Dajemy dobry przykład

Strategia EIOD

2015-2019

EDPS

European Data Protection Supervisor

Strategia EIOD

2015-2019

Dajemy dobry przykład

O TYM DOKUMENCIE

Nadszedł niezwykle ważny moment dla ochrony danych, okres bezprecedensowych zmian o ogromnym znaczeniu politycznym, nie tylko w Europie, ale na skalę międzynarodową. W tym kontekście, nowy Europejski Inspektor Ochrony Danych (EIOD) sfinalizował opracowywanie strategii działań na najbliższe pięć lat, dzięki której wizja stanie się rzeczywistością, a innowacyjne rozwiązania będą szybko identyfikowane.

W planie na lata 2015–2019 przedstawiono:

- główne wyzwania w obszarze ochrony danych i prywatności na nadchodzące lata;
- trzy cele strategiczne i 10 działań towarzyszących, których realizacja ma pomóc nam zmierzyć się z tymi wyzwaniami;
- sposób realizacji strategii dzięki efektywnemu zarządzaniu zasobami, sprawnej komunikacji i ocenie naszej działalności.

Swoje cele i ambicje będziemy realizować w oparciu o nasze dotychczasowe sukcesy oraz to, co stanowi naszą siłę, korzystając z doświadczeń zdobytych podczas realizacji *Strategii 2013–2014: Ku doskonałości w ochronie danych*.

O EIOD

Europejski Inspektor Ochrony Danych (EIOD) jest stosunkowo nowym, ale coraz bardziej wpływowym, niezależnym organem nadzorczym odpowiedzialnym za monitorowanie przetwarzania danych osobowych przez instytucje i organy UE, doradztwo w zakresie polityki i ustawodawstwa mającego wpływ na ochronę prywatności oraz współpracę z podobnymi organami w celu zapewnienia spójnej ochrony danych.

W grudniu 2014 r. Parlament Europejski i Rada UE mianowały Giovanniego Buttarellego inspektorem, a Wojciecha Wiewiórowskiego jego zastępcą. Oprócz zagwarantowania niezależności, mandat EIOD przyznaje [1] kompetencje w zakresie:

- opracowywania i przekazywania ogólnej wizji, rozważań w szerokim kontekście i proponowania konkretnych zaleceń i praktycznych rozwiązań;
- udzielania wskazówek strategicznych w celu podołania nowym i nieprzewidzianym wyzwaniom w dziedzinie ochrony danych;
- reprezentowania na najwyższych szczeblach oraz opracowywania i utrzymywania relacji z różnymi grupami interesów w innych instytucjach UE, państwach członkowskich, państwach niebędących członkami UE oraz z innymi organizacjami krajowymi lub międzynarodowymi.

Inspektorów wspiera biuro EIOD – dynamiczny zespół wykwalifikowanych i doświadczonych prawników, specjalistów w zakresie informatyki i administratorów. Biuro służy jako bezstronne centrum doskonałości w celu egzekwowania ochrony danych i wzmacniania ochrony prywatności w UE, zarówno w praktyce, jak i w przepisach prawa.

WIZJA, CELE I DZIAŁANIA W LATACH 2015–2019

Wizja EIOD ma pomóc UE dawać przykład w prowadzonym na skalę globalną dialogu na temat ochrony danych i prywatności w epoce cyfrowej. Nasze trzy cele strategiczne i 10 działań:

1 Digitalizacja ochrony danych

(1) Promowanie technologii na potrzeby skuteczniejszej ochrony danych i prywatności;
(2) Identyfikacja interdyscyplinarnych rozwiązań politycznych;
(3) Zwiększanie przejrzystości, kontroli i odpowiedzialności użytkowników w procesie przetwarzania dużych zbiorów danych.

2 Budowanie globalnych partnerstw

(4) Rozwój etycznego wymiaru ochrony danych;
(5) Spójne stanowisko UE na arenie międzynarodowej;
(6) Uwzględnianie kwestii ochrony danych w polityce międzynarodowej.

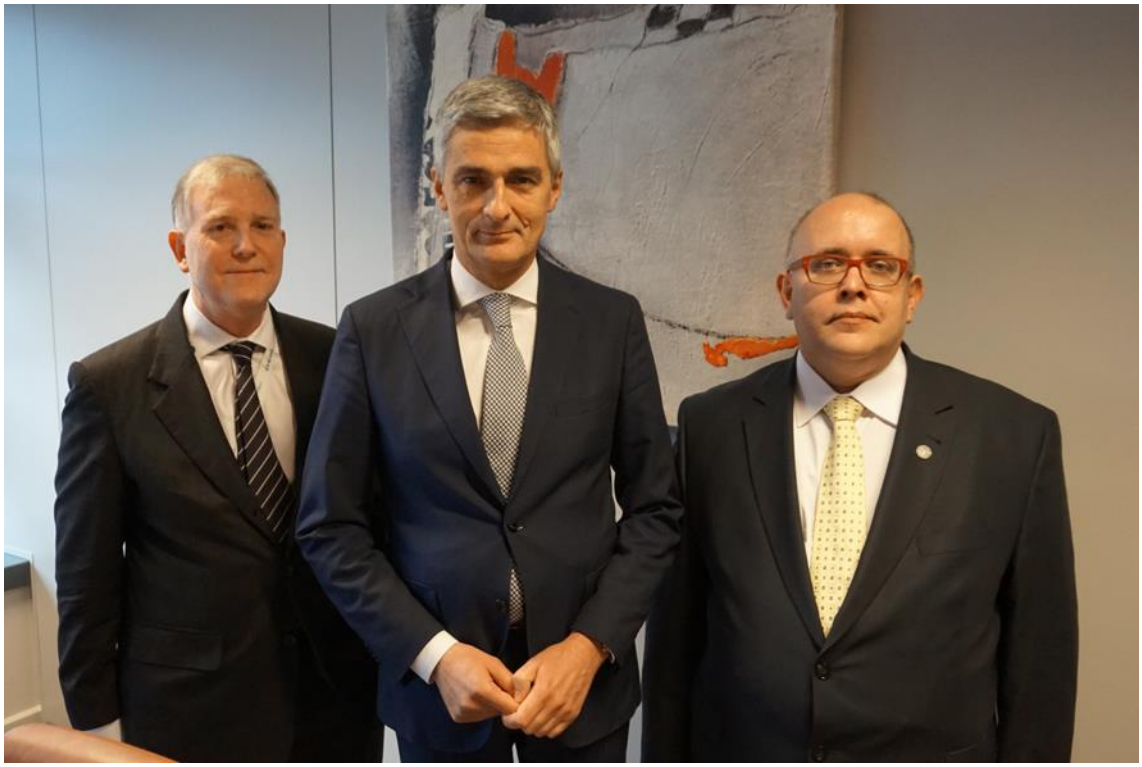
3 Nowy rozdział w ochronie danych w UE

(7) Przyjmowanie i wdrażanie aktualnych zasad ochrony danych;
(8) Zwiększenie odpowiedzialności organów UE gromadzących, wykorzystujących i przechowujących dane osobowe;
(9) Ułatwianie odpowiedzialnego i świadomego kształtowania polityki;
(10) Zachęcanie do dojrzałej dyskusji na temat bezpieczeństwa i prywatności.

PODSTAWOWE WARTOŚCI EIOD

- **Bezstronność** – działanie w wyznaczonych ramach prawnych i politycznych, niezależność i obiektywność, znalezienie właściwej równowagi pomiędzy interesami poszczególnych podmiotów i grup.
- **Uczciwość** – utrzymywanie najwyższych standardów postępowania i podejmowanie słusznych działań, nawet jeśli nie cieszą się one popularnością.
- **Przejrzystość** – wyjaśnianie czym się zajmujemy i dlaczego w sposób zrozumiały i przystępny dla wszystkich.
- **Pragmatyzm** – rozumienie potrzeb zainteresowanych stron oraz poszukiwanie rozwiązań, które sprawdzają się w praktyce.

SPIS TREŚCI



Giovanni Buttarelli, inspektor (w środku), Wojciech Wiewiórowski, zastępca inspektora (po prawej) i Christopher Docksey, dyrektor (po lewej), wspólnie tworzący Zarząd.

SŁOWO WSTĘPNE

Znajdujemy się w historycznym dla ochrony danych momencie.

W ciągu ostatnich 25 lat, zdobycze technologii zmieniły nasze życie na lepsze w stopniu, jakiego nikt nie był w stanie przewidzieć. Duże zbiory danych, internet przedmiotów, chmura obliczeniowa: wszystkie te rozwiązania są w stanie pod wieloma względami ułatwić nam życie. Możemy spodziewać się, że duże zbiory danych staną się jeszcze większe, ponieważ lepsza jakość danych osobowych jest konieczna do przeprowadzenia skutecznej analizy, a w konsekwencji podnoszenia wartości. Nie powinno to jednak odbywać się kosztem podstawowych praw jednostek ani zagrażać ich godności w społeczeństwie cyfrowym przyszłości.

Duże zbiory danych będą zatem wymagać równie dużej ochrony.

Europa musi stać się liderem w procesie kształtowania globalnego standardu prywatności i ochrony danych, w którym nacisk kładzie się na prawa człowieka i ochronę jego godności. UE ma teraz możliwość przyjęcia przyszłościowych standardów, których potrzebujemy, i które mogłyby stać się inspiracją na poziomie globalnym.

Możemy tego dokonać dając przykład i dbając o poszanowanie praw cyfrowych. Musimy pokazać obywatelom UE i naszym partnerom międzynarodowym, że nasze działania są zgodne z wyznawanymi przez nas wartościami. Europa ma obowiązek poprowadzenia dialogu na temat prawnych i etycznych konsekwencji nowych technologii.

W praktyce oznacza to przyjęcie reformy ochrony danych już w tym roku. Nowoczesny, przyszłościowy zestaw reguł jest niezbędny, jeśli Europa chce skutecznie zmierzyć się z wyzwaniami ery cyfrowej. Potrzebujemy przepisów unijnych, które są wystarczająco innowacyjne i skuteczne, by poradzić sobie z wciąż pojawiającymi się wyzwaniami związanymi z nowymi technologiami i transgranicznymi przepływami danych. Digitalizacja ochrony danych

Instytucje i organy UE powinny dawać przykład odpowiedzialnego przetwarzania danych w praktyce. EIOD nadal będzie aktywnym partnerem, dostarczającym instytucjom UE praktyczne i dynamiczne rozwiązania, dzięki którym większa zgodność z przyjętymi zasadami będzie stanowić przykład dla innych.

Ochrona danych pozostanie istotnym czynnikiem w większości obszarów polityki UE. Ma kluczowe znaczenie z punktu widzenia legitymizacji polityk i zwiększania publicznego zaufania do nich. Będziemy pomagać instytucjom i organom UE w przyjmowaniu pełnej odpowiedzialności i zapewnianiu, że ochrona danych stanowi integralną część ich propozycji legislacyjnych.

Zagadnienia te nie ograniczają się oczywiście do terytorium Europy, ale mają charakter globalny. Przepisy dotyczące ochrony danych ograniczają się do terytorium danego kraju, ale zasięg samych danych jest dużo szerszy. Oznacza to, że Europa musi dawać przykład tworząc nowe, globalne partnerstwa, które staną się fundamentem podstawowych zasad. Musimy zainwestować w lepszy dialog z innymi organami regulacyjnymi, przemysłem i społeczeństwem obywatelskim, który pozwoli nam zrozumieć w jaki sposób uczynić współpracę międzynarodową, w szczególności umowy transatlantyckie, bardziej sprawiedliwymi i wyważonymi.

Aby osiągnąć ten cel, Europa musi mówić jednym głosem i przyjąć wspólne stanowisko w odniesieniu do strategicznych kwestii ochrony danych. Podejmujemy wszelkie starania, by wspierać współpracę z innymi, niezależnymi organami ochrony danych.

W nowej strategii przedstawiliśmy to, co wspólnie z Wojciechem Wiewiórowskim, Christopherem Dockseyem i naszymi utalentowanymi i dynamicznymi kolegami z Biura EIOD pragniemy osiągnąć. Mamy

nadzieję, że EIOD będzie rozwijać się jako ośrodek ochrony danych, forum debaty i miejsce, w którym wszystkie osoby zainteresowane współpracą na rzecz ochrony naszych praw podstawowych są mile widziane.

Giovanni Buttarelli

DIGITALIZACJA OCHRONY DANYCH

Technologia cyfrowa jest niezwykłym katalizatorem wszystkich form ekspresji i zmian społecznych. Od zabawnych nagrań i gier, po rewolucje, w których ważną rolę odegrały media społecznościowe, nowoczesne technologie umożliwiają zwykłym obywatelom kwestionowanie decyzji możnych. Technologie są niewątpliwie źródłem wielu korzyści, zarówno na planie indywidualnym, jak i społecznym.

Jako organ regulacyjny do spraw ochrony danych, musimy wykazać się otwartością umysłu, aby zidentyfikować przyszłe szanse i możliwości w zakresie dobrobytu i dobrostanu społeczeństw, a także innych korzyści, szczególnie tych związanych z istotnymi interesami publicznymi.

Z drugiej strony, mamy do czynienia z bezprecedensowym upowszechnieniem zjawiska gromadzenia i wykorzystywania ogromnej ilości danych osobowych, możliwym dzięki chmurze obliczeniowej, analityce dużych zbiorów danych i technikom nadzoru elektronicznego.

W rezultacie, ochrona danych odgrywa coraz większą rolę w nowoczesnym podejściu regulacyjnym. Jednak o ile tempo innowacji technologicznych jest zawrotne, reakcje ze strony instytucji pozostają powolne.

Środowisko cyfrowe determinuje przede wszystkim:

- sposób, w jaki komunikujemy się, konsumujemy i uczestniczymy w życiu społecznym i politycznym na świecie, w którym technologia dużych zbiorów danych stała się rzeczywistością;
- sposób, w jak firmy generują zyski;
- sposób, w jaki rządy interpretują swój obowiązek ochrony interesów publicznych i osób;

oraz

- sposób, w jaki inżynierowie projektują i tworzą nowe technologie.

To jak reagujemy na następujące w szybkim tempie zmiany i pojawiające się wyzwania, w tym zagrożenia dla bezpieczeństwa, będzie miało konsekwencje dla nas i przyszłych pokoleń, które odziedziczą cyfrowy świat. Stoimy w obliczu wyjątkowej szansy, by otworzyć nowy rozdział ochrony danych w erze cyfrowej.

Aby umożliwić korzystanie z nowych technologii i chronić prawa jednostki, nowy EIOD ma stać się epicentrum kreatywnych pomysłów i innowacyjnych rozwiązań, dostosowującym obowiązujące zasady ochrony danych do wymogów globalnego sektora cyfrowego.

To innowacyjne myślenie odnosi się zarówno do agendy cyfrowej UE, jak i zasad ochrony danych. Nie chodzi o to, by napisać te zasady od nowa, ale by dostosować je do potrzeb cyfrowej rzeczywistości. Musimy uczynić obowiązujące zasady skuteczniejszymi w praktyce, w naszym opartym na technologii społeczeństwie oraz uwzględnić je w nowych założeniach, opracowanych specjalnie na potrzeby epoki cyfrowej i gospodarki, której motorem są technologie dużych zbiory danych.

WYMIAR MIĘDZYNARODOWY

Przepisy dotyczące ochrony danych ograniczają się do terytorium danego kraju, ale zasięg samych danych jest dużo szerszy. W związku z tym, międzynarodowy wymiar ochrony danych od lat jest przedmiotem dyskusji. Szczegółowo omówiliśmy możliwości większego zaangażowania i osiągnięcia spójności na skalę globalną. Debata na ten temat nasiliła się w ciągu ostatnich dwóch lat, od kiedy po raz pierwszy ujawniono przypadki inwigilacji na masową skalę. Chociaż udało się sformułować wiele cennych wniosków, zabrakło praktycznego działania.

Ochrona danych musi zostać uwzględniona w politykach UE w możliwie najszerszym zakresie. Jest to jeden z najważniejszych priorytetów politycznych. Prowadząc współpracę z krajami spoza UE, Europa powinna znaleźć się w czołówce państw kształtujących globalny standard ochrony danych cyfrowych i prywatności.

Tworząc ten standard, należy skoncentrować się na jednostkach, ich prawach i swobodach, a także ich tożsamości i bezpieczeństwie.

W takim globalnym scenariuszu, zbiór przejrzystych, nowoczesnych i zorientowanych na przyszłość zasad ma również kluczowe znaczenie dla stojącego przed Europą wyzwania cyfryzacji.

EIOD stara się pomóc UE stać się przykładem poszanowania praw podstawowych.

Możemy przekuć zagrożenia na szansę, czyniąc przyjęte w UE zasady i najlepsze praktyki na tyle skutecznymi, by mogły sprostać wyzwaniom związanym z dużymi zbiorami danych, w coraz większym stopniu stającymi się naszą rzeczywistością.

DUŻE ZBIORY DANYCH = DUŻA ODPOWIEDZIALNOŚĆ

Popularność Internetu w dużej mierze można przypisać temu, że potrafił spełnić naturalne, społeczne potrzeby człowieka. Masowa popularność produktów i technologii zależy od tego, czy przemawiają do konsumentów i stanowią odpowiedź na ich potrzebę poczucia bezpieczeństwa i akceptacji społecznej.

Niemniej jednak powszechne gromadzenie ogromnych ilości danych osobowych oznacza przejęcie kontroli nad tymi danymi i odebranie jej jednostkom, a w konsekwencji ograniczenie ich możliwości swobodnego uczestnictwa w cyfrowym świecie.

Duże zbiory danych stanowią wyzwanie dla regulatorów i niezależnych władz, ponieważ wymagają od nich zapewnienia, że przyjęte zasady profilowania, rozpoznawalności, jakości danych, ograniczania celów, minimalizacji danych i ograniczania okresów ich zatrzymywania są skutecznie stosowane w praktyce.

Technologia dużych zbiorów danych, której przedmiotem jest przetwarzanie ogromnych ilości danych osobowych, wymaga przyjęcia bardziej odpowiedzialnej postawy wobec osób, których dane są przetwarzane. Obywatele chcą zrozumieć, w jaki sposób algorytmy mogą tworzyć korelacje i formułować dotyczące ich założenia, oraz jak tworzenie zbiorów ich danych osobowych może zostać wykorzystane na potrzeby przewidywania ich zachowań.

W związku z tym, należy udostępnić obywatelom jasne informacje na temat:

- podmiotów odpowiedzialnych za zbieranie i wykorzystanie informacji,
- celów takich działań,
- rodzaju informacji, które są przetwarzane: zarówno tych świadomie i dobrowolnie przekazywanych, jak i tych, które wynikają z obserwacji i zostały wywnioskowane bez wiedzy danej osoby na podstawie jej zachowań,
- sposobu przetwarzania informacji, w tym logiki stosowanej przez algorytmy w celu formułowania założeń i prognoz na temat jednostek,
- okresu przechowywania informacji i tego, komu są udostępniane.

Technologie cyfrowe muszą być opracowywane zgodnie z zasadami ochrony danych, dając poszczególnym osobom większe możliwości decydowania o sposobie i celu wykorzystania ich danych osobowych oraz dokonywania bardziej świadomych wyborów, w sytuacjach, w których jest to możliwe. Analityka danych jest coraz skuteczniejsza, chociaż nadal podatna na nieprawidłowe założenia i błędy w stosunku do jednostek. Obywatelom należy zapewnić możliwość zakwestionowania takich błędów oraz dostęp do informacji o sposobie i celu wykorzystania dotyczących ich informacji. Oznacza to, że musimy położyć kres nieprzejrzystym politykom prywatności, które zachęcają użytkowników do rezygnacji z przysługujących im praw ochrony danych poprzez zaznaczenie wskazanego pola.

Przyszłość oferuje nam możliwości, które mogą być źródłem inspiracji oraz potencjał, który do tej pory nie został wykorzystany. Potężne firmy działające w sieci oferują niezwykłe rozwiązania i możliwości, które możemy – z pozoru bezpłatnie - wykorzystać w codziennym życiu. A jednak płacimy za nie pewną cenę. Technologia cyfrowa w coraz większym stopniu determinuje nasze życie: kilka potężnych firm dysponuje zaawansowanym oprogramowaniem o szerokim zastosowaniu, działającym w czasie rzeczywistym.

Nasze wartości i nasze prawa podstawowe nie są na sprzedaż. Nowe technologie nie powinny dyktować nam wartości. Powinniśmy mieć możliwość korzystania z nowych technologii bez uszczerbku dla naszych praw podstawowych.

Obawy te nie są niczym nowym: wyrażano je już w momencie pojawienia się pierwszych komputerów. Wszechobecność danych, globalne zjawiska chmury obliczeniowej, technologia dużych zbiorów danych, internet przedmiotów i techniki masowej inwigilacji elektronicznej sprawiły jednak, że problem jest obecnie bardziej palący niż kiedykolwiek.

Jednym z rozwiązań jest ocena wymiaru etycznego, wykraczająca ponad stosowanie przepisów o ochronie danych. Organizacje, przedsiębiorstwa i władze publiczne, które przetwarzają dane osobowe są odpowiedzialne za sposób, w jaki informacje są gromadzone, wymieniane i przechowywane, bez względu na to, czy decyzje podejmowane są przez ludzi, czy też bazują na algorytmach. Zgodnie z podejściem z etycznym, możliwe, użyteczne i opłacalne przetwarzanie danych nie zawsze jest jednoznaczne ze zrównoważonym. W podejściu tym podkreśla się znaczenie odpowiedzialności, która jest ważniejsza niż mechaniczne przestrzeganie litery prawa.

Chcemy zachęcić do bardziej świadomej dyskusji o tym, w jaki sposób technologie dużych zbiorów danych i internet przedmiotów wpłyną na nasze prawa cyfrowe. Zagadnienia te nie ograniczają się do Europy, ale dotyczą całego świata.

BUDOWANIE GLOBALNYCH PARTNERSTW

Odpowiedzialność w zakresie przetwarzania danych osobowych jest globalnym wyzwaniem.

Etyczny wymiar ochrony danych polega na wyjściu poza wspólnotę unijnych urzędników, prawników i specjalistów do spraw technologii informacyjnych i zaangażowanie myślicieli, którzy są w stanie ocenić średnio- i długoterminowe skutki zmian technologicznych i rozwiązań regulacyjnych.

Zamierzamy prowadzić bliską współpracę z naszymi kolegami pracującymi na szczeblu krajowym, co pozwoli wzmocnić współpracę i zachęcić UE do przyjęcia wspólnego stanowiska na globalnych forach dotyczących prywatności i ochrony danych.

Jako organ ochrony danych, jesteśmy w stanie wykorzystać doświadczenie, które zdobyliśmy doradzając organom UE w zakresie transferów międzynarodowych, projektowania i realizacji usług e-administracji oraz nadzoru wielkoskalowych systemów informatycznych.

Będziemy prowadzić dialog z ekspertami ds. technologii informacyjnych, przedstawicielami przemysłu i społeczeństwa obywatelskiego, który pozwoli nam zrozumieć, w jaki sposób usprawnić współpracę międzynarodową; liczymy na to, że uda nam się przyjąć wspólne ustalenia w zakresie obecnych i przyszłych przepływów danych, zgodne z interesem jednostek.

Będziemy również inwestować w budowanie globalnych partnerstw z innymi ekspertami z krajów spoza UE, władzami i organizacjami międzynarodowymi, które pozwolą na podejmowanie wspólnych działań na rzecz konsensusu społecznego dotyczącego zasad, mogących stać się podstawą dla wiążących przepisów oraz działalności gospodarczej i technologii, a także zakresu interoperacyjności różnych systemów ochrony danych.

NOWY ROZDZIAŁ W OCHRONIE DANYCH W UE

UE zajmuje obecnie uprzywilejowaną pozycję, stanowiąc punkt odniesienia w zakresie prywatności i ochrony danych dla większości krajów świata. Pomimo tego, aby UE pozostała wiarygodnym liderem w erze cyfrowej, musi przestrzegać podstawowych zasad ochrony danych i prywatności, podejmując niezwłocznie stosowne działania.

Po wielu latach dyskusji na ten temat, reforma unijnych zasad ochrony danych stała się kwestią niecierpiącą zwłoki. Ani społeczeństwo, ani technologia nie będą czekać, aż Europa dotrzyma kroku zachodzącym zmianom. Im dłużej trwa proces opracowywania nowego zestawu reguł, tym większe ryzyko, że w momencie przyjęcia okażą się one przestarzałe.

Reforma nie może doprowadzić do spowolnienia tempa innowacji, ale powinna zapewnić nam nowoczesną i skuteczną ochronę praw podstawowych, dzięki której uda się odbudować zaufanie w społeczeństwie cyfrowym, nadszarpnięte na skutek stosowania tajnych i nieproporcjonalnych w stosunku do celu narzędzi nadzoru.

Ogromne znaczenia ma uproszczenie ochrony danych i uczynienie jej bardziej przejrzystą i mniej zbiurokratyzowaną, pozwalając jej współtworzyć podstawy cyfrowego świata teraz i w przyszłości.

Choć obecne przepisy UE dotyczące przetwarzania danych osobowych służyły Europejczykom stosunkowo dobrze, należy odejść od fragmentarycznego podejścia do ochrony danych w przepisach krajowych, ponieważ w obecnych warunkach nie jest ono w stanie spełniać swojego celu. Gdy w 1990 r. przyjęto unijną dyrektywę o ochronie danych, Internet był jeszcze w powijakach i nikt nie przeczuwał, w jakim stopniu sieć wpłynie na nasze społeczeństwo i gospodarkę. Podobnej zmiany paradygmatu możemy oczekiwać teraz. Technologie będą rozwijać się i zmieniać w sposób, którego nie są w stanie przewidzieć nawet ich twórcy.

Osoby prywatne, władze publiczne, przedsiębiorstwa i naukowcy potrzebują zbioru jednoznacznych i wszechstronnych przepisów, który będzie można stosować przez kolejne dwa dziesięciolecia. Taki zbiór przepisów byłby egzekwowany przez sądy europejskie i krajowe, a także prawdziwie niezależne organy ochrony danych. Zasady te muszą zapewnić skuteczną ochronę praw dorastającego dzisiaj pokolenia Internetu.

EIOD będzie bardziej aktywnym partnerem w dyskusjach prowadzonych pomiędzy Komisją Europejską, Parlamentem a Radą w sprawie reformy systemu ochrony danych, w szczególności w trakcie rozmów trójstronnych. Unikając nadmiernej biurokracji, będziemy szukać praktycznych i skutecznych rozwiązań, które są na tyle elastyczne, by poradzić sobie z innowacjami technologicznymi i transgranicznymi przepływami danych.

Pomożemy w opracowaniu pragmatycznych rozwiązań ustawodawczych służących wzmocnieniu roli jednostek i organów nadzorczych oraz odpowiedzialności kontrolerów, przy jednoczesnym uproszczeniu istniejących zbędnych wymogów formalnych. Ochrona danych musi być bardziej dynamiczna i mniej zbiurokratyzowana.

Biorąc pod uwagę aktualne trendy, w latach 2015–2030 (spodziewany czas trwania reform) możemy spodziewać się przyspieszenia tempa rozwoju technologii oraz epokowych zmian. Jeśli diabeł tkwi w szczegółach, my dostrzegamy go w niektórych nadmiernie sztywnych i drobiazgowych przepisach reformy. Powstaje ryzyko, że niektóre z przepisów staną się nieskuteczne lub przestarzałe jeszcze zanim pełny pakiet poddany zostanie ponownemu przeglądowi. Powstaje ryzyko, że niektóre z przepisów staną się nieskuteczne lub przestarzałe jeszcze zanim pełny pakiet poddany zostanie ponownemu przeglądowi. Przepisy te można lepiej dostosować do wymogów rzeczywistości bez obniżania poziomu ochrony, zapewniając im elastyczność bez dwuznaczności. Skalowalność niektórych zobowiązań także jest problematyczna.

W zmodernizowanych ramach regulacyjnych na rzecz gospodarki cyfrowej przyszłości, ochrona dużych zbiorów danych może stanowić siłę napędową zrównoważonego wzrostu. Solidna agenda cyfrowa UE może opierać się na solidnych podstawach nowoczesnego systemu ochrony danych.

UE powinna odgrywać wiodącą rolę w dostosowaniu zasad do nowych, wciąż zmieniających się realiów komunikacji międzyludzkiej i prowadzenia działalności gospodarczej.

Europejczycy reprezentują 12% ludności świata, a zarazem ponad 26% użytkowników internetu. Tymczasem podmioty europejskie stanowią zaledwie niewielki odsetek wiodących firm technologicznych, a rynek technologii ochrony prywatności został całkowicie zdominowany przez rynek analityki danych.

Sposób, w jaki Europa radzi sobie z wyzwaniami posłuży jako przykład dla innych krajów i regionów na całym świecie zmagających się z tymi samymi problemami.

ODPOWIEDZIALNOŚĆ ORGANÓW UE

Organy UE, w tym Europejski Inspektor Ochrony Danych, muszą ponosić pełną odpowiedzialność za sposób przetwarzania danych osobowych: jeżeli pretendujemy do pozycji lidera, nasza własna postawa musi być nienaganna.

Pragniemy wykorzystać nasze doświadczenie dynamicznego organu nadzoru doradzającego instytucjom UE w sprawie reformy obecnych zasad, która pozwoli nam sprostać globalnym wyzwaniom. Chcemy podnosić społeczną świadomość w zakresie znaczenia zasad ochrony danych oraz zasad ich stosowania w poszczególnych sektorach, w praktyce i w procesie tworzenia polityk.

Będziemy dążyć do coraz sprawniejszej interakcji z instytucjami i organami UE, które monitorujemy, starając się zapewnić swoim działaniom większą skuteczność.

Zależy nam na tym, by działać w sposób bardziej selektywny, interweniując tylko wtedy, gdy w grę wchodzą ważne interesy lub podejmując działania, które są w stanie pozytywnie wpłynąć na kulturę ochrony danych i skłaniają do przyjęcia odpowiedzialnej postawy w obrębie instytucji UE nie jako odrębna dyscyplina, ale stając się elementem ich codziennej, dobrej administracji.

Zamierzamy nadal korzystać ze swoich uprawnień wykonawczych i dbać o przestrzeganie przyjętych zasad nie stosując dyktatu, ale raczej skuteczną perswazję i dając przykład zgodnie z zasadą odpowiedzialności i zachęcając do zaangażowania kierownictwo wyższego szczebla w instytucjach UE.

Korzystając ze zdobytych przez nas doświadczeń w zakresie wdrażania przepisów dotyczących ochrony danych w instytucjach UE, zgodnie z treścią rozporządzenia 45/2001, będziemy aktywnie współpracować z unijnym ustawodawcą w zakresie modernizacji tych przepisów równolegle z przeprowadzaną reformą systemu ochrony danych.

CZAS NA NOWĄ DYSKUSJĘ NA TEMAT BEZPIECZEŃSTWA I PRYWATNOŚCI

Bezpieczeństwo publiczne oraz zwalczanie przestępczości i terroryzmu są ważnymi celami publicznymi. Nie można przy tym zapominać, że niepotrzebny, nieproporcjonalny, a nawet nadmierny nadzór prowadzony przez lub w imieniu rządów sieje nieufność i podważa wysiłki ustawodawcy w zakresie rozwiązywania wspólnych problemów związanych z bezpieczeństwem.

Wskazanie skutecznych środków, które nie zagrażałyby podstawowym prawom do prywatności i ochrony danych jest od kilku lat przedmiotem starań Unii Europejskiej; dąży ona do opracowania i wprowadzenia środków, które są konieczne, skuteczne i proporcjonalne. Jesteśmy świadomi realnych zagrożeń dla bezpieczeństwa naszego stylu życia i swobód, które mogą ewoluować w przyszłości. W jaki sposób uniknąć sytuacji, w której większość obywateli staje się niewinnymi ofiarami? Priorytetem powinno być opracowanie spójnego i systematycznego mechanizmu śledzenia zachowań i działań osób podejrzanych o działalność kryminalną i terrorystyczną, a nie masowe gromadzenie danych osobowych.

Nadzór nad koniecznością i proporcjonalnością określonych środków walki z przestępczością i terroryzmem wymaga szerokiej debaty. Zasady te zapisane są w Karcie Praw Podstawowych, a ich odzwierciedleniem jest orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej, czyli wymagania prawne obowiązujące w UE, które EIOD ma za zadanie chronić. Jako organ niezależny, EIOD nie występuje automatycznie za lub przeciw danemu środkowi; jesteśmy w pełni zaangażowani w misję doradzania instytucjom UE w sprawie skutków polityk, które mają poważny wpływ na prawa podstawowe. Jesteśmy gotowi do podjęcia bliższej współpracy z ustawodawcą w celu opracowania innowacyjnych rozwiązań prawnych i technologicznych.

Traktując reformę ochrony danych jako pakiet i biorąc pod uwagę, w jaki sposób obecne i przyszłe umowy dwustronne i międzynarodowe mogą zostać wykorzystane w bardziej zrównoważony sposób, musimy ustanowić jasny i kompleksowy zbiór zasad i kryteriów, którymi będą kierować się ograny ścigania i bezpieczeństwa narodowego w sytuacji, gdy ich działania stanowią potencjalne zagrożenie dla naszych praw podstawowych.

NASZE ZOBOWIĄZANIE

Zależy nam na tym, by UE dawała przykład poszanowania ochrony danych i prywatności, przyjmując wspólną, wiarygodną i świadomą postawę w stosunku do praw podstawowych w erze cyfrowej.

Ważnym elementem naszej działalności jest wyjaśnianie europejskiego podejścia do ochrony danych w prosty i przejrzysty sposób oraz zapewnienie, że ochrona obowiązuje i ma zastosowanie pomimo gwałtownych zmian technologicznych.

Sprawując nadzór nad instytucjami UE, będziemy działać poprzez edukację, perswazję i przykład, jedynie w ostateczności stosując przysługujące nam uprawnienia do egzekwowania przepisów.

Dla tak niewielkiej organizacji, strategia ta jest wyzwaniem i stanowi ambitny program. Wiemy jednak, że możemy liczyć na umiejętności naszych doświadczonych i zmotywowanych pracowników. Dzięki ich wsparciu, jesteśmy w stanie osiągnąć znacznie więcej.

Jesteśmy w pełni świadomi tego, że nasza skuteczność zależy od aktywnego i konstruktywnego partnerstwa, od współpracy z krajowymi organami ochrony danych i grupą roboczą utworzoną na mocy art. 29 dyrektywy. Po ustanowieniu Europejskiej Rady Ochrony Danych, będziemy skutecznie realizować zadania powierzone nam przez ustawodawców, usprawniając i wspierając świadomy dialog pomiędzy władzami krajowymi.

Strategia ta stanowi nasze publiczne zobowiązanie do realizacji tej wizji w ciągu najbliższych pięciu lat. Jest to zobowiązanie do przejrzystości, odpowiedzialności i selektywności naszych działań.

Mamy teraz niepowtarzalną szansę kształtowania globalnego, cyfrowego standardu poszanowania prywatności i ochrony danych osobowych.

Nadszedł czas, aby przeprowadzić cyfryzację ochrony danych, ponieważ nasze społeczeństwo już teraz jest społeczeństwem cyfrowym.

PLAN DZIAŁANIA

Analizując powyższe problemy, zidentyfikowaliśmy trzy cele strategiczne i 10 działań priorytetowych, których realizacja pomoże nam uczynić UE wzorowym liderem w erze cyfrowej.

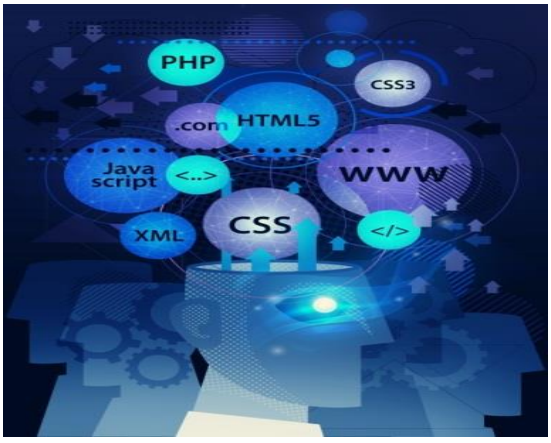
1 DIGITALIZACJA OCHRONY DANYCH

DZIAŁANIE 1: PROMOWANIE TECHNOLOGII NA POTRZEBY SKUTECZNIEJSZEJ OCHRONY DANYCH I PRYWATNOŚCI;

- współpraca z programistami, twórcami i specjalistami ds. technologii informacyjnych w celu promowania idei uwzględniania ochrony prywatności już na etapie projektowania i projektowania z domyślnymi ustawieniami prywatności z wykorzystaniem inżynierii ochrony prywatności;
- wspieranie opracowywania modułów i narzędzi służących do tworzenia aplikacji i usług nie naruszających prywatności, takich jak biblioteki, wzorce projektowe, fragmenty kodów, algorytmy, metody i praktyki, które mogą być łatwo wykorzystane w praktyce;
- rozbudowa Sieci na rzecz Inżynierii Prywatności w Internecie (ang. Internet Privacy Engineering Network, IPEN), umożliwiając jej współdziałanie z jeszcze bardziej różnorodnym zakresem grup umiejętności, w celu uwzględniania kwestii ochrony danych i prywatności na wszystkich etapach tworzenia systemów, usług i aplikacji;
- opracowywanie kreatywnych wytycznych dotyczących stosowania zasad ochrony danych w procesie tworzenia technologii i projektowania produktu;
- podkreślanie, że ochrona danych jest czynnikiem budującym zaufanie konsumentów i zwiększającym efektywność współpracy gospodarczej, a tym samym potencjalnie sprzyjającym wzrostowi gospodarczemu;
- współpraca z uczelniami wyższymi i naukowcami w sektorze publicznym i prywatnym, z naciskiem na innowacyjne obszary rozwoju technologicznego, które mają wpływ na ochronę danych osobowych, która będzie wyznaczać kierunki naszych działań służących monitorowaniu technologii.

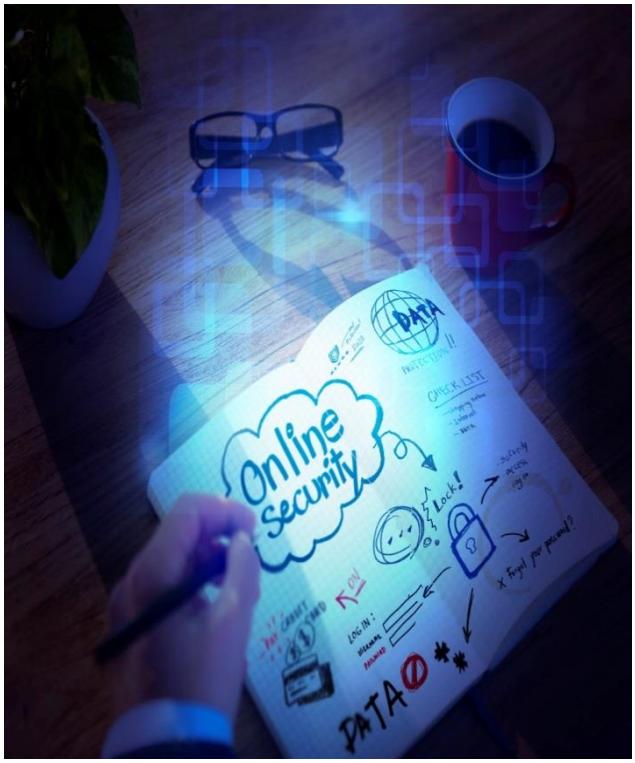
DZIAŁANIE 2: IDENTYFIKACJA INTERDYSCYPLINARNYCH ROZWIĄZAŃ POLITYCZNYCH

- inicjowanie i wspieranie ogólnoeuropejskiego dialogu pomiędzy organami UE i organami regulacyjnymi, naukowcami, przedstawicielami przemysłu, sektora technologii informacyjnych, organizacjami ochrony praw konsumentów i innymi, na temat technologii dużych zbiorów danych, internetu przedmiotów i praw podstawowych w sektorze publicznym i prywatnym;
- podejmowanie działań interdyscyplinarnych w celu rozwiązania kwestii politycznych w zakresie prywatności i ochrony danych osobowych;
- inicjowanie dyskusji dotyczących ogólnych zagadnień, w których uwzględnia się opinie przedstawicieli różnych dziedzin, oraz koordynacja działań szkoleniowych służących przekazywaniu pracownikom wiedzy z zakresu pokrewnych dyscyplin.



DZIAŁANIE 3: ZWIĘKSZANIE PRZEJRZYSTOŚCI, KONTROLI I ODPOWIEDZIALNOŚCI UŻYTKOWNIKÓW W PROCESIE PRZETWARZANIA DUŻYCH ZBIORÓW DANYCH

- opracowanie modelu polityk dotyczących przetwarzania informacji, zwłaszcza w odniesieniu do usług internetowych świadczonych przez organy UE, wyjaśniającego w prosty sposób, jak procesy biznesowe mogą wpływać na prawa osób fizycznych do prywatności i ochrony danych osobowych, w tym zagrożenia dla osób fizycznych związane z ponowną identyfikacją danych anonimowych, pseudoanonimowych lub zagregowanych;
- wspieranie rozwoju innowacyjnych rozwiązań technicznych w celu przekazywania informacji i kontroli użytkownikom, zmniejszając tym samym asymetrię informacji i zwiększając autonomię użytkowników.



2 BUDOWANIE GLOBALNYCH PARTNERSTW

DZIAŁANIE 4: ROZWÓJ ETYCZNEGO WYMIARU OCHRONY DANYCH

- ustanowienie zewnętrznej grupy doradczej ds. etycznego wymiaru ochrony danych w celu zbadania zależności pomiędzy prawami człowieka, technologiami, rynkami i modelami biznesowymi w XXI wieku;
- włączenie zagadnień etycznych w naszą codzienną pracę i działania, które prowadzimy jako niezależny organ regulacyjny i doradca polityczny.

DZIAŁANIE 5: UWZGLĘDNIANIE KWESTII OCHRONY DANYCH W POLITYCE MIĘDZYNARODOWEJ

- doradzanie instytucjom UE w zakresie spójnego i konsekwentnego stosowania unijnych zasad ochrony danych podczas negocjowania umów handlowych (a także porozumień w sektorze organów ścigania), podkreślając, że ochrona danych nie stanowi przeszkody dla współpracy, ale przeciwnie, raczej jej sprzyja;
- monitorowanie wdrażania istniejących umów międzynarodowych, w tym porozumień handlowych, aby zagwarantować, że nie stanowią one

zagrożenia dla praw podstawowych osób fizycznych.

DZIAŁANIE 6: PRZYJĘCIE SPÓJNEGO STANOWISKA UE NA ARENIE MIĘDZYNARODOWEJ

- promowanie globalnego sojuszu z organami ochrony danych i prywatności w celu znalezienia technicznych i prawnych rozwiązań kluczowych problemów związanych z ochroną danych, takich jak duże zbiory danych, internet przedmiotów i masowy nadzór.
- współpraca z władzami krajowymi w celu zapewnienia skuteczniejszego i skoordynowanego nadzoru nad wielkoskalowymi systemami teleinformatycznymi, w połączeniu z bazami danych na poziomie UE i krajowym, oraz zachęcanie ustawodawców do zharmonizowania poszczególnych, istniejących platform;
- maksymalne zaangażowanie w dyskusje na forach międzynarodowych, w tym w Radzie Europy i OECD, na temat ochrony danych i prywatności;
- rozwijanie naszych własnych umiejętności w zakresie wykładni porównawczej w odniesieniu do norm ochrony danych.

3 NOWY ROZDZIAŁ W OCHRONIE DANYCH W UE

DZIAŁANIE 7: PRZYJMOWANIE I WDRAŻANIE AKTUALNYCH ZASAD OCHRONY DANYCH

- nakłanianie Parlamentu Europejskiego, Rady i Komisji, by jak najszybciej wypracowały porozumienie w sprawie pakietu reform dotyczących ochrony danych;
- poszukiwanie praktycznych rozwiązań ograniczających biurokrację i stanowiących elastyczne podejście do innowacji technicznych i transgranicznych przepływów danych oraz umożliwiają osobom fizycznym skuteczniejsze egzekwowanie swoich praw w Internecie oraz poza nim;
- w okresie po przyjęciu reform: dążenie do ich prawidłowego, spójnego i terminowego wdrożenia, którego głównym motorem są organy nadzoru;
- jeżeli EIOD utworzy Sekretariat dla nowej Europejskiej Rady Ochrony Danych (EDPB), przygotowanie tego organu do niezwłocznego podjęcia bliskiej współpracy z personelem organów krajowych, w szczególności poprzez opracowanie odpowiednich rozwiązań przejściowych, które umożliwią sprawne przekazanie kompetencji grupy roboczej utworzonej na mocy art. 29;
- partnerska współpraca z władzami za pośrednictwem EDPB, w celu opracowywania szkoleń i świadczenia usług doradztwa tym osobom lub organizacjom, które zbierają, wykorzystują, udostępniają i przechowują dane osobowe, w celu zapewnienia zgodności z treścią rozporządzenia już z początkiem 2018 r.;
- większe zaangażowanie w opracowanie ustawodawstwa wykonawczego lub przepisów prawnych dotyczących poszczególnych sektorów;
- stworzenie internetowego repozytorium informacji na temat ochrony danych jako źródła informacji dla osób zainteresowanych.

DZIAŁANIE 8: ZWIĘKSZENIE ODPOWIEDZIALNOŚCI ORGANÓW UE PRZETWARZAJĄCYCH DANE OSOBOWE

- współpraca z Parlamentem Europejskim, Radą i Komisją w celu zapewnienia, że aktualne przepisy wprowadzone na mocy rozporządzenia nr 45/2001 są zgodnie z treścią ogólnego rozporządzenia o ochronie danych, i że zmienione ramy wejdą w życie najpóźniej z początkiem 2018 r.;
- kontynuowanie szkoleń i udzielanie porad organom UE w zakresie najlepszych rozwiązań w obszarze poszanowania zasad ochrony danych w praktyce; położenie nacisku na te technologie przetwarzania danych, które stwarzają duże ryzyko dla osób fizycznych;
- wspieranie instytucji UE w odchodzeniu od podejścia opartego wyłącznie na zgodności na rzecz uwzględniania odpowiedzialności i ścisłej współpracy z oficerami ochrony danych;
- udoskonalenie naszej metodyki przeprowadzania kontroli i wizyt, a w szczególności usprawnienie metody kontrolowania systemów informatycznych.

DZIAŁANIE 9: UŁATWIENIE ODPOWIEDZIALNEGO I ŚWIADOMEGO KSZTAŁTOWANIA POLITYKI

- opracowanie kompleksowego zestawu narzędzi polityki na rzecz organów UE, na który składa się pisemne poradnictwo, warsztaty i szkolenia, wspieranego przez sieć;
- wskazywanie każdego roku tych kwestii polityki UE, które mają największy wpływ na prywatność i ochronę danych oraz opracowanie odpowiednich analiz i doradztwa prawnego, zarówno w postaci publikowanych opinii, jak i nieformalnych porad;
- wzbogacanie naszej wiedzy na temat poszczególnych sektorów, tak aby udzielane przez nas porady były oparte na wiarygodnych informacjach i przydatne;
- opracowanie skutecznych metod współpracy z Parlamentem, Radą i Komisją, a także aktywne gromadzenie informacji zwrotnych na temat wartości naszego wsparcia;
- budowanie dialogu z Trybunałem Sprawiedliwości Unii Europejskiej na temat praw podstawowych i wspieranie Trybunału we wszystkich stosownych przypadkach występując w roli strony postępowania lub eksperta.

DZIAŁANIE 10: ZACHĘCANIE DO DOJRZAŁEJ DYSKUSJI NA TEMAT BEZPIECZEŃSTWA I PRYWATNOŚCI

- zachęcanie do świadomej dyskusji na temat definicji takich pojęć jak bezpieczeństwo narodowe, bezpieczeństwo publiczne i poważna przestępczość;
- zachęcanie ustawodawców do praktycznego gromadzenia i badania dowodów pochodzących z państw członkowskich (w ramach zamkniętych sesji, jeśli to konieczne), które wymagają zebrania dużych ilości danych osobowych, m.in. na potrzeby bezpieczeństwa publicznego i przejrzystości finansowej, mogących mieć wpływ na prawo do prywatności; wykorzystanie ich na potrzeby usług doradztwa w sprawie konieczności i proporcjonalności działań, świadczonych na rzecz prawodawcy unijnego;
- wspieranie konwergencji pomiędzy różnymi przepisami dotyczącymi ochrony danych w obszarze współpracy policyjnej i sądowej, a także spójności nadzoru wielkoskalowych systemów informatycznych. Powinno to obejmować szybkie przyjęcie projektu dyrektywy w sprawie przetwarzania danych do celów zapobiegania, dochodzenia, wykrywania lub ścigania przestępstw.

REALIZACJA STRATEGII

Staramy się realizować naszą strategię poprzez staranne zarządzanie naszymi zasobami, przejrzystą komunikację oraz regularne monitorowanie i ocenę naszej działalności.

EFEKTYWNE ZARZĄDZANIE ZASOBAMI

Zamierzamy nadal solidnie planować i monitorować wykorzystanie środków finansowych.

Będziemy zarządzać naszym personelem i wspierać jego rozwój w celu wzbogacania naszej wiedzy i rozbudowywania sieci.

Zamierzamy kontynuować tworzenie sprawnej, elastycznej i profesjonalnej organizacji. Będziemy nadal drobiazgowo ustalać priorytety i usprawniać nasze strategiczne zarządzanie zasobami ludzkimi.

Rozwiniemy i wdrożymy kompleksowy system zarządzania jakością.

Będziemy dawać przykład odpowiedzialności i postępowego podejścia do przetwarzania danych osobowych.

JASNA KOMUNIKACJA

Ochrona danych jest często postrzegana jako dziedzina wymagająca specjalistycznej wiedzy technicznej i niezrozumiała dla laików. Aby zmienić to przekonanie, będziemy posługiwać się prostym językiem, czyniąc kwestie techniczne bardziej przystępnymi.

W trosce o przejrzystość, zobowiązujemy się do komunikacji w jasny i zwięzły sposób, zrozumiały dla różnych grup odbiorców i unikając żargonu.

Dotyczy to wszystkich naszych działań, tj. wydawanych opinii, wskazówek, treści publikowanych na stronie internetowej oraz interakcji z mediami, bez względu na złożoność danego zagadnienia prawnego lub technicznego.

POMIAR NASZEJ WYDAJNOŚCI

Będziemy działać w sposób przejrzysty i odpowiedzialny, przyjmując roczny plan zarządzania, publikując raport roczny i uwzględniając w naszych działaniach zbiór kluczowych wskaźników wydajności związanych z celami niniejszej strategii.

Pod koniec każdego roku będziemy przyjmować program prac na rok następny, obejmujący główne priorytety w zakresie ochrony danych w UE, odpowiadające strategicznym celom i działaniom priorytetowym.

Sprawozdanie roczne służyć będzie ocenie naszych postępów w realizacji celów w poprzednim roku, ze szczególnym uwzględnieniem kluczowych wskaźników wydajności (KPI). KPI, które zidentyfikowano w styczniu 2013 r. w poprzedniej Strategii na lata 2013–2014, zostaną poddane przeglądowi w ciągu pierwszego roku realizacji bieżącej strategii; pozwoli to ocenić, czy wymagają dostosowania.

Pełniejszy średniookresowy przegląd Strategii zostanie przeprowadzony w porozumieniu z zainteresowanymi stronami, tj. organami UE i innymi podmiotami. Wyniki przeglądu zostaną uwzględnione w raporcie rocznym EIOD za rok 2017 r., który zamierzamy opublikować na początku 2018 r.

Europejski Inspektor Ochrony Danych

www.edps.europa.eu

@EU_EDPS

EDPS

European Data Protection Supervisor