Nowe ramy ochrony danych osobowych w UE. Wyzwania dla Polski.

Raport pokonferencyjny

Cyberlaw.pl

Warszawa, 24 września 2015

Raport stanowi podsumowanie konferencji o tym samym tytule, która odbyła się 18 września 2015r. w Warszawie oraz zawiera praktyczne komentarze. Z uwagi na jego charakter zostało w nim zawarte sprawozdanie z konferencji oraz najciekawsze pytania uczestników.

Tym samym raport ten otwiera cykl dokumentów tworzonych przez Cyberlaw, których celem jest przybliżenie wiedzy na temat zmieniających się przepisów na arenie europejskiej oraz przepisów krajowych (więcej informacji na s.17).

Dokument ten jak i pozostałe pomogą aktywnie monitorować zmiany i przygotować się do sprawnego wdrożenia nowych regulacji

Nowe ramy ochrony danych osobowych w UE.
Wyzwania dla Polski.

Raport pokonferencyjny

bez potrzeby generowania nadmiernych kosztów i działań.

Dziękuję mówcom konferencji za ich aktywny wkład w dyskusję oraz autoryzację ich wypowiedzi w krótkim czasie. Dziękuję czytelnikom za zainteresowanie tematyką zmieniających się przepisów i zapraszam do lektury.

Beata Marek
cyberlaw.pl

Wydawca, grafika, skład i łamanie

Cyberlaw.pl

Cyberlaw jest firmą prawniczą, specjalizującą się
w prawie nowych technologii.

www.cyberlaw.pl

Spis treści:

Podziękowanie za współpracę przy stworzeniu raportu pokonferencyjnego

GIODO
Generalny Inspektor
Ochrony Danych Osobowych

Podziękowanie za promocję raportu pokonferencyjnego

LEX
a Wolters Kluwer business

Sprawozdanie z konferencji „Nowe ramy ochrony danych osobowych w UE. Wyzwania dla Polski".

W dniu 18 września 2015r. w Warszawie została zorganizowana przez Generalnego Inspektora Ochrony Danych Osobowych we współpracy z Ministerstwem Administracji i Cyfryzacji oraz Posłem do Parlamentu Europejskiego Michałem Bonim konferencja „Nowe ramy prawne ochrony danych osobowych w UE. Wyzwania dla Polski.

W trakcie otwarcia wydarzenia **dr Edyta Bielak-Jomaa** (GIODO) zaznaczyła, że obecnie projekt jednolitego rozporządzenia o ochronie danych osobowych znajduje się w fazie trilogu i po jego zakończeniu należy spodziewać się wdrożenia nowych przepisów. **Michał Boni** dodał, że od połowy 2016r. do połowy 2018r. będziemy wdrażać nową regulację w Unii Europejskiej, a nowe rozporządzenie sprzyja interoperacyjności. Przypomniał, że w Parlamencie Europejskim zaczynają się prace nad jednolitym rynkiem cyfrowym i nowe rozporządzenie jest potrzebne. Podkreślił, że potrzebujemy jasnego planu wdrożenia tych przepisów. Wdrożenie powinno wiązać się także z edukacją obywateli - użytkowników Internetu, firm i pozostałych partnerów, którzy będą te przepisy stosować. **Jurand Drop** (Podsekretarz stanu w Ministerstwie Administracji i Cyfryzacji) wskazał, że obecnie rozpoczynamy ważną dyskusję jak wdrożyć zmianę paradygmatu, która wynika ze zmian technologicznych i zmian funkcjonowania społeczeństw. Dodał, że dla MAiC kierunkiem zasadniczym przy tworzeniu nowych regulacji z zakresu ochrony danych osobowych jest zwiększenie ochrony danych bez nadmiernego obciążania biznesu. **Jan Philip Albrecht** (Poseł sprawozdawca w sprawie rozporządzenia o ochronie danych) podsumował, że nowe przepisy umożliwią lepszą współpracą partnerów biznesowych działających w Unii Europejskiej jak i poza jej obszarem. Stanie się tak dzięki ujednoliceniu standardów. Podsumował, że do końca tego roku powinny zostać przeprowadzone ostatnie uzgodnienia w zakresie rozdziału II i III projektu rozporządzenia i planowane jest, by zakończyć negocjacje co do dyrektywy w zakresie ochrony danych osobowych przetwarzanych na potrzeby ścigania przestępstw. Jeśli tak się stanie to wiosną 2018r. nowe regulacje zaczną obowiązywać.

Sesję pierwszą (Reforma ochrony danych osobowych: wyzwania na lata 2015 – 2018) rozpoczęło wystąpienie **dr Edyty Bielak-Jomaa**, GIODO. Podkreśliła ona, że nowe przepisy unijne wymuszą reformę krajowego porządku prawnego. Przepisy rozporządzenia będą stosowane bezpośrednio we wszystkich krajach czlonkowskich, co doprowadzi do ujednolicenia prawa materialnego. Niezbedne jednak bedzie wprowadzenie nowych uregulowań proceduralnych określających m.in. status i kompetencje organów ds. ochrony danych osobowych, w każdym państwie UE. Ponadto polski ustawodawca musi dokonać przeglądu wielu aktów prawnych, m.in. po to, aby ujednolicić definicje i wprowadzić nowe.

W rozporządzeniu są pewne rewolucyjne rozwiązania w stosunku do tych, które są obecnie przyjęte w Polsce. Dlatego GIODO zaraz po przedstawieniu pakietu zmian przez Komisję Europejską w 2012r. rozpoczął daleko idącą współpracę z MAiC i różnymi organizacjami, by stworzyć ramy prawne dla prawidłowego funkcjonowania przepisów w polskim porządku prawnym.

Z punktu widzenia GIODO ważnym rozwiązaniem jest przyznanie orgranom ds. ochrony danych kompetencji do nakładania kar finansowych. Jest to niezbędne do skutecznej realizacji prawa do ochrony danych osobowych. Instytucja *privacy by*

design czy *prviacy by default* dotąd nieznane polskiej regulacji będą obligowały GIODO, by spojrzeć na ochronę danych osobowych na nowo w kontekście odpowiedzialności wszystkich tych podmiotów, które tych zasad będą musiały przestrzegać. Dlatego tak ważne jest ciągłe podnoszenie poziomu wiedzy na temat zmieniajacych sie przepisów, co należy do priorytetów działalności GIODO.

Minister Edyta Bielak – Jomaa podkreślała również, jak ważne jest takie skonstruowanie nowych przepisów, by były elastyczne, nadążały za rozwojem cywilizacyjnym i technologicznym, a jednocześnie nie obniżyły dotychczasowego poziomu ochrony danych.

Michał Boni dodał, że reformę ochrony danych należy widzieć w kontekście rewolucji cyfrowej. Przepisy mają zmierzać do stworzenia wspólnego rozwiązania dla UE i tym samym zwiększenia rozwoju przedsiębiorstw, umożliwienia łatwiejszego wejścia na rynki. Jednocześnie rozporządzenie może być podstawą dla tworzenia rozwiązań dla państw trzecich. Nadmienił, że w urzędach zmieniło się myślenie na temat ochrony danych osobowych. Nastąpiło to dzięki jedności działania administracji z innymi partnerami i tu w szczególności rolę takiej spajającej jednostki odgrywa MAiC, który nowe przepisy widzi całościowo i współpracuje z różnymi partnerami, prowadząc otwarty dialog.

Pomiędzy organami we Wspólnocie musi istnieć współpraca zwłaszcza w zakresie prawidłowego działania procedury *one-stop-shop*, którą przewiduje projekt rozporządzenia. Natomiast Europejska Rada Ochrony Danych, w skład której mają wejść przedstawiciele wszystkich 28 niezależnych organów nadzorczych, a która zastąpi obecną Grupę Roboczą Art. 29, powinna mieć prawo tworzenia kodeksów dobrych praktyk i możliwość wiążącej interpretacji przepisów.
Zdaniem Michała Boniego proponowane podejście do zabezpieczenia danych osobowych oparte na samodzielnej analizie ryzyka (ang. *Risk Based Approach*) jest istotne. Samo jego zdefiniowanie jest trudne na gruncie przepisów, ale jest wiele rozwiązań, na których można się oprzeć w jego wdrożeniu. Jeżeli administrator danych nie będzie potrafił zdefiniować ryzyka i go zmierzyć, to powołanie oficera ochrony danych, który będzie to potrafił, okaże się niezbędne.

Dyskusyjny jest aspekt zdefiniowania anonimizacji danych i określenia własności danych. Widać to zwłaszcza na przykładzie danych medyczynych gdzie problematyczne wydaje się dookreślenie, kiedy lekarz jest właścicielem danych, a kiedy osoba fizyczna, której dane dotyczą. Podobnie rzecz ma się z monetyzacją danych osobowych i ich personalizacją, co z jednej strony jest korzystne, ale i może okazać się ryzykowne dla osób, których dane dotyczą.

W regulacji powinny być zostawione elastyczne furtki, by dostosować regulację do zmieniającego się otoczenia informatycznego, a rolą Europejskiej Rady będzie interpretacja przepisów.

Jurand Drop kontynuował rozpoczęty przez Michała Boniego wątek o potrzebie istnienia MAiC i pełnienia przez urząd specyficznej roli łącznika i podmiotu dobrze zorientowanego w zmieniających się technologiach informacyjnych i komunikacyjnych oraz potrzebach wprowadzenia regulacji adekwatnych do tych zmian. Dlatego też to Ministerstwu odpowiedzialnemu za rozwój społeczeństwa informacyjnego powierzone zostały prace nad rozporządzeniem dotyczącym ochrony danych osobowych. Dodał, że pracując przy tworzeniu europejskich aktów prawnych i

uczestnicząc w dyskusjach o rynku cyfrowym dostrzegł problem „odrębność światów“ interesariuszy z różnych obszarów gospodarki i życia społecznego. Instytucje, organizacje czy firmy zajmujące się inteligentnymi sieciami w energetyce rzadko dostrzegają kwestię ochrony danych osobowych – dopiero Komisja Europejska musi o tym przypominać. Dyskusje wokół inteligetnych domów i miast traktują dostęp do danych osobowych jako całkowicie naturalny, nie stwarzający zagrożeń dla mieszkańców. Firmy czy legislatorzy zajmujący się biznesem traktują ochronę danych osobowych jako temat marginalny. Dlatego zdaniem podsekretarza stanu w MAiC należy podkreślać wpływ przepisów o ochronie danych osobowych w różnych sektorach gospodarki, ich horyzontalne znaczenie. Samo ministerstwo jest właśnie reprezentantem tego tematu w rozmaitych gremiach decyzyjnych.

MAiC już dzisiaj przygotowuje się do dostosowania legislacji polskiej do zmian spowodowanych przez rozporządzenie unijne. Jak wskazał min. Drop, ministerstwo liczy w tym zakresie na wsparcie i zaangażowanie w te prace ze strony GIODO, najlepiej zorientowanej instytucji w praktycznym stosownaniu prawa ochrony danych osobowych.

MAiC dostrzega jednocześnie, że w wyniku zmian technologicznych poziom ochrony praw może zostać łatwo obniżony – dane te mogą wyciec łatwiej, są globalnie przetwarzane i przekazywane. Nowe przepisy powinny zwiększyć poziom ochrony danych obywateli i jednocześnie znaleźć równowagę ochrony z łatwością prowadzenia biznesu. Rolą nowych przepisów nie jest bowiem ograniczanie możliwosci firm do wykorzystania danych, ale umożliwienie im tego bez naruszenia praw obywateli. Większy poziom ochrony danych osobowych przez przedsiębiorstwa przekłada się również na większe zaufanie użytkowników , a co za tym idzie – na szersze wykorzystanie dostępnych w Internecie usług i większe dochody przedsiębiorstw.

Jurand Drop podkreślił, że w tworzeniu prawa w Unii Europejskiej bierze udział wielu interesariuszy, negocjacje są prowadzone długo i skrupulatnie, dzięki czemu akty prawne są dobrze przemyślane. Jest to niewątpliwa zaleta stanowienia prawa właśnie na poziomie europejskim. Rozporządzenie ma szansę być wzorem dla światowych regulacji, a także dla przepisów europejskich w innych dziedzinach. Przykładem może być dyrektywa dot. bezpieczeństwa sieci i informacji (ang. *Network & Information Security*) gdzie np. problemy terytorialności i jurysdykcji można próbować rozwiązać analogicznie jak w przepisach rozporządzenia dot. ochrony danych osobowych.

Dr Karolina Mojzesowicz (Komisja Europejska) przypomniała motywy, którymi kierowała się i nadal kieruje Komisja Europejska w projekcie rozporządzenia. Jako najważniejsze wskazała:

1. Dostosowanie przepisów do zmieniającego się środowiska i uproszczenie norm prawnych. Obecnie mamy do czynienia z fragmentacją przepisów. Jest tyle praw ochrony danych ile państw członkowskich. Ochrona danych powinna być zatem zmodernizowana, co jest równoznaczne z jej uproszczoniem.

2. Zredukowanie kosztów dla przedsiebiorstw, w tym startupów. Modernizacja obowiązków administorów danych powinna zmierzać do tego, by rozgraniczyć ich zakres do rodzaju i ilości danych, które są przetwarzane. W tym celu pomocne może być dostosowanie ilości środków ochronnych do stopnia ryzyka przetwarzania danych osobowych.

Jednocześnie rewizja obowiązków i dostosowanie ich do nowych technologii.

3. Otworzenie rynku, a tym samym zwiększenie konkurencyjności. Nowa regulacja ma prowadzić do pozbycia się barier wejścia na rynek dla małych i średnich przedsiębiorstw oraz startupów. Dużo ponad połowa rozwoju UE oparte jest właśnie na nich. Komisja Europejska dostrzega to i dlatego pokłada duże nadzieje w stworzeniu takiego paradygmatu, gdzie ochrona danych będzie ukierunkowana na ochronę i jednocześnie zwiększenie konkurencyjności dla tych podmiotów.

4. Więcej kontroli dla klientów. Kontrola oznacza nie tylko egzekwowanie, ale i łatwiejszy wybór firm przez klientów. Egzekucja przestrzegania przepisów powinna faktycznie zwiększać odpowiedzialność administratorów danych. W tym celu Komisja Europejska przewidziała takie instrumenty jak kary finansowe i procedurę *one-stop-shop*.

5. Regulacja powinna być spójna. Organem pomocniczym będzie Europejska Rada Ochrony Danych, której istotną rolą będzie stanie na straży spójności stosowania przepisów.

Z punktu widzenia Komisji Europejskiej obecnie poszukiwany jest kompromis w zakresie wejścia w życie przepisów. Zakończenie trilogu do końca roku (negocjacje Komisji Europejskiej, Parlamentu Europejskiego i Rady) jest możliwe, gdyż jest na to zgoda polityczna i dążenie Parlamentu. Jednocześnie zostało wypracowane wspólne stanowisko, że dyrektywa 95/46/WE przewiduje wyjściowe standardy. Wszędzie tam gdzie nie ma owocnej dyskusji i trudno znaleźć kompromis następuje odwołanie do dyrektywy 95.

Sesję drugą (nowe zasady ochrony danych osobowych – wybrane zagadnienia z rozporządzenia ogólnego o ochronie danych osobowych) rozpoczął **dr Wojciech Wiewiórowski** (zastępca Europejskiego Inspektora Ochrony Danych) od wskazania, że Europejski Inspektor Ochrony Danych w lipcu 2015r. przygotował opinię na temat tekstów projektowanego rozporządzenia, gdzie zostały opisane i zasugerowane zmiany zmierzające do rozwiązania pewnych zagadnień ujętych w projekcie, w sposób bardziej praktyczny. Z materiałem tym można zapoznać się m.in za pośrednictwem dedykowanej aplikacji mobilnej (więcej informacji).

3 lata pracy nad rozporządzeniem przyniosły z punktu widzenia wielu krajów członkowskich pewne, dość zaskakujące odpowiedzi. Jedna z takich odpowiedzi to np., że polska ustawa jest dobra. O ile do pewnych rozwiązań się przyzwyczailiśmy na gruncie krajowej ustawy, o tyle w rozporządzeniu jest wiele „nowości“ i pewne znane nam rozwiązania, jak np. szczególne rozwiązania w zakresie marketingu bezpośredniego jako prawnie usprawiedlionego celu (art. 23 ust. 4 ustawy), przestaną obowiązywać. Jest to jeden z największych kłopotów w UE dlatego, że nowa regulacja będzie próbą odzwyczajenia się od pewnych rozwiązań, znaczenia pewnych instytucji. Rozporządzenie będzie bezpośrednio stosowane i to wskazywaliśmy już w 2012r. z jednej strony jako problem, a z drugiej jako sukces.

Kwestia wnoszenia skarg do organu kontrolnego wciąż wymaga dyskusji w Polsce. Wydaje się, że zasada selekcjonowania skarg (np. w Wielkiej Brytanii rozpatrywane są te skargi, które zostaną przez inspektora uznane za ważne bądź nowe) odciążyłaby organy kontrolne i poprawiła ich wydolność. Obecnie w Polsce nie jest to rozwiązanie dopuszczalne. Warto przyjrzeć się temu zagadnieniu szerzej, gdyż jeżeli zostaną zniesione opłaty przy wnoszeniu skarg (czasem żartobliwie zwane

„ekologicznymi“), to ich liczba drastycznie się zwiększy. Istotne będzie wtedy „wyłapanie“ tych, które faktycznie są ważne.

Prace nad rozporządzeniem są wyzwaniem podobnie jak prace nad dyretywą. W trilogu nie został jeszcze omówiony np. aspekt ewentualnego wyłączenia norm rozporządzenia w odniesieniu do administracji publicznej. Warto jednak podkreślić, że takie wyłączenia powinny następować jedynie w sytuacji, gdy poziom ochrony zapewniony byłby na wyższym poziomie przez przepisy krajowe.

Dr Arwid Mednis (Uniwersytet Warszawski) omówił koncepcję zgody w projektowanym rozporządzeniu. Zgoda w dalszym ciągu będzie równorzędną innym przesłanką przetwarzania danych osobowych. Oprócz zgody, przetwarzanie będzie dopuszczalne dla potrzeb realizacji umowy, wykonania obowiązku wynikającego z przepisu prawa, dla ochrony żywotnych interesów podmiotu danych (ta przesłanka będzie dotyczyła także danych zwykłych, a nie tak jak w obecnej ustawie tylko danych sensytywnych), realizacji zadań w interesie publicznym czy realizacji prawnie usprawiedliwionego interesu administratora danych.

W związku ze zmieniającą się praktyką rynkową warto przeanalizować postanowienia projektu, szczególnie w kontekście zjawiska tzw. kupowania zgód. Ma ono miejsce wtedy, gdy wyrażamy zgodę np. na marketing, w zamian otrzymując usługę w atrakcyjniejszej cenie. GIODO wyraził swego czasu pogląd i póki co to się nie zmieniło, że jeżeli osoba ma szansę otrzymać ekwiwalent usługi bez wyrażania zgody, to zgoda w zamian za niższą cenę usługi nie jest wymuszona. Pod warunkiem, że osoba ta została dokładnie poinformowana, na co się zgadza.

Definicja zgody w projektowanym rozporządzeniu jest nam znana na gruncie rozwiązań krajowych. Nie odbiega bowiem od dotychczasowej koncepcji zgody. Zgoda dla swej ważności powinna być wyrażona w sposób swobodny (okienko z zaznaczoną zgodą nie jest akceptowane), świadomy i wyraźny. Nie musi być to zawsze konkretne oświadczenie, wystarczy zachowanie wskazujące wyraźnie na akceptację przez osobę wykorzystania jej danych.

Warunki uznawania zgody zostały określone w art. 7 projektowanego rozporządzenia i to jest *novum* w stosunku do obecnych regulacji. Przesądzono w nim m.in., że ciężar dowodu jej uzyskania spoczywa na administratorze danych. Nie jest natomiast jasne czy jedna zgoda będzie mogła obejmować wiele celów, z obecnego brzmienia projektów może wynikać, że tak. Zgoda może być odwołana, a w sytuacji, gdy jest wyrażona dla obsługi procesu niezbędnego dla świadczenia usługi, administrator danych powinien informować o skutku cofnięcia zgody. Problem kupowania zgód nie jest rozstrzygnięty jednoznacznie, jednakże projekt sugeruje, że można uzależnić świadczenie usługi od wyrażenia zgody w przypadku, gdy przetwarzanie jest niezbędne do świadczenia usługi (choć wtedy może wchodzić w grę inna przesłanka legalności).

Zgoda nie będzie uznana za swobodnie wyrażoną jeśli pomiędzy stronami istniałaby znacząca nierównowaga. Dyskusyjne pozostaje, jak oceniać „znaczący” charakter owej nierównowagi i kto miałby to oceniać. Na uwagę zasługuje porządkująca propozycja Europejskiego Rzecznika Ochrony Danych Osobowych, w której zgoda nie byłaby uznawana za swobodną jeśli pomiędzy stronami występuje znacząca nierównowaga lub jeśli uzależnia się świadczenie usługi od zgody, podczas

gdy przetwarzanie danych nie jest do tej usługi niezbędne.
Problematyka zgody szczególnie w kontekście zatrudnienia jest szeroko dyskutowana. Generalnie zgoda w stosunkach pracy może być uznana za wymuszoną, niemniej jedna z wersji projektu przewiduje, że państwa UE będą mogły samodzielnie określać warunki legalności zgody w stosunkach pracowniczych.

Magdalena Piech (Konfederacja Lewiatan) omówiła założenia tzw. punktu kompleksowej obsługi (ang. *one-stop-shop*) i rozbudowanej współpracy pomiędzy organami i rozstrzygania w sprawach dotyczacych administratorów danych, przetwarzających dane w kilku państwach członkowskich UE.

Organem nadzorczym, właściwym dla sprawowania kontroli wobec takich podmiotów będzie organ siedziby głównej administratora. Decyzje będą podejmowane zgodnie z mechanizmem zgodności, w który zaangażowana będzie, złożona z krajowych organów ds. ochrony danych, Europejska Rada Ochrony Danych. Zadaniem Rady będzie dbanie o jednolite stosowanie przepisów w całej UE. Od projektu Komisji, poprzez Parlament i na Radzie kończąc mechanizm „one stop shop“ zmienił swój kształt. Rada wprowadziła istotne odstępstowa od tej zasady, pozwalające m.in na rozstrzyganie w sprawach „lokalnych“ organom innym niż organ siedziby głównej. Ostateczne brzmienie przepisów w tym zakresie nie jest jeszcze przesądzone. Zdaniem Magdaleny Piech, aby zrealizować założenia przyświecające reformie, konieczne jest precyzyjne określenie przesłanek uruchamiajacych mechanizm zgodności oraz przyjęcie wąskich kryteriów angażowania innych organów nadzorczych w podejmowanie decyzji przez organ siedziby głównej. W przeciwnym razie mechanizm zgodności stanie się normalnym trybem podejmowania decyzji przez organy danych, co znacznie wydłuży procedurę wydawania decyzji i nie da administratorom pewności co do tego, który organ sprawuje nad nim kontrolę.

Katarzyna Szymielewicz (Fundacja Panoptykon) przypomniała, że nie ma legalnej definicji profilowania i jej wypracowanie to jedno z głównych wyzwań w pracach nad nowym rozporządzeniem. Na potrzeby prac w polskiej grupie roboczej przedstawiciele biznesu i organizacji społecznych zgodzili się jednak, że profilowanie jest procesem złożonym. Co do zasady, można je podzielić trzy etapy:

1. Analiza statystyczna prowadząca do kategoryzacji zachowań lub cech (jeszcze w oderwaniu od danych osobowych).

2. Przyporządkowanie konkretnej osoby ze względu na jej cechy lub zachowanie do danej kategorii.

3. Podjęcie decyzji w oparciu o tę kategoryzację (np. o zawarciu lub odmowie zawarcia umowy, o kształcie wystosowanej oferty czy dopasowaniu reklamy).

Jest to zatem proces w swojej istocie inny niż standardowe przetwarzanie danych – opiera się na analizie korelacji statystycznych i prowadzi do kategoryzowania ludzi ze względu na określone cechy (np. poziom dochodów, płeć, wiek, upodobania konsumenckie).

Z tym wiąże się szczególne ryzyko związane z marginesem błędu. Z perspektywy podmiotu przetwarzającego dane ten margines może być nieznaczny, jednak z perspektywy osoby, która się w nim mieści, taki błąd ma zasadnicze znaczenie

– może prowadzić do dyskryminacji na tle rasowym, wykluczenia z dostępu do istotnej usługi, dyskryminacji cenowej, naruszenia prywatności i innych negatywnych skutków.

Istniejąca w polskim prawie regulacja profilowania (art. 26a ustawy o ochronie danych osobowych) ogranicza się do tego ostatniego etapu, zakazując w pełni automatycznego podejmowania decyzji w oparciu o analizę danych (prawo do uzyskania tzw. ludzkiej interwencji). Obecnie nie istnieją jednak gwarancje, które dotyczyłyby samej kategoryzacji (przyporządkowania osoby do określonej kategorii w oparciu o analizę statystyczną), mimo że już na tym etapie uwidaczniają się niektóre ryzyka.

Projekt Komisji opiera się na podobnej logice - reguluje jedynie „środki oparte o profilowanie”, czyli ostatni etap podejmowania decyzji. Jednocześnie nie przewiduje w tym zakresie zakazu, tylko formułuje warunki: istnienie podstawy prawnej, niezbędność do zawarcia umowy (pod warunkiem, że rozstrzygnięcie było pozytywne dla profilowanej osoby) i zgodę osoby, której ten porces dotyczy.

Parlament Europejski poszedł krok dalej i zdefiniował profilowanie jako automatyczny proces, który ma na celu ocenę, analizę lub przewidzenie zachowania lub cechy danej osoby (‚*Profiling*’ *means any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person or to analyse or predict in particular that natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviou*r). Projekt Parlamentu również nie zakazuje profilowania i bazuje na podobnych zasadach, co propozycja Komisji Europejskiej (zgoda, niezbędność do zawarcia umowy i przepis prawa jako przesłanki legalności). Wprowadza jednak doadtkowe, istotne gwarancje - w tym prawo jednostki do poznania logiki działania profilowania i wytłumaczenia skutków procesu - już na etapie samej kategoryzacji i analizy danych. Projekt Parlamentu wzmacnia również prawo do ludzkiej interwencji, które (w słabszej formie) pojawiło się już w projekcie Komisji. Wreszcie, przewiduje bezwzględne prawo podmiotu danych (profilowanej osoby) do wniesienia sprzeciwu.

Projekt Rady miał być próbą kompromisu między dwiema wcześniejszymi wersjami (np. utrzymuje definicję samego profilowania i niektóre gwarancje), jednak zasadniczo wraca do logiki zaproponowanej przez Komisję Europejską. Osłabia też kluczowe gwarancje ochrony praw podmiotu danych - np. przewiduje, że ludzka interwencja nie jest wymagana, jeśli profilowanie jest oparte o przepis prawa. Rada nie utrzymała też twardego zakazu dyskryminacji, który w swojej wersji zaproponował Parlament. W jej projekcie znajdziemy tylko - dość miękkie - ograniczenie możliwości wykorzystywania do profilowania danych wrażliwych.

Zdaniem Katarzyny Szymielewicz na dalszym etapie prac w ramach trilogu kluczowa będzie dyskusja o tym, które gwarancje, w jakim kształcie i na jakim etapie procesu profilowania powinny obowiązywać. Zdaniem Fundacji Panoptykon najlepsza w tym aspekcie jest propozycja Parlamentu Europejskiego.

Dr Paweł Litwiński (Instytut Allerhanda) skupił się na omówieniu roli inspektora ochrony danych (red. odpowiednik ABI, zwany także „oficerem ochrony danych”) w nowej regulacji. W tym zakresie odwołał się do art. 35-37 projektowanego rozporządzenia. Jak wskazał są to przepisy prawa materialnego, a instytucja inspektora będzie w całości regulowana przez rozporządzenie. W nowych przepisach znajdzie się też element procesowy, tj. umocowanie inspektora do

występowania w imieniu administratora danych w relacji z GIODO i podmiotami danych osobowych.

Wdrożenie obowiązujących od stycznia br. przepisów o ochronie danych osobowych w Polsce jest pomocne w przygotowaniu się do wejścia w życie rozporządzenia. Przepisy będą bowiem w przeważającej większości zgodne. Ponieważ prace nad rozporządzeniem nadal trwają, nie ustalone na dzisiaj pozostaje, czy inspektor ochrony danych będzie powoływany dobrowolnie, czy też obligatoryjnie we wskazanych przypadkach. Administrator danych będzie zobowiązany informować, kto jest inspektorem ochrony danych i będzie to osoba do kontaktu nie tylko dla GIODO, ale osób, których dane dotyczą. Dozwolone będzie, by jeden inspektor ochrony danych był wspólny dla kilku podmiotów. Podstawy zatrudnienia będą analogiczne, jak dzisiaj: umowa o pracę lub outsourcing. Wiedza i kwalifikacje będą elementami istotnymi dla inspektora ochrony danych zaś wymaganie posiadania pełnej zdolności do czynności prawnych oraz niekaralności nie pojawia się w negocjowanych tekstach rozporządzenia, więc należy się tutaj spodziewać zmiany względem polskich przepisów.

Rozporządzenie może przewidywać kadencyjność dla inspektora ochrony danych. Nie jest to jednak przesądzone. W przeciwieństwie do jego statusu, który z pewnością nie ulegnie zmienia względem polskiej regulacji - niezależne stanowisko, inspektor ochrony danych podległy bezpośrednio kierownikowi jednostki i – co będzie nowością – właściwie włączony do wszystkich kwestii dotyczących ochrony danych osobowych w organizacji.

Tylko w projekcie rozporządzenia zaproponowanym przez Parlament Europejski pojawia się aspekt tajemnicy zawodowej inspektora ochrony danych. Nie wydaje się, by zostało to utrzymane. W ramach trilogu negocjowane jest, by inspektor ochrony danych miał możliwość wykonywania innych obowiązków, a także by uczestniczył aktywnie w dokonywaniu *Privacy Impact Assesment*.

Sesję trzecią (konsekwencje wejścia w życie nowych ram ochrony danych osobowych) otworzyła **Adrianna Jasińska-Cichoń** (Główny Inspektorat Pracy), która podkreśliła, że inspektorzy pracy maja wieloletnie doświadczenie w nakladaniu kar na podmioty łamiące przepisy. W toku kontroli stwierdzają, czy doszło do naruszeń przepisów prawa pracy (w tym bhp) oraz legalności zatrudnienia. Jeżeli je wykryją to PIP nakłada kary grzywny – za wykroczenia przeciwko prawom pracowników - w drodze mandatu, za niewykonanie decyzji - grzywny w celu przymuszenia. Za naruszenia przewidziane w ustawie o transporcie drogowym nakładane są kary pieniężne. Jednorazowo nałożona grzywna w celu przymuszenia nie moze przekroczyć 10 000 zł. a gdy jest nakładana wielokrotnie do 50 000 zł. W przypadku osób prawnych i jednostek organziacyjnych nie posiadajacych osobowosci prawnej - odpowiednio 50 000 zł. i 200 000 zł.

Z przedstawionych statystyk wynika, że w 2014r. Państwowa Inspekcja Pracy nałożyła grzywny w celu przymuszenia w łącznej wysokości blisko 4 mln 300 tys. złotych, a w transporcie drogowym - gdzie przepisy przewiduja taryfikator wysokosci kar – kary pieniężne na prawie 1 mln. 800 tys.

Konrad Miłoszewski (Rządowe Centrum Legislacji) podkreślił, że wyzwanie związane z przeglądem prawodawstwa i potrzeby dokonania zmian z uwagi na mające obowiązywać rozporządzenie już się rozpoczęło. Pełen proces konsultacji powinien obejmować nie tylko listę aktów przesłanych przez

ministerstwa, ale także konsultacje społeczne.

Projekt ustawy polskiej dostosowującej regulacje do rozporządzenia będzie musiał przejść przez wszystkie komitety, a później trafi do parlamentu. Obecnie są dwa pomysły na jego wdrożenie: opracowanie jednego aktu albo wprowadzanie zmian jednostkowych w poszczególnych aktach prawnych. W opinii RCL jeden duży projekt, który regulowałby przepisy wykonawcze, proceduralne i jeden koordynator projektu (np. MAiC), który będzie czuwał nad spójnością może okazać się najefektywniejsze i być rozsądnym kierunkiem.

Dr Marlena Sakowska-Baryła (Urząd Miasta w Łodzi) omówiła aspekt krajowych przepisów sektorowych w odniesieniu do zmian, które wprowadzi rozporządzenie ogólne (rozdział IX, art. 80-83 projektowanego rozporządzenia). Najważniejsze zagadnienia omówione podczas konferencji koncentrowały się wokół następujących kwestii sektorowych:

a) przepisów dotyczących działalności prasowej i realizacji wolności wypowiedzi, które w głównej mierze będą regulowane przez przepisy krajowe;

b) przetwarzania danych dotyczących zdrowia - tu podkreślono między innymi, że informacje o zdrowiu należą do najbardziej prywatnej sfery informacyjnej jednostki. Wskazano również, że istotne jest transgraniczne przekazywanie informacji o stanie zdrowia, a w związku z tym uregulowanie podstaw ich przekazywania. Zaznaczono, że w dalszym ciągu problemem będzie elektroniczne przetwarzanie danych medycznych i to będzie wymagać osobnej regulacji;

3. przetwarzania danych w kontekście zatrudnienia - rozporządzenie będzie kompleksowo regulować sprawy związane z prawem pracy i zawierać odesłania do przepisów krajowych, w tym do układów zbiorowych pracy. Przepisy rozporządzenia mają zagwarantować dużo dalej idącą ochronę informacyjnej sfery pracownika, a przy tym dookreślić granice przetwarzania jego danych osobowych w różnych kontekstach i okolicznościach. Rozporządzenie będzie określać minimum standardów, odsyłając do regulacji krajowych;

4. przetwarzania danych do celów statystyki, badań naukowych, archiwów, które z założenia, choć z pewnymi wyjątkami, powinny być przetwarzanie w sposób ograniczający możliwość identyfikacji osoby fizycznej.

Dr Marlena Sakowska-Baryła wskazała, że obecnie jest dobry moment na to, by rozpocząć swoistą rewizję polskich przepisów sektorowo regulujących problematykę ochrony danych osobowych i określających procedury przetwarzania danych, tak, aby lepiej przygotować się do wdrożenia przepisów ogólnego rozporządzenia. Szczególnie istotne jest to dla podmiotów stosujących tzw. przepisy sektorowe, ale także dla organów władzy publicznej odpowiadających za kształt polskiego prawodawstwa. Należy dokonać skrupulatnej analizy ustaw i rozporządzeń, które regulują kwestie dysponowania danymi osobowymi po to, by wyeliminować ryzyko, że krajowe przepisy będą niespójne z rozporządzeniem ogólnym.

Dr Grzegorz Sibiga (Instytut Nauk Prawnych Polskiej Akademii Nauk) podkreślił, że zmiany w zakresie nowych ram prawnych nie dotyczą tylko rozporządzenia, ale również nowej dyrektywy zawierającej szczególne regulacje dotyczące ochrony danych dla sektora odpowiedzialnego za egzekwowanie prawa. W tym znaczeniu jest

to pakiet regulacji, w którym przepisy krajowe odgrywają istotną rolę i pomimo podstawowego znaczenia prawa Unii Europejskiej będziemy mieli do czynienia z jego przeplataniem się z przepisami krajowymi i innymi formami regulacji (np. kodeksami deontologicznymi).

Powstały w ten sposób nowy system można roboczo podzielić na 3 trzy elementy:

1. Pakiet rozporządzenie i dyrektywa oraz akty prawa krajowego z nimi powiązane. Dyrektywa dla sektora odpowiedzialnego za egzekwowanie prawa będzie wymagała implementacji w prawie krajowym. Pytanie brzmi, czy w jednej, czy też w kilku ustawach. Z kolei projekt rozporządzenia również odsyła w niektórych kwestiach do przepisów krjowych (np. zasad ustrojowych krajowego organu ds. ochrony danych osobowych). Zresztą w sumie rozporządzeniami będzie uzupełniane aż 3 rodzajami regulacji: aktami wydawanymi przez Komisję Europejską, przepisami krajowymi oraz innymi źródłami, do których zaliczymy kodeksy deontologiczne oraz mechanizmy certyfikacyjne.

2. Krajowe akty normatywne mające charakter autonomiczny względem przepisów rozporządzenia i dopuszczone przez rozporządzenia jako wyjątki od jego regulacji.

3. Inne przepisy prawa Unii Europejskiej (w szczególności prawa wtórnego) i umowy międzynarodowe dotyczące ochrony danych osobowych oraz akty krajowe wdrażające je przez państwo, jeżeli takie wdrożenie jest potrzebne.

Również przyszłe regulacje dotyczące organu ds. ochrony danych osobowych (obecnie GIODO) będziemy odnajdywali zarówno w prawie Unii Europejskiej jak i w prawie krajowym.

Na działalność każdego organu władzy publicznej składają się trzy rodzaje przepisów: materialne, ustrojowe i proceduralne.

Już teraz można zauważyć, że przepisy materialne będą bardziej wchodziły w zakres rozporządzenia, natomiast ustrojowe i proceduralne bardziej będą należały do decyzji prawodawcy krajowego. Zasadne jest użycie tutaj zwrotu „bardziej“, ponieważ również rozporządzenie określa podstawowe zasady ustrojowe (np. niezależność organu) oraz kwestie proceduralne (np. procedurę *one-stop-shop* i związany z nią mechanizm zgodności). Z kolei mimo że projekt rozporządzenia określa kompetencje organu to w prawie krajowym można nałożyć jeszcze na niego inne zadania związane z ochroną danych osobowych, czy nawet szerzej prywatnością. Przykładem niech będzie trwająca dyskusja na temat powierzenia GIODO kompetencji w zakresie spraw związanych kontrolą operacyjną w telekomunikacji czy monitoringiem wizyjnym. Na marginesie, niektóre kompetencje zawarte w projekcie rozporządzenia mogą budzić wątpliwości, ze względu na nieostrość regulacji. Na przykład o wiele precyzyjniejsze – w zakresie współdziałania GIODO i ABI - są obecne przepisy polskiej ustawy o ochronie danych osobowych w stosunku do bardzo ogólnego obowiązku współpracy organu krajowego i inspektora ochrony danych (red. zwanego także „oficerem ochrony danych”) znajdującego się w projekcie rozporządzenia.

Podsumowując, do prawodawcy krajowego będzie należała znacząca część decyzji dotyczących organu krajowego ds. ochrony danych osobowych. Pokazując tylko kilka dylematów z tym związanych wskażmy, że to ten prawodawca zdecyduje, czy będzie to jeden czy więcej organów, czy będzie on

jedno- czy wieloosobowy, czy jego postępowanie będzie regulowane przede wszystkim w k.p.a., czy też zostaną wprowadzone daleko idące odmienności, a wreszcie jaki charakter będzie miała kontrola sądowa nad jego działalnością, ponieważ wcale nie jest przesądzone, że w każdym przypadku będzie to kontrola sądów administracyjnych (co choćby ma znaczenie dla sposobu kontroli sądu nałożenia przez organ kary pieniężnej).

Andrzej Lewiński (Zastępca GIODO) podkreślił, że organ szuka aktywnej drogi do wzmocnienia realnego przestrzegania przepisów. Wskazał, że GIODO powinien mieć prawo do selekcji skarg, by móc efektywnie kontrolować i wkraczać faktycznie tam, gdzie jest taka potrzeba. Wybór ten powinien być uzasadniony i dotyczyć przypadków odmowy prowadzenia postępowań tam, gdzie sprawy się już toczą przed innymi organami.

Ponieważ obecnie kończą się prace zarówno nad projektem unijnego rozporządzenia dotyczącecgo ochrony danych osobowych, jak i nad dyrektywą odnoszącą się do ochrony danych osobowych w sektorze policji i wymiaru sprawiedliwości, w GIODO powstała, kierowana przez z-cę GIODO, komisja, której zadaniem jest przygotowanie Polski do wdrożenia przepisów unijnych. Obecnie trwają także prace nad nowelizacją polskiej ustawy, tak by możliwość wprowadzenia kar wprowadzić wcześniej. Celem jest łatwiejsze przygotowanie się do nowych przepisów i płynniejsze ich wdrożenie.

Zdaniem ministra Andrzeja Lewińskiego pozycja obecnego ABI, a już niedługo oficera ochrony danych (red. zwanego także „inspektorem ochrony danych”) musi wzrosnąć. Organ widzi realną potrzebę współpracy z tymi osobami. Obecnie jest już 11 500 zarejestrowanych ABI, a 8 000 zgłoszeń czeka na rejestrację. Liczba ta powinna jeszcze sukcesywnie rosnąć.

Jednym z zadań ABI jest wykonywanie sprawdzeń, które w ocenie organu będą pomocne w zapewnianiu większej ochrony danych osobowych. W tym znaczeniu GIODO widzi w nim swojego partnera, a nawet podmiot, który jako pierwszy mógłby analizować skargi dotyczące nieprawidłowości w przetwarzaniu danych u administratora, który go powołał. Do tego potrzebna jest jednak współpraca i wola ze strony administratorów danych, by wyznaczani oficerowie byli kompetentni.

Oficer ochrony danych nie jest i nie będzie „agentem” GIODO, lecz swego rodzaju łącznikiem współpracującym z nim na bieżąco, przy zachowaniu jego pełnej niezależności. GIODO bedzie przeprowadzał inspekcje dwiema drogami - poprzez sprawdzenia przez ABI-ch oraz poprzez kontrole jednostek, w których taki urzędnik nie został wyznaczony lub nie działa. Może to bowiem stanowić domniemanie, iż poziom ochrony danych osobowych w tych jednostkach jest niewystarczajacy. Kontrole mogą być też przeprowadzane w podmiotach, które mają ABI-ego, jeśli zaistnieją przesłanki świadczące, iż przetwarzanie danych jest niewłaściwe.

Minister Lewiński poinformował ponadto, że GIODO planuje wydawanie czasopisma edukacyjnego mającego popularyzować wiedzę na temat ochrony danych osobowych.

Pytania i odpowiedzi.

1. **Jak rozumieć *Risk Based Approach* w odniesieniu do projektowanej regulacji i wdrożenia przez organizację? Jak zapewnić mierzalność ryzyka, która będzie dla legislatora zadowolająca? W regulacji jest mowa ogólnie o analizie ryzyka i każdy może wybierać dowolnie standardy analizy ryzka.**

Dr Karolina Mojzesowicz (Komisja Europejska)**:** *Risk Based Approach* opiera się na samoocenie. Administrator danych dokonuje każdorazowo samodzielnie oceny, jakie dane przetwarza. Klasyfikacje są różne. Podstawowa, czy przetwarza dane zwykłe, czy wrażliwe. Art. 33 projektu rozporządzenia dookreśla, jakiego rodzaju przetwarzanie danych może nieść duże zagrożenie (np. dyskryminacja, kradzież tożsamości). ADO powinien każdorazowo ocenić, jak duże jest zagrożenie przy przetwarzaniu danych. ADO ma możliwość zwrócić się z tym do oficera ochrony danych (przyp. zastąpi polską instytucję ABI), który może mu w tym pomóc. Powinna być to osoba mająca wiedzę z zakresu bezpieczeństwa informacji. Jest wiele przyjętych standardów i programów certyfikujących opartych na analizie ryzyka, które są powszechnie akceptowane. Rozporządzenie nie będzie ingerować w dobrowolność wyboru metodyki. Istotne jest, by opierała się ona na akceptowalnym powszechnie standardzie. Pomocniczą rolę w tym zakresie może przyjąć Europejska Rada (a obecnie można czerpać z zasobów Grupy Roboczej Art. 29).

Dr Wojciech Wiewiórowski (zastępca Europejskiego Inspektora Ochrony Danych): Paradoksalnie wstępna ocena ryzyka czyli tzw. *Risk Based Approach*, która traktowana jest jako ułatwienie dla ADO, może być traktowana jednocześnie jako dodatkowy formalny obowiązek. Istotne jest wsparcie ADO w zakresie pewności co do poprawności prowadzonej wstępnej analizy ryzyka. Europejska Rada Ochrony Danych mogłaby tworzyć przewodniki w tym zakresie. Problem w tym, że ich przygotowanie jest możliwe dopiero, jak zacznie działać rozporządzenie. Wcześniej istnieć będzie wciąż Grupa Robocza Art. 29, która co prawda może zacząć przygotowywać takie dokumenty. Musimy jednak pamiętać, że powołana w przyszłości Rada nie musi wprost podtrzymać decyzji Grupy Art. 29.

2. **Czy procedura *one-stop-shop* jest lepsza niż kierowanie zapytań do jednego organu, który ma jednolitę praktykę orzekania? Wydaje się, że zarówno dla organów ochrony danych, jak i dla ADO i samych obywateli procedura *one-stop-shop* może być zbyt skomplikowana.**

Karolina Mojzesowicz: Na poziomie prac nad projektem rozporządzenia nikt nie chciał utworzenia jednej agencji. Procedura *one-stop-shop* przez państwa członkowskie wskazywana była i jest jako możliwość przedstawiania wniosków/skarg do swoich GIODO przez obywateli w ojczystym języku i do znanego im organu. Organy będą musiały faktycznie ze sobą współpracować i szukać kompromisowego rozwiązania, ale Europejska Rada będzie miała ostateczny głos i w tym zakresie nie ma podstaw do obawiania się procedury *one-stop-shop*. Przytym *one-stop-shop* dotyczy wyłącznie spraw, ktore mają aspekt „międzynarodowy" , czyli dotyczą więcej niż jednego kraju członkowskiego.

Dr Wojciech Wiewiórowski: Tak z punktu widzenia ochrony praw podstawowych w Unii Europejskiej jak i z punktu widzenia wspólnego rynku cyfrowego jedną z podstawowych wartości jest jednolita interpretacja Traktatów i rozporządzenia w całej Europie. Nie mam wątpliwości, że zasada *one-stop-shop* i towarzysząca jej procedura

prowadząca do wspólnych decyzji organów ochrony danych jest tym samym konieczna. Nie mam natomiast wątpliwości, że nie będzie to zadanie łatwe, jak zawsze gdy próbujemy dojść w indywidualnych sprawach do ogólnoeuropejskich odpowiedzi. Jestem też pewien, że nie będzie to pojedyncza procedura, jako że – ze względów praktycznych - ledwie niewielki ułamek spraw może ostatecznie trafiać na forum Europejskiej Rady Ochrony Danych.

3. **Czy będą prowadzone konsultacje społeczne w ramach przeglądu przepisów, które zmieni rozporządzenie?**

Jurand Drop (Podsekretarz stanu w Ministerstwie Administracji i Cyfryzacji): Sposób prowadzenia prac nad unijnym rozporządzeniem przez MAiC jest maksymalnie otwarty i transparentny. Przedstawiano na stronie internetowej informacje, organizowano regularne spotkania ekspertów reprezentujących wszystkie strony społeczne – biznes, środowisko naukowe, organizacje pozarządowe i administrację publiczną. Na podstawie tych spotkań, warsztatów i konsultacji pisemnych Ministerstwo wypracowywało polskie stanowisko promowane później na forum UE. Uwzględniało postulaty zgłaszane przez uczestników konsultacji w optymalnym stopniu – co nie było łatwe, gdyż były one często ze sobą sprzeczne.

Podobne działania będą również prowadzone w przyszłości w ramach przeglądu przepisów, które zmieni rozporządzenie. Obecnie wstępny przegląd przepisów odbywa się między ministerstwami i urzędami centralnymi na poziomie Komitetu Rady Ministrów ds. Cyfryzacji. Później, po przyjęciu ogólnego rozporządzenia, zostaną przeprowadzone konsultacje społeczne, co do koniecznych zmian. Następnie w ciągu całego procesu legislacyjnego, Ministerstwo nastawia się na intensywny dialog z zainteresowanymi stronami.

Informacje o dotychczas prowadzonych konsultacjach, w zakresie unijnej reformy ochrony danych, dostępne są na stronie MAiC pod adresem https://mac.gov.pl/projekty/ochrona-prywatnosci-w-sieci/warsztaty.

4. **Projekt rozporządzenia przewiduje drakońskie kary. Czy będzie przewidziana specjalistyczna procedura kontrolna? Czy czynności kontrolne w większości będą mocniej sformalizowane?**

Dr Edyta Bielek-Jomma (Generalny Inspektor Ochrony Danych Osobowych): Obecnie toczone są prace nad możliwymi zmianami w zakresie działań kontrolnych oraz decyzji organu, jakie mogą zapadać. Jest jednak jesze zbyt wcześnie, by mówić o konkretnych propozycjach, które można byłoby poddać pod szerszą dyskusję.

Bądź na bieżąco ze zmianami
Przygotuj się do wdrożenia przepisów

Czytaj więcej na s.17

Bądź na bieżąco ze zmianami i przygotuj się do wdrożenia przepisów

Dowiedz się więcej | Usystematyzuj informacje | Przygotuj się do zmian

Raz w miesiącu będziemy wydawać raport z nowym tematem przewodnim.
Raport będzie zawierał odesłania do artykułów na dedykowanej stronie. Łącznie wydamy 12 raportów.

Zyskaj dostęp do strony będącej kompendium wiedzy na temat
reformy przepisów ochrony danych osobowych w Unii Europejskiej.
Dostęp tylko dla zalogowanych.

Strona podzielona na sekcje:

„Status” (informacje jak wyglądają prace nad nową regulacją) ,
„Przepisy” (analizujemy co dokładnie się zmieni od strony praktycznej przepis po przepisie),
„Zmiany sektorowe” (analizujemy jak poszczególne zmiany odczuje omawiany sektor),
„Opinie” (opinie, analizy zaproszonych ekspertów) ,
„Przydatne dokumenty” (rekomendacje, które możesz wdrożyć w organizacji wraz z omówieniem)
„Waszym zdaniem” (forum)

Jako Użytkownik będziesz mógł zadawać pytania bądź wyrażać swoje wątpliwości/uwagi a my będziemy zwracać się z tymi pytaniami/uwagami do organów i prosić o odpowiedź.

Opłata jest jednorazowa za prenumeratę 12 raportów.

Do 30 października prowadzimy przedsprzedaż w cenie 66 zł. Kupując teraz dokonujesz zakupu taniej.

Szczególnie polecane dla ABI, prawników i inżynierów bezpieczeństwa informacji

Zapisz się

Nowe ramy ochrony danych osobowych w UE. Wyzwania dla Polski.

Raport pokonferencyjny

Cyberlaw.pl

Warszawa, 24 września 2015