

EUROPEJSKI
INSPEKTOR OCHRONY DANYCH

SPRAWOZDANIE ROCZNE 2014

STRESZCZENIE



SPRAWOZDANIE ROCZNE 2014

STRESZCZENIE

**Europe Direct to serwis, który pomoże Państwu
znaleźć odpowiedzi na pytania dotyczące Unii Europejskiej.**

**Numer bezpłatnej infolinii (*):
00 800 6 7 8 9 10 11**

(*) Informacje są udzielane nieodpłatnie, większość połączeń również jest bezpłatna
(niektórzy operatorzy, hotele lub telefony publiczne mogą naliczać opłaty).

Więcej informacji o Unii Europejskiej można znaleźć w portalu Europa (<http://europa.eu>).

Luksemburg: Urząd Publikacji Unii Europejskiej, 2015

PDF ISBN 978-92-9242-076-5 ISSN 1831-0583 doi:10.2804/1287 QT-AB-15-001-PL-N

© Unia Europejska, 2015

Powielanie materiałów dozwolone pod warunkiem podania źródła.

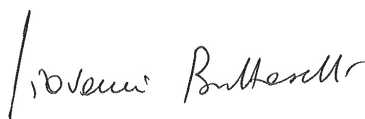
WPROWADZENIE

W ostatnich latach ochrona danych przestała być kwestią marginalną, a stała się zasadniczym elementem podejmowania decyzji politycznych i planowania biznesowego.

W przypadku UE rok 2014 może być zapamiętany w przyszłości jako okres przełomowy, moment, w którym prawa do prywatności i ochrony danych osobowych, ustanowione w Karcie praw podstawowych, zdecydowanie przeniosły się z teorii prawa do rzeczywistości. Trybunał Sprawiedliwości w swoich przełomowych orzeczeniach dotyczących *Dyrektywy w sprawie zatrzymywania danych* i *Google Spain* wskazał na odpowiedzialność prawodawców i administratorów danych za zapewnienie, aby dane osobowe były przetwarzane rzetelnie i w sposób proporcjonalny do realizowanego uzasadnionego celu. Narady nad reformą zbioru przepisów UE, które obecnie trwają już od czterech lat, zbliżają się do końca – Parlament Europejski wyraził zdecydowane poparcie dla zmienionego tekstu ogólnego rozporządzenia o ochronie danych, zaś Rada zmagająca się z kluczowymi kwestiami wykonania i spójności. Tymczasem wzrosło zaniepokojenie masowym nadzorem i zaczęto sobie coraz bardziej zdawać sprawę z konieczności zrewidowania i wyjaśnienia parametrów przepływu danych między UE a jej partnerami na świecie.

Rok 2014 był rokiem zmian dla całej UE, jak również dla naszej instytucji. W niniejszym sprawozdaniu rocznym przedstawiono przegląd działań Europejskiego Inspektora Ochrony Danych i naszych wysiłków mających na celu zwiększenie zdolności organów UE do odpowiedzialnego przetwarzania danych oraz do bardziej aktywnego uwzględniania przepisów i zasad w dziedzinie ochrony danych w kształtowaniu polityki. Oprócz kontroli wstępnych operacji przetwarzania i inspekcji oraz licznych opinii i uwag na temat inicjatyw politycznych, w tym uwag na temat trwających reform w zakresie ochrony danych, opublikowaliśmy szereg kluczowych wytycznych, dotyczących na przykład praw osób, których dane dotyczą, przekazywania danych i ochrony danych w regulacji usług finansowych.

To zakorzenienie ochrony danych w głównym nurcie polityki UE stanowi sukces odniesiony dzięki spokojnemu autorytetowi i niestrudżonemu wysiłkowi Petera Hustinksa, którego 10-letnia kadencja jako Europejskiego Inspektora Ochrony Danych dobiegła końca w 2014 r., oraz dzięki talentom i zaangażowaniu osób, które pracują dla tej instytucji. W oparciu o spuściznę Petera Hustinksa nasze priorytety na najbliższe pięć lat, określone w naszej strategii opublikowanej w marcu 2015 r., obejmują ściślejszą niż kiedykolwiek współpracę z krajowymi organami ochrony danych, jak również z Parlamentem i państwami członkowskimi, tak aby UE mówiła jednym głosem, wiarygodnym i spójnym, stojąc na straży praw i interesów jednostki w naszym coraz bardziej zglobalizowanym i ucyfrowionym społeczeństwie.



Giovanni Buttarelli
Europejski Inspektor Ochrony Danych



Wojciech Wiewiórowski
Zastępca Inspektora

NAJWAŻNIEJSZE WYDARZENIA W 2014 R.

Rok 2014 był dla EIOD rokiem zmian, w którym miał miejsce opóźniony wybór i mianowanie nowego inspektora i jego zastępcy. Nominacje, których oczekiwano na początku roku, nastąpiły dopiero na jego koniec. Chociaż wynikająca z tej sytuacji niepewność miała wpływ na planowanie działalności całej instytucji EIOD, nadal wykonywaliśmy obowiązki zgodnie z naszymi zobowiązaniami na mocy [rozporządzenia \(WE\) nr 45/2001](#).

Nadzór i egzekwowanie przepisów

Podobnie jak w poprzednich latach ważną część naszych zadań stanowiły podstawowe działania w zakresie nadzoru i egzekwowania przepisów w odniesieniu do przetwarzania danych osobowych przez ponad 60 instytucji i agencji europejskich. Kontrole wstępne, konsultacje, skargi, inspekcje i wizyty stanowiły zasadniczą część naszej pracy w tej dziedzinie. Mimo stosunkowo dużej liczby spraw udało nam się poprawić efektywność naszego przepływu pracy.

Ponadto w ścisłej współpracy z inspektorami ochrony danych powołanymi w każdej instytucji i każdym organie UE nadal przez cały rok działaliśmy na rzecz podnoszenia świadomości i zapewnialiśmy wytyczne, aby pomóc w promowaniu kultury ochrony danych w instytucjach UE. Szczególnie istotne były:

- **wytyczne** dotyczące praw osób fizycznych (praw osób, których dane dotyczą), przyjęte w lutym,
- **stanowisko** w sprawie przekazywania danych, przyjęte w lipcu, oraz
- **wytyczne** dotyczące konfliktów interesów, przyjęte w grudniu;
- szereg spotkań z administratorami danych na temat konkretnych kwestii ochrony danych w administracji UE;
- trzy konferencje w Europejskiej Szkole Administracji (EUSA) i jedno warsztaty dla koordynatorów do spraw ochrony danych;

- dwa spotkania z inspektorami ochrony danych – w czerwcu i listopadzie.

Bardziej aktywne doradztwo w zakresie polityki

W 2014 r. przeanalizowaliśmy, jak wywiązujemy się ze spoczywającego na EIOD zobowiązania prawnego doradzania instytucjom. W naszym [dokumencie strategicznym](#) pt. „EIOD jako doradca instytucji UE w zakresie polityki i prawodawstwa: czerpanie z dziesięciu lat doświadczenia”, opublikowanym w czerwcu, powtórzyliśmy, że EIOD opiera się na zasadach bezstronności, uczciwości, przejrzystości i pragmatyzmu, oraz podkreśliliśmy nasze szerokie, pluralistyczne i aktywne kontakty z zainteresowanymi stronami. Chcemy rozwijać kulturę odpowiedzialności we wszystkich instytucjach i organach UE poprzez szkolenia oraz ogólne i sektorowe wytyczne, aby umożliwić instytucjom podejmowanie świadomych decyzji w sprawie skutków nowych wniosków dla ochrony danych. Rozpoczęliśmy już nawiązywanie kontaktów z mniej znanymi rozmówcami, w tym z Dyrekcją Generalną ds. Rynku Wewnętrznego i Usług (DG MARKT) Komisji oraz z prezydencją Rady, którzy są coraz bardziej świadomi znaczenia ochrony danych. Ponadto nawiązaliśmy regularne kontakty i wymianę informacji z Agencją Praw Podstawowych Unii Europejskiej (FRA) i instytucjami międzynarodowymi, w tym z Radą Europy.

Publikując w marcu 2014 r. wstępną opinię na temat [Prywatności i konkurencyjności w dobie dużych zbiorów danych](#), rozpoczęliśmy analizę interakcji między prawem w dziedzinie ochrony danych, konkurencji i prawem konsumenckim. Dyskusję na ten temat rozpoczęto podczas warsztatów w czerwcu 2014 r., w których udział wzięli eksperci we wszystkich trzech dziedzinach prawa z UE i Stanów Zjednoczonych.

Na podstawie konstruktywnego i ukierunkowanego dialogu z instytucjami podjęliśmy się opracowania „zestawu narzędzi na potrzeby polityki” – w tym wytycznych tematycznych lub sektorowych – służącego politykom i prawodawcom jako wskazówki odnośnie do znaczenia praw

podstawowych do prywatności i do ochrony danych w konkretnych sektorach.

W listopadzie 2014 r. dostarczyliśmy pierwsze z tych narzędzi – dotyczy ono regulacji usług finansowych, czyli dziedziny, która w ostatnich latach była przedmiotem intensywnych reform ustawodawczych. Nasze wytyczne sektorowe opierały się na wiedzy uzyskanej podczas seminarium prowadzonego przez DG MARKT w lutym 2014 r.

W kierunku nowych ram prawnych w zakresie ochrony danych: koniec jest blisko?

Reforma ram ochrony danych stanowiła jedno z największych i najbardziej skomplikowanych wyzwań dla prawodawców UE w ostatnich latach. Na szczeblu krajowym, europejskim i międzynarodowym panuje duże zainteresowanie ewolucją obu projektów wniosków – dotyczących ogólnego rozporządzenia o ochronie danych oraz dyrektywy w sprawie danych osobowych przetwarzanych do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania albo wykonywania kar kryminalnych. EIOD nadal ściśle współpracował z Parlamentem, Radą i Komisją podczas krytycznych negocjacji, które miały miejsce w 2014 r.

Współpraca

W 2014 r., podobnie jak w 2013 r., zapewniliśmy sekretariat na potrzeby nowej grupy ds. koordynacji nadzoru systemu informacyjnego Schengen drugiej generacji (SIS II) i przewodniczyliśmy grupom ds. koordynowania nadzoru nad EURODAC, wizowym systemem informacyjnym (VIS) i systemem informacji celnej (CIS).

W dalszym ciągu aktywnie uczestniczyliśmy również w pracach Grupy Roboczej ds. Ochrony Osób Fizycznych w zakresie Przetwarzania Danych Osobowych (Grupa Robocza Art. 29), pełniąc funkcję sprawozdawcy w odniesieniu do działań następczych dotyczących opinii w sprawie uzasadnionych interesów (konsultacje z zainteresowanymi stronami oraz analiza ich uwag) oraz współsprawozdawcy w odniesieniu do opinii i dokumentu roboczego w sprawie inwigilacji komunikacji elektronicznej na potrzeby wywiadu i bezpieczeństwa narodowego

oraz w odniesieniu do dokumentu dotyczącego umowy w sprawie międzynarodowej koordynacji egzekwowania przepisów.

Rozwój technologiczny a ochrona danych

Istotne tematy w 2014 r. obejmowały wpływ szerszego rozprzestrzeniania się połączonych urządzeń mobilnych i dużą liczbę incydentów związanych z naruszeniem bezpieczeństwa. Te i inne zagadnienia technologiczne poruszyliśmy w [biuletynie EIOD](#).

Uwzględnialiśmy również elementy technologiczne w naszych opiniach w sprawie polityki oraz uwagach i decyzjach w dziedzinie nadzoru, a także w wytycznych, np. w wytycznych dotyczących e-komunikacji, które w 2014 r. rozprawdano w celu konsultacji.

W 2014 r. utworzyliśmy informatyczne laboratorium polityki EIOD wyposażone w sprzęt i narzędzia, z którego można korzystać do oceny funkcji ochrony prywatności w produktach lub systemach używanych w dziedzinie naszej pracy dotyczącej nadzoru.

Laboratorium informatyczne jest obecnie gotowe do pracy. Zostanie uzupełnione mobilnym zestawem informatycznym, tak aby można było przeprowadzać pokazy, eksperymenty lub testy techniczne na miejscu w kontekście kontroli i audytów.

Zwróciliśmy również uwagę na ochronę danych i prywatności z technicznego punktu widzenia. W 2014 r. uruchomiliśmy Sieć na rzecz Inżynierii Prywatności w Internecie (ang. Internet Privacy Engineering Network, [IPEN](#)) we współpracy z krajowymi organami ochrony danych, programistami i naukowcami z tego sektora, środowiska akademickiego oraz społeczeństwa obywatelskiego. Celem tej inicjatywy jest opracowywanie praktyk w zakresie inżynierii, w których uwzględnia się obawy związane z prywatnością, i zachęcanie inżynierów do wprowadzania mechanizmów ochrony prywatności do internetowych standardów, usług i aplikacji.

Pierwsze [warsztaty IPEN](#) odbyły się w dniu 26 września 2014 r. w Berlinie i zostały zorganizowane wspólnie przez kilka organów ochrony danych i innych organizacji. Warsztaty dotyczyły praktycznego podejścia do identyfikacji luk w ochronie prywatności w istniejących technologiach i opracowania przydatnych rozwiązań. W 2015 r. sieć będzie rozwijała się i kontynuowała prace w kierunku ustalonym w 2014 r.

Sprawy sądowe

Jeżeli chodzi o działania sądowe, EIOD został dopuszczony w charakterze interwenienta przez Trybunał Sprawiedliwości i złożył pisemne oświadczenie w postępowaniu odwoławczym w sprawie C-615/13 P, wniesionej przez ClientEarth i PAN Europe, która dotyczyła przejrzystości/dostępu do dokumentów.

Informacje i komunikacja

Działania w zakresie informacji i komunikacji odgrywają istotną rolę w poszerzaniu wiedzy o EIOD oraz jego mandacie, zasadach i decyzjach.

W 2014 r. promowaliśmy działania EIOD podczas szeregu wydarzeń, takich jak Dzień Ochrony Danych Osobowych w styczniu, Dzień Otwarty UE w maju i cztery konferencje popołudniowe w Europejskiej Szkole Administracji (EUSA).

W zakresie naszych kompetencji odpowiedzieliśmy na 132 pisemne wnioski obywateli o udzielenie informacji, 38 pisemnych wniosków o udzielenie informacji i 42 prośby prasy o udzielenie wywiadu.

Na koniec 2014 r. mieliśmy 2373 subskrybentów biuletynu EIOD i 2000 osób śledzących EIOD na Twitterze. Liczba odwiedzin strony internetowej EIOD wyniosła 194 637, a w siedzibie EIOD odbyło się siedem wizyt studyjnych. Wszystkie te dane potwierdzają, że w coraz większym stopniu stajemy się punktem odniesienia w kwestiach ochrony danych na poziomie UE.

Budżet i administrowanie zasobami ludzkimi

W 2014 r. budżet przeznaczony na EIOD wyniósł 8 018 796 EUR, co stanowi wzrost o 4,66% w porównaniu z budżetem na 2013 r.

W 2014 r. pozostaliśmy w pełni oddani unijnej polityce oszczędnościowej i konsolidacji budżetu i ściśle trzymaliśmy się kierunku wytyczonego przez Komisję. Niemniej jednak w naszym projekcie budżetu musieliśmy uwzględnić niezbędne środki na spełnienie oficjalnych obowiązków związanych z końcem kadencji pracowników urzędu EIOD.

Wdrożyliśmy politykę oszczędnościową zalecaną przez Komisję poprzez zmniejszenie lub zamrożenie zdecydowanej większości naszych środków na 0% przez trzeci rok i przeprowadzenie znacznych cięć

w kluczowych pozycjach budżetowych, takich jak: tłumaczenia (-17%), publikacje (-25%) i działania instytucji (-17%).

Opóźnienia w procedurze wyboru nowego zespołu inspektorów doprowadziło do wprowadzenia budżetu korygującego na potrzeby zwrotu niewykorzystanych środków związanych z tymczasowym przedłużeniem mandatu do budżetu ogólnego UE w czerwcu 2014 r.

W 2014 r. wskaźnik wykonania naszego budżetu przekroczył planowany poziom 85%.

Rok 2014 był szczególnie udany pod względem zasobów ludzkich. Z jednej strony wejście w życie nowego regulaminu pracowniczego w styczniu 2014 r. wymagało uaktualnienia wielu środków wykonawczych. Pełny pakiet przepisów wykonawczych został przyjęty przed końcem roku.

Z drugiej strony przyjęto również szereg ważnych dokumentów strategicznych, w szczególności nową politykę uczenia się i rozwoju oraz dotyczący jej dokument wykonawczy, dwa projekty pilotażowe oraz dokumenty na temat DNA, stresu i komunikacji wewnętrznej. Ponadto nowy kodeks postępowania dla pracowników EIOD został przyjęty i przedstawiony personelowi.

Najważniejsze liczby dotyczące działalności EIOD w 2014 r.

- Przyjęto 144 opinie dotyczące kontroli wstępnych i 26 innych opinii
- Otrzymano 110 skarg, w tym 39 dopuszczalnych
- Przeprowadzono 48 konsultacji dotyczących środków administracyjnych
- Przeprowadzono 4 kontrole na miejscu i 4 wizyty
- Opublikowano 2 zbiory wytycznych i 1 dokument przedstawiający stanowisko
- Wydano 14 opinii legislacyjnych i 1 opinię wstępną
- Wydano 13 zestawów formalnych uwag
- Wydano 33 zestawy nieformalnych uwag

Strategia na lata 2013–2014

W naszej strategii na lata 2013–2014 zdefiniowaliśmy kilka celów strategicznych, które przyczynią się do zwiększenia wpływu prowadzonych przez nas podstawowych działań na ochronę danych na poziomie europejskim. Aby ocenić postępy, określiliśmy działania odgrywające kluczową rolę w osiągnięciu wyznaczonych przez nas celów. Związane z nimi kluczowe wskaźniki efektywności (KPI) wymienione w tabeli pomogą nam monitorować i dostosować, jeśli okaże się to konieczne, wpływ naszej pracy i skuteczność wykorzystania dostępnych środków.

W niniejszym rozdziale omówiono realizację działań EIOD w 2014 r. zgodnie z celami strategicznymi i planem działania określonymi w strategii na lata 2013–2014. Działania wdrażające plan działania streszczono powyżej, w ogólnym przeglądzie roku 2014.

W ogólnym ujęciu wyniki wskazują na pozytywną tendencję w realizacji naszych celów. Można uznać, że wdrażanie strategii postępuje, i że na tym etapie nie są potrzebne żadne środki naprawcze.

Ponadto przyjęcie strategii na lata 2015–2019 w marcu 2015 r. będzie wymagało oceny KPI, aby uwzględnić cele i priorytety nowej strategii. W rezultacie w celu zapewnienia spójności i trafności KPI może zająć potrzeba poddania przed opublikowaniem jednego lub większej liczby nowych wskaźników wnikliwym konsultacjom wewnętrznym.

Tablica wyników kluczowych wskaźników efektywności (KPI) zawiera krótki opis ich samych oraz metody dokonywania obliczeń.

W większości przypadków pomiar wskaźników odbywa się poprzez porównanie ich do wstępnie wyznaczonych celów. W przypadku trzech wskaźników wyniki uzyskane w 2013 r. stanowią punkt odniesienia na 2014 r.

Kluczowe wskaźniki efektywności służą wdrażaniu następujących celów strategicznych:

1. Promowanie *kultury ochrony danych* w instytucjach i organach UE, tak aby były one świadome swoich obowiązków i odpowiedzialne za zgodność z wymogami w zakresie ochrony danych.
KPI nr 1, 2 i 3. Osiągnięto wszystkie cele.
2. Zapewnienie, aby prawodawca UE (Komisja Europejska, Parlament Europejski i Rada) był świadomy wymogów w zakresie ochrony danych, a ochrona danych była uwzględniona w nowym prawodawstwie.
KPI nr 4 i 5. Cel wyznaczony w odniesieniu do KPI nr 5 został osiągnięty. Wyniki dotyczące KPI nr 4 odpowiadają wynikom za 2013 r. w odniesieniu do uwag formalnych i nieformalnych, natomiast liczba opinii zmalała w 2014 r. Było to z jednej strony spowodowane wyższym poziomem selektywności, a z drugiej strony faktem, że Komisja usunęła lub opóźniła kilka swoich inicjatyw, które zidentyfikowaliśmy (na przykład negocjacje TAXUD z WTO i Rosją).
3. Poprawa współpracy z organami ochrony danych, w szczególności z Grupą Roboczą Art. 29, w celu zapewnienia większej spójności ochrony danych w UE.
Wyniki osiągnięte w 2013 r. określają cel KPI nr 6. Wyniki w 2014 r. były wielkim sukcesem, ponieważ znacznie przekraczały cel. KPI nr 7 odnosi się do celów strategicznych 1, 2 i 3. Cel w dużym stopniu przekroczono.
4. Opracowanie efektywnej strategii komunikacji.
Wyniki osiągnięte w 2013 r. określają cel KPI nr 8. Pod tym względem liczba odwiedzin strony internetowej EIOD zmniejszyła się w 2014 r. Głównym powodem była opóźnione mianowanie nowych inspektorów. Podczas przedłużenia mandatu o rok miało miejsce mniej nowych decyzji lub projektów. Miało to wpływ na zainteresowaniem odwiedzaniem naszej strony internetowej.
5. Zwiększenie wykorzystania zasobów ludzkich, finansowych, technicznych i organizacyjnych EIOD (dzięki odpowiednim procesom, władzy i wiedzy).
KPI nr 9 i 10. Osiągnięto oba cele.

KPI	Opis	Wyniki w 2013 r.	Wyniki w 2014 r.	Cel
KPI 1	Liczba przeprowadzonych kontroli/wizyt. Pomiar: w porównaniu z przyjętym celem	3 wizyty 8 kontroli	4 wizyty 4 kontrole	minimum 8
KPI 2	Liczba inicjatyw szkoleniowych oraz działań służących podnoszeniu świadomości w instytucjach i organach UE, zorganizowanych lub współorganizowanych przez EIOD (warsztaty, spotkania, konferencje, szkolenia i seminaria). Pomiar: w porównaniu z przyjętym celem	4 szkolenia 4 warsztaty (3 we współpracy z ITP)	8 (3 dla EUSA, 1 dla koordynatorów ds. ochrony danych, 2 dla inspektorów ochrony danych, 1 dla EIPA, 1 dla DG COMM)	8 (warsztatów + szkoleń)
KPI 3	Poziom zadowolenia inspektorów ochrony danych/koordynatora ds. ochrony danych ze szkoleń i wytycznych. Pomiar: badanie zadowolenia inspektorów ochrony danych/koordynatorów ds. ochrony danych przeprowadzane po każdym szkoleniu lub publikacji wytycznych	Szkolenie podstawowe dla inspektorów ochrony danych: 70% pozytywnych informacji zwrotnych Szkolenie dla pracowników EDA: 92% pozytywnych informacji zwrotnych	100%	60% pozytywnych informacji zwrotnych
KPI 4	Liczba formalnych i nieformalnych opinii przekazanych ustawodawcy przez EIOD. Pomiar: w porównaniu z poprzednim rokiem	Opinie: 20 Formalne uwagi: 13 Nieformalne uwagi: 33	Opinie: 15 Formalne uwagi: 13 Nieformalne uwagi: 33	Rok 2013 jako punkt odniesienia.
KPI 5	Wskaźnik wdrażania przypadków zawartych w spisie i wymagających podjęcia działań. Pomiar: odsetek „czerwonych” inicjatyw (w których termin przekazania komentarzy minął), wdrożonych zgodnie z planem zawartym w spisie na 2013 r.	90% (18/20)	89%	90%
KPI 6	Liczba przypadków, którymi zajęła się Grupa Robocza Art. 29 przy istotnym udziale EIOD. Pomiar: w porównaniu z poprzednim rokiem	13	27	Rok 2013 jako punkt odniesienia
KPI 7	Liczba przypadków, w których przekazano wskazówki dotyczące rozwoju technologicznego. Pomiar: w porównaniu z przyjętym celem	21	58	20
KPI 8	Liczba odwiedzin strony internetowej EIOD. Pomiar: w porównaniu z poprzednim rokiem	293 029 (+63% w porównaniu z 2012 r.)	194 637	Rok 2013 jako punkt odniesienia
KPI 9	Wskaźnik wykonania budżetu. Pomiar: suma płatności zrealizowanych w ciągu roku podzielona przez roczny budżet.	84,7%	85,8%	85%
KPI 10	Wskaźnik realizacji szkoleń dla personelu EIOD Pomiar: liczba dni szkoleń rzeczywiście przeprowadzonych podzielona przez szacowaną liczbę dni szkoleń	85%	87,4%	80%

NADZÓR I EGZEKWOWANIE PRZEPISÓW

Jednym z najważniejszych zadań EIOD jest niezależny nadzór nad przeprowadzanymi przez instytucje lub organy europejskie operacjami przetwarzania danych. Ramy prawne określone są w rozporządzeniu (WE) nr 45/2001 o ochronie danych, w którym ustanowiono szereg obowiązków spoczywających na podmiotach przetwarzających dane oraz prawa podmiotów, których dane osobowe są przetwarzane.

Zakres zadań nadzorczych sięga od doradzania inspektorom ochrony danych i wspierania ich poprzez kontrolę wstępną ryzykownych operacji przetwarzania danych po przeprowadzanie dochodzeń, w tym kontroli na miejscu i rozpatrywanie skarg. Doradztwo dla organów administracji UE może również przybrać formę konsultacji w zakresie środków administracyjnych lub publikacji tematycznych wytycznych.

Nasz cel strategiczny

Promowanie „kultury ochrony danych” w instytucjach i organach UE, tak aby były one świadome swoich obowiązków i odpowiedzialne za zgodność z wymogami w zakresie ochrony danych

Inspektorzy ochrony danych

W 2014 r. otrzymaliśmy powiadomienia o mianowaniu 9 nowych inspektorów ochrony danych w instytucjach UE.

Wzięliśmy udział w spotkaniach inspektorów ochrony danych, które odbyły się w Brukseli w czerwcu (gospodarzem był Parlament Europejski i Komisja Europejska) oraz w Salonikach (gospodarzem było Europejskie Centrum Rozwoju Kształcenia Zawodowego, Cedefop) w listopadzie.

Na spotkaniu czerwcowym przedstawiliśmy aktualne informacje na temat unijnej reformy prawodawstwa w zakresie ochrony danych i na temat odpowiedniego orzecznictwa w tej dziedzinie. Spotkanie to było dla nas również sposobnością do przedstawienia naszych wytycznych dotyczących

praw osób, których dane dotyczą. Wywołały one szczegółową dyskusję na temat sposobów zajęcia się takimi wnioskami w praktyce.

Spotkanie w Cedefop było okazją do refleksji nad mandatem nowego EIOD i rolą inspektorów ochrony danych na scenie międzynarodowej. Zaprezentowaliśmy również nasze stanowisko w sprawie przekazywania danych, które zostało przyjęte w lipcu 2014 r., oraz nasze wytyczne dotyczące konfliktów interesów. Oba dokumenty doprowadziły do interesujących dyskusji. Dobrze przyjęte zostały również nasze aktualne informacje na temat kwestii bezpieczeństwa i technologii ze szczególnym uwzględnieniem doświadczeń EIOD w zakresie korzystania z chmury i postępowania w przypadku naruszenia bezpieczeństwa. Zaprezentowaliśmy także kilka godnych uwagi kwestii, którymi zajmowaliśmy się w ramach nadzoru i egzekwowania przepisów, takich jak procedura konsultacji w CCA (Collège des Chefs d'administration), zaangażowanie inspektorów ochrony danych w rozpatrywanie skarg oraz znaczenie dokumentowania odroczenia praw zgodnie z art. 20 rozporządzenia.

W czerwcu 2014 r. zorganizowaliśmy szkolenie, a następnie spotkanie dla inspektorów ochrony danych. Ponadto odbyły się indywidualne sesje pracowników EIOD i niektórych inspektorów ochrony danych dotyczące ich konkretnych potrzeb w zakresie wskazówek. Wizyty doradcze służyły także zaspokojeniu szczególnych potrzeb inspektorów ochrony danych.

W odpowiedzi na rosnącą liczbę otrzymywanych zapytań telefonicznych utworzyliśmy infolinię dla inspektorów ochrony danych, która jest czynna w określonym czasie w tygodniu. Obsługuje ją pracownik EIOD. Infolinia pozwala nam udzielać konkretnych wskazówek w odpowiedzi na proste pytania inspektorów ochrony danych w szybki i nieformalny sposób. Wzmacnia dobrą współpracę i komunikację między EIOD a inspektorami ochrony danych w instytucjach UE. W 2014 r. infolinia obsługiwała średnio około 4 połączeń miesięcznie.

Kontrole wstępne

Duża liczba (80% w 2014 r.) zgłoszonych nam ryzykownych operacji przetwarzania danych związana była z procedurami administracyjnymi wspólnymi dla wszystkich instytucji i organów UE, takimi jak rekrutacja pracowników, ich roczna ocena lub postępowania administracyjne.

Ponieważ w latach 2013 i 2014 otrzymaliśmy znaczną liczbę powiadomień, a w odniesieniu do jeszcze większej liczby zaleceń musimy przeprowadzić działania następcze, opracowaliśmy kryteria, które pomogą nam bardziej selektywnie wybierać zalecenia, których wdrożenie powinniśmy skontrolować. Ta selektywność umożliwi nam skoncentrowanie wysiłków na zarządzaniu ryzykownymi operacjami przetwarzania. Innych naszych zaleceń przestrzegają inspektorzy ochrony danych konkretnego organu lub instytucji, zgodnie z zasadą odpowiedzialności.

Kontrole wstępne stanowią sposób systematycznego uzyskiwania wiedzy o działalności instytucji i organów UE oraz umożliwiają EIOD zrozumienie wzorców lub niedociągnięć we wdrażaniu zasad ochrony danych. Kontrole wstępne stanowią dla nas matrycę wiedzy. Duża liczba wydanych opinii pomaga opracować inne narzędzia nadzoru, takie jak: kontrole, badania, zapytania, wizyty dotyczące zgodności i wizyty konsultacyjne.

W 2014 r. otrzymaliśmy 80 powiadomień dotyczących wstępnych kontroli, przy czym jedno później wycofano. Poczyniono postępy w likwidowaniu zaległości związanych z powiadomieniami *ex post* otrzymanymi w 2013 r.

W 2014 r. wydaliśmy 144 opinie dotyczące kontroli wstępnych (wzrost o około 58% w stosunku do 2013 r.) i 26 opinii w sprawie innych kontroli (wzrost o 24% w porównaniu z 2013 r.)¹. Ogółem zbadaliśmy 185 powiadomień, z czego niektóre doprowadziły do wydania opinii wspólnych. Zbadano różne kwestie, przy czym niektóre z nich omówiono w pełnej wersji niniejszego sprawozdania.

¹ W przypadku gdy EIOD otrzymuje powiadomienie, lecz operacja przetwarzania nie wchodzi w zakres stosowania art. 27, EIOD może pomimo tego wydać zalecenia.

Skargi

Zgodnie z rozporządzeniem (WE) nr 45/2001 EIOD w ramach swoich podstawowych obowiązków „wysłuchuje i bada skargi” oraz „przeprowadza dochodzenia zarówno z własnej inicjatywy, jak i na podstawie skarg” (art. 46).

W 2014 r. EIOD otrzymał 110 skarg, co stanowi wzrost o około 41% w porównaniu z 2013 r. Spośród nich 72 stanowiły skargi niedopuszczalne, przy czym większość odnosiła się do przetwarzania danych na poziomie krajowym, a nie do ich przetwarzania przez instytucję lub organ UE.

Pozostałe 39 skarg wymagało dogłębnego dochodzenia (wzrost o około 30% w porównaniu z 2013 r.). Ponadto 18 dopuszczalnych skarg wniesionych w poprzednich latach (trzy w 2011 r., trzy w 2012 r. i 12 w 2013 r.) nadal było przedmiotem dochodzenia, przeglądu lub działań następczych w dniu 31 grudnia 2014 r.

Monitorowanie przestrzegania przepisów

EIOD odpowiada za monitorowanie i zapewnienie stosowania rozporządzenia (WE) nr 45/2001. Monitorowanie prowadzone jest na kilka sposobów: poprzez okresowe badania ogólne odbywające się co pół roku lub bardziej ukierunkowane formy monitorowania, jak wizyty lub kontrole.

Niedawno wprowadziliśmy nowy rodzaj wizyty na miejscu, nazywany **wizytą konsultacyjną**. W związku z tym dwóch pracowników EIOD mianowano na stanowisko konsultantów na miejscu. Ten rodzaj wizyty stanowi praktyczne narzędzie rozwiązywania określonych problemów, podnoszenia poziomu wiedzy, poprawy współpracy i zwiększania odpowiedzialności danego organu. W jednym przypadku po wizycie konsultacyjnej zastosowaliśmy działania następcze w postaci **oddelegowania** pracownika EIOD na krótki okres.

Od stycznia do grudnia 2014 r. przeprowadziliśmy wizyty w czterech agencjach UE: Europejskim Funduszu Inwestycyjnym, Centrum Satelitarnym UE, Organie Nadzoru Europejskiego GNSS i Instytucie Unii Europejskiej Studiów nad Bezpieczeństwem.

W 2014 r. EIOD kontynuował działania następcze w odniesieniu do wcześniejszych kontroli. Ponadto przeprowadziliśmy kontrole w agencji Frontex i Parlamencie Europejskim, a także ukierunkowaną

kontrolę danych dotyczących zdrowia w Komisji Europejskiej i Radzie.

Konsultacje w sprawie środków administracyjnych

EIOD wydaje opinie w kwestiach ochrony danych na wniosek instytucji UE albo własnej inicjatywy. EIOD może wydać opinię na temat decyzji lub dowolnego innego aktu administracyjnego **o zasięgu ogólnym** związanego z przetwarzaniem danych osobowych prowadzonym przez daną instytucję UE (art. 28 ust. 1). EIOD może również doradzać w kwestiach dotyczących **konkretnych działań związanych z przetwarzaniem danych lub odpowiadać na pytania** o wykładnię przepisów rozporządzenia (art. 46 lit. d)).

Do zarządzania konsultacjami stosuje się zasadę **odpowiedzialności**. Instytucje UE powinny w pierwszej kolejności zwrócić się o wewnętrzną poradę do swojego inspektora ochrony danych i dlatego włączają swojego inspektora ochrony danych w opracowywanie środków wpływających na prawo do ochrony danych. Jeżeli inspektor ochrony danych nie może zapewnić odpowiedniego rozwiązania, można skonsultować się z EIOD. Konsultacje muszą odnosić się do **nowych** lub **złożonych kwestii** (brak precedensów w tej dziedzinie, brak doktryny lub brak przejrzystości w definicji określonych pojęć w rozporządzeniu).

W 2014 r. miało miejsce 48 konsultacji dotyczących środków administracyjnych. Zbadano różne kwestie, przy czym niektóre z nich omówiono w pełnej wersji niniejszego sprawozdania.

Wytyczne dotyczące ochrony danych

W lutym 2014 r. opublikowaliśmy **wytyczne dotyczące praw osób w odniesieniu do przetwarzania danych osobowych**.

Treść wytycznych opiera się na stanowisku EIOD w dziedzinie praw osób, których dane dotyczą, przedstawionym w szeregu opinii EIOD w sprawie operacji przetwarzania danych w UE. W wytycznych opisano nasze stanowisko i zalecenia dotyczące określonych zasad zawartych w rozporządzeniu (WE) nr 45/2001 oraz uwzględniono informacje na temat obecnych najlepszych praktyk oraz innych istotnych kwestii. Na przykład podkreślono w nich szeroko rozumiane pojęcie danych osobowych

w rozporządzeniu, zgodnie z którym dane osobowe odnoszą się do znacznie większej ilości danych niż tylko imię i nazwisko określonej osoby fizycznej.

W dniu 14 lipca 2014 r. przyjęliśmy **dokument przedstawiający stanowisko w sprawie przekazywania danych**, który ma stanowić wytyczne dla instytucji i organów UE odnośnie do sposobu interpretowania i stosowania zasad określonych w rozporządzeniu (WE) nr 45/2001 przy przekazywaniu danych osobowych na poziomie międzynarodowym.

Nasze wytyczne dotyczą głównie metodologicznej analizy, którą instytucje i organy UE muszą przeprowadzić przed przekazaniem danych osobowych państwom trzecim lub organizacjom międzynarodowym.

Wytyczne mają ułatwić pracę administratorom danych i inspektorom ochrony danych stosującym te przepisy. Zawierają także listę kontrolną, w której wyszczególniono krokami, według których trzeba postępować podczas stosowania art. 9 rozporządzenia (WE) nr 45/2001. W dokumencie tym znajdują się również ważne informacje na temat funkcji nadzoru i egzekwowania przepisów pełnionych przez EIOD w kontekście przekazywania danych.

W grudniu 2014 r. opublikowaliśmy **wytyczne dotyczące gromadzenia, przetwarzania i publikowania danych osobowych w odniesieniu do deklaracji związanych z zarządzaniem konfliktami interesów w instytucjach i organach UE**. Wytyczne te zapewniają instytucjom i organom UE praktyczne wskazówki na temat poszanowania zasad ochrony danych i równowagi między interesem publicznym związanym z przejrzystością a prawami osób fizycznych do prywatności i ochrony danych. Dążenie do tej równowagi może wzmocnić wysiłki instytucji w zakresie zdobywania zaufania społeczeństwa, jak również osób, które dla nich pracują.

W ramach zwiększania odpowiedzialności instytucji UE chętnie zapewniamy **szkolenia i wytyczne** przeznaczone dla inspektorów ochrony danych, koordynatorów ds. ochrony danych i administratorów danych, aby lepiej rozumieć zasady ochrony danych i swoje ewentualne obowiązki.

W dniu 28 stycznia 2014 r., w unijnym Dniu Ochrony Danych Osobowych, uczestniczyliśmy w posiedzeniu koordynatorów ds. ochrony danych

w Komisji Europejskiej, podczas którego EIOD wygłosił przemówienie na temat rozporządzenia (WE) nr 45/2001 w świetle obecnej reformy ogólnych ram ochrony danych. Była to okazja do refleksji z koordynatorami ds. ochrony danych nad specyfiką tego rozporządzenia jako instrumentu służby publicznej UE oraz możliwych usprawnień, które byłyby z zadowoleniem przyjęte przy okazji rewizji tego instrumentu.

W dniu 13 czerwca 2014 r. zorganizowaliśmy ogólne szkolenie dla inspektorów ochrony danych z instytucji i organów UE, które dotyczyło wypełniania formularza powiadomienia.

Na życzenie przeprowadziliśmy również specjalne sesje szkoleniowe dla pracowników niektórych

agencji (Frontex) lub ich inspektorów ochrony danych (ECDC, IUESB, EFI) oraz szkolenie dla stażystów z Rady, Komitetu Regionów oraz Komitetu Ekonomiczno-Społecznego.

W czerwcu i grudniu 2014 r. przedstawiliśmy prezentację na kursach szkoleniowych zorganizowanych przez Europejski Instytut Administracji Publicznej (EIPA) w Maastricht, w których udział wzięli inspektorzy ochrony danych, koordynatorzy do ochrony danych i administratorzy danych. Mówiliśmy o specyfice rozporządzenia (WE) nr 45/2001, roli EIOD w kontekście nadzoru i egzekwowania przepisów, a także przedstawiliśmy dwa studia przypadków – dotyczące międzynarodowego przekazywania danych osobowych oraz prawa dostępu w kontekście skargi.

POLITYKA I KONSULTACJE

EIOD udziela instytucjom i organom Unii Europejskiej porad dotyczących kwestii ochrony danych w różnych dziedzinach polityki. Ta rola konsultacyjna ma zastosowanie do wniosków dotyczących nowych aktów prawnych oraz innych inicjatyw, które mogą mieć wpływ na ochronę danych osobowych w UE. Konsultacje mają zazwyczaj postać formalnej opinii, ale EIOD może również udzielać wskazówek w formie uwag lub dokumentów strategicznych.

Nasz cel strategiczny

Zapewnienie, aby prawodawca UE (Komisja Europejska, Parlament Europejski i Rada) był świadomy wymogów w zakresie ochrony danych i uwzględniał ochronę danych w nowym prawodawstwie

Priorytety na 2014 r.

Jeżeli chodzi o konkretne inicjatywy, w naszym spisie na 2014 r. przewidziano pięć obszarów o strategicznym znaczeniu dla ochrony danych. Poniżej streszczono nasze działania w tych obszarach (bardziej szczegółowo omówiono je w pełnej wersji sprawozdania).

- W kierunku nowych ram prawnych w zakresie ochrony danych
- Odbudowa zaufania do globalnego przepływu danych w następstwie PRISM
- Inicjatywy stymulujące wzrost gospodarczy i wspierające agendę cyfrową
- Dalszy rozwój przestrzeni wolności, bezpieczeństwa i sprawiedliwości
- Reforma sektora finansowego.

W kierunku nowych ram prawnych w zakresie ochrony danych: koniec jest w zasięgu wzroku?

Reforma ram ochrony danych stanowiła jedno z największych i najbardziej skomplikowanych wyzwań dla prawodawców UE w ostatnich latach. Na szczeblu krajowym, europejskim i międzynarodowym panuje duże zainteresowanie ewolucją obu projektów wniosków – dotyczących ogólnego rozporządzenia o ochronie danych oraz dyrektywy w sprawie danych osobowych przetwarzanych do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania albo wykonywania kar kryminalnych. EIOD nadal ściśle współpracował z Parlamentem, Radą i Komisją podczas krytycznych negocjacji, które miały miejsce w 2014 r.

Odbudowa zaufania do globalnego przepływu danych w następstwie PRISM

Masowy nadzór nad obywatelami UE ze strony agencji wywiadu i organów ścigania, ujawniony w 2013 r., stanowił wyraźne naruszenie praw osób fizycznych do prywatności i ochrony danych osobowych. EIOD poruszył ten temat podczas otwartego posiedzenia Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych Parlamentu Europejskiego w październiku 2013 r., podkreślając poważne obawy i potrzebę sprawowania przez UE kontroli nad naszą prywatnością. Sformułowaliśmy to przesłanie w naszej opinii z dnia 20 lutego 2014 r. w sprawie komunikatu Komisji do Parlamentu Europejskiego i Rady pt. „Odbudowa zaufania do przepływów danych między Unią Europejską a Stanami Zjednoczonymi”. Wyraziliśmy poparcie dla amerykańskiej ustawy o prywatności i wezwaliśmy do promowania międzynarodowych standardów prywatności przy jednoczesnym przyjęciu reform unijnych ram ochrony danych.

Inicjatywy stymulujące wzrost gospodarczy i wspierające agendę cyfrową

EIOD konstruktywnie uczestniczył w wielu różnych projektach politycznych w tak różnych obszarach, jak: konkurencyjność i ochrona konsumenta, zarządzanie internetem, funkcjonowanie rynku wewnętrznego, jednolity rynek treści cyfrowych oraz cła i rolnictwo. Uważnie monitorowaliśmy również wydarzenia związane z porozumieniem w sprawie zasad bezpiecznego transferu danych osobowych oraz negocjacje Komisji w sprawie nowych porozumień handlowych (np. TTIP, TISA) pod kątem ich potencjalnego wpływu na prywatność i ochronę danych.

Dalszy rozwój przestrzeni wolności, bezpieczeństwa i sprawiedliwości

W 2014 r. oprócz rozważenia szeregu konkretnych inicjatyw, takich jak dotyczące przyszłości

Europolu, Eurojustu i utworzenia Prokuratury Europejskiej, kontroli broni i zamrożenia aktywów, UE dokonała oceny swoich postępów na drodze do stworzenia przestrzeni wolności, bezpieczeństwa i sprawiedliwości. Nadal braliśmy czynny udział w kształtowaniu tego szeroko zakrojonego programu.

Reforma sektora finansowego

EIOD pogłębiał swoją wiedzę ekspercką na temat stosowania norm ochrony danych osobowych przy opracowywaniu i wdrażaniu regulacji usług finansowych. Wydaliśmy pierwszy zestaw wytycznych dotyczących tego sektora oraz udzielaliśmy porad na temat konkretnych proponowanych środków w dziedzinie praw udziałowców, odporności systemu bankowego i przejrzystości transakcji finansowania papierów wartościowych.

WSPÓŁPRACA

EIOD współpracuje z innymi organami ochrony danych w celu wspierania jednolitej ochrony danych w całej Europie. Ta rola polegająca na współpracy obejmuje również współpracę z organami nadzorczymi ustanowionymi w ramach dawnego „trzeciego filaru” UE i w kontekście wielkoskalowych systemów informatycznych.

Nasz cel strategiczny

Poprawa współpracy z organami ochrony danych, w szczególności z Grupą Roboczą Art. 29, w celu zapewnienia większej spójności ochrony danych w UE

W 2014 r. nadal czynnie włączaliśmy się w działania **Grupy Roboczej Art. 29** w celu zapewnienia większej spójności ochrony danych w UE.

Jako członek tej grupy EIOD uczestniczy w jej działaniach, biorąc na siebie część pracy porównywalną do tej, jaką wykonują większe organy ochrony danych. Udział ten jest jednak oparty na podejściu selektywnym i skupieniu się na tych obszarach, w których wkład EIOD będzie stanowił wartość dodaną, szczególnie poprzez uwzględnienie perspektywy UE, jak na przykład w opiniach Grupy Roboczej Art. 29 w sprawie uzasadnionych interesów otwartych danych. Jesteśmy również bardzo zaangażowani w formułowanie opinii w sprawie urządzeń do identyfikacji daktyloskopijnej, dronów i internetu przedmiotów.

Bezpośrednia współpraca z organami krajowymi jest coraz ważniejszym obszarem w kontekście powstawania wielkich międzynarodowych systemów, takich jak: Eurodac, wizowy system informacyjny (VIS), system informacyjny Schengen drugiej generacji (SIS II) lub system informacji celnej (CIS), które wymagają skoordynowanego podejścia do nadzoru. Ta współpraca ma charakter uzupełniający naszą pracę w dziedzinie nadzoru w tym obszarze (zob. rozdział 2). W 2014 r., podobnie jak w 2013 r., zapewniliśmy sekretariat na potrzeby nowej grupy ds. koordynacji nadzoru SIS II i przewodniczyliśmy grupom ds. koordynowania nadzoru nad EURODAC, VIS i CIS. Nasza rola obejmowała:

- odpowiednie planowanie szybkiego przydzielenia zasobów finansowych i ludzkich;
- koordynowanie posiedzeń grup;

- opracowywanie i rozpowszechnianie stosownych dokumentów;
- utrzymywanie kontaktów z członkami grup między spotkaniami w celu przygotowania działań.

W dniu 5 czerwca 2014 r. EIOD uczestniczył w **Europejskiej Konferencji Organów Ochrony Danych** w Strasburgu, zorganizowanej wspólnie przez Radę Europy i francuską Commission Nationale de l' Informatique et des Libertés (CNIL).

W trakcie konferencji w 2014 r. skupiono się na sposobach osiągnięcia lepszej współpracy organów ochrony danych w kontekście globalizacji. Przyjęto rezolucję, w której wezwano Radę Europy, aby – w ramach jej obrad nad unowocześnieniem Konwencji nr 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych – wzmocniła ochronę praw osób fizycznych, w szczególności poprzez ustanowienie niezależnych organów nadzoru, które są w stanie efektywnie egzekwować prawo i współpracować ze sobą.

W 2014 r. **konferencję międzynarodową** zorganizował urząd ochrony danych Mauritiusa; odbyła się w dniach 12–16 października.

W programie konferencji znalazło się kilka tematów, w tym prywatność i ochrona danych w rozwijającym się świecie; punkt kompleksowej obsługi: centralizacja a bliskość; nadzór a kontrola danych; prywatność w epoce cyfrowej – rezolucja zgromadzenia ogólnego ONZ; e-zdrowie a ochrona danych; etyka, prawa podstawowe i duże zbiory danych; oraz neutralność sieci a ochrona danych. EIOD wziął udział w warsztatach poświęconych odpowiedzialności oraz w panelu dotyczącym „prywatności bez ograniczeń terytorialnych”, a dyrektor EIOD w trakcie panelu wygłosił prelekcję na temat neutralności sieci.

Istotnym osiągnięciem tej konferencji było przyjęcie na zamkniętej sesji organów ochrony danych (w dniach 13–14 października) **porozumienia i uchwały w sprawie międzynarodowej współpracy organów egzekwowania**. Projekt ten był przedmiotem wieloletnich dyskusji, a EIOD był bardzo zaangażowany we wspieranie negocjacji. Szybki rozwój takich technologii, jak przetwarzanie

w chmurze, duże zbiory danych i internet przedmiotów, uwydatnił potrzebę zapewnienia ram umożliwiających organom ochrony danych współpracę transgraniczną.

Na zamkniętej sesji EIOD przedstawił również krótką prezentację na temat [inicjatywy IPEN](#), która spotkała się z dużym zainteresowaniem.

Nadal braliśmy również udział w najważniejszych posiedzeniach lub komentowaliśmy istotne dokumenty omawiane w Radzie Europy (komitety konsultacyjne Konwencji nr 108 o ochronie osób w związku z automatycznym przetwarzaniem danych

osobowych i Konwencji o cyberprzestępczości), OECD, APEC, GPEN, francuskojęzycznym stowarzyszeniu organów ochrony danych osobowych (AFAPDP), iberoamerykańskiej sieci ochrony danych, Międzynarodowej Grupie Roboczej ds. Ochrony Danych w Telekomunikacji (Grupa Berlińska) oraz międzynarodowej konferencji rzeczników ochrony danych i prywatności.

Staramy się również – o ile to konieczne i możliwe – monitorować rozwój ochrony danych w państwach nienależących do UE oraz politykę prywatności w organizacjach międzynarodowych, takich jak UNHCR, oraz udzielać porad i uwag w tym zakresie.

SPRAWY SĄDOWE

Prawo EIOD do interweniowania w postępowaniach przed sądem zostało uznane przez Trybunał Sprawiedliwości Unii Europejskiej w sprawach PNR (sprawy C-317/04 i C-318/04, orzeczenia z dnia 17 marca 2005 r.). Trybunał oparł prawo do interwencji na art. 41 ust. 2 akapit drugi rozporządzenia (WE) nr 45/2001, zgodnie z którym EIOD jest odpowiedzialny „za doradzanie instytucjom i organom wspólnotowym i podmiotom danych we wszystkich kwestiach związanych z przetwarzaniem danych osobowych”. Doradzanie obejmuje nie tylko przetwarzanie danych osobowych przez te instytucje lub organy. Trybunał zinterpretował uprawnienia przyznane EIOD na mocy art. 47 rozporządzenia w świetle celów art. 41.

W 2014 r. EIOD interweniował w kilku sprawach:

- T-115/13 Dennekamp przeciwko Parlamentowi (przejrzystość/dostęp do dokumentów)
- T-343/13 CN przeciwko Parlamentowi (publikacja szczególnie chronionych danych osobowych na stronie internetowej)
- C-615/13 P ClientEarth/PAN Europe (interpretacja pojęcia danych osobowych w kontekście przejrzystości/dostępu do dokumentów i zgodność z art. 8 lit. b) rozporządzenia (WE) nr 45/2001, a także różnica pomiędzy prawem podstawowym do prywatności a prawem podstawowym do ochrony danych osobowych)

Na mocy rozporządzenia (WE) nr 45/2001 sprawę przeciwko EIOD można wnieść do Trybunału Sprawiedliwości Unii Europejskiej (art. 32). Na przykład od decyzji EIOD w sprawie skargi (zob. rozdział 2) można odwołać się do Trybunału Sprawiedliwości Unii Europejskiej. Jak dotąd trzech skarżący wnieśli sprawy. Wszystkie trzy skargi zostały odrzucone.

DOSTĘP DO DOKUMENTÓW/ PRZEJRZYSTOŚĆ

Jako instytucja UE i zgodnie ze swoim regulaminem wewnętrznym EIOD podlega również rozporządzeniu z 2001 r. w sprawie publicznego dostępu do dokumentów. Liczba wniosków o publiczny dostęp do dokumentów przechowywanych przez EIOD w ostatnich latach stopniowo rosła. Liczba ta podwoiła się w 2013 r. z 12 do 24 wniosków. W 2014 r. zajmowaliśmy się 18 wnioskami, z czego 4 stanowiły ponowne wnioski dotyczące naszych wstępnych odpowiedzi.

Rosnąca liczba przypadków w tym obszarze wskazuje na potrzebę opracowania bardziej

szczegółowych wytycznych dotyczących praktycznego wdrożenia rozporządzenia w sprawie publicznego dostępu do dokumentów. Obecnie pracujemy nad skonsolidowaniem metodyki udzielania odpowiedzi w oparciu o najnowszą praktykę. W 2015 r. będziemy udzielać instytucjom i organom UE praktycznych porad dotyczących sposobu zrównoważenia przejrzystości i potrzeby ochrony danych osobowych w świetle orzeczenia Trybunału Sprawiedliwości w sprawie Bavarian Lager.

TECHNOLOGIA MONITOROWANIA

W 2014 r. kontynuowaliśmy ocenianie ryzyka dla prywatności wynikającego z nowych technologii, gromadząc i analizując informacje w stosownych przypadkach. Udzielaliśmy również administratorom danych wskazówek w różnej postaci dotyczących technicznych aspektów zgodności z zasadami ochrony danych. Niektóre z tych działań pokrótce opisano w niniejszym dokumencie, lecz więcej informacji można znaleźć w pełnej wersji niniejszego sprawozdania, jak również w [biuletynach](#) EIOD.

Coraz więcej urządzeń (na przykład do noszenia na ciele lub montowanych w samochodach) wyposażonych jest w interfejsy umożliwiające przesyłanie danych, które gromadzą.

Istnieją obawy, że zabezpieczenia mogą być niewystarczające przy rosnącej ilości gromadzonych i przesyłanych danych osobowych. Rośnie również liczba wykrytych poważnych luk w zabezpieczeniach powszechnie stosowanych systemów: w 2014 r. wykryto, że jedne z najpopularniejszych urządzeń mobilnych były podatne na przechwytywanie pozornie zaszyfrowanych wiadomości. Okazało się również, że fragment kodu wykryty w wielu systemach Linux miał lukę umożliwiającą atakującym obejście zabezpieczeń. Wykryto również lukę w systemach operacyjnych w smartfonach – procesor odpowiedzialny za komunikację w sieci mógł obchodzić wszystkie ograniczenia chroniące „inteligentną” część telefonu, a tym samym uzyskać dostęp do wszystkich informacji przechowywanych w smartfonie.

W 2014 r. szereg luk w zabezpieczeniach powszechnie wykorzystywanych systemów wzbudził duże zainteresowanie. Niektórym z tych luk nadano nazwy, np. Heartbleed, Gotofail i Poodle. Błąd Heartbleed² został wykryty w OpenSSL, popularnym narzędziu szyfrującym w komunikacji internetowej. Heartbleed umożliwia przeglądanie danych, które powinny być chronione, i daje dostęp do nich.

Wiele popularnych usług internetowych wydawało się zagrożonych, a ich autorzy najwyraźniej zastosowali niezbędne środki, aby szybko

naprawić ten błąd w swoich systemach. Instytucje europejskie również zabezpieczyły swoje usługi. Użytkownikom zagrożonych usług zalecono zmienić hasła i zmieniono certyfikaty wykorzystywane do szyfrowania ruchu internetowego między stronami internetowymi dotkniętymi tym problemem. Pomimo podjęcia tych wszystkich środków możliwe jest, że istnieją serwery, które nie zostały jeszcze zaktualizowane, a tym samym nadal korzystają z oprogramowania zawierającego luki.

W 2014 r. utworzono informatyczne laboratorium EIOD wyposażone w sprzęt i narzędzia. Można z niego korzystać do oceny funkcji ochrony prywatności w produktach lub systemach używanych w dziedzinie naszej pracy dotyczącej nadzoru.

Laboratorium informatyczne jest obecnie gotowe do pracy. Zostanie uzupełnione mobilnym zestawem informatycznym, tak aby można było przeprowadzać pokazy, eksperymenty lub testy techniczne na miejscu w kontekście kontroli i audytów.

W 2014 r. uruchomiliśmy Sieć na rzecz Inżynierii Prywatności w Internecie (ang. Internet Privacy Engineering Network, [IPEN](#)) we współpracy z krajowymi organami ochrony danych, programistami i naukowcami z sektora przemysłu, środowiska akademickiego oraz społeczeństwa obywatelskiego. Celem tej inicjatywy jest opracowywanie praktyk w zakresie inżynierii, w których uwzględnia się obawy związane z prywatnością, i zachęcanie inżynierów do wprowadzania mechanizmów ochrony prywatności do internetowych standardów, usług i aplikacji.

Pierwsze [warsztaty](#) IPEN, które odbyły się w dniu 26 września 2014 r. w Berlinie, dotyczyły praktycznego podejścia do identyfikacji luk w ochronie prywatności w istniejących technologiach i opracowania przydatnych rozwiązań.

Po sukcesie pierwszych warsztatów inicjatywa IPEN obecnie skupia się na opracowaniu i realizacji zidentyfikowanych projektów. IPEN nadal będzie szukać sposobów opracowania technologii przyjaznych dla prywatności i zapewnienia, aby

prywatność stała się kluczowym czynnikiem dla wszystkich programistów.

W listopadzie 2014 r. na posiedzeniu grupy roboczej ds. zarządzania i prywatności przy Komisji Europejskiej zaprezentowaliśmy przegląd mających zastosowanie unijnych ram ochrony danych oraz istotnych elementów reformy, zgodnie z celem dotyczącym udzielania porad prawodawcy UE. Podczas posiedzenia odbyły się dyskusje na temat wdrażania współpracujących inteligentnych systemów transportowych (C-ITS). Aspekty prywatności są bardzo ważne przy wdrażaniu C-ITS, ponieważ dane mogą być wykorzystywane do profilowania lub śledzenia. Będziemy nadal monitorować tę inicjatywę w 2015 r.

Aby wykorzystać nasze możliwości w zakresie udzielania administratorom danych porad dotyczących technicznych środków efektywnego wdrażania ochrony danych w systemach informatycznych, pracowaliśmy nad wytycznymi odnośnie do określonych obszarów technologii informatycznych. Wytyczne te będą dostępne w 2015 r.

W 2012 r. zostaliśmy poinformowani o systematycznym blokowaniu przez strony UE dostępu z [sieci Tor](#). Chociaż jako uzasadnienie dla tego restrykcyjnego środka przytaczano obawy o bezpieczeństwo sieci, zaznaczyliśmy, że w ramach regulacyjnych UE wyraźnie uznaje się anonimową komunikację oraz że trzeba będzie

właściwie ocenić konieczność i proporcjonalność tego środka. W rezultacie doszło do zmiany polityki bezpieczeństwa i sieć Tor nie jest już systematycznie blokowana, z korzyścią dla obywateli państw UE i nienależących do UE, którzy chcą lub muszą chronić swoją prywatność w kontekście przeglądania stron internetowych.

Nasza wiedza ekspercka w obszarze technologii i polityki IT odgrywa cenną rolę w wykonywaniu przez EIOD zadań w zakresie współpracy z innymi organami ochrony danych. W 2014 r. uczestniczyliśmy w szeregu posiedzeń grup roboczych, grup zadaniowych lub podgrup. Odwiedziliśmy również siedzibę eu-LISA – Europejskiej Agencji ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości – w Tallinie, aby podnieść poziom wiedzy na temat kwestii związanych z ochroną danych i rozpocząć dyskusje na temat technologii informacyjnych i zarządzania bezpieczeństwem systemów informatycznych. Odbyło się to niezależnie od kontroli, którą rozpoczęliśmy w siedzibie eu-LISA w Strasburgu pod koniec 2014 r. w celu skontrolowania bezpieczeństwa systemu i zarządzania operacyjnym systemem.

Włączyliśmy się między innymi również w wysiłki Komisji w dziedzinie inteligentnych liczników i sieci oraz w opracowanie przez nią podejścia do korzystania z przetwarzania w chmurze w administracji publicznej.

GŁÓWNE CELE NA ROK 2015

Na rok 2015 określono główne cele wymienione poniżej w ramach ogólnej strategii na lata 2015–2019. Sprawozdania z osiągniętych wyników zostaną przedstawione w 2016 r.

Nadzór i egzekwowanie przepisów

W 2015 r. nadal będziemy promować odpowiedzialność organów UE przy przetwarzaniu danych osobowych.

- **Biblioteka doświadczeń**
Wykorzystując nasze dziesięcioletnie doświadczenie w stosowaniu rozporządzenia (WE) nr 45/2001 opracujemy wewnętrzne repozytorium naszego orzecznictwa, aby zapewnić skatalogowanie naszej wartościowej wiedzy eksperckiej;
- **Rozporządzenie (WE) nr 45/2001**
W oparciu o to solidne doświadczenie będziemy pracować z Parlamentem Europejskim, Radą i Komisją w celu dopilnowania, aby istniejące zasady ustanowione w rozporządzeniu (WE) nr 45/2001 zostały dostosowane do ogólnego rozporządzenia o ochronie danych.
- **Szkolenia i interakcje**
Nadal będziemy szkolić organy UE w zakresie najlepszego poszanowania zasad ochrony danych w praktyce i udzielać im porad, skupiając nasze wysiłki na tych rodzajach przetwarzania, które stwarzają duże ryzyko dla osób fizycznych. Będziemy utrzymywać ścisłą współpracę z organami UE, oferując im stosowną wiedzę i porady, co z kolei pomoże nam zwiększyć naszą wiedzę praktyczną o ich realiach.
- **Inspektorzy ochrony danych**
W ścisłej współpracy z inspektorami ochrony danych nadal będziemy wspierać instytucje UE w wykraczaniu poza podejście oparte tylko na zgodności i w przyjmowaniu podejścia, które opiera się również na odpowiedzialności. W szczególności będziemy z nimi współpracować przy opracowywaniu ocen skutków dla prywatności danych oraz przy zawiadamianiu o naruszeniach ochrony danych.

- **Skoordynowany nadzór**
Nadal będziemy sprawować nadzór nad wielkoskalowymi systemami informatycznymi w ścisłej współpracy z krajowymi organami ochrony danych.
- **Kontrole**
Poprawimy naszą metodykę przeprowadzania kontroli i wizyt, a w szczególności usprawnimy metodę kontrolowania systemów informatycznych.

Polityka i konsultacje

W ramach realizacji strategii EIOD na lata 2015–2019 określono pięć kluczowych obszarów dla naszych działań w zakresie polityki i konsultacji w 2015 r.:

- **Duże zbiory danych i jednolity rynek treści cyfrowych**
Przedstawimy wizję tego, w jaki sposób UE powinna zapewniać osobom fizycznym możliwość korzystania z kontroli użytkownika, wykorzystywać duże zbiory danych i zapewniać, aby organizacje i przedsiębiorstwa w sposób przejrzysty i odpowiedzialny przetwarzały dane osobowe, za które ponoszą odpowiedzialność. Poprzez udział w wydarzeniach i rozmowy z organami regulacyjnymi przeprowadzimy intensywną debatę w oparciu o naszą wstępną opinię w sprawie prawa konkurencji, ochrony konsumentów, prywatności i gospodarki cyfrowej.
- **Zakończenie reformy ram ochrony danych**
Przed latem 2015 r. przedstawimy briefing dla instytucji, aby przekazać im informacje oraz pomóc w znalezieniu praktycznych i elastycznych rozwiązań w trakcie zbliżających się rozmów trójstronnych w sprawie ogólnego rozporządzenia o ochronie danych i dyrektywy o ochronie danych osobowych w ramach współpracy organów ścigania. Skupimy się również – w ścisłej współpracy z krajowymi organami nadzoru – na wdrażaniu nowych zasad. W szczególności pomożemy przygotować się na płynne przejście do nowej Europejskiej Rady Ochrony Danych bez uszczerbku dla przyszłej decyzji współprawodawców dotyczącej organizacji sekretariatu Rady. Zaangażujemy się na wczesnym etapie w dyskusję polityczną

dotycząca opracowania prawodawstwa wykonawczego lub sektorowego, takiego jak wniosek dotyczący zmiany dyrektywy 2002/58/WE.

- **Porozumienia międzynarodowe**

Będziemy aktywnie współpracować z instytucjami UE w celu zapewnienia, aby zasady ochrony danych były właściwie i spójnie brane pod uwagę w trakcie negocjowania międzynarodowych porozumień handlowych oraz egzekwowania prawa, takich jak: transatlantyckie partnerstwo handlowo-inwestycyjne (TTIP), porozumienie w sprawie handlu usługami (TISA) oraz zasady bezpiecznego transferu danych osobowych, a także podczas planowanego automatycznego przedłużenia umowy ze Stanami Zjednoczonymi dotyczącej programu śledzenia środków finansowych należących do terrorystów. W stosownych przypadkach będziemy oferować również naszą wiedzę i pomoc w ramach monitorowania istniejących umów, takich jak dwustronne umowy w sprawie danych dotyczących przelotu pasażera.

- **Wspieranie decydentów w sektorze spraw wewnętrznych**

W porozumieniu z ekspertami Komisji zamierzamy przygotować wytyczne dotyczące uwzględniania zasad ochrony danych we wnioskach i polityce w dziedzinie bezpieczeństwa wewnętrznego, zarządzania granicami i migracji. Nowa Europejska agenda bezpieczeństwa musi obejmować szersze ujednoczenie różnych przepisów w zakresie ochrony danych w tym obszarze oraz spójność nadzoru nad wielkoskalowymi systemami informatycznymi. W przypadku określonych środków, takich jak dyrektywa UE w sprawie danych dotyczących przelotu pasażera i pakiet dotyczący inteligentnych granic, w sprawie których trwają rozmowy, zaofiarowaliśmy się współpracować z instytucjami nad znalezieniem sposobów zminimalizowania ingerencji w prawa do prywatności i do ochrony danych dużej liczby osób fizycznych potencjalnie zagrożonych tymi środkami. Nasze porady będą opierać się na najnowszym orzecznictwie, przede wszystkim orzeczeniu Trybunału Sprawiedliwości Unii Europejskiej dotyczącym dyrektywy w sprawie zatrzymywania danych w sprawie Digital Rights Ireland. Przygotujemy również dokument informacyjny na temat pojęć konieczności i proporcjonalności, szczególnie w świetle

najnowszego orzecznictwa, oraz na temat sposobu, w jaki należy stosować te pojęcia we wnioskach, które mają wpływ na ochronę danych.

- **Uzgodnianie metod pracy z instytucjami i organami UE**

Jak zapowiedzieliśmy w naszym dokumencie strategicznym, będziemy starali się uzgodnić skuteczne sposoby współpracy z instytucjami, w stosownych przypadkach w formie protokołów ustaleń, w ramach naszej roli dotyczącej polityki i konsultacji. Będziemy zabiegać o informacje zwrotne na temat wartości naszych porad. Będzie to opierać się na niedawnej ścisłej współpracy z włoską prezydencją nad projektem dyrektywy w sprawie automatycznej wymiany danych dotyczących rachunków bankowych między organami podatkowymi. Nadal będziemy utrzymywać bliskie kontakty z Agencją Praw Podstawowych Unii Europejskiej w odniesieniu do kwestii będących przedmiotem wspólnego zainteresowania.

Współpraca

Naszą ambicją jest, aby UE wypowiadała się jednym głosem w kwestiach prywatności i ochrony danych. Dlatego głównym czynnikiem w naszej strategii będzie ścisła współpraca z innymi organami ochrony danych.

- **Skoordynowany nadzór**

Nadal będziemy priorytetowo traktować efektywne i lojalne zaangażowanie i wsparcie w obszarze skoordynowanego nadzoru nad CIS, EURODAC, IMI, SIS II oraz VIS. Naszym celem jest przejście na bardziej skonsolidowany i efektywny model zarządzania systemami w ramach dawnego „trzeciego filaru”.

- **Grupa Robocza Art. 29**

Będziemy ściśle współpracować z Grupą Roboczą Art. 29 nie tylko w celu zapewnienia płynnego przejścia do Europejskiej Rady Ochrony Danych, ale również przy opracowywaniu i komentowaniu opinii w sprawie polityki, zarówno na posiedzeniach podgrup, jak i na posiedzeniach plenarnych, w stosownych przypadkach w charakterze sprawozdawcy, oraz w obszarze nadzoru operacyjnego nad agencjami UE i systemami informatycznymi.

- **Państwa nienależące do UE i organizacje międzynarodowe**

Będziemy promować globalny sojusz z organami ochrony danych i prywatności, aby znaleźć techniczne i prawne rozwiązania kluczowych problemów związanych z ochroną danych, takich jak: duże zbiory danych, internet przedmiotów i masowy nadzór. Będziemy również w pełni zaangażowani w dyskusje na forach międzynarodowych, w tym w Radzie Europy i OECD, na temat ochrony danych i prywatności.

Polityka w zakresie technologii informacyjnych

- **Ochrona danych przechodzi na technologię cyfrową**

Jednym z naszych głównych działań służących osiągnięciu tego celu strategicznego będzie poprawa naszych relacji z zainteresowanymi stronami, szczególnie z osobami zajmującymi się kwestiami technicznymi, aby nawiązać bardziej interdyscyplinarną współpracę w zakresie uwzględniania ochrony danych już w fazie projektowania i w sposób domyślny.

- **Sieć na rzecz Inżynierii Prywatności w Internecie**

Nadal będziemy skupiać się na ochronie danych i prywatności z technicznego punktu widzenia. Ponieważ sieć IPEN obejmuje ekspertów w dziedzinie technologii z organów ochrony danych, sektora przemysłu, środowiska akademickiego oraz społeczeństwa obywatelskiego, co odróżnia ją od innych sieci, jej działania ukierunkowane są na kwestie mające znaczenie praktyczne. W 2015 r. sieć będzie rozwijała się i kontynuowała prace w kierunku ustalonym w 2014 r.

- **Monitorowanie technologii**

Nasze działania w zakresie monitorowania technologii staną się bardziej widoczne i dostępne dla innych zainteresowanych stron, aby wspomóc ich pracę. Poza informacjami na potrzeby naszych własnych działań, współpracy z organami ochrony danych i grupami ekspertów ds. technologii na szczeblu UE udostępniemy nasze sprawozdania publicznie.

- **Wytyczne dotyczące technologii i ochrony danych**

Aby promować kulturę ochrony danych w instytucjach UE objętych nadzorem EIOD, w 2015 r. zakończą się prace nad wytycznymi dotyczącymi określonych obszarów technicznych, takich jak: urządzenia mobilne, usługi internetowe i przetwarzanie w chmurze, które uzupełnione zostaną wytycznymi dotyczącymi konkretnych obszarów takich jak zarządzanie ryzykiem.

- **Bezpieczeństwo informatyczne**

Przez lata wzrosło znaczenie zarządzania bezpieczeństwem informatycznym. Nadal będziemy rozwijać naszą wiedzę ekspercką na temat bezpieczeństwa informatycznego i jego systematycznego stosowania – jako organ nadzoru w trakcie naszych działań w zakresie kontroli i audytu oraz jako partner w ramach współpracy ze społecznością z branży bezpieczeństwa informatycznego, ze szczególnym uwzględnieniem instytucji UE.

Inne dziedziny

Informacje i komunikacja

Rok 2015 jest rokiem zmian w EIOD. Z uwagi na nowy mandat i strategię obecnie staramy się przewidzieć i zbadać, co można osiągnąć w ciągu najbliższych pięciu lat. Odzwierciedla to opracowanie kilku poważnych projektów informacyjnych i komunikacyjnych, które zostaną zrealizowane. Dotyczą one m.in.:

- **Nowej identyfikacji wizualnej**

Ważnym projektem na 2015 r. będzie zmiana naszej identyfikacji wizualnej, która będzie polegała na wprowadzeniu nowego logo i diagramu. Efektem domina spowodowanym zmianą naszej identyfikacji wizualnej jest również konieczność aktualizacji wszystkich materiałów informacyjnych EIOD (takich jak: materiały promocyjne, publikacje, strona internetowa itd.). Będzie to projekt długoterminowy, ponieważ nadal będziemy korzystać z materiałów, które posiadamy, i zaktualizujemy je dopiero wtedy, gdy się skończą lub gdy korzystanie z nich nie będzie już możliwe;

- **Aktualizacji strony internetowej EIOD**

Przeprowadzimy również pewną poważną aktualizację techniczną naszej strony internetowej i skorzystamy z tej okazji, aby odświeżyć jej wygląd i charakter;

- **Przejrzystego języka**

W ciągu ostatnich kilku lat nadal czyniliśmy ogromne postępy w zakresie wypracowania przejrzystego języka. Naszym nadrzędnym celem jest skorygowanie nadmiernie prawniczego i technicznego obrazu ochrony danych. Kwestia ta pozostaje priorytetem, zatem w 2015 r. nadal będziemy używać prostego języka, aby kwestie techniczne były omówione bardziej przystępnie, wraz z przykładami, z którymi społeczeństwo może się identyfikować.

Zarządzanie zasobami i profesjonalizacja zarządzania zasobami ludzkimi

Nowy mandat EIOD oraz nowa strategia pociągną za sobą zmiany, które będą miały wpływ na nasze zasoby ludzkie i wywrą dodatkową presję na kurczący się budżet wskutek realizowanej od kilku lat polityki oszczędnościowej.

- Wśród tych zmian prawdopodobne przyjęcie nowego rozporządzenia o ochronie danych, zastępującego dyrektywę 95/46/WE, może bezpośrednio wpłynąć na strukturę organizacyjną EIOD, szczególnie jeżeli – jak przewidziano we wniosku Komisji – EIOD powierzone zostanie pełnienie funkcji sekretariatu nowej Europejskiej Rady Ochrony Danych (EROD). W konsekwencji w budżecie na 2015 r. ujęto już nowy tytuł III, dotyczący EROD, a w drugiej połowie roku utworzona zostanie grupa zadaniowa ds. EROD.

- W 2015 r. opracujemy dwa dokumenty dotyczące sposobów wzmocnienia odpowiedzialności i wymiaru etycznego naszej instytucji: nowy kodeks postępowania dla zespołu inspektorów oraz politykę sygnalizowania nieprawidłowości w oparciu o zalecenia Europejskiego Rzecznika Praw Obywatelskich.

W ramach naszego celu polegającego na dawaniu przykładu będziemy ściśle współpracować z inspektorami EIOD przy ocenie skutków dla prywatności i zmianą powiadomień o ochronie danych po wejściu w życie nowego regulaminu pracowniczego.

www.edps.europa.eu



Urząd Publikacji

ISBN 978-92-9242-076-5

