Tomasz Błoński

Wyzwania stojące przed Zakładem Ubezpieczeń Społecznych w związku z wejściem w życie ogólnego rozporządzenia o ochronie danych (2016/679)

1. Wprowadzenie – kształtowanie się przepisów UE dotyczących ochrony osób fizycznych w związku z przetwarzaniem danych osobowych

Rozwój zautomatyzowanych technik przetwarzania informacji, wykorzystujących coraz nowocześniejsze metody i środki informatyki i telekomunikacji, stwarza nowe oraz znacząco zwiększa dotychczasowe możliwości dokonywania różnorodnych operacji na danych. Przynosi także ogromny wzrost wydajności. Ta tendencja – generalnie pozytywna – rodzi jednak nowe zagrożenia. Dotyczą one m.in. stanowionych praw człowieka i podstawowych wolności, a w szczególności prawa do ochrony życia prywatnego, rodzinnego, czci i dobrego imienia oraz decydowania o swoim życiu osobistym.

Prywatność w szerokim rozumieniu to prawo do bycia pozostawionym w spokoju, do samodzielnego kształtowania swojego życia i ochrony miru domowego. Jako wartość prawnie chronioną zaczęto ją rozpatrywać po raz pierwszy na kontynencie amerykańskim pod koniec XIX w. Od tamtego czasu przepisy chroniące prawo człowieka do prywatności były wprowadzane i uaktualniane w poszczególnych krajach budujących demokrację. Pojawiła się węższa definicja prywatności jako prawa osoby do kontrolowania treści oraz przepływu informacji, które jej dotyczą (tzw. prywatność informacyjna).

W społeczności międzynarodowej od kilku dekad próbuje się wytyczyć kierunki prawnej ochrony podstawowych praw i wolności osób fizycznych, w tym prawa do ochrony danych osobowych, które jest ucieleśnieniem prawa do prywatności informacyjnej. Do tych działań można zaliczyć przede wszystkim opracowanie i przyjęcie następujących aktów prawa europejskiego:

– Konwencji o ochronie praw człowieka i podstawowych wolności[1] z 1950 r., której art. 8 ust. 1 brzmi: „Każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji";
– Konwencji nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych o charakterze danych osobowych[2] z 1981 r., której art. 1 brzmi: „Niniejsza Konwencja ma na celu zagwarantowanie, na terytorium każdej ze Stron, każdej osobie fizycznej, niezależnie od jej narodowości i miejsca zamieszkania, poszanowanie jej praw i podstawowych wolności, w szczególności prawa

1 Zob. informacje na stronie internetowej Rady Europy: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005 oraz stronie MSZ: http://bip.ms.gov.pl/pl/prawa-czlowieka/europejski-trybunal-praw-czlowieka/tekst-europejskiej-konwencji-praw-czlowieka-i-podstawowych-wolnosci-wraz-z-protokolami-dodatkowymi/.

2 Zob. informacje na stronie internetowej Rady Europy: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108.

do prywatności, w związku z automatycznym przetwarzaniem dotyczących jej danych osobowych (»ochrona danych«).";

– Karty praw podstawowych Unii Europejskiej[3], której art. 8 brzmi: [...] „Każdy ma prawo do ochrony danych osobowych, które go dotyczą./ [...] Dane te muszą być przetwarzane rzetelnie w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą. Każdy ma prawo dostępu do zebranych danych, które go dotyczą[,] i prawo do spowodowania ich sprostowania./ [...] Przestrzeganie tych zasad podlega kontroli niezależnego organu".

W celu zapewnienia odpowiedniej ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych Parlament Europejski i Rada Unii Europejskiej przyjęli 24 października 1995 r. dyrektywę 95/46/WE[4], która przestanie obowiązywać 25 maja 2018 r. W art. 32 zobowiązuje ona państwa członkowskie Unii Europejskiej do wprowadzenia w życie aktów prawa krajowego (ustaw, rozporządzeń i przepisów administracyjnych) koniecznych do jej wdrożenia.

Polska również stara się zapewnić ochronę prawa do prywatności. W rezultacie tych działań od 19 stycznia 1993 r. obowiązuje w naszym kraju europejska konwencja o ochronie praw człowieka i podstawowych wolności[5], a od 21 kwietnia 1999 r. – konwencja nr 108 Rady Europy[6].

Podstawowym źródłem prawa zapewniającego obywatelom Polski ochronę praw i wolności osób fizycznych, w tym prawa do prywatności, są przepisy Konstytucji Rzeczypospolitej Polskiej[7] oraz akty prawne o ochronie danych osobowych, które są wynikiem wdrożenia do polskiego porządku prawnego przepisów dyrektywy 95/46/WE – ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[8] oraz akty wykonawcze do tej ustawy.

Po ponaddwudziestoletnim okresie obowiązywania dyrektywy 95/46/WE Parlament Europejski i Rada przyjęli 27 kwietnia 2016 r. ogólne rozporządzenie o ochronie danych[9].

Prace nad rozporządzeniem 2016/679 zostały podjęte, ponieważ w ocenie Komisji Europejskiej należało wypracować kompleksowe i spójne podejście gwarantujące pełne

---

3 Karta praw podstawowych Unii Europejskiej (Dz. Urz. UE C 83 z 30.03.2010).

4 Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz. Urz. WE L 281 z 23.11.1995; polskie wydanie specjalne z 2004 r. rozdz. 13, t. 15, s. 355 z późn. zm.).

5 Konwencja o ochronie praw człowieka i podstawowych wolności sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2 (Dz.U. z 1993 r. nr 61, poz. 284).

6 Konwencja Nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzona w Strasburgu dnia 28 stycznia 1981 r. (Dz.U. z 2003 r. nr 3, poz. 25).

7 Konstytucja Rzeczpospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. nr 78, poz. 483).

8 Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz.U. z 2016 r. poz. 922), dalej jako: u.o.d.o.

9 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) (Tekst mający znaczenie dla EOG) (Dz. Urz. UE L 119 z 4.05.2016 r.), dalej jako: rozporządzenie 2016/679.

poszanowanie podstawowego prawa osób fizycznych do ochrony danych osobowych, szczególnie z uwagi na:

– oddziaływanie nowych technologii przetwarzania danych,
– brak dostatecznej harmonizacji obowiązujących w poszczególnych państwach członkowskich UE przepisów o ochronie danych osobowych, mimo wspólnych unijnych ram prawnych,
– globalizację oraz potrzebę poprawy międzynarodowego przekazywania danych w związku z tym, że coraz powszechniej powierza się przetwarzanie danych podmiotom zewnętrznym, bardzo często spoza UE, i pojawiają się problemy z ustaleniem prawa, które ma zastosowanie do przetwarzania oraz ustalania związanej z tym odpowiedzialności,
– potrzebę zapewnienia lepszych rozwiązań instytucjonalnych, aby skutecznie egzekwować przepisy o ochronie danych osobowych,
– potrzebę zwiększenia spójności ram prawnych w zakresie ochrony danych osobowych.

Rozporządzenie 2016/679 weszło w życie 25 maja 2016 r., jednak zgodnie z jego art. 99 ma ono zastosowanie dopiero od 25 maja 2018 r. Jego przepisy będą miały bezpośrednie zastosowanie we wszystkich krajach członkowskich UE zgodnie z art. 288 traktatu o funkcjonowaniu Unii Europejskiej[10].

Dwuletni okres przejściowy ma umożliwić przygotowanie krajów członkowskich do stosowania jego przepisów, w tym w szczególności dostosowanie aktów prawnych poszczególnych krajów członkowskich UE do jego postanowień.

2. Prawo do ochrony danych osobowych a ochrona innych podstawowych praw i wolności osób fizycznych

Z treści przepisów dyrektywy 95/46/WE oraz rozporządzenia 2016/679 wynika, że ich celem nie jest wyłącznie ochrona prawa do ochrony danych osobowych. Obejmują one ochronę wszystkich podstawowych praw i wolności osób fizycznych, które mogą zostać naruszone w wyniku rezultatów niepożądanych zdarzeń zaistniałych w trakcie przetwarzania danych osobowych, takich jak przypadkowe lub niezgodne z prawem zniszczenie, utracenie bądź zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Prawo do ochrony danych osobowych jest traktowane w rozporządzeniu 2016/679 jako jedno spośród praw i wolności osób fizycznych. Z drugiej strony niektóre zdarzenia,

10 Traktat o funkcjonowaniu Unii Europejskiej (Dz. Urz. UE C 326 z 26.10.2012).

których przyczyną jest nieodpowiednia ochrona danych osobowych, są postrzegane jako przyczyna naruszenia innych praw i wolności. W związku z tym można przyjąć, że ochrona osób fizycznych w związku z przetwarzaniem dotyczących ich danych osobowych polega na przeciwdziałaniu i zapobieganiu tym naruszeniom podstawowych praw i wolności osób fizycznych, których źródłem są niepożądane zdarzenia występujące podczas przetwarzania danych osobowych. Z treści rozporządzenia wynika, że ochrona ta wymaga wdrożenia środków technicznych i organizacyjnych odpowiednich w odniesieniu do zidentyfikowanego i oszacowanego ryzyka wiążącego się z przetwarzaniem danych osobowych.

Naruszenie praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych może polegać na naruszeniu prawa do ochrony danych osobowych, które jest szczególnym prawem wśród podstawowych praw i wolności osób fizycznych, albo na naruszeniu innych praw i wolności osób fizycznych, które jest rezultatem niepożądanych zdarzeń zaistniałych podczas przetwarzania danych osobowych. Inne naruszenia zawsze są spowodowane wcześniejszym naruszeniem prawa osób fizycznych do ochrony danych osobowych.

Naruszenie prawa do ochrony danych osobowych będzie polegało przede wszystkim na działaniu niezgodnym z przepisami rozporządzenia 2016/679 precyzującymi prawa osób, których dane dotyczą, oraz obowiązki następujących podmiotów, które decydują o przetwarzaniu danych osobowych lub przetwarzają dane osobowe:

– administratora (który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych),
– podmiotu przetwarzającego (który przetwarza dane osobowe w imieniu administratora), osoby przetwarzającej dane osobowe z upoważnienia administratora lub podmiotu przetwarzającego.

Z kolei naruszenie praw i wolności osób fizycznych innych niż prawo do ochrony danych osobowych, które jest rezultatem niepożądanych zdarzeń zaistniałych podczas przetwarzania danych osobowych, zgodnie z uwagą 75 wprowadzenia do rozporządzenia 2016/679 może polegać na uszczerbku fizycznym lub szkodach majątkowych lub niemajątkowych, w szczególności na:

– dyskryminacji,
– kradzieży tożsamości lub oszustwie dotyczącym tożsamości,
– naruszeniu dobrego imienia,
– naruszeniu poufności danych osobowych chronionych tajemnicą zawodową,
– nieuprawnionym odwróceniu pseudonimizacji lub wszelkiej innej znacznej szkodzie gospodarczej lub społecznej,
– pozbawieniu możliwości sprawowania kontroli nad swoimi danymi osobowymi.

Do naruszenia wymienionych praw i wolności osób fizycznych może dochodzić w szczególności, jeżeli:

– przetwarzane są dane osobowe ujawniające:
  • pochodzenie rasowe lub etniczne,
  • poglądy polityczne,
  • wyznanie lub przekonania światopoglądowe,
  • przynależność do związków zawodowych,

- dane genetyczne,
- dane dotyczące zdrowia lub seksualności,
- dane dotyczące wyroków skazujących i naruszeń prawa lub związanych z tym środków bezpieczeństwa,

– oceniane są czynniki osobowe, w szczególności analizowane lub prognozowane aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się – w celu tworzenia lub wykorzystania profili osobistych,
– przetwarzane są dane osób wymagających szczególnej opieki, w szczególności dzieci,
– przetwarzanie dotyczy dużej ilości danych osobowych i wpływa na dużą liczbę osób, których dane dotyczą.

3. Cel przetwarzania danych osobowych w ZUS oraz kategorie osób, których dotyczą przetwarzane dane

Dane osobowe są przetwarzane w Zakładzie Ubezpieczeń Społecznych zgodnie z celem prowadzonej przezeń działalności, w szczególności takiej jak ustalanie, wymierzanie i pobieranie składek na ubezpieczenia społeczne, ubezpieczenie zdrowotne, Fundusz Pracy, Fundusz Gwarantowanych Świadczeń Pracowniczych i Fundusz Emerytur Pomostowych oraz ustalanie uprawnień do świadczeń z ubezpieczeń społecznych i wypłacanie tych świadczeń.

Zakład przetwarza dane osobowe dotyczące następujących kategorii osób:
– klientów Zakładu,
– pracowników Zakładu,
– stażystów i praktykantów świadczących pracę na rzecz Zakładu,
– osób świadczących usługi dla Zakładu na podstawie umów cywilnoprawnych,
– osób uprawnionych do korzystania z Funduszu Świadczeń Socjalnych Zakładu Ubezpieczeń Społecznych.

Zgodnie z *Planem finansowym Zakładu Ubezpieczeń Społecznych na rok 2017*[11] Zakład obsługuje rocznie około 24,5 mln klientów. W szczególności przetwarza dane osobowe około 14,5 mln osób w związku z prowadzeniem kont ubezpieczonych; 24 mln osób w związku z pobieraniem, rozliczaniem i przekazywaniem do Narodowego Funduszu Zdrowia składek na ubezpieczenie zdrowotne oraz 7,5 mln osób, dla których ustala uprawnienia, oblicza wysokość oraz dokonuje przeliczeń i wypłat emerytur i rent.

11 Załącznik do uchwały nr 35 Zarządu Zakładu z dnia 20 września 2016 r.

Wśród klientów Zakładu, których dane są przetwarzane, są następujące kategorie osób:

– osoby, które mają założone konto ubezpieczonego, na którym ewidencjonowane są składki oraz informacje dotyczące przebiegu ubezpieczeń społecznych; zgodnie z art. 36 ust. 9 ustawy o systemie ubezpieczeń społecznych[12] konto ubezpieczonego jest zakładane na podstawie pierwszego zgłoszenia do ubezpieczeń społecznych,
– ubezpieczeni w rozumieniu ustawy o emeryturach i rentach z FUS[13] , w tym osoby uprawnione do długoterminowego świadczenia z ubezpieczenia społecznego wypłacanego przez Zakład, takiego jak np. emerytura, renta z tytułu niezdolności do pracy, dodatek pielęgnacyjny czy świadczenie przedemerytalne,
– osoby, którym wydawane są zaświadczenia lekarskie o czasowej niezdolności do pracy z powodu choroby, pobytu w szpitalu albo innym zakładzie leczniczym albo o konieczności osobistego sprawowania przez pracownika opieki nad chorym członkiem rodziny,
– osoby uprawnione do uzyskania:
  • środków z subkonta w razie rozwodu, unieważnienia małżeństwa albo śmierci osoby, dla której Zakład prowadzi subkonto,
  • całości lub części wypłaty gwarantowanej zgodnie z dyspozycją emeryta, w wypadku jego śmierci w okresie trzech lat od miesiąca, od którego po raz pierwszy wypłacono emeryturę,
  • zasiłku pogrzebowego,
– osoby, którym wydawane są orzeczenia/ zaświadczenia lekarskie dla celów pozaubezpieczeniowych:
  • sędziowie,
  • prokuratorzy,
  • członkowie rodzin żołnierzy zawodowych,
  • członkowie rodzin funkcjonariuszy Policji, Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego, Centralnego Biura Antykorupcyjnego, Straży Granicznej, Biura Ochrony Rządu, Państwowej Straży Pożarnej i Służby Więziennej,
  • urzędnicy państwowi mianowani,
  • pracownicy samorządowi mianowani,
  • notariusze,
  • mianowani pracownicy Najwyższej Izby Kontroli,
  • mianowani nauczyciele akademiccy,
  • kuratorzy, kuratorzy zawodowi,
  • urzędnicy służby cywilnej,
  • funkcjonariusze celni,

12 Ustawa z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (tekst jednolity: Dz.U. z 2016 r. poz. 963 z późn. zm.).

13 Ustawa z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (tekst jednolity: Dz.U. z 2016 r. poz. 887 z późn. zm.).

  - komornicy sądowi i asesorzy komorniczy,
  - mianowani pracownicy naukowi,
  - mianowani pracownicy Państwowej Inspekcji Pracy,
  - inspektorzy kontroli skarbowej,
- osoby, których zgłoszenia do ubezpieczenia zdrowotnego są kierowane do Zakładu, w tym:
  - członkowie rodzin ubezpieczonych w rozumieniu ustawy o systemie ubezpieczeń społecznych,
  - członkowie rodzin emerytów, rencistów, osób uprawnionych do renty socjalnej, osób uprawnionych do świadczenia przedemerytalnego lub zasiłku, osób uprawnionych do nauczycielskiego świadczenia kompensacyjnego,
  - inne osoby objęte obowiązkiem ubezpieczenia zdrowotnego, niespełniające warunków do objęcia ubezpieczeniami społecznymi,
- lekarze, lekarze dentyści, felczerzy i starsi felczerzy, którzy zgłosili do Zakładu Ubezpieczeń Społecznych wniosek w sprawie upoważnienia ich do wystawiania zaświadczeń lekarskich,
- osoby, których dane osobowe są wykorzystane do identyfikowania płatników składek,
- osoby, które przekazały (osobiście, pocztą, telefonicznie lub przy pomocy środków komunikacji elektronicznej) sprawy do rozpatrzenia w Zakładzie Ubezpieczeń Społecznych,
- osoby, których dane są rejestrowane z uwagi na planowaną lub realizowaną wizytę na terenie obiektów użytkowanych przez Zakład.

4. Obowiązki ZUS wynikające z rozporządzenia 2016/679

W rozumieniu dotychczas obowiązujących przepisów o ochronie danych osobowych Zakład występuje w roli administratora danych, czyli podmiotu, który decyduje o celach i środkach przetwarzania danych. Jego obowiązki są opisane w ustawie o ochronie danych osobowych oraz rozporządzeniach wykonawczych do tej ustawy.

Definicja zawarta w rozporządzeniu 2016/679 jest podobna: zgodnie z tym aktem prawnym Zakład pełni funkcję administratora, czyli podmiotu, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych. Do podstawowych obowiązków Zakładu jako administratora będzie należało w szczególności:

- przetwarzanie danych osobowych zgodnie z podstawowymi zasadami określonymi w tym rozporządzeniu,
- wykonywanie obowiązków wynikających z praw osób, których te dane dotyczą,
- zapewnienie odpowiedniego poziomu bezpieczeństwa tych danych.

Dokładność i rzetelność podczas realizowania przez Zakład obowiązków wynikających z rozporządzenia 2016/679 będzie miała ogromne znaczenie z uwagi na liczbę osób, których dotyczą przetwarzane w Zakładzie dane, zakres tych danych oraz cele ich przetwarzania.

4.1. Obowiązki ZUS dotyczące przetwarzania danych osobowych zgodnie z podstawowymi zasadami określonymi w rozporządzeniu 2016/679

W zakresie podstawowych zasad dotyczących przetwarzania danych osobowych, które są określone w rozporządzeniu 2016/679, na uwagę zasługują dwie zmiany lub uzupełnienia w odniesieniu do analogicznych uregulowań dyrektywy 95/46/EC oraz polskiej ustawy o ochronie danych osobowych. Po pierwsze oprócz tego, że administrator ma obowiązek rzetelnego i zgodnego z prawem przetwarzania danych osobowych, zgodnie z art. 5 ust. 1 lit. a dane te muszą być przetwarzane w sposób przejrzysty dla osoby, której dotyczą (to jedno z jej podstawowych praw wynikających z prawa do ochrony danych osobowych); sposób realizacji tego obowiązku przez administratora jest szczegółowo opisany w art. 12. Po drugie obowiązek określony w art. 5 ust. 1 lit. f – mówiący o tym, że dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo tych danych – został zakwalifikowany do podstawowych zasad przetwarzania danych osobowych; szczegóły dotyczące stosowania wymienionej zasady w praktyce są określone w przepisach rozporządzenia 2016/679 zawartych w rozdziale IV, zatytułowanym „Administrator i podmiot przetwarzający", w tym w szczególności w sekcji 2 tego rozdziału, zatytułowanej „Bezpieczeństwo danych osobowych".

Spełnienie obowiązku przetwarzania danych osobowych zgodnie z prawem oznacza, że dane są przetwarzane przez administratora wyłącznie w przypadkach określonych w art. 6 ust. 1 rozporządzenia 2016/679.

Z punktu widzenia Zakładu podstawę przetwarzania danych osobowych w odniesieniu do klientów Zakładu będą mogły stanowić moim zdaniem:

– zgodnie z art. 6 ust. 1 lit. c rozporządzenia 2016/679 – przepisy określone w prawie krajowym lub w prawie Unii, z których wynika obowiązek prawny dla Zakładu, do wypełnienia którego niezbędne jest przetwarzanie tych danych;
– zgodnie z art. 6 ust. 1 lit. a rozporządzenia 2016/679 – zgoda osoby na udostępnienie tych danych podmiotom spoza Zakładu w jednym lub większej liczbie określonych celów.

W odniesieniu do szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 rozporządzenia 2016/679, podstawę ich przetwarzania w odniesieniu do klientów Zakładu będą stanowić:

– zgodnie z art. 9 ust. 2 lit. b rozporządzenia 2016/679 – przepisy określone w prawie krajowym lub w prawie Unii, z których wynika, że przetwarzanie danych jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez

Zakład lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego lub ochrony socjalnej,

– zgodnie z art. 9 ust. 2 lit. a rozporządzenia 2016/679 – wyraźna zgoda osoby na udostępnienie tych danych podmiotom spoza Zakładu w jednym lub kilku konkretnych celach.

Wymienione wyżej podstawy pochodzące z rozporządzenia 2016/679 nie różnią się w sposób zasadniczy od podstaw wymienionych w obowiązującej w Polsce ustawie o ochronie danych osobowych. Obecnie podstawę do przetwarzania danych osobowych dotyczących klientów Zakładu stanowią:

– w odniesieniu do tzw. danych osobowych zwykłych:
  • zgodnie z art. 23 ust. 1 pkt 2 ustawy u.o.d.o – przepisy określone w prawie krajowym lub w prawie Unii, z których wynika, że przetwarzanie danych jest niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z tych przepisów,
  • zgodnie z art. 23 ust. 1 pkt 1 u.o.d.o. – zgoda osoby na udostępnienie dotyczących jej danych,
– w odniesieniu do tzw. danych osobowych wrażliwych:
  • zgodnie z art. 27 ust. 2 pkt 2 u.o.d.o. – przepis szczególny innej ustawy, który zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony,
  • zgodnie z art. 27 ust. 2 pkt 1 u.o.d.o. – zgoda osoby wyrażona na piśmie na udostępnienie dotyczących jej danych.

4.2. Obowiązki ZUS wynikające z praw osób, których dotyczą dane osobowe przetwarzane w Zakładzie

Zgodnie z obowiązującymi w Polsce przepisami ustawy o ochronie danych osobowych prawa osób, których dane dotyczą, są sformułowane w:

– art. 24 ust. 1 u.o.d.o. jako „obowiązek informacyjny administratora danych w przypadku zbierania danych osobowych od osoby, której dane dotyczą" – ustalono, że wymieniony obowiązek nie dotyczy Zakładu z uwagi na art. 24 ust. 2 tej ustawy, zgodnie z którym art. 24 ust. 1 nie stosuje się, jeżeli osoba, której dane dotyczą, posiada informacje, o których mowa w art. 24 ust. 1 pkt 2 u.o.d.o.,

– art. 25 ust. 1 u.o.d.o. jako „obowiązek informacyjny administratora danych w przypadku zbierania danych osobowych nie od osoby, której dane dotyczą" – ustalono, że obowiązek nie dotyczy Zakładu z uwagi na art. 25 ust. 2 pkt 5 tej ustawy, zgodnie z którym art. 25 ust. 1 nie stosuje się, jeżeli dane są przetwarzane przez administratora danych, o którym mowa w art. 3 ust. 1 u.o.d.o., na podstawie przepisów prawa,

– w przepisach rozdziału 4, zatytułowanego „Prawa osoby, której dane dotyczą", precyzujących zakres prawa każdej osoby do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych – Zakład realizuje te prawa.

Przepisy rozporządzenia 2016/679 znacznie wzmacniają standard ochrony danych osobowych. Zgodnie z rozdziałem III tego rozporządzenia 2016/679 do podstawowych praw osób, których dane są przetwarzane, będzie należało w szczególności:

– prawo do uzyskania od administratora w momencie zbierania przez niego danych informacji wyszczególnionych w art. 13 ust. 1 tego rozporządzenia oraz dodatkowo innych informacji niezbędnych do zapewnienia rzetelności i przejrzystości przetwarzania, które są wyszczególnione w art. 13. ust. 2 rozporządzenia i ewentualnie w art. 13 ust. 3 rozporządzenia – w odniesieniu do Zakładu można przyjąć, że wymienione prawo nie ma zastosowania z uwagi na art. 13 ust. 4 rozporządzenia, przy założeniu, że osoba, której dotyczą przetwarzane w Zakładzie dane, dysponuje informacjami, do których uzyskania jest uprawniona,
– prawo do uzyskania od administratora w rozsądnym terminie (najpóźniej w ciągu miesiąca) informacji wyszczególnionych w art. 14 ust. 1 rozporządzenia oraz dodatkowo innych informacji niezbędnych do zapewnienia rzetelności i przejrzystości przetwarzania wyszczególnionych w art. 14 ust. 2 rozporządzenia, jeżeli administrator uzyskał dane nie od osoby, której dotyczą – w odniesieniu do Zakładu można przyjąć, że wymienione prawo nie ma zastosowania z uwagi na przepis art. 14 ust. 5 rozporządzenia, zakładając, że pozyskiwanie lub ujawnianie danych przez Zakład jest wyraźnie uregulowane prawem Unii lub prawem polskim, przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą,
– prawo do uzyskania na życzenie od administratora powiadomienia, czy przetwarzane są dane dotyczące danej osoby, a jeżeli tak – prawo do uzyskania dostępu do tych danych, prawo do uzyskania informacji niezbędnych do zapewnienia rzetelności i przejrzystości przetwarzania oraz informacji o prawie wniesienia skargi do organu nadzorczego (w Polsce takim organem jest obecnie Generalny Inspektor Ochrony Danych Osobowych),
– prawo do otrzymania od administratora kopii swoich danych osobowych podlegających przetwarzaniu, w myśl art. 15 ust. 3,
– prawo żądania od administratora niezwłocznego sprostowania swoich danych osobowych, które są nieprawidłowe,
– prawo żądania od administratora niezwłocznego usunięcia swoich danych osobowych („prawo do bycia zapomnianym"); administrator będzie miał obowiązek usunąć dane bez zbędnej zwłoki, jeżeli będą zachodzić okoliczności określone w art. 17 ust. 1,
– prawo żądania od administratora ograniczenia przetwarzania danych w przypadkach określonych w art. 18 ust. 1,
– prawo do otrzymania w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego swoich danych osobowych dostarczonych administratorowi oraz prawo do przesłania tych danych innemu administratorowi bez przeszkód ze strony poprzedniego administratora, jeżeli przetwarzanie odbywa się na podstawie zgody lub na podstawie umowy, której stroną jest osoba, której dane dotyczą, oraz przetwarzanie odbywa się w sposób

zautomatyzowany – można przyjąć, że wymienione prawo nie ma zastosowania w odniesieniu do Zakładu z uwagi na to, że Zakład nie przetwarza danych dotyczących swoich klientów na podstawie zgody w myśl art. 6 ust. 1 lit. a lub art. 9 ust. 2 lit. a lub na podstawie umowy w myśl art. 6 ust. 1 lit. b,
- prawo do wniesienia w dowolnym momencie sprzeciwu (z przyczyn związanych z ich szczególną sytuacją) wobec przetwarzania danych dotyczących tych osób opartego na art. 6 ust. 1 lit. e lub f – można przyjąć, że wymienione prawo nie ma zastosowania w odniesieniu do Zakładu z uwagi na to, że Zakład nie przetwarza danych dotyczących swoich klientów na podstawie art. 6 ust. 1 lit. e lub f,
- prawo do tego, by nie podlegać decyzji, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje skutki prawne wobec osoby lub w podobny sposób istotnie na nią wpływa.

Biorąc powyższe pod uwagę, warto przeanalizować rozporządzenie 2016/679 i ustalić, które z praw osób, których dotyczą dane przetwarzane w ZUS, i w jakim zakresie mają zastosowanie w odniesieniu do Zakładu. Ponadto należy rozważyć, które z praw oraz wynikające z tych praw obowiązki Zakładu należy ograniczyć polskim aktem prawnym w myśl art. 23 ust. 1. Ważne jest również, aby określić, kto, w jakim zakresie i w jaki sposób będzie realizował obowiązki Zakładu wynikające z tych praw.

4.3. Obowiązki ZUS, których realizacja ma na celu zapewnienie odpowiedniego poziomu bezpieczeństwa przetwarzanych danych osobowych

Obowiązki administratora, których realizacja ma na celu zapewnienie odpowiedniego poziomu bezpieczeństwa przetwarzanych danych osobowych oraz wskazówki, w jaki sposób należy ten cel osiągać, są określone w szczególności w art. 32 oraz uwadze 83 wprowadzenia do rozporządzenia 2016/679.

Zgodnie z wymienionym przepisem poziom bezpieczeństwa przetwarzanych danych osobowych powinien być odpowiedni do zidentyfikowanego ryzyka naruszenia praw i wolności osób fizycznych wiążącego się z przetwarzaniem danych. W celu zapewnienia odpowiedniego poziomu bezpieczeństwa Zakład jako administrator jest zobowiązany do wdrożenia odpowiednich środków technicznych i organizacyjnych, z uwzględnieniem charakteru, zakresu, kontekstu i celów przetwarzania oraz ryzyka naruszenia praw i wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia.

Rozporządzenie wprost nie nakłada na administratorów obowiązku zarządzania ryzykiem naruszenia praw i wolności osób fizycznych, które wiąże się z przetwarzaniem danych, jednak z treści i logiki przepisów tego rozporządzenia wynika, że właściwą drogą do zapewnienia poziomu bezpieczeństwa odpowiedniego do tego ryzyka jest zarządzanie tym ryzykiem.

Jednocześnie w art. 32 ust. 1 lit. a, b, c i d jest umieszczona wskazówka, że w stosownym przypadku należy wdrażać następujące środki techniczne i organizacyjne, które zapewniają stopień bezpieczeństwa odpowiadający zarządzanemu ryzyku:

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

Termin „ryzyko" nie jest zdefiniowany w rozporządzeniu, chociaż wielokrotnie pojawia się w jego treści w różnym kontekście.

Z uwagi na to, że ryzyko naruszenia praw i wolności osób fizycznych, o którym mowa w rozporządzeniu 2016/679, jest związane z przetwarzaniem danych osobowych, a dane osobowe są szczególnym rodzajem informacji, zarządzanie tym ryzykiem można realizować zgodnie z normą PN-ISO/IEC 27005 dotyczącą zarządzania ryzykiem w bezpieczeństwie informacji oraz innych norm należących do rodziny norm z zakresu systemów zarządzania bezpieczeństwem informacji serii ISO/IEC 27000.

W treści przepisów rozporządzenia 2016/679 występuje wiele terminów, do których można dopasować odpowiednie definicje umieszczone w normie PN-ISO/IEC 27000:2014-11. Do takich pojęć należą w szczególności:
– bezpieczeństwo przetwarzania,
– poufność,
– integralność,
– dostępność,
– odporność systemów i usług przetwarzania,
– ciągłe zapewnianie poufności, integralności, dostępności i odporności systemów i usług przetwarzania – co zgodnie z normą PN-ISO/IEC 27000:2014-11 oznacza ciągłe zapewnienie bezpieczeństwa informacji,
– ryzyko o różnym prawdopodobieństwie i wadze zagrożenia,
– stopień bezpieczeństwa odpowiadający ryzyku,
– ryzyka wiążące się z przetwarzaniem.

Zasadność zarządzania ryzykiem naruszenia praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych zgodnie z normami serii ISO/IEC 27000, gdy dane osobowe są przetwarzane przez podmioty realizujące zadania publiczne, wynika wprost z krajowych przepisów prawa, w szczególności z ustawy o informatyzacji podmiotów realizujących zadania publiczne[14] oraz rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności[15].

Ponadto, niezależnie od nałożonego pośrednio na administratorów obowiązku realizacji procesu zarządzania ryzykiem naruszenia praw i wolności osób fizycznych wiążącego

14 Ustawa z dnia 17 lutego 2005 r. o informatyzacji podmiotów realizujących zadania publiczne (tekst jednolity: Dz.U. z 2014 r. poz. 1114 z późn. zm.).

15 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (tekst jednolity: Dz.U. z 2016 r. poz. 113 z późn. zm.).

się z przetwarzaniem danych, rozporządzenie 2016/679 zobowiązuje Zakład jako administratora do następujących działań, które można traktować jako obligatoryjnie wdrażane techniczne i organizacyjne środki ochrony przetwarzanych danych osobowych:

– prowadzenia rejestru przetwarzanych danych osobowych, obejmującego informacje wymienione w art. 30 ust. 1 tego rozporządzenia; wymieniony rejestr można opracować, wykorzystując w szczególności:
  • istniejącą w Zakładzie dokumentację opisującą sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, która składa się z *Polityki bezpieczeństwa danych osobowych przetwarzanych w Zakładzie Ubezpieczeń Społecznych* oraz *Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Zakładzie Ubezpieczeń Społecznych*,
  • prowadzony przez administratora bezpieczeństwa informacji w Zakładzie Ubezpieczeń Społecznych rejestr zbiorów danych przetwarzanych w Zakładzie,
– współpracy z Generalnym Inspektorem Ochrony Danych Osobowych (GIODO) jako organem nadzorczym – na jego żądanie oraz w ramach wykonywanych przez niego zadań; zakres zadań wykonywanych w Polsce przez organ nadzorczy zostanie doprecyzowany w wyniku dostosowania polskiego prawa do rozporządzenia,
– zgłaszania naruszeń ochrony danych osobowych GIODO; termin „naruszenie ochrony danych osobowych" zasługuje na szczególną uwagę, ponieważ został zdefiniowany jako „naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych"; zgłoszeniu do GIODO nie będą podlegać naruszenia ochrony danych osobowych, jeżeli w ocenie Zakładu będzie mało prawdopodobne, by skutkowały ryzykiem naruszenia praw lub wolności osób fizycznych,
– niezwłocznego zawiadamiania osób, których dane dotyczą, o naruszeniu ochrony danych osobowych; zawiadomienia będą realizowane tylko wówczas, gdy w ocenie Zakładu naruszenie ochrony danych osobowych będzie mogło spowodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych,
– dokonywania oceny skutków planowanych operacji przetwarzania danych osobowych przed rozpoczęciem przetwarzania, 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,
– wyznaczenia inspektora ochrony danych o odpowiednich kwalifikacjach zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych, a także wspierania go w wypełnianiu przez niego zadań; obowiązek wyznaczenia inspektora ochrony danych wynika z tego, że Zakład jest

podmiotem publicznym i że jego główna działalność polega m.in. na przetwarzaniu na dużą skalę danych o stanie zdrowia, które należą do szczególnej kategorii danych osobowych.

5. Podsumowanie

Na Zakładzie jako administratorze spoczywa obowiązek, by zapewnić odpowiedni poziom bezpieczeństwa przetwarzanych przezeń danych osobowych. W związku z tym należy wykorzystać okres przejściowy przewidziany w rozporządzeniu 2016/679 na przygotowanie ZUS do realizacji tych zadań po 25 maja 2018 r.

Tomasz Błoński
zastępca administratora bezpieczeństwa informacji
Zakład Ubezpieczeń Społecznych