Z najważniejszych regulacji wprowadzanych przez wskazane wyżej rozporządzenie UE można wskazać w szczególności:

1. **Zasady przetwarzania danych osobowych:**

Dane osobowe muszą być:

a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;
b) 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;
c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;
d) 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;
e) 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 wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą;
f) 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.

Administrator jest odpowiedzialny za przestrzeganie tych obowiązków i musi być w stanie wykazać ich przestrzeganie.

2. **Przetwarzanie danych osobowych dopuszczalne jest co do zasady gdy:**

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 – punkt ten nie ma zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań.

3. **W przypadku gdy przetwarzanie następuje na podstawie zgody:**

1. Należy pamiętać, iż 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.
2. Administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych.
3. Jeżeli osoba, której dane dotyczą, wyrażą zgodę w pisemnym oświadczeniu, które dotyczy także innych kwestii, 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.
4. 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.
5. Oceniając, czy zgodę wyrażono dobrowolnie, w jak największym stopniu uwzględnia się, czy między innymi od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy.

4. Przetwarzanie szczególnych kategorii danych

Co do zasady, z wyjątkami wprost wynikającymi z rozporządzenia RODO zabronione jest przetwarzanie 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.

5. Obowiązek informacyjny

1) Jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, administrator podczas pozyskiwania danych osobowych podaje jej wszystkie następujące informacje:
   a) swoją tożsamość i dane kontaktowe 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 celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią - 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 odpowiedniego stopnia ochrony lub w określonych przypadkach, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych.

2) Oprócz powyższych informacji, podczas pozyskiwania danych osobowych administrator podaje osobie, której dane dotyczą, również:
   a) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
   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 - informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
   d) informacje 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 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.

Jeżeli administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji, o których mowa wyżej.

Powyższe nie ma zastosowania, gdy - i w zakresie, w jakim - osoba, której dane dotyczą, dysponuje już tymi informacjami.

Podobne obowiązki informacyjne istnieją w przypadku gdy danych osobowych nie pozyskano od osoby, której dane dotyczą.

6. **Uprawnienia osób których dane są przetwarzane:**

a) Prawo do informacji o tym czy dane dotyczące danej osoby są przetwarzane i jeżeli tak to w jakim zakresie;
b) Prawo do sprostowania danych;
c) Prawo do ich usunięcia w określonych przypadkach (np. gdy dane osobowe stały się zbędne do celów do których były zebrane lub przetwarzane)
d) Prawo żądania ograniczenia przetwarzania;
e) Prawo do przenoszenia danych;
f) Prawo do sprzeciwu w przypadku przetwarzania danych w oparciu o niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi lub cele wynikające z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią.

7. Należy pamiętać, iż informacje o których w pkt 5 lub komunikacja w sprawach o których mowa w pkt. 6 powinna być prowadzona w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem - w szczególności gdy informacje są kierowane do dziecka. Informacji udziela się na piśmie lub w inny sposób, w tym w stosownych przypadkach - elektronicznie. Jeżeli osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie, o ile innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą.

   Co do zasady osoby których dane są przetwarzane powinny być niezwłocznie, nie dalej niż w okresie miesiąca (z pewnymi wyjątkami) informowane o działaniach podjętych w związku z ich wnioskami.

Informacje czy też działania są wolne od opłat. Natomiast w przypadku gdy żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, administrator może pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań; albo odmówić podjęcia działań w związku z żądaniem.

8. Obowiązki administratora danych

1) Wdrożenie odpowiednich środków technicznych i organizacyjnych, przy uwzględnieniu charakteru, zakresu, kontekstu i celów przetwarzania oraz ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, aby przetwarzanie odbywało się zgodnie z rozporządzeniem RODO i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane. Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki te powinny obejmować wdrożenie przez administratora odpowiednich polityk ochrony danych.
2) Uwzględnienie potrzeb związanych z ochroną danych już na etapie podejmowania decyzji o przetwarzaniu danych (sposobie i zakresie świadczonych usług z którym to przetwarzanie jest związane).
3) Prowadzenie rejestru czynności przetwarzania danych osobowych, zawierającego:
   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;
   c) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
   d) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
   e) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w pewnych przypadkach, dokumentacja odpowiednich zabezpieczeń;
   f) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
   g) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

Przy czym powyższe obowiązki nie mają zastosowania do przedsiębiorcy lub podmiotu zatrudniającego mniej niż 250 osób, chyba że przetwarzanie, którego dokonują, może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą, nie ma charakteru sporadycznego lub obejmuje szczególne kategorie danych osobowych lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa.

4) Ustalenie i wdrożenie, przy uwzględnieniu stanu wiedzy technicznej, kosztu wdrażania oraz charakteru, zakresu, kontekstu i celów przetwarzania oraz ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, środków bezpieczeństwa polegających m.in. na:
   a) pseudonimizacji i szyfrowaniu danych osobowych;
   b) zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
   c) zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
   d) regularnym testowaniu, mierzeniu i ocenianiu skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.
   e) Przy ocenie 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.

Wywiązywanie się z obowiązku wdrożenia odpowiednich środków bezpieczeństwa można wykazać między innymi poprzez stosowanie zatwierdzonego kodeksu postępowania lub zatwierdzonego mechanizmu certyfikacji.

5) Zgłaszania naruszenia ochrony danych osobowych organowi nadzorczemu w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, 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 należy dołączyć wyjaśnienie przyczyn opóźnienia. Zgłoszenie powinno:
   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, od którego można uzyskać więcej informacji;
   c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
   d) 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.

Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator o takim naruszeniu bez zbędnej zwłoki zawiadamia także osobę, której dane dotyczą, chyba że:
   a) administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
   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.

6) Jeżeli dany rodzaj przetwarzania - w szczególności z użyciem nowych technologii - ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę.

9. Inspektor danych osobowych

1) Administrator powołuje inspektora ochrony danych, zawsze gdy:
   a) przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;
   b) główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę; lub
   c) główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa.
   d) 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 wynikających z rozporządzenia RODO. Winien on być niezależny, podlegać najwyższemu kierownictwu administratora a także być wspierany przy wykonywaniu swoich zadań.

2) Do zadań inspektora należy:
   a) 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;
   b) 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;
   c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania;
   d) współpraca z organem nadzorczym;
   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.

10. Kodeksy postępowania i certyfikacja

Rozporządzenie RODO nie wprowadza żadnych minimalnych standardów odnośnie środków bezpieczeństwa, które obowiązany jest przyjąć administrator przewiduje natomiast możliwość dobrowolnego wypracowania i stosowania przez zrzeszenia i inne podmioty reprezentujące określone kategorie administratorów lub podmioty przetwarzające kodeksów postępowania doprecyzowujących postanowienia rozporządzenia RODO. Kodeks taki musi być jednakże odpowiednio zatwierdzony a jego przestrzeganie monitorowane.
Alternatywą dla kodeksów postępowań miałby być system dobrowolnej certyfikacji dający potwierdzenie iż dane osobowe przetwarzane są w danym podmiocie zgodnie z prawem.

11. Kary

Wprowadzona została możliwość nakładania wysokich kwotowo kar za naruszenia zasad ujętych w rozporządzeniu RODO. Pojedyncza kara pieniężna może wynieść nawet 20 milionów euro lub 4% całkowitego rocznego obrotu światowego danego podmiotu.

Poruszone wyżej kwestie, mają zastosowanie, co oczywiste, nie tylko do samych administratorów danych ale również do wszelkiego rodzaju podmiotów którym administratorzy takie dane powierzają do przetwarzania.

Należy mieć również na uwadze, iż ostateczny zakres obowiązków i warunków koniecznych do spełnienia przy przetwarzaniu danych osobowych zależeć będzie od rozwiązań przyjętych na gruncie krajowym, w szczególności od ostatecznego kształtu nowej ustawie o ochronie danych osobowych, nad którą trwają obecnie prace legislacyjne.

Warto również pamiętać, iż, na chwilę obecną – zgodnie z przywołanym wyżej projektem ustawy o ochronie danych osobowych, osoba która będzie pełnić w dniu 24 maja 2018 r. funkcję administratora bezpieczeństwa informacji, stanie się z mocy prawa inspektorem ochrony danych i będzie pełniła swoją funkcję do dnia 1 września 2018 r., chyba że do tego dnia (24 maja 2018 r.) administrator zawiadomi Prezesa Urzędu Ochrony Danych Osobowych o wyznaczeniu innej osoby na to stanowisko. Oczywiście osoba ta może sprawować funkcję inspektora danych osobowych również po dniu 1 września 2018 r., wymaga to jednakże odpowiedniego zgłoszenia.