LEWIATAN

Uwagi dotyczące zmian w prawie krajowym koniecznych w związku z przyjęciem rozporządzenia w sprawie ochrony danych osobowych.

I. Wstęp

W związku z koniecznością dostosowania polskiego prawa do unijnego Rozporządzenia 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). Konfederacja Lewiatan przedstawia wstępne stanowisko dotyczące obszarów wymagających zmiany. Będzie ono uzupełnianie w toku dalszych prac.

Przed przejściem do uwag Konfederacji pragniemy podkreślić, że prace „wdrożeniowe" powinny w naszej ocenie opierać się na następujących założeniach:

- **dążeniu do utrzymania**- osiągniętej w rozporządzeniu- **harmonizacji na poziomie unijnym,** żeby realnie ułatwić przedsiębiorcom działalność transgraniczną,
- uwzględnieniu, że „doregulowanie" niektórych obszarów przez prawodawcę krajowego może **zmniejszyć konkurencyjność polskiej gospodarki** na tle innych państw UE,
- potraktowaniu tych prac jako **szansy na dostosowanie polskich przepisów do gospodarki cyfrowej** poprzez uchylenie aktów archaicznych (np. tzw. rozporządzenia w sprawie warunków technicznych[1]) lub przez uchwalenie przepisów pozwalających na korzystanie z potencjału danych (np. dotyczących anonimizacji danych telekomunikacyjnych),
- zapewnieniu jasnych i spójnych ram prawnych- **konieczność uchylenia aktów prawnych lub ich części niespójnych z rozporządzeniem,**
- **bliskiej współpracy ze środowiskiem przedsiębiorców**, wzorowanej na modelu z okresu prac nad projektem rozporządzenia, zapoczątkowanej przez Ministerstwo Cyfryzacji.

Poniżej sygnalizujemy kwestię, które będą wymagały uregulowania. Następnie wskazujemy konkretne propozycje zmian.

[1] Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

LEWIATAN

II. Uwagi Ogólne

1. Podstawy przetwarzania danych

Należy zauważyć, że w rozporządzeniu zaszły zmiany, które wpływają na podstawy przetwarzania danych przez administratorów danych i podmioty przetwarzające. Najważniejsze z nich to:

- **zmiana podstawy przetwarzania wynikającej z przepisów prawa**. Dotychczas, zgodnie z ustawą o ochronie danych osobowych (art. 23 ust 1 pkt. 2) administrator mógł przetwarzać dane osobowe jeśli było to niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa. Obecnie – zgodnie z literalną wykładania przepisu- jedynie wynikający z przepisu prawa obowiązek będzie podstawą przetwarzania. Wobec tego wątpliwości może budzić przetwarzanie w oparciu np. o art. 161 ust. 2 Prawa telekomunikacyjnego (mówiący o prawie do przetwarzania określonych danych przez dostawcę usług telekomunikacyjnych) lub przepisy o zamówieniach publicznych stanowiące o możliwości żądania przez zamawiającego danych członków zarządu wykonawcy z KRK. W zależności od charakteru przetwarzania, konieczne będzie zastąpienie obecnego uprawnienia wynikającego z ustawy obowiązkiem przetwarzania danych lub uznanie uprawnienia do przetwarzania wynikającego z ustawy za niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora, które przeważają nad interesem podmiotu danych. W przeciwnym razie, administrator musiałby każdorazowo wykazywać, że jego interes ma charakter nadrzędny w stosunku do interesu podmiotu danych mimo, że działa on w oparciu o obowiązujące przepisy.
- **zawężenie podstaw prawnych pozwalających na przetwarzanie danych wrażliwych.** Dotychczas katalog przepisów mogących zapewniać taka podstawę nie był ograniczony przedmiotowo. Zgodnie z art. 27 ust 2 pkt 2 dane wrażliwe mogły być przetwarzane, jeżeli „przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą i stwarza pełne gwarancje ich ochrony". Zgodnie z RODO, przetwarzanie jest dopuszczalne jeśli 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". Wskazuje to, że konieczne będzie dokonanie szeregu zmian w przepisach prawa pracy, zgodnie z art. 88 RODO (o czym szerzej poniżej). Należy wskazać, że w związku z brzmieniem art. 88 RODO, zasadne byłoby szerokie rozumienie przepisów należących do ww. dziedzin. Oznacza to, że mogłyby to być także ustawy inne niż Kodeks Pracy, w tym ustawy „sektorowe", o ile regulują one kwestie przetwarzania danych osobowych w związku z zatrudnieniem, m.in. w związku z ochroną własności pracodawcy lub klienta, planowaniem i organizacji pracy.
- **w celu zapewnienia zgodności z rozporządzeniem należy usunąć znajdujące się w innych ustawach wymogi uzyskiwania zgody na przetwarzanie danych osobowych w formie pisemnej.** RODO podchodzi szeroko do form wyrażania zgody na przetwarzanie danych „zwykłych". Również w odniesieniu do danych wrażliwych, wymóg zgody pisemnej wykraczałby poza wymóg rozporządzenia, tj. zgody „wyraźnej". Przykładem jest np. art. 38 i 39 ustawy o działalności

LEWIATAN

ubezpieczeniowej i reasekuracyjnej, która wymaga zgody na piśmie na przetwarzanie danych medycznych[2].

2. Konieczność zapewnienia podstaw prawnych do niektórych operacji przetwarzania, jeśli są one niezbędne do realizacji szeroko rozumianych interesów publicznych. Chodzi m.in. o **profilowanie** w calach zwalczania prania pieniędzy, nadużyć finansowych, badania wiarygodności finansowej. Warto zaznaczyć, że takie działania są uzasadnione (a czasem wymagane, np. przez KNF) nie tylko na etapie zawierania umowy (czego dotyczy art. 22 ust.12 pkt a), ale także na jej dalszych etapach. Poleganie na przesłance uzasadnionego interesu administratora i możliwość zgłoszenia sprzeciwu przez podmiot danych nie gwarantuje wystraczającej pewności prawa dla administratorów. Wydaje się zasadne by w ustawie wdrażającej lub w ustawach sektorowych umożliwić profilowanie w celu oceny ryzyka kontraktowego. Środkiem zabezpieczającym, którego wprowadzenia wymaga Rozporządzenie w art., 22 ust 2 b mogłaby być możliwość uzyskania ludzkiej interwencji ze strony administratora, wyrażenie własnego stanowiska i zakwestionowanie decyzji opartej na środkach zautomatyzowanych.

3. **Uchylenie obowiązujących aktów prawnych**

Szereg aktów prawnych dotyczących przetwarzania danych osobowych wymaga **uchylenia,** gdyż państwa członkowskie utraciły możliwość regulowania niektórych kwestii lub ponieważ równoległa realizacja obowiązków krajowych i wynikających z rozporządzenia byłaby niemożliwa. Należy wśród nich wymienić:

- Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych.
- Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji.
- Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.
- Przepisy Rozdziału VII ustawy Prawo telekomunikacyjne, regulujące przetwarzanie danych osobowych, w zakresie w jakim przepisy te nie stanowią implementacji przepisów unijnych.

[2] Art. 38 ust 6 stanowi, że „Wystąpienie zakładu ubezpieczeń o informacje, o których mowa w ust. 2, wymaga pisemnej zgody ubezpieczonego lub osoby, na rachunek której ma zostać zawarta umowa ubezpieczenia, albo jej przedstawiciela ustawowego"

- Rozdział IV ustawy o świadczeniu usług drogą elektroniczną. Reguluje on zasady ochrony danych osobowych w związku ze świadczeniem usług drogą elektroniczną, ale przepisy te nie są implementacją aktów unijnych[3].
- Odnosząc się do konieczności uchylenia ustawy o ochronie danych osobowych warto wspomnieć, że zasadne byłoby wprowadzenie w ustawie „wdrożeniowej" przepisu przejściowego, zgodnie z którym osoby zgłoszone dotychczas do GIODO jako ABI powinny zostać uznane za IOD, o ile administrator nie poinformuje GIODO o jego odwołaniu przez określonym w ustawie terminem. Pozwoli to uniknąć ponownych zgłoszeń (zgodnie z art. 37 ust. 7 RODO administrator musi zawiadomić organ nadzorczy o danych kontaktowych Inspektora).

4. Opcje regulacyjne w rozporządzeniu

Przepisy RODO pozwalają Państwom członkowskim na doprecyzowanie niektórych kwestii w prawie krajowym:

- Zgoda rodzica na przetwarzanie danych dziecka (art. 13 RODO).

Opowiadamy się za obniżeniem wieku, poniżej którego wymagana jest zgoda rodzica lub opiekuna na przetwarzanie danych osobowych dziecka z 16 do 13 lat. Takie rozwiązanie jest spójne z rozwiązaniami prawa cywilnego (zgodnie z art. 15 KC małoletni to osoba, która ukończyła 13 rok życia) oraz dużo bardziej odpowiada stopniowi dojrzałości, która wymagałaby wsparcia dorosłych w udzielaniu zgody na przetwarzanie. Osoby powyżej lat trzynastu posiadają ograniczoną zdolność do czynności prawnych i mogą zawierać umowy należące do umów powszechnie zawieranych w drobnych bieżących sprawach życia codziennego bez zgody przedstawiciela ustawowego. Tym samym zasadne wydaje się ustalenie granicy wieku na poziomie lat trzynastu.

- Zmiany w Kodeksie pracy (art. 88 RODO).

Konieczne jest rozszerzenie katalogu danych, jakie może przetwarzać pracodawca. Chodzi przede wszystkim o dane przetwarzane na etapie rekrutacji, a także o przetwarzanie danych wrażliwych jeśli jest to niezbędne dla celu zapewnienia bezpieczeństwa (np. danych biometrycznych) lub danych o skazaniach za przestępstwa w sprawach gospodarczych (szczegółowe propozycje poniżej).

- przetwarzanie krajowego numeru indentyfikacyjnego (art. 87 RODO)

Przy okazji prac wdrożeniowych wskazane jest uregulowanie kwestii dostępu przedsiębiorców do bazy PESEL w celach wersyfikacji podawanych przez klientów danych osobowych lub realizacji obowiązków

[3] Zob. Komentarz do ustawy o świadczeniu usług drogą elektroniczną, [w:] Świadczenie usług drogą elektroniczną oraz dostęp warunkowy. Komentarz do ustaw Lubasz Dominik (red.), Namysłowska Monika (red.), Opublikowano: LexisNexis 2011. uwagi do artykułu 16 pkt 2 i n.

ustawowych (np. obowiązek rejestracji przez operatorów telekomunikacyjnych kart pre-paid, zgodnie z ustawą „antyterrorystyczna")
W odniesieniu do numeru NIP osoby fizycznej prowadzącej działalność gospodarczą należałoby wskazać, iż przepisy RODO nie mają zastosowania do przetwarzania numeru NIP osoby fizycznej wykonującej działalność gospodarczą.

5. **Realizacja prawa do bycia zapomnianym**

Należy zapewnić, żeby realizacja tego uprawnienia nie naruszała zobowiązań do przechowywania danych wynikających z innych przepisów prawa. Zwłaszcza w przypadkach gdy ustawy nie odnoszą się wprost do przetwarzania danych, ale spełnienie wynikającego z nich obowiązku wymusza przetwarzanie danych, należy zapewnić solidną podstawę przetwarzania.

Aktualnie w ustawie o rachunkowości znajdują się przepisy obligujące do przechowywania danych przez określony czas, jednak z uwagi na wprowadzenie w RODO prawa do ograniczenia przetwarzania danych klient, który nie będzie mógł wyegzekwować prawa do zapomnienia, będzie wnosił o usuniecie danych osobowych, których przedsiębiorca nie potrzebuje przechowywać na potrzeby określone w ustawie o rachunkowości – np. nr telefonu czy adres email. Byłby to duży problem, żeby ingerować w dane takiego „zamkniętego" klienta i próbować zanonimizować czy usunąć takie, które według klienta są zbędne dla realizacji ww. celu. Dlatego w przepisach sektorowych bądź ustawie o rachunkowości powinno być wskazane, że dane klienta przetwarzane w celu realizacji obowiązków wynikających z ustawy o rachunkowości itp. nie są objęte prawem do zapomnienia, czy prawem do ograniczenia danych, jak również, że mogą być przetwarzane w kopiach zapasowych. Według obecnego podejścia GIODO i sądów należy je usuwać również z kopii zapasowych, co nie jest możliwe do wykonania, jak również może ingerować w integralność danych pozostałych klientów.

6. **Klauzula prasowa**- obowiązek państw członkowskich uregulowania relacji rozporządzenia i przepisów dotyczących wolności wypowiedzi (obecna klauzula prasowa z art. 3a ust 2 uodo)- art. 85 RODO.

Propozycja brzmienia przepisu
„Do prasowej działalności dziennikarskiej w rozumieniu ustawy z dnia 26 stycznia 1984 r. – Prawo prasowe (Dz. U. Nr 5, poz. 24, z późn. zm.2) oraz do działalności literackiej lub artystycznej, nie stosuje się przepisów rozdziałów II-VII i IX GDPR, chyba że wolność wyrażania swoich poglądów i rozpowszechniania informacji istotnie narusza prawa i wolności osoby, której dane dotyczą."

7. Konieczność kompleksowego uregulowania kwestii **przetwarzania danych o wyrokach i przestępstwach, zgodnie z art. 10 RODO.** (szerzej na ten temat poniżej). W Polsce, możliwość tzw." background screening" jest niezwykle ograniczona.

LEWIATAN

III. Prawo pracy

Należy sformułować przepisy prawa krajowego tak, aby wynikało z nich uprawnienie do przetwarzania danych sensytywnych na potrzeby stosunku pracy, a przepisy przewidywały odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą (art. 9 ust. 2 lit. b Rozporządzenia). Należy zmienić i doprecyzować przepisy KP aby wprost wskazywały na podstawę prawną do przetwarzania danych pracowników/kandydatów do pracy oraz obowiązek pracownika do przekazania danych pracodawców. Ponadto, rozszerzenie zakresu danych chociażby o dane dotyczące zamieszkania, referencje czy też opinie innych pracodawców o pracowniku etc.
Propozycja brzmienia przepisów zostanie przekazana na dalszym etapie prac.

IV. Uwagi branżowe

1. Biura Informacji Gospodarczych

Podstawą zgłaszanych niżej uwag jest ustawa z dnia 9 kwietnia 2010 r. o udostępnianiu informacji gospodarczych i wymianie danych gospodarczych (t. j. Dz.U. z 2014 r. poz. 1015) (dalej jako uouig).
Po pierwsze wątpliwość budzi przesłanka prawna do przekazania przez wierzyciela informacji gospodarczej o zobowiązaniu dłużnika, tj. art. 14, 15, 16 uouig w związku z art. 23 ust. 1 pkt 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (dalej jako uodo) w zakresie w **jakim przepis ten wskazuje na uprawnienie**. Projekt rozporządzenia unijnego daje możliwość administratorowi danych przetwarzania danych na podstawie przepisów prawa krajowego w celu spełnienia obowiązku prawnego. Pojawia się zatem pytanie czy na podstawie aktualnie obowiązującej uouig wierzyciel nadal będzie mógł przekazać informacje gospodarczą o zobowiązaniu dłużnika na podstawie art. 14, 15, 16 uouig do BIG. Jeśli przetwarzanie danych przez wierzyciela, tj. przekazanie danych do BIG może stać w sprzeczności w unijnym rozporządzeniem to chcielibyśmy wprowadzić takie zapisy do uouig, które nie budziłyby wątpliwości interpretacyjnych, że wierzyciel ma prawo przekazać do BIG dane dłużnika
Wątpliwości budzi również podstawa prawna do przetwarzania danych osobowych przez BIG. W przepisach ustawy nie pojawia się wprost zapis stanowiący o obowiązku przetwarzania danych przez BIG. Takie prawo BIG wynika przede wszystkim z wykładni celowościowej. Tutaj propozycja zmiany przepisów uouig powinna polegać na wskazaniu wprost na obowiązek przetwarzania danych przez BIG stanowiących element informacji gospodarczej.
Ponadto działalność BIG w zakresie przetwarzania danych osobowych opiera się na art. 3 uouig. Oznacza to m.in. udzielanie informacji o danych osobowych będących częścią informacji gospodarczych przetwarzanych przez BIG tylko w trybie uouig. Tutaj propozycja zmiany przepisów uouig powinna polegać na wskazaniu wprost wyłączenia stosowania niektórych zapisów rozporządzenia unijnego.

LEWIATAN

Propozycje szczegółowe:

W związku z obowiązywaniem od maja 2018 r. Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE w celu zapewnienia prawidłowego funkcjonowania biur informacji gospodarczych w Polsce należy wprowadzić następujące zmiany w obowiązującej ustawie z dnia 9 kwietnia 2010 r. o udostępnianiu informacji gospodarczych i wymianie danych gospodarczych (t. j. Dz.U. z 2014 r. poz. 1015):

Art. 1 ust. 2 / ew. dodanie art. 1 ust. 4:
Udostępnianie informacji gospodarczych stanowi realizację celów publicznych w zakresie zapewnienia dostępu do informacji w celu oceny wiarygodności płatniczej oraz stanowi realizację uzasadnionych interesów wierzycieli oraz odbiorców informacji gospodarczych.

Art. 3
W sprawach nieuregulowanych w niniejszej ustawie w zakresie przetwarzania danych osobowych osób fizycznych zastosowanie ma RODO, z wyłączeniem: rozdział III: sekcja 1 (informowanie) sekcja 2 (obowiązek informacyjny), sekcja 3 (poprawianie, „prawo do bycia zapomnianym", przenoszenie danych), sekcja 4 art. 19 ust. 1 (sprzeciw wobec przetwarzania danych opartego na art. 6 ust. 1 lit. e i f).

W odniesieniu do wprowadzenia wyłączenia stosowania, art. 3, należy wskazać, iż te obowiązki uregulowane są przez przepisy ustawy o udostępnianiu informacji gospodarczych i wymianie danych gospodarczych, tj.:

- Informowanie – każdy podmiot ma prawo zwrócić się do biura informacji gospodarczej (dalej jako BIG), w trybie art. 23 ustawy o udostępnianiu informacji gospodarczych i wymianie danych gospodarczych, uzyskać dostęp do informacji gospodarczych (w tym również rejestr zapytań), które go dotyczą.
- Obowiązek informacyjny - wierzyciel zobowiązany jest do wysłania wezwania do zapłaty ze wskazaniem pełnej nazwy i adresu BIG, do którego ma zamiar przekazać informacje gospodarczą. Z wezwania do zapłaty jasno wynika również w jakim celu i zakresie dane będą przetwarzanie przez BIG. Tym samym na BIG nie powinien ciążyć kolejny obowiązek informacyjny. Ponadto należy wskazać, iż w praktyce biuro występuje jako pośrednik w udostępnianiu informacji gospodarczych zatem to nie BIG powinien spełniać obowiązek informacyjny.
- Poprawianie – wierzyciel zobowiązany jest do przekazywania aktualnych informacji gospodarczych, w tym danych osobowych, podobnie jak biuro zobowiązane jest do ujawniania tylko aktualnych danych. Zatem kwestia aktualizacji danych jest już uregulowana w ustawie o udostępnianiu informacji gospodarczych i wymianie danych gospodarczych.
- „prawo do bycia zapomnianym" – podstawową funkcją BIG jest ujawnianie aktualnych informacji dotyczących wiarygodności płatniczej. Zatem jeśli dłużnik żądałby usunięcia informacji gospodarczej

pomimo jej prawdziwości i aktualności to cel, dla którego BIG-i zostały powołane nie byłby realizowany. Zarówno przepisy ustawy o udostępnianiu informacji gospodarczych i wymianie danych gospodarczych jak również Regulaminami Zarządzania Danymi BIG-ów, które uzyskały pozytywne opinie GIODO regulują kwestie usunięcia informacji gospodarczej jak również procesy w jaki sposób można złożyć wnioski o usunięcie informacji gospodarczej.

- Przenoszenie danych – BIG-i są podmiotami prywatnymi jak również posiadają zupełnie odrębne systemy informatyczne. Możliwość przenoszenia danych z jednego BIG do innego BIG będzie olbrzymim obciążeniem dla każdego BIG.
- Sprzeciw – przetwarzanie danych przez BIG odbywać się będzie na postawie art. 6 ust. 1 lit. e i f RODO. Tym samym taki sprzeciw nie powinien mieć zastosowania w przypadku przetwarzania danych osobowych będących elementem informacji gospodarczych. Podstawową funkcją BIG jest ujawnienie aktualnych informacji dotyczących wiarygodności płatniczej. Zatem jeśli dłużnik złożyłby sprzeciw wobec przetwarzania jego danych przez BIG, co w rzeczywistości oznaczać będzie żądanie usunięcia informacji gospodarczej pomimo jej prawdziwości i aktualności to cel, dla którego BIG-i zostały powołane nie byłby realizowany.

Art. 7 ust. 1

Przedmiotem działalności gospodarczej biura jest pośrednictwo w udostępnianiu informacji gospodarczych, polegające na przyjmowaniu informacji gospodarczych od wierzycieli, przechowywaniu i ujawnianiu tych informacji jak również przetwarzaniu danych osobowych będących częścią informacji gospodarczych.

2. Ustawa Prawo telekomunikacyjne

a. Rozporządzenie co do zasady nie zmienia regulacji wynikających z dyrektywy 2002/58, tzw. e-privacy - patrz motyw 173, art. 95 Rozporządzenia. Należy wyraźnie podkreślić, że dyrektywa ta dotyczy przede wszystkim takich kwestii jak przetwarzanie danych transmisyjnych, danych o lokalizacji, umieszczania plików cookie czy przesyłania komunikatów handlowych. Znaczna część przepisów działu VII ustawy Prawo telekomunikacyjne pt. „Tajemnica telekomunikacyjna i ochrona danych użytkowników końcowych” **wykracza poza te kwestie** i wprowadza dodatkowy reżim ochrony dotyczący danych osobowych abonentów, jakim jest „tajemnica telekomunikacyjna”. Przykładem może być włączenie innych danych (osobowych) niż transmisyjne i dane o lokalizacji, czyli „danych o użytkowniku”, do kategorii „tajemnica telekomunikacyjna” (art. 159 PT) i objęcie ich szczególną regulacją (m.in. 161, 162, 172, 174, ale także o inne z rozdziału o tajemnicy telekomunikacyjnej, art. 57 ust. 1 pkt 3). Taka dodatkowa regulacja, jeśli utrzyma się w mocy, **stanie się niezgodna z Rozporządzeniem**. Dlatego powstaje konieczność uważnego przejrzenia przepisów Prawa telekomunikacyjnego pod kątem ich zgodności z - nadrzędnym wobec polskiej ustawy - Rozporządzeniem i wyeliminowania przepisów sprzecznych z Rozporządzeniem.

b. Upoważnienie do profilowania klienta na potrzeby weryfikacji jego **zdolności kredytowej przy zawieraniu umowy** o świadczenie usług telekomunikacyjnych lub na potrzeby wykrywania nadużyć telekomunikacyjnych w trakcie wykonywania umowy powinno zostać określone wprost w prawie krajowym (w związku z art. 22 ust. 2 lit. b Rozporządzenia). Bez tych narzędzi prowadzenie działalności telekomunikacyjnej stanie się obciążone dodatkowym ryzykiem (które nie występuje dziś).

c. Warto byłoby również rozważyć **poszerzenie katalogu danych dozwolonych do przetwarzania przez przedsiębiorców telekomunikacyjnych,** ułatwiających weryfikację tożsamości klientów, w tym m.in. wciąż problematyczna kwestia skanów dowodów osobistych, czy też innych dokumentów tożsamości ze zdjęciem (problem ich kopiowania i przechowywania), co wydaje się również zbieżne z nowo nałożonym obowiązkiem rejestracji kart prepaid wraz z weryfikacją tożsamości klientów.

d. Implementacja RODO jest dobrą okazją żeby uporządkować, kwestie związane z ochroną danych użytkowników końcowych/abonentów w PT.

RODO przewiduje możliwość przetwarzania danych w przypadku pozbawieniu ich charakteru identyfikującego konkretną osobę (pseudonimizacja), podobnie Dyrektywa 2002/58/WE dopuszcza możliwość przetwarzania danych po ich uprzedniej anonimizacji. W aktualnie obowiązujących przepisach Pt nie można znaleźć jednoznacznej odpowiedzi na pytanie czy i w jakich warunkach dopuszczalne jest przetwarzanie danych użytkowników końcowych po dokonaniu anonimizacji podczas gdy w innych krajach UE przepisy określają warunki w jakich jest to dopuszczalne. Z informacji jakie docierają do nas z Czech i Niemiec wynika, że w krajach tych instytucje państwowe czy samorządowe korzystają z rozwiązań dostarczanych przez operatorów telekomunikacyjnych, pozwalających na analizy Big Data zanonimizowanych danych transmisyjnych (danych o ruchu). Rozwiązania te umożliwiają m.in. dostęp do unikalnych informacji o rozmieszczeniu i przemieszczaniu się ludności w skali oraz szczegółowości niedostępnej dotychczas żadnymi innymi technikami. Pozwala to m.in. na monitorowanie imprez masowych, wykrywanie dużych skupisk ludności (np. niezgłoszone wcześniej imprezy masowe, nielegalne wyścigi etc.), odpowiednie reagowanie w przypadku wystąpienia sytuacji kryzysowych, projektowanie nowych dróg, linii kolejowych w miejscach, w których jest to najpilniejsze, monitorowanie ruchu na autostradach (szybkie wykrywanie zatorów) i zarządzanie nim etc. Rozwiązania oparte o analizy Big Data zanonimizowanych danych o ruchu mogą przynieść wymierne korzyści dla państwa, obywateli i przedsiębiorców.
Do poczytania ogólnodostępna opinia prof. Piątka http://ikar.wz.uw.edu.pl/numery/22/pdf/45.pdf

e. Kolejną kwestią, wartą poruszenia jest dostęp do bazy PESEL dla operatorów dla celów potwierdzenia zgodności podanych (imię, nazwisko, numer PESEL) przez abonenta danych ze stanem faktycznym. Od potwierdzenia zgodności danych uzależnione będzie rozpoczęcie świadczenia usług przedpłaconych po wejściu w życie ustawy antyterrorystycznej. Dostawca usług telekomunikacyjnych nie posiada natomiast kompletnej bazy danych zawierającej imię, nazwisko, numer PESEL wszystkich potencjalnych abonentów. Z punktu widzenia bezpieczeństwa państwa i

obywateli (ograniczenie rejestrowania kart na cudze dane albo dane nieprawdziwe) jak również w celu zminimalizowania obciążeń jakie w związku z koniecznością rejestracji ponosić będą przedsiębiorcy postulat ten jest uzasadniony.

3. Propozycje zmian w prawie w zakresie ubezpieczeń na życie i wypadkowych – dział I

a) Doprecyzowanie kwestii **podstaw prawnych przetwarzania danych,** w tym wrażliwych niezbędnych zakładowi ubezpieczeń w celu ustalenia ryzyka ubezpieczeniowego oraz do ustania odpowiedzialności towarzystwa w przypadku zgłoszenia roszczeń dotyczących zdarzeń ubezpieczeniowych w zakresie ubezpieczeń na życie i wypadkowych.

- Zamiana wymogu zgody pisemnej na zgodę wyraźną

W obecnym stanie prawnym, przetwarzanie danych wrażliwych przez zakłady ubezpieczeń poddane jest wymogowi zdobycia pisemnej zgody ubezpieczonego (art. 38 i 39 ustawy o działalności ubezpieczeniowej i reasekuracyjnej – UUIR), którego dane medyczne mają być przetwarzane. RODO wymaga złożenia wyraźniej zgody w przypadku przetwarzania danych wrażliwych, co oznacza, że forma pisemna na przetwarzanie takich danych, jak jest to uregulowane w art. 38 i 39 UUIR, nie powinna być wymagana. Należy odpowiednio zmienić przepis UUIR, by wymagana była zgoda wyraźna.

- Dookreślenie obowiązku/uprawnienia dotyczącego przetwarzania danych przez zakład ubezpieczeń, w tym danych wrażliwych, związanych z oceną ryzyka ubezpieczeniowego oraz dochodzeniem/obroną roszczeń jako podstawy prawnej wynikającej z przepisów prawa a nie ze zgody podmiotu danych.

Przy okazji zmian warto byłoby zaadresować istniejący obecnie problem uzależniania możliwości dokonania oceny ryzyka ubezpieczeniowego- niezbędnego do zawarcia umowy- do zgody podmiotu danych. Przetwarzanie danych wrażliwych przez zakład ubezpieczeń jest czynnością konieczną do określenia ryzyka ubezpieczeniowego oraz odpowiedzialności zakładu ubezpieczeń co jest związane ściśle z prowadzeniem działalności ubezpieczeniowej na rynku regulowanym. Mówi o tym art. 33 UUIR np. odnośnie ustalania poziomu składki ubezpieczeniowej. W obecnym stanie prawnym zbieranie danych, w tym wrażliwych, w celu oceny ryzyka jest uprawnieniem zakładu ubezpieczeń do przetwarzania danych wrażliwych, za zgodą podmiotu danych (Art. 38 ust 2 pkt 6 UUIR), jak i ich udostępniania innemu zakładowi ubezpieczeń (Art. 39 ust 1 UUIR). Wątpliwości budzi dobrowolność wyrażenia tej zgody/ jej odwołania, gdyż bez niej może nie dojść, w przypadkach wymagających oceny ryzyka, do zawarcia umowy ubezpieczenia, o co wnioskuje do zakładu ubezpieczeń ubezpieczający, lub może dojść do wypłaty nieadekwatnych świadczeń na szkodę zakładu ubezpieczeń. Rodzi to duże ryzyko ubezpieczeniowe dla zakładu ubezpieczeń związane z brakiem wiedzy na temat stanu zdrowia ubezpieczonego oraz możliwość nadużyć w postaci ubezpieczenia od zdarzenia znanego ubezpieczonemu, które może nastąpić na skutek znanego mu, lecz zatajonego przed zakładem

ubezpieczeń stanu zdrowia, np. stan nieuleczalnej choroby, która kończy się śmiercią ubezpieczonego (to nie jest wypadek losowy tylko stan znany).
Ponadto w przypadku odwołania zgody lub złożenia sprzeciwu w tym zakresie w terminie późniejszym zakład ubezpieczeń może nie móc prawidłowo wykonać oceny ryzyka lub ustalić swej odpowiedzialności z tytułu roszczeń (np. nie może już uzyskać informacji o stanie zdrowia z placówek medycznych gdzie leczył się ubezpieczony). Może to prowadzić do prób wyłudzeń w obszarze roszczeń. Ma to też negatywny wpływ na rozpatrywanie reklamacji w wyniku braku możliwości ustalenia przez zakład ubezpieczeń stanu faktycznego. Zasadniczo złożenie sprzeciwu/odwołanie zgody w powyższym zakresie powinno skutkować rozwiązaniem umowy ubezpieczenia, lecz w obecnym stanie prawnym nie ma takiej możliwości.
Biorąc pod uwagę powyższe oraz zapisy art. 9 ust 2 RODO, które nie umożliwiają przetwarzania danych wrażliwych przez zakład ubezpieczeń na podstawie przepisu prawa, wskazanym by było, aby przepis UUIR jasno wskazywał na obowiązek i uprawnienie przetwarzania przez zakład ubezpieczeń danych osobowych w tym danych wrażliwych w celach wykonywania działalności ubezpieczeniowej, a w szczególności wykonywania umów ubezpieczenia w tym ustalenia, dochodzenia lub obrony roszczeń jako podstawa prawna umożliwiająca prawidłowe wykonywanie działalności ubezpieczeniowej przez zakład ubezpieczeń bez zgody podmiotu danych.
Nadmienić należy, że prawidłowa ocena ryzyka ubezpieczeniowego oraz ustalenie odpowiedzialności zakładu ubezpieczeń ma wpływ na wyliczanie składek ubezpieczeniowych oraz sum ubezpieczenia. Zwrócić należy uwagę, że sama chęć zawarcia umowy ubezpieczenia przez podmiot danych, co wiąże się/może się wiązać z przetwarzaniem danych wrażliwych, dotyczy również przetwarzania tych danych przez zakład ubezpieczeń w celach ściśle związanych z prowadzoną działalnością gospodarczą. Zatem dodatkowe zgody podmiotu danych dotyczące danych osobowych przetwarzanych w związku z wykonaniem umowy ubezpieczenia wydają się nieuzasadnione i wprowadzają sytuacje niejednoznaczne interpretacyjnie w zakresie przetwarzania tych danych.
W razie gdyby przetwarzanie miało nadal opierać się o zgodę podmiotu danych należałoby wprowadzić w UUIR doprecyzowanie, że cofnięcie zgody/wyrażenie sprzeciwu w zakresie przetwarzania danych osobowych skutkować winno rozwiązaniem umowy ubezpieczenia/odstąpieniem od udzielanej ochrony ubezpieczeniowej w przypadku umów zawieranych na cudzy rachunek. Działanie takie byłoby określane jako zawinione przez podmiot danych, ponieważ uniemożliwia rzetelne wykonanie umowy ubezpieczenia przez zakład ubezpieczeń, co może skutkować wyłudzeniami.
Biorąc pod uwagę powyższe propozycje w naszej ocenie rozwiązanie z określeniem podstawy prawnej przetwarzania danych wrażliwych (pozyskiwanie od placówek medycznych /udostępnianie innym zakładom ubezpieczeń/pozyskiwanych z NFZ) niezbędnych do wykonania umowy ubezpieczenia wprost w UUIR wydaje się lepsze.

b) Profilowanie w odniesieniu do oceny ryzyka i ustalenia odpowiedzialności zakładu ubezpieczeń.

Profilowanie jest częścią procesu oceny ryzyka w zakładzie ubezpieczeń. Ocena ta może być wykonywana przez człowieka jak również w sposób zautomatyzowany. Biorąc pod uwagę zapisy art. 6 ust 1 pkt f) RODO, podmiot danych może złożyć sprzeciw dotyczący profilowania, taki sprzeciw może

uniemożliwić prawidłową ocenę ryzyka ubezpieczeniowego oraz podnieść koszty wykonania tej oceny. Biorąc pod uwagę, że ocena ryzyka jest ściśle związana z wykonywaniem działalności ubezpieczeniowej, wskazanym byłoby dookreślenie uprawnienia zakładu ubezpieczeń do profilowania w celu i zakresie niezbędnym do oceny ryzyka ubezpieczeniowego jako podstawy prawnej do przetwarzania danych, w tym wrażliwych, przez zakład ubezpieczeń w tym zakresie. W ślad za tym wskazane by było, dla zachowania spójności, zniesienie obowiązku informowania podmiotu danych przez zakład ubezpieczeń w zakresie określonym w art. 21 ust. 1.
W wyniku doregulowania zakład ubezpieczeń dysponowałby podstawą prawną do dokonywania profilowania w celu oceny ryzyka ubezpieczeniowego oraz nie musiałby informować o prawie sprzeciwu podmiotu danych w tym zakresie. Bez takiego doprecyzowania przepisów UUIR biorąc pod uwagę treść art. 21 ust 1 RODO trudno będzie wskazać podstawę prawną do profilowania w celu oceny ryzyka ubezpieczeniowego przez zakład ubezpieczeń w szczególności gdy podmiot danych złoży w tym zakresie sprzeciw, co przy obecnym kształcie przepisów UUIR uniemożliwiałoby wykonanie prawidłowej oceny ryzyka, w szczególności gdy proces ten zachodziłby w sposób zautomatyzowany lub w dużej części zautomatyzowany. Nadmienić trzeba, że przy prostych produktach ubezpieczeniowych proces ten może być wykonany w całości w sposób automatyczny np. przy zawieraniu umowy drogą elektroniczną. Jak wskazano powyżej profilowanie to wiąże się ściśle z wykonywaniem działalności ubezpieczeniowej i ma wpływ na możliwość jej prawidłowego prowadzenia.
Taka zmiana miałaby pozytywny wpływ na uproszczenie zawierania i wykonania umowy ubezpieczenia, klarowność praw i obowiązków stron (ubezpieczających a także ubezpieczonych w zakresie w jakim umowa daje im określone prawo), przeciwdziałanie wyłudzeniom na skutek odwołania przez podmiot danych zgody na przetwarzanie danych niezbędnych do wykonania umowy ubezpieczenia przez zakład ubezpieczeń.

4. Uwagi sektora bankowego i finansowego

W prawie bankowym powinna być zostać wskazana **podstawa do profilowania przez banki.** Aktualnie takiej podstawy można szukać w przepisach prawa bankowego nakazującym badanie zdolności kredytowej, jednak banki profilują klientów również na inne potrzeby –antyfraudowe, anty money laundering-owe. RODO wymaga uzyskania zgody na profilowanie, stąd- żeby umożliwić realizację tych celów lepsza dla banków byłaby samoistna podstawa wynikająca z prawa bankowego, pozwalająca profilować bez zgody a np. pod warunkiem uprzedniego powiadomienia klienta.
Profilowanie powinno być również przewidziane w przepisach mających zastosowanie do podmiotów prowadzących działalność gospodarczą w zakresie udzielania kredytów konsumenckich jako instytucja pożyczkowa w rozumieniu ustawy z dnia 12 maja 2011 r. o kredycie konsumenckim (Dz. U. z 2015 r. poz. 1357).
Propozycje dalszych zmian zostaną przekazane na dalszym etapie prac.

Konfederacja Lewiatan, 18/07/2016r.
KP/304/142/MP/2016