EDPS

EUROPEJSKI INSPEKTOR
OCHRONY DANYCH

SPRAWOZDANIE ROCZNE

STRESZCZENIE '22

Szczegółowe informacje na temat EIOD można znaleźć na naszej stronie internetowej: edps.europa.eu.

Na stronie EIOD można także zaprenumerować nasz newsletter.

Waterford, Irlandia - Bruksela, Belgia: Trilateral Research Ltd, Vrije Universiteit Brussel, 2023 r.

PRINT ISBN 978-92-9242-745-0 doi: 10.2804/240996 QT-AB-23-001-PL-C

PDF ISBN 978-92-9242-732-0 ISSN 1831-0583 doi: 10.2804/57919 QT-AB-23-001-PL-N

PRZEDMOWA

Mam przyjemność przekazać Państwu roczne sprawozdanie EIOD za 2022 r. Spoglądam na miniony rok z dużą dozą refleksji. Był to rok obfitujący w wydarzenia: pełen wyzwań i nadziei, trudny, ale pozytywny - zarówno dla całego świata, jak i dla EIOD.

W tym roku, w związku z inwazją Rosji na Ukrainę, Unia Europejska (UE) okazała bezprecedensową reakcję. W ciągu ostatniego roku UE udowodniła, że jest w stanie znaleźć ogólnounijne rozwiązania, zwłaszcza w obliczu zagrożenia zewnętrznego, nie tylko dowodząc w ten sposób solidarności, lecz także stojąc na straży naszych kluczowych wartości i zasad. W tym duchu EIOD starał się również wykazać w ubiegłym roku zaangażowanie w przestrzeganie podstawowego prawa do ochrony danych, nawet w sytuacjach kryzysowych, w których podejmowane przez nas środki i reakcje musiały być szybkie i skuteczne. Nasze wysiłki na rzecz wspierania unijnych prawodawców w procesie legislacyjnym i nadzorowania rozwoju Eurojustu, Agencji Unii Europejskiej ds. Współpracy Wymiarów Sprawiedliwości w Sprawach Karnych, są wyrazem przekonania, że razem jesteśmy silniejsi.

Pomimo tak burzliwych wydarzeń na świecie, ubiegły rok był również rokiem aspiracji i rozwoju - okazją do refleksji nad kształtowaniem jutra, które skutecznie stawi czoła dzisiejszym wyzwaniom. W pełni uwzględniając rzeczywistość po pandemii, w dniach 16-17 czerwca zorganizowaliśmy w Brukseli spotkanie pt. „Przyszłość ochrony danych - skuteczne egzekwowanie przepisów w cyfrowym świecie". Konferencja zgromadziła 2000 uczestników - biorących w niej udział zarówno osobiście, jak i na odległość - wokół jednego kluczowego celu, jakim jest wspieranie postępów w debacie na temat przyszłości egzekwowania ogólnego rozporządzenia o ochronie danych cztery lata po jego wejściu w życie. Jestem dumny z tego wydarzenia i z zagorzałych dyskusji, które toczyły się podczas dwudniowej konferencji i wywołały konkretne działania w społeczności zajmującej się ochroną danych. Zobowiązania Europejskiej Rady Ochrony Danych, które znalazły odzwierciedlenie w oświadczeniu ze szczytu w Wiedniu, czy też plany Komisji Europejskiej dotyczące zaproponowania przepisów harmonizujących niektóre proceduralne aspekty współpracy transgranicznej między organami ochrony danych to dwa istotne przykłady następstw naszej konferencji. Z niecierpliwością oczekuję na to, dokąd zaprowadzi nas ta rozmowa i jestem wdzięczny całej naszej społeczności za odwagę w tych rozważaniach.

Jako organ ochrony danych nadzorujący instytucje, urzędy, agencje i organy UE,

EIOD pełni szczególną rolę polegającą na nadzorowaniu wyłącznie organów publicznych. Rola ta pociąga za sobą poczucie odpowiedzialności za wkład w refleksje na temat funkcji państwa w społeczeństwie demokratycznym. Świadomość ta skłoniła nas na przykład do podzielenia się uwagami wstępnymi EIOD na temat nowoczesnego oprogramowania szpiegującego, stanowiącymi próbę stworzenia lepszego demokratycznego nadzoru nad praktykami związanymi z egzekwowaniem prawa lub bezpieczeństwem narodowym.

W tym kontekście EIOD wydał również skierowany do Europolu nakaz usunięcia dużych zbiorów danych, które nie mają związku z działalnością przestępczą. Reakcja ustawodawcy na tę kwestię oraz kolejny wniosek EIOD do Trybunału Sprawiedliwości Unii Europejskiej o stwierdzenie nieważności z mocą wsteczną przepisów zmienionego rozporządzenia w sprawie Europolu są oznaką naszego głębokiego przekonania, że Unia Europejska może - i powinna - ustanawiać światowe normy w zakresie praworządności i wartości demokratycznych.

Aby tak się stało, należy nadal dążyć do najwyższych standardów w samej UE. W nadchodzących latach nadal będziemy wnosić wkład w to ważne przedsięwzięcie. Jestem pewien, że przyszły rok przyniesie nowe wyzwania i odkrycia, ale z niecierpliwością czekam, aby się z nimi zmierzyć, wraz z dynamicznym i oddanym zespołem EIOD.

Wojciech Wiewiórowski
Europejski Inspektor Ochrony Danych

ROZDZIAŁ 1

O nas

1.1.
EIOD

Kim jesteśmy?

Europejski Inspektor Ochrony Danych (EIOD) jest niezależnym organem Unii Europejskiej do spraw ochrony danych i odpowiada za nadzorowanie przetwarzania danych osobowych przez europejskie instytucje, organy i jednostki organizacyjne (instytucje UE).

Doradzamy im w sprawie nowych wniosków ustawodawczych i inicjatyw dotyczących ochrony danych osobowych.

Monitorujemy wpływ nowych technologii na ochronę danych i współpracujemy z organami nadzoru w celu zapewnienia spójnego egzekwowania unijnych przepisów o ochronie danych.

Nasza misja

Ochrona danych jest prawem podstawowym chronionym na mocy przepisów prawa europejskiego. Promujemy silną kulturę ochrony danych w instytucjach UE.

Nasze wartości i zasady

Nasza praca opiera się na czterech wymienionych poniżej wartościach.

- **Bezstronność** - działanie w ramach legislacyjnych i politycznych, które nam powierzono, w sposób niezależny i obiektywny, znalezienie właściwej równowagi między różnymi interesami.
- **Rzetelność** - utrzymanie najwyższych standardów postępowania i zawsze czynienie tego, co jest słuszne.
- **Przejrzystość** - wyjaśniamy, co robimy i dlaczego, w zrozumiałym i przystępnym dla wszystkich języku.
- **Pragmatyzm** - zrozumienie potrzeb zainteresowanych stron i poszukiwanie rozwiązań, które sprawdzą się w praktyce.

Czym się zajmujemy?

EIOD prowadzi działalność w czterech głównych obszarach:

- **Nadzór i egzekwowanie** - monitorujemy przetwarzanie danych osobowych przez instytucje UE, aby zapewnić ich zgodność z przepisami o ochronie danych.
- **Polityka i konsultacje** - doradzamy Komisji Europejskiej, Parlamentowi Europejskiemu i Radzie w sprawie wniosków ustawodawczych i inicjatyw związanych z ochroną danych.
- **Technologia i prywatność** - monitorujemy i oceniamy postępy technologiczne mające wpływ na ochronę danych osobowych. Sprawdzamy, czy w systemach wspomagających przetwarzanie danych osobowych przez instytucje UE wdrażane są odpowiednie zabezpieczenia zapewniające zgodność z przepisami o ochronie danych. Wdrażamy transformację cyfrową EIOD.
- **Współpraca** - współpracujemy z organami ochrony danych w celu promowania spójnej ochrony danych w całej UE. Naszą główną platformą współpracy z organami ochrony danych jest Europejska Rada Ochrony Danych, dla której prowadzimy sekretariat i z którą zawarliśmy protokół ustaleń określający zasady współpracy.

Nasze uprawnienia

Nasze uprawnienia jako organu ochrony danych instytucji UE określono w rozporządzeniu (UE) 2018/1725.

Na mocy tego rozporządzenia możemy na przykład ostrzegać lub pouczać instytucje Unii, które przetwarzają dane osobowe w sposób niesprawiedliwy lub niezgodny z prawem; nakazać im, aby zastosowały się do wniosków o wykonywanie praw osób fizycznych; nałożyć tymczasowy lub definitywny zakaz w odniesieniu do konkretnej operacji przetwarzania danych; nałożyć administracyjne kary pieniężne na instytucje Unii; skierować sprawę do Trybunału Sprawiedliwości Unii Europejskiej.

Mamy również szczególne uprawnienia do nadzorowania sposobu, w jaki następujące organy i agencje przetwarzają dane osobowe: Europol - Agencja Unii Europejskiej ds. Współpracy Organów Ścigania na mocy rozporządzenia 2016/794; Eurojust - Agencja Unii Europejskiej ds. Współpracy Wymiarów Sprawiedliwości w Sprawach Karnych na mocy rozporządzenia 2018/1727; oraz EPPO - Prokuratura Europejska na mocy rozporządzenia (UE) 2017/1939; jak również Frontex - Europejska Agencja Straży Granicznej i Przybrzeżnej.

Więcej informacji na temat EIOD można znaleźć na naszej stronie internetowej zawierającej najczęściej zadawane pytania.

Więcej informacji na temat ochrony danych w ujęciu ogólnym można znaleźć w naszym glosariuszu na stronie internetowej EIOD.

1.2.
Strategia EIOD na lata 2020-2024

W świecie połączonym licznymi powiązaniami i transgranicznymi przepływami danych europejska i międzynarodowa solidarność pomoże wzmocnić prawo do ochrony danych oraz sprawić, że dane będą wykorzystywane z pożytkiem dla społeczeństwa w całej UE i poza jej terytorium.

Strategia EIOD na lata 2020-2024 skupia się na trzech filarach: **perspektywiczności**, **aktywności** i **solidarności**, aby stworzyć bezpieczniejszą, bardziej sprawiedliwą i zrównoważoną przyszłość cyfrową.

- **Perspektywiczność** - chcemy być inteligentną instytucją, która w perspektywie długoterminowej uwzględnia tendencje w dziedzinie ochrony danych oraz kontekst prawny, społeczny i technologiczny.

- **Aktywność** - pragniemy proaktywnie opracowywać narzędzia umożliwiające europejskim instytucjom, organom i jednostkom organizacyjnym (instytucjom UE) odgrywanie roli światowych liderów w zakresie ochrony danych. Promujemy spójność działań organów egzekwowania prawa w UE, kładąc nacisk na faktyczną europejską solidarność, podział obowiązków i wspólne podejście.

- **Solidarność** - wierzymy, że sprawiedliwość wymaga ochrony prywatności wszystkich osób i we wszystkich obszarach polityki UE, a głównym uzasadnieniem przetwarzania danych w interesie publicznym powinien być zrównoważony rozwój.

ROZDZIAŁ 2

Przyszłość - nasze cele na 2023 r. i kolejne lata

Śródokresowy przegląd strategii - „Kształtowanie bezpieczniejszej cyfrowej przyszłości"

Strategię EIOD na lata 2020-2024 „Kształtowanie bezpieczniejszej cyfrowej przyszłości" opracowano u progu globalnych przemian. W sporządzonym na początku 2020 r. dokumencie przedstawiono trzy kluczowe filary strategiczne dla EIOD: **perspektywiczność**, **aktywność** i **solidarność**. Jednak nawet nasi najlepsi eksperci ds. prognozowania nie mogli przewidzieć zmiany paradygmatu, która miała nastąpić. Pandemia COVID-19, wojna w Ukrainie i światowy kryzys gospodarczy - wszystkie te czynniki złożyły się na pełne wyzwań otoczenie, w którym znaleźliśmy się po przyjęciu naszej strategii na 2020 r.

Dlatego w 2022 r. postanowiliśmy przeprowadzić śródokresowy przegląd naszej strategii na lata 2020-2024. Przegląd śródokresowy - rozpoczęty z zamiarem oceny postępów w realizacji celów wymienionych w strategii - stanowił kluczowy moment rozważań, czy zmiana kierunku instytucjonalnego jest konieczna w świetle zmieniającego się kontekstu światowego. W kolejnym rozdziale sprawozdania rocznego przedstawiono wyniki przeglądu śródokresowego oraz określono zmienioną wizję i priorytety EIOD pozostałej części strategii.

Procedura przeglądu śródokresowego

Wdrożono oddolne podejście do przeglądu śródokresowego, w ramach którego ocena strategii została przeprowadzona od wewnątrz. Decyzję tę podjęto z zamiarem wykorzystania świeżego spojrzenia pracowników EIOD, mając na uwadze rozwój instytucjonalny, jaki nastąpił od 2020 r. Podejście to pozwoliło nam wykorzystać wewnętrzne interdyscyplinarne doświadczenie i wiedzę pracowników EIOD, aby określić kluczowe obszary naszej pracy w nadchodzących latach.

Przegląd śródokresowy przeprowadzono w dwóch etapach. Pierwszy etap polegał na analizie luk. Analizę tę przeprowadzono na podstawie procesu mapowania, w którym uczestniczyli wszyscy pracownicy EIOD. Działanie oficjalnie rozpoczęto dyskusją między Inspektorem a pracownikami EIOD - Inspektor przedstawił w niej planowaną procedurę otwartej refleksji i rozważań personelu. Po otrzymaniu cennych informacji na szczeblu personelu rozpoczęto proces mapowania. W analizie przedstawiono przegląd 57 celów wymienionych w strategii EIOD na lata 2020-2024 - pracownicy przedstawili refleksje na temat tego, czy i w jakim stopniu cele te osiągnięto. W następstwie tej wstępnej oceny przeprowadzono analizę luk na potrzeby ustalenia stanu postępów w osiąganiu celów.

Wyniki analizy sytuacji wskazały na znaczne postępy we wdrażaniu i osiąganiu celów wymienionych w strategii. Analiza luk wykazała, że spośród 57 celów wymienionych w strategii dotychczas osiągnięto 15, kolejnych 40 jest w toku, a tylko 2 są na wczesnym etapie realizacji.

Pozytywne wyniki analizy luk stanowiły podstawę drugiego etapu przeglądu śródokresowego. Na tym drugim etapie o charakterze konsultacyjnym przeprowadzono konsultacje z pracownikami EIOD w sprawie przyszłości EIOD i poproszono ich o zastanowienie się, w jaki sposób nowe realia naszego otoczenia mogą uzasadniać zmianę priorytetów w pozostałej części strategii. Szczególną uwagę poświęcono określeniu obszarów docelowych, na których EIOD chciałby skoncentrować intensywniejsze wysiłki z myślą o pozostałej części strategii.

Wyniki przeglądu śródokresowego - od kształtowania bezpieczniejszej cyfrowej przyszłości po wspieranie jej tworzenia

Wyniki etapu konsultacji doprowadziły do wyłonienia kilku priorytetów instytucjonalnych, które uważamy za kluczowe i zobowiązujemy się do poświęcenia im dodatkowej uwagi oraz przeznaczenia na nie zasobów podczas realizacji pozostałej części strategii na lata 2020-2024.

Priorytet nr 1: Skuteczne egzekwowanie ochrony danych w nowym otoczeniu regulacyjnym

Wraz z przyjęciem wielu inicjatyw ustawodawczych w dziedzinie technologii cyfrowych EIOD oraz społeczność organów ochrony danych znalazły się w znacznie bardziej złożonym otoczeniu regulacyjnym. To nowe otoczenie regulacyjne, obejmujące przepisy takie jak akt w sprawie zarządzania danymi, akt o rynkach cyfrowych i akt o usługach cyfrowych - z jednej strony oraz proponowany akt w sprawie sztucznej inteligencji i akt w sprawie danych - z drugiej strony, skutkuje planowaniem wprowadzenia przez prawodawcę nowych funkcji regulacyjnych i organów regulacyjnych.

Chociaż akty te zasadniczo nie naruszają ani nie zmieniają RODO (ani EUDPR), niektóre przepisy w tych nowych lub przyszłych rozporządzeniach wyraźnie odnoszą się do definicji, pojęć i obowiązków zawartych w RODO. Ponadto, chociaż przetwarzanie danych osobowych ma kluczowe znaczenie dla działań uregulowanych w poszczególnych aktach prawnych, organów ochrony danych nie wyznaczono jako głównych właściwych organów. Egzekwowanie przepisów powierza się - w całości lub w bardzo

dużym stopniu - organom, których zadania dotyczą przede wszystkim celów polityki innych niż ochrona danych lub prywatność. W związku z tym konieczne jest zapewnienie spójnego podejścia do działań regulacyjnych w otoczeniu cyfrowym. Skupimy się zatem na zaplanowaniu naszej roli w odniesieniu do tych organów oraz nad określeniem oczekiwań tych organów wobec EIOD.

Opierając się na swoim skonsolidowanym i powszechnie uznanym doświadczeniu w zapewnianiu spójnego podejścia w ekosystemie cyfrowym, będziemy zatem kierować pracami odpowiednich forów koordynacyjnych przewidzianych prawem, takich jak grupa wysokiego szczebla ds. aktu o rynkach cyfrowych i inne odpowiednie fora koordynacyjne przewidziane prawem, zarówno jako EIOD, jak i jako członek Europejskiej Rady Ochrony Danych, oraz będziemy czynnie uczestniczyć w tych pracach.

Będziemy również aktywnie wspierać ścisłą współpracę z właściwymi organami w przypadkach, gdy prawo nie przewiduje konkretnego organu koordynującego, ale egzekwowanie przepisów będzie wymagało ścisłego dialogu z organami odpowiedzialnymi za stosowanie przepisów mających wpływ na prywatność i ochronę danych.

Ponadto będziemy dążyć do zapewnienia, aby zasady i przepisy dotyczące ochrony danych nie zostały naruszone przez stosowanie i egzekwowanie nowych przepisów. EIOD będzie zatem nadal pełnił swoją funkcję doradczą, aby monitorować i naświetlać potencjalne konsekwencje wynikające z praktycznego wdrażania nowych ram regulacyjnych. W razie potrzeby EIOD rozważy również środki przymusu.

W tym kontekście EIOD stoi również w obliczu swojej potencjalnej roli jako organu nadzorującego instytucje, urzędy, organy i agencje UE (instytucje UE) w zakresie sztucznej inteligencji. Z punktu widzenia zarówno organizacyjnego, jak i metodycznego przewiduje się intensywne przygotowania, aby upewnić się, że od samego początku jesteśmy gotowi do wykonania naszego nowego zadania.

Projekt cyfrowego euro ma dla nas również duże znaczenie strategiczne i wymaga ścisłej współpracy między ekspertami w obszarach polityki, prawa, technologii i nadzoru. Chociaż wiele będzie zależało od dokonanych wyborów projektowych, projekt cyfrowego euro niewątpliwie będzie miał znaczący wpływ na prywatność i ochronę danych. Inne wnioski dotyczące sektora finansowego również wymagają dogłębnej analizy, np. wniosek ustawodawczy w sprawie otwartych ram finansowych, który ma na celu umożliwienie wymiany danych i dostępu stron trzecich dla wielu sektorów i produktów finansowych. W związku z tym rozważymy z najwyższą uwagą możliwe interakcje z aktem w sprawie zarządzania danymi i aktem w sprawie danych.

Konferencja EIOD na temat *„Przyszłość ochrony danych - skuteczne egzekwowanie przepisów w cyfrowym świecie”* odbyła się w czerwcu 2022 r. i była katalizatorem znacznych i bardzo potrzebnych postępów w debacie publicznej na temat egzekwowania ogólnego rozporządzenia o ochronie danych (RODO). Związane z tym zmiany, zwłaszcza tzw. deklaracja wiedeńska EROD, oraz zapowiedziany wniosek Komisji Europejskiej dotyczący rozporządzenia harmonizującego niektóre aspekty krajowych przepisów proceduralnych pokazują, że w nadchodzących latach nadal będzie przeważać debata nad potencjalnymi usprawnieniami funkcjonowania RODO. Sukces konferencji EIOD - w znaczeniu interesu publicznego i jej oddziaływania - pokazuje, że EIOD, jako niezależna instytucja UE, odgrywa w tej debacie istotną rolę orędownika ogólnoeuropejskiego podejścia, które zapewnia pełne poszanowanie Karty praw podstawowych UE.

Priorytet nr 2: Interoperacyjność jako wyzwanie wymagające zrewidowanego podejścia nadzorczego

Wraz z początkiem interoperacyjności EIOD staje w obliczu istotnych obowiązków mających na celu zapewnienie skutecznego podejścia nadzorczego. Wprowadzenie unijnych ram interoperacyjności, w których przyjęto nowe podejście do zarządzania danymi dotyczącymi granic i bezpieczeństwa sprawia, że ponownie zastanawiamy się również nad metodyką nadzoru nad wielkoskalowymi systemami informatycznymi. Zmiany interoperacyjności proponowane w ramach UE doprowadziłyby do powiązania kilku wielkoskalowych systemów informatycznych z bazami danych Europolu i Interpolu, co stanowiłoby ekosystem przepływu danych zwiększający ryzyko - wynikające z funkcjonowania systemów bazowych - dla osób, których dane dotyczą.

Zidentyfikowaliśmy kilka problemów, które należy rozwiązać. Złożoność ogólnej architektury i rozdrobnienie przepisów o ochronie danych wymaga przeskalowania nadzoru, który koncentruje się na przepływach danych, a nie na oddzielnym monitorowaniu przetwarzania danych w różnych systemach. Podobnie wprowadzenie dodatkowych działań w zakresie przetwarzania danych, których pierwotnie nie określono w akcie prawnym regulującym ustanowienie każdego z podstawowych wielkoskalowych systemów informatycznych, wymaga dogłębnej analizy zasady celowości. Ponadto mogą zostać podjęte decyzje, które mają istotny wpływ na ochronę danych, związane z procedurami komitetowymi i przekazywaniem obowiązków na rzecz Agencji Unii Europejskiej ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (eu-LISA). Brak jednego kanału jednoczesnego wykonywania we wszystkich systemach praw osób, których dane dotyczą, może prowadzić do rozdrobnienia tych praw.

W związku z tym EIOD skoncentruje się na następujących trzech obszarach priorytetowych, które będą stanowić podstawę naszego nadzoru nad ramami interoperacyjności do końca kadencji:

(1) Prawa osób, których dane dotyczą - Mając na celu rozwiązanie problemu ryzyka rozdrobnienia praw osób, których dane dotyczą, za pomocą różnych interoperacyjnych baz danych z wieloma administratorami, zbadamy możliwość skoordynowanego nadzoru (także podejmując wspólną refleksję z organami ochrony danych na temat usprawnienia procedur dotyczących praw osób, których dane dotyczą). Ponadto będziemy dążyć do opracowania proaktywnego podejścia do praw osób, których dane dotyczą, w szczególności do prawa do informacji.

(2) Strategia audytu - Opracowanie dostosowanej do potrzeb strategii kontroli ochrony danych w wielkoskalowych systemach informatycznych i elementach interoperacyjności, dostosowanej do nowego ekosystemu, mogącej stanowić przejście od silosowych systemów kontroli do przepływów danych. Strategia obejmie wspólne podejście do kontroli interoperacyjności poprzez uwzględnienie dalszych obowiązków kontrolnych wobec agencji UE (Europolu, Frontexu, Eurojustu), aby zagwarantować stosowanie zasady celowości i sprawdzić, czy podmioty te mają dostęp do danych i przetwarzają je zgodnie z ich odpowiednimi mandatami. To wspólne podejście będzie obejmowało część prawną i techniczną. Ponieważ regulacje dotyczące wielkoskalowych systemów informatycznych wyraźnie wymagają od EIOD przeprowadzenia *„audytów zgodnie z międzynarodowymi standardami rewizji finansowej"*, konieczna będzie ponadto wspólna interpretacja tego wymogu.

(3) Profilowanie algorytmiczne - prace nad profilowaniem algorytmicznym będą miały na celu w szczególności określenie pozycji EIOD w odniesieniu do stosowania tego narzędzia w ramach interoperacyjności (ETIAS i VIS) oraz - w ogólnym ujęciu - szczególne uwzględnienie kwestii dyskryminacji, wiarygodności, proporcjonalności i przejrzystości. Nadzór nad profilowaniem algorytmicznym jest złożonym zagadnieniem, znajdującym się dopiero na wczesnym etapie, i wymaga współpracy z innymi agencjami i organami w dziedzinie praw człowieka i niedyskryminacji oraz ewentualnie z innymi podmiotami społeczeństwa obywatelskiego i środowiska akademickiego. Taki nadzór będzie stanowić wsparcie dla naszego wkładu w prace rady ETIAS, europejskiego systemu informacji o podróży oraz zezwoleń na podróż, i rady VIS ds. wytycznych w zakresie praw podstawowych, i będzie miał na celu opracowanie odpowiednich narzędzi monitorowania i nadzoru dla tego nowego obszaru nadzoru.

Priorytet nr 3: Współpraca międzynarodowa w celu promowania wspólnych globalnych podejść do prywatności i ochrony danych

Uważamy, że aktywne zaangażowanie we współpracę międzynarodową ma fundamentalne znaczenie. Dzięki temu możemy zaangażować szerszą społeczność, także poza Europą, oraz promować wspólne rozumienie i podejście do wyzwań związanych z ochroną danych i prywatnością. Planujemy dalsze zwiększenie wysiłków w dziedzinie współpracy międzynarodowej, ponieważ na forach międzynarodowych omawia się kilka tematów o dużym znaczeniu strategicznym.

W szczególności zamierzamy wspierać koordynację działań i strategii członków EROD na forach międzynarodowych, w dalszym ciągu angażować się w prace prowadzone w kontekście Globalnego Zgromadzenia ds. Prywatności, Rady Europy, a także w ramach okrągłego stołu G-7 i Organizacji Współpracy Gospodarczej i Rozwoju (OECD), zapewniając aktywny udział i skuteczne reprezentowanie poglądów organów europejskich i EROD. Będziemy również dążyć do pogłębienia współpracy z organizacjami międzynarodowymi oraz z regionalnymi sieciami ochrony danych.

Priorytet nr 4: Nowe podejście do procesów EIOD w celu zapewnienia efektywności w szybko zmieniającym się otoczeniu

Strategia EIOD na lata 2020-2024 jest wdrażana w okresie, w którym kryzysy następowały jeden po drugim. Od pandemii COVID-19, przez rosyjską inwazję na Ukrainę, po rosnące koszty energii i inflację, musieliśmy dostosować nasze metody pracy i procesy, aby nadal osiągać rezultaty. Chociaż udało nam się co do zasady wywiązać ze zobowiązań przyjętych w strategii, analiza wewnętrzna wskazuje na potrzebę dalszego dostosowania podejścia do niektórych procesów, aby poprawić naszą skuteczność i długoterminowe standardy, zarówno jako administracji publicznej UE, jak i jako organu ochrony danych.

W tym drugim przypadku odnosi się to między innymi do rezultatów, takich jak działania następcze w związku ze zgłoszeniami naruszeń ochrony danych, rozpatrywanie skarg lub zdolność do proaktywnego identyfikowania krytycznych kwestii związanych ze zgodnością w drodze dochodzeń lub audytów.

Przeprowadzona zostanie dalsza analiza nowych narzędzi umożliwiających internetową lub zdalną ocenę zgodności. Jednocześnie ograniczenia kadrowe i budżetowe stanowią istotną przeszkodę w wypełnianiu zadań nadzorczych EIOD.

Podobnie wojna w Ukrainie nakłada na EIOD nowe odrębne zadania. W 2021 r. Komisja Europejska zaproponowała pakiet legislacyjny mający na celu zmianę rozporządzenia w sprawie Eurojustu, aby umożliwić przetwarzanie dowodów zgromadzonych na potrzeby dochodzeń w sprawie zbrodni wojennych popełnionych przez Rosję. W 2022 r. uchwalono kolejną zmianę legislacyjną, która wyznaczyła Eurojust jako europejskie centrum gromadzenia, przechowywania i analizowania dowodów dotyczących najpoważniejszych zbrodni wagi międzynarodowej. Powierzono nam ważną rolę w tworzeniu nowej bazy danych dotyczących dowodów. W styczniu 2023 r. Komisja Europejska ogłosiła utworzenie międzynarodowego centrum ścigania zbrodni agresji popełnianych w Ukrainie (ICPA) w Eurojuście. Wszystkie te zmiany legislacyjne już doprowadziły lub doprowadzą do powstania istotnych dodatkowych zadań dla nas. Zważywszy na polityczne znaczenie wsparcia UE dla Ukrainy, a także znaczny nakład pracy z tym związany, nasze działania w tym obszarze będą uznawane za jeden z kluczowych priorytetów.

W związku z rosnącym społecznym zainteresowaniem pracą EIOD, o czym świadczy m.in. liczba wniosków o dostęp do dokumentów, zobowiązujemy się również do przestrzegania wyższych standardów przejrzystości, nie tylko w kontekście dobrej administracji, ale również jako istotnego sposobu udostępniania naszej pracy osobom fizycznym. Zobowiązujemy się również do dalszego zapewniania wysokiego poziomu ochrony danych i rozliczalności oraz do dawania przykładu nie tylko poprzez przestrzeganie wymogów prawnych, lecz także poprzez badanie i korzystanie z najwyższej klasy narzędzi i usług sprzyjających ochronie prywatności i danych. Jeśli chodzi o cyberbezpieczeństwo, będziemy musieli dostosować się do nowych regulacji mających na celu zapewnienie wysokiego wspólnego poziomu cyberbezpieczeństwa we wszystkich instytucjach UE.

ROZDZIAŁ 3

Najważniejsze wydarzenia w 2022 r.

3.1.
Wykorzystanie naszych uprawnień do ochrony osób fizycznych

Naszym celem jako organu nadzorczego ds. ochrony danych, który odpowiada za nadzór nad instytucjami, organami i jednostkami organizacyjnymi UE (instytucje UE), jest zapewnienie, aby przestrzegały one unijnych przepisów o ochronie danych oraz chroniły osoby fizyczne i ich podstawowe prawa do prywatności i ochrony danych.

Aby pomóc w osiągnięciu tego celu, udzielamy instytucjom UE wskazówek, zaleceń, uwag i opinii, przeprowadzamy audyty, oferujemy szkolenia, a także inne zasoby mające na celu wyposażenie ich w odpowiednie narzędzia do wdrażania ochrony danych w praktyce podczas ich codziennych zadań, decyzji lub środków wymagających przetwarzania danych osobowych osób fizycznych.

3.1.1.
Nadzór nad przestrzenią wolności, bezpieczeństwa i sprawiedliwości

Wśród tematów, które wymagały naszej interwencji, szczególny nacisk położono na nadzór nad unijną przestrzenią wolności, bezpieczeństwa i sprawiedliwości, który obejmuje takie obszary polityki jak zarządzanie granicami zewnętrznymi, współpraca sądowa w sprawach cywilnych i karnych, a także azyl, migracja, zwalczanie przestępczości. Przestrzeń wolności, bezpieczeństwa i sprawiedliwości obejmuje takie unijne agencje jak Europol - Agencja Unii Europejskiej ds. Współpracy Wymiarów Sprawiedliwości w Sprawach Karnych, Frontex - Europejska Agencja Straży Granicznej i Przybrzeżnej, EPPO - Prokuratura Europejska, Eurojust - Agencja Unii Europejskiej ds. Współpracy Wymiarów Sprawiedliwości w

Sprawach Karnych. Nasza rola w tym obszarze była bardzo istotna, przede wszystkim zważywszy na charakter informacji szczególnie chronionych będących w trakcie przetwarzania oraz znaczący wpływ, jaki mogłoby to mieć w przypadku niewłaściwego zarządzania.

3.1.2.
Przekazywanie danych osobowych do państw niebędących członkami UE/EOG

Temat międzynarodowego przekazywania danych osobowych do państw spoza UE lub Europejskiego Obszaru Gospodarczego (EOG) również w coraz większym stopniu przykuwał naszą uwagę na przestrzeni lat, także w 2022 r., wymagając od nas mobilizacji znacznych zasobów, aby zapewnić odpowiedni poziom ochrony danych osobowych osób fizycznych.

W tym celu przeprowadziliśmy szereg inicjatyw i przedstawiliśmy porady i zalecenia dotyczące sposobu, w jaki instytucje UE powinny spełniać wymogi unijnego prawa o ochronie danych przy korzystaniu z usług lub zawieraniu umów z podmiotami mającymi siedzibę poza UE/EOG.

Korzystanie z produktów i usług spoza UE/EOG

Nasze inicjatywy obejmują prowadzone przez nas dochodzenia w sprawie korzystania przez instytucje UE z produktów i usług w chmurze, świadczonych przez podmioty spoza UE/EOG, w szczególności korzystania przez Komisję Europejską z Microsoft Office 365; ponadto obejmują wydawanie wytycznych i strategii politycznych, a także prowadzenie szkoleń dla instytucji UE. Działania te mają na celu zwiększenie świadomości instytucji UE na temat zagrożeń wynikających z korzystania z narzędzi lub prowadzenia działań w zakresie przetwarzania danych, które wiążą się z przekazywaniem danych poza

UE/EOG. Dążymy również do poszerzenia wiedzy instytucji UE na temat klauzul umownych i porozumień administracyjnych, a także innych środków mających na celu zapewnienie, aby dane osobowe osób fizycznych były chronione w zasadniczo równoważny sposób poza UE/EOG.

W ramach prac w tej dziedzinie i w świetle uprawnień EIOD zezwoliliśmy na przekazywanie szeregu danych osobowych do państw spoza UE/EOG, w których instytucje UE były w stanie udowodnić solidne procedury i środki ochronne na potrzeby zagwarantowania ochrony danych osobowych osób fizycznych w wyniku przekazywania danych.

Dążąc do tego, by dawać przykład w tej dziedzinie, pracujemy również nad wykorzystaniem alternatywnych produktów i usług podmiotów z siedzibą w UE/EOG, i zachęcamy instytucje UE do ich rozważenia.

3.1.3.
Audyt wielkoskalowych systemów informatycznych

Jednym z naszych kluczowych zadań jest zapewnienie ochrony danych osobowych i prywatności w kontekście wielkoskalowych systemów informatycznych w przestrzeni wolności, bezpieczeństwa i sprawiedliwości. Do naszych zadań należy m.in. audyt tych systemów w celu zapewnienia ich zgodności z przepisami dotyczącymi ochrony danych i prywatności.

Sprawując funkcję kontrolną, oceniamy środki techniczne i organizacyjne wprowadzone przez operatorów systemów i dbamy o to, by systemy uwzględniały ochronę prywatności już w fazie projektowania. Promujemy również najlepsze praktyki, dzieląc się ustaleniami i zaleceniami z kontroli z innymi unijnymi organami ochrony danych, wspierając kulturę doskonałości w zakresie ochrony danych i prywatności w całej UE.

W ramach działań kontrolnych staramy się zwiększyć świadomość instytucji UE i ogółu społeczeństwa na temat znaczenia ochrony danych i prywatności w wielkoskalowych systemach informatycznych. Pełniąc tę ważną rolę, pomagamy chronić dane osobowe obywateli UE i zapewniamy, aby wielkoskalowe systemy informatyczne spełniały najwyższe standardy ochrony danych i prywatności.

W październiku 2022 r. przeprowadziliśmy kontrolę na miejscu trzech wielkoskalowych systemów informatycznych w siedzibie eu-LISA - Agencji Unii Europejskiej ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości w Strasburgu:

Eurodac, europejskiej bazy danych odcisków palców do celów azylowych, która pomaga w rozpatrywaniu wniosków o udzielenie azylu.

SIS II, który wspiera bezpieczeństwo wewnętrzne i wymianę informacji na temat osób i przedmiotów między policją krajową, organami kontroli granicznej, organami celnymi, wizowymi i sądowymi.

VIS, który wspiera stosowanie wspólnej polityki wizowej UE oraz ułatwia kontrole graniczne i współpracę konsularną.

Kontrola objęła analizę metodyki i praktyk, które eu-LISA stosuje do opracowania i testowania, przy jednoczesnym zapewnieniu stosowania bezpieczeństwa i ochrony danych poprzez uwzględnienie ochrony danych w fazie projektowania i domyślną ochronę danych. Ponadto skontrolowaliśmy środki związane z zarządzaniem bezpieczeństwem informatycznym, incydentami dotyczącymi bezpieczeństwa IT i naruszenia ochrony danych osobowych, a także sprawdziliśmy stosowanie zaleceń z poprzednich kontroli.

3.2.
Ochrona naszej niezależności

Nowe rozporządzenie w sprawie Europolu: Skarga prawna EIOD do Trybunału Sprawiedliwości Unii Europejskiej

16 września 2022 r. zwróciliśmy się do Trybunału Sprawiedliwości Unii Europejskiej (TSUE) o stwierdzenie nieważności dwóch przepisów zmienionego rozporządzenia w sprawie Europolu, które weszło w życie 28 czerwca 2022 r. (sprawa T-578/22 - EIOD przeciwko Parlamentowi i Radzie). Te dwa przepisy mają wpływ na operacje dotyczące danych osobowych prowadzone w przeszłości przez Europol. Tym samym przepisy poważnie podważają pewność prawa w odniesieniu do danych osobowych osób fizycznych i zagrażają niezależności EIOD.

3.3.
Kształtowanie bezpieczniejszej cyfrowej przyszłości

Zgodnie ze strategią EIOD na lata 2020-2024 doceniamy inicjatywy, w których dane generowane w Europie są przekształcane w wartość dla europejskich przedsiębiorstw i osób fizycznych i przetwarzane zgodnie z europejskimi wartościami, aby kształtować bezpieczniejszą cyfrową przyszłość. Podążając w tym kierunku, doradzaliśmy prawodawcy unijnemu w wielu sprawach: na przykład w obszarze zdrowia, sztucznej inteligencji, czy też inicjatyw pomagających w zwalczaniu przestępczości.

Zazwyczaj udzielamy prawodawcy unijnemu porad w sprawie projektu aktu prawnego w postaci formalnych opinii lub komentarzy. Nasze **opinie** są wydawane w odpowiedzi na obowiązkowe wnioski Komisji Europejskiej, która jest prawnie zobowiązana do poszukiwania wskazówek dotyczących wszelkich wniosków ustawodawczych, a także zaleceń i wniosków kierowanych do Rady w kontekście umów międzynarodowych mających wpływ na ochronę danych. **Formalne uwagi** wydawane są w odpowiedzi na wniosek Komisji Europejskiej dotyczący projektów aktów wykonawczych lub aktów delegowanych.

W przypadku, gdy wniosek ustawodawczy lub inny stosowny wniosek ma szczególne znaczenie dla ochrony danych osobowych, Komisja Europejska może również skonsultować się z Europejską Radą Ochrony Danych (EROD). W takich przypadkach EIOD i EROD współpracują na potrzeby wydania **wspólnej opinii**.

Unijny akt w sprawie danych

EIOD wraz z EROD wydał wspólną opinię na temat wniosku dotyczącego aktu w sprawie danych, którego celem jest ustanowienie zharmonizowanych przepisów dotyczących dostępu do danych generowanych z szerokiego wachlarza produktów i usług oraz ich wykorzystania, w tym przedmiotów podłączonych do internetu („internet rzeczy"), wyrobów medycznych oraz wirtualnych asystentów.

W opinii podkreślono, że dane muszą być przetwarzane zgodnie z europejskimi wartościami, jeżeli chcemy kształtować bezpieczniejszą cyfrową przyszłość. Powstają nowe możliwości wykorzystania danych, dlatego należy zapewnić, aby istniejące ramy ochrony danych pozostały w pełni nienaruszone. Podkreśliliśmy również, że dostęp organów publicznych do danych powinien być zawsze odpowiednio zdefiniowany i ograniczony do tego, co jest absolutnie niezbędne i proporcjonalne – nie ma to miejsca w przypadku projektu aktu w sprawie danych.

Europejska przestrzeń danych dotyczących zdrowia

Wydaliśmy również wspólną opinię w sprawie wniosku dotyczącego europejskiej przestrzeni danych dotyczących zdrowia, w której opowiedzieliśmy się za wzmocnieniem ochrony elektronicznych danych dotyczących zdrowia.

Wniosek dotyczący europejskiej przestrzeni danych dotyczących zdrowia jest pierwszym z serii wniosków w sprawie wspólnych europejskich przestrzeni danych dotyczących poszczególnych dziedzin. Przestrzeń ta będzie nieodłączną częścią budowania Europejskiej Unii Zdrowotnej, dążącej do umożliwienia UE pełnego wykorzystania potencjału bezpiecznej i pewnej wymiany, wykorzystania i ponownego wykorzystania danych dotyczących zdrowia.

Wraz z EROD wyraziliśmy kilka obaw, zwłaszcza w odniesieniu do wtórnego wykorzystywania elektronicznych danych dotyczących zdrowia.

Sztuczna inteligencja

Jak podkreślono w strategii EIOD na lata 2020-2024, sztuczna inteligencja (AI) jest coraz częściej wykorzystywana w służbach publicznych i sądownictwie karnym. Naszym zadaniem jest zapewnienie, aby ta nowa technologia była wykorzystywana zgodnie z unijnymi przepisami o ochronie danych i z poszanowaniem prywatności osób fizycznych.

Oprócz innych inicjatyw, które wypracowaliśmy lub w których uczestniczyliśmy, wydaliśmy opinię w sprawie zalecenia dotyczącego decyzji Rady w sprawie upoważnienia do podjęcia negocjacji w imieniu Unii Europejskiej dotyczących konwencji Rady Europy w sprawie sztucznej inteligencji, praw człowieka, demokracji i praworządności (Konwencja w sprawie sztucznej inteligencji), którą uważamy za ważny krok w kierunku opracowania pierwszego prawnie wiążącego międzynarodowego instrumentu dotyczącego sztucznej inteligencji zgodnie z europejskimi standardami i wartościami w dziedzinie praw człowieka, demokracji i praworządności, uzupełniającego unijny akt w sprawie sztucznej inteligencji. Podkreśliliśmy jednak potrzebę uwzględnienia odpowiednich, silnych i jasnych gwarancji ochrony danych na potrzeby ochrony osób, na które stosowanie systemów sztucznej inteligencji może mieć wpływ.

Zwalczanie przestępczości

Opublikowaliśmy wybór opinii na temat różnych wniosków w dziedzinie prawa karnego.

Na przykład jedna z naszych opinii, wydana wspólnie z EROD, skupiła się na proponowanym rozporządzeniu mającym na celu zapobieganie niegodziwemu traktowaniu dzieci w celach seksualnych i jego zwalczanie (materiały przedstawiające niegodziwe traktowanie dzieci w celach seksualnych). Wyraziliśmy poparcie dla celów i założeń wniosku, wyrażając jednak zaniepokojenie, że może on stwarzać większe ryzyko dla jednostek, a tym samym dla ogółu społeczeństwa, niż dla przestępców ściganych w związku z materiałami przedstawiającymi niegodziwe traktowanie dzieci w celach seksualnych.

Inny godny uwagi przykład naszych zaleceń i wytycznych dotyczył tematu współpracy międzynarodowej w walce z przestępczością. W szczególności wydaliśmy opinię na temat dwóch wniosków: jeden w sprawie upoważnienia państw członkowskich UE do podpisania drugiego protokołu dodatkowego do „budapeszteńskiej" Konwencji o cyberprzestępczości, a drugi - upoważnienie państw członkowskich UE do ratyfikowania tego protokołu.

Chociaż prowadzenie dochodzeń i ściganie przestępstw jest uzasadnionym celem, w którym istotną rolę odgrywa współpraca międzynarodowa, w tym wymiana informacji, podkreśliliśmy, jak ważne jest, by UE zawarła trwałe umowy o wymianie danych osobowych z państwami spoza UE do celów egzekwowania prawa. Umowy te powinny być w pełni zgodne z prawem Unii, w tym z podstawowymi prawami do prywatności i ochrony danych.

3.4.
Przyszłość ochrony danych - skuteczne egzekwowanie przepisów w cyfrowym świecie

W czerwcu 2022 r. zorganizowaliśmy konferencję EIOD pt. „Przyszłość ochrony danych - skuteczne egzekwowanie przepisów w cyfrowym świecie", w której uczestniczyło ponad 2000 osób, zarówno na

miejscu w Brukseli, jak i online. W konferencji wzięło udział ponad stu prelegentów, odbyły się trzy sesje główne, szesnaście sesji tematycznych, dziewięć indywidualnych wystąpień głównych i pięć imprez towarzyszących. Dwudniowe wydarzenie sprzyjało kluczowym dyskusjom na temat przyszłości ochrony danych, ze szczególnym uwzględnieniem egzekwowania ogólnego rozporządzenia o ochronie danych (RODO).

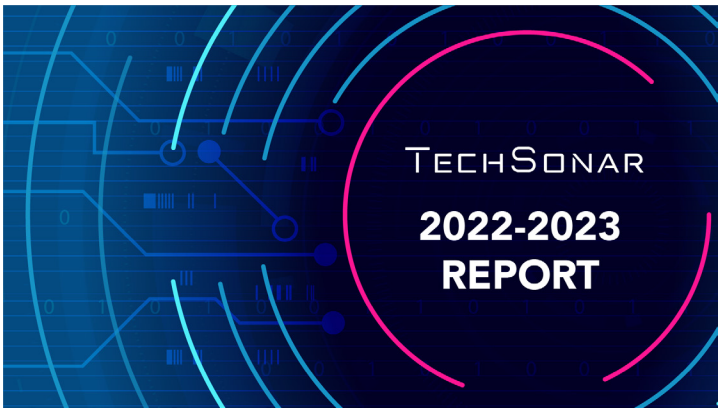
Nasza długoterminowa wizja przyszłości ochrony danych jest jasna: konieczne jest podejście do egzekwowania prawa w sposób ogólnoeuropejski, aby zapewnić rzeczywisty i spójny wysoki poziom ochrony osób fizycznych i wywiązywać się z obietnicy RODO.

3.5.
Monitorowanie technologii i perspektywiczność

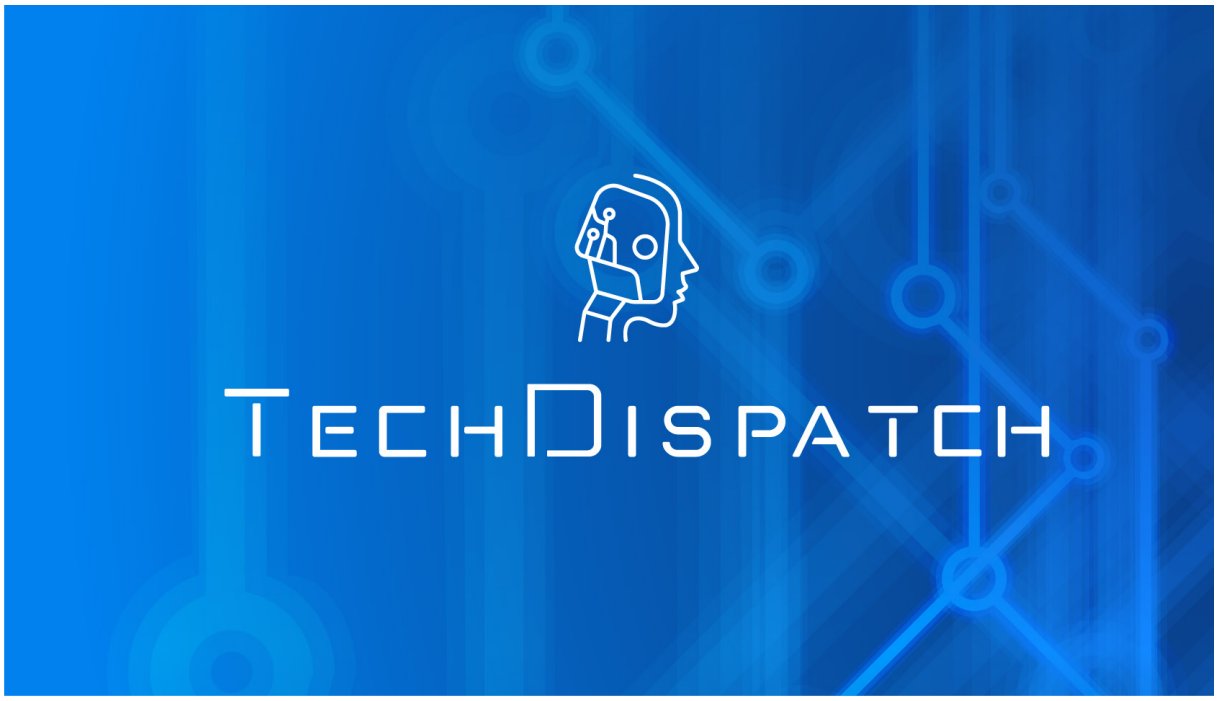
Jednym z trzech głównych filarów strategii EIOD na lata 2020-2024 jest **perspektywiczność**, a mianowicie nasza chęć bycia inteligentną instytucją, która w perspektywie długoterminowej uwzględnia tendencje w dziedzinie ochrony danych oraz kontekst prawny, społeczny i technologiczny.

Jednym ze sposobów stosowania prognoz w praktyce jest współpraca z ekspertami, specjalistami i organami ochrony danych. Dążymy do zrozumienia technologii, przeanalizowania ich wpływu na prywatność i ochronę danych osób fizycznych w celu dzielenia się wiedzą i pobudzania rozwoju tych nowych i powstających technologii w sposób zgodny z zasadami prywatności. **TechSonar** i **TechDispatch** to dwie z naszych inicjatyw w tym obszarze.

TechSonar ma na celu przewidywanie pojawiających się trendów technologicznych. Głównym celem tej inicjatywy jest lepsze zrozumienie przyszłych zmian w sektorze technologicznym z punktu widzenia ochrony danych. Opierając się na naszych wspólnych wysiłkach, poprzez rozpoznanie tendencji, burzę mózgów, przegląd, publikację, rzecznictwo i stałe monitorowanie, dążymy do wniesienia wkładu w szerszą debatę na temat prognoz w instytucjach UE. Opublikowane 10 listopada 2022 r. drugie roczne sprawozdanie TechSonar prezentuje pięć technologii wartych monitorowania w nadchodzącym roku. Są to: cyfrowa waluta banku centralnego, metawersum, dane syntetyczne, uczenie maszynowe [ang. „federated learning"] i systemy wykrywania fałszywych informacji.



TechDispatch ma na celu objaśnianie nowych przemian technologicznych. Sprawozdania w TechDispatch, za które zdobyliśmy nagrodę Global Privacy Assembly w 2021 r., wpisują się w szersze działania EIOD w zakresie monitorowania technologii. Każdy TechDispatch zawiera opisy nowej technologii, wstępną ocenę jej możliwego wpływu na prywatność i ochronę danych osobowych - w ich aktualnym rozumieniu - oraz linki do dalszych zalecanych lektur. Tegoroczna edycja TechDispatch, opublikowana w lipcu 2022 r., koncentruje się na Fediwersum [ang. „Fediverse"] i zrzeszonych platformach mediów społecznych.

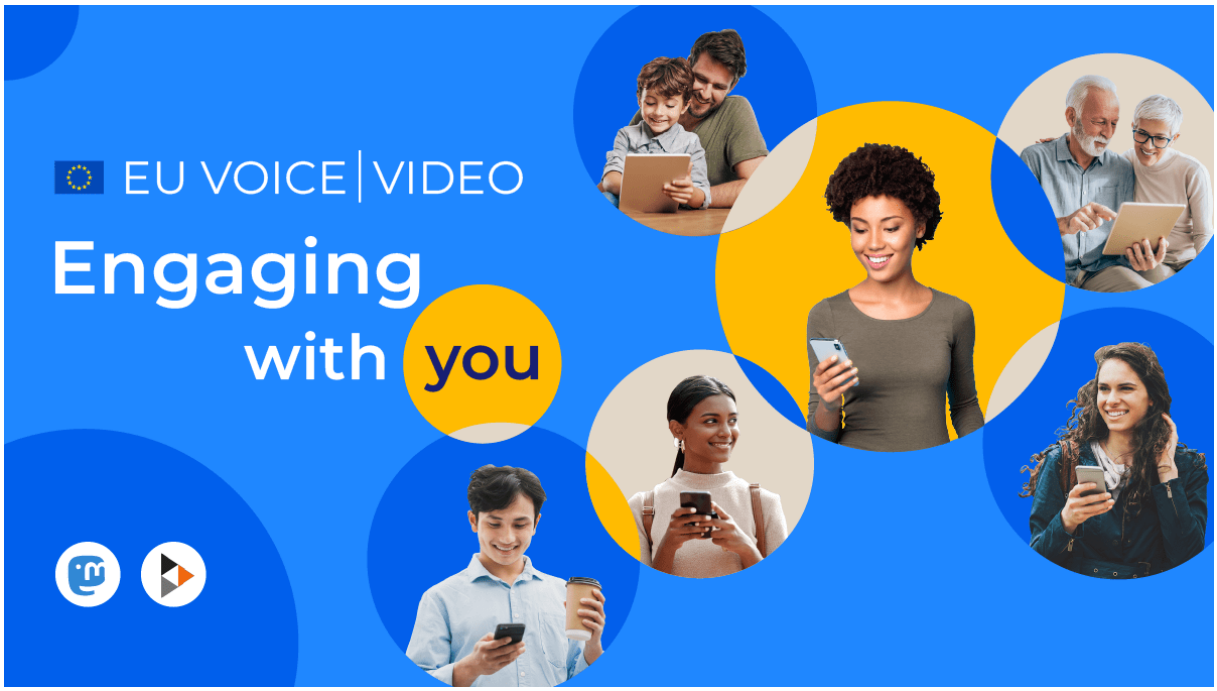


3.6.
Innowacje cyfrowe

Promowanie narzędzi przyjaznych ochronie danych, które przestrzegają praw podstawowych osób fizycznych i traktują je priorytetowo w całym procesie opracowywania i stosowania tych praw, jest jednym z naszych głównych celów strategii EIOD na lata 2020-2024. Aby osiągnąć te cele, poszukiwaliśmy i nadal poszukujemy alternatywnych narzędzi, zwłaszcza narzędzi komunikacji i współpracy, które są zgodne z unijnymi przepisami i normami w zakresie ochrony danych. Korzystając z tych alternatywnych narzędzi, dążymy do zachęcenia instytucji UE, by poszły za naszym przykładem. W ten sposób możemy wspólnie zminimalizować naszą zależność od monopolu, aby uniknąć szkodliwego uzależnienia od jednego dostawcy.

Odgrywamy istotną rolę w promowaniu innowacji cyfrowych, np. poprzez wykorzystywanie aplikacji i platform open source, które oferują sprzyjające prywatności alternatywy dla produktów i usług dostarczanych przez duże przedsiębiorstwa technologiczne. Nasze zaangażowanie na rzecz ochrony prywatności obejmuje zarówno sieci społecznościowe, jak i narzędzia współpracy, w tym inicjatywy takie jak EU Video, EU Voice oraz pilotażowe projekty Nextcloud.

W lutym 2022 r. zainicjowaliśmy fazę pilotażową dwóch platform mediów społecznościowych: EU Voice - aby publikować regularnie posty na temat naszych działań oraz EU Video, aby publikować materiały wideo jako dodatkowe, alternatywne kanały komunikacji umożliwiające interakcję z naszymi odbiorcami. Obie platformy są częścią zdecentralizowanych, bezpłatnych i ogólnodostępnych sieci mediów społecznościowych, które łączą użytkowników w środowisku zorientowanym na prywatność, bazując na oprogramowaniu Mastodon i PeerTube. Oba projekty kładą nacisk na ochronę danych i prywatność użytkowników, zapewniając unijnym organom regulacyjnym dostęp do narzędzi komunikacyjnych zgodnych z europejskimi wartościami i zasadami, bez uszczerbku dla ich danych osobowych.



Oprócz sieci społecznościowych popieramy przyjęcie alternatywnych narzędzi współpracy, które sprzyjają ochronie prywatności. Głównym przykładem tego zobowiązania jest projekt pilotażowy „Nextcloud". Nextcloud to otwarta, niehostowana platforma w chmurze, która umożliwia użytkownikom bezpieczne przechowywanie, wymianę i współpracę w zakresie plików, kalendarza i kontaktów. Propagując i wykorzystując narzędzia uwzględniające prywatność, takie jak Nextcloud, pokazujemy zaangażowanie we wspieranie ekosystemu cyfrowego, który przestrzega zasad ochrony danych i prywatności, w efekcie sprzyjając rozwojowi innowacyjnych i bardziej przyjaznych dla prywatności rozwiązań.

W czerwcu 2022 r. podczas konferencji EIOD pt. „Przyszłość ochrony danych: skuteczne egzekwowanie przepisów w cyfrowym świecie" opracowaliśmy również specjalne rozwiązanie wideokonferencyjne, które w pełni spełniało wymogi RODO i rozporządzenia (UE) 2018/1725 w zakresie przekazywania danych, co pozwoliło nam dać dobry przykład i utorować drogę do zapewnienia zgodności z wymogami ochrony danych. Istotne dla nas jako organu ochrony danych odpowiedzialnego za nadzór nad wszystkimi instytucjami UE było dowiedzenie, że możliwe jest wykazanie wzorcowej zgodności w odniesieniu do narzędzi wideokonferencyjnych, a w szczególności przestrzeganie przepisów dotyczących przekazywania danych osobowych do państw spoza UE i EOG.

3.7.
Przekazywanie informacji na temat ochrony danych

Wyjaśnienie, co robimy i dlaczego, w przejrzysty, jasny i interaktywny sposób należy do naszych celów jako organizacji, ponieważ istotne jest, aby obywatele UE rozumieli przysługujące im prawa do ochrony danych i sposób, w jaki mogą na nie wpływać.

Coraz większa obecność w internecie

EIOD ma ugruntowaną obecność w internecie w kilku kanałach mediów społecznościowych, a mianowicie Twitter (29 100 obserwujących), LinkedIn, gdzie w tym roku przekroczono 63 000 obserwujących, YouTube (2750), EU Voice (5100) i EU Video (690), dzięki którym jesteśmy w stanie łatwo i szybko dotrzeć do globalnej publiczności.

Ogółem tworzymy treści promujące kampanie zwiększające widoczność, a także relacje na żywo z udziału EIOD w wydarzeniach.

Przybliżenie ochrony danych obywatelom

Ochrona danych może być czasem dość skomplikowana, dlatego też staramy się publikować treści przeznaczone zarówno dla ekspertów, jak i osób niebędących ekspertami w kwestiach ochrony danych, przybliżając naszą pracę społeczeństwu.

Obejmuje to opracowywanie comiesięcznego newslettera, zawierającego krótkie, drobne wyjaśnienia na temat naszych najnowszych inicjatyw i ich wpływu na opinię publiczną; sporządzanie broszur informacyjnych, w których przedstawiamy kluczowe pojęcia z zakresu ochrony danych, a także prowadzenie kampanii w mediach społecznościowych oraz współpracę z innymi instytucjami UE w celu zwiększania świadomości w kwestiach związanych z ochroną danych.

Idąc dalej w tym kierunku, w tym roku zainaugurowaliśmy nową serię podcastów - Newsletter Digest, aby dotrzeć do szerszego grona odbiorców i poinformować ich o tym, co robimy, aby chronić ich dane.

Media i public relations

Często kontaktujemy się z mediami, zwłaszcza za pośrednictwem naszych komunikatów prasowych na temat ważnych inicjatyw w zakresie ochrony danych, które mają istotny wpływ w całej UE. W tym roku najwięcej uwagi poświęcono kilku tematom, takim jak nadzór nad Europolem i Frontexem oraz czerwcowa konferencja EIOD.

Ponadto utrzymujemy nasze stosunki z ogółem społeczeństwa, odpowiadając na publiczne prośby o informacje dotyczące naszej pracy i kompetencji jako instytucji UE oraz organizując wizyty studyjne w naszych siedzibach.

Zwiększenie tempa działań po pandemii COVID-19

Ograniczenia związane z COVID-19 były stopniowo minimalizowane, dlatego udało nam się wznowić organizowanie wydarzeń, zwiększyć liczbę działań, w których można uczestniczyć osobiście, przy jednoczesnym dostosowaniu wydarzeń do świata po pandemii COVID-19. Nasze wydarzenia i działania zostały opracowane z myślą o uczestnictwie zarówno przez internet, jak i osobiście, a jednocześnie pomogły nam jako organizacji zmniejszyć wpływ na środowisko. Z powodzeniem zorganizowaliśmy dwa duże wydarzenia hybrydowe: konferencję pt. „Przyszłość ochrony danych – skuteczne egzekwowanie przepisów w cyfrowym świecie" w czerwcu 2022 r., w której wzięło udział 2000 osób zarówno online, jak i osobiście, oraz „Konferencja nadzorcza –ochrona danych i wymiar sprawiedliwości w sprawach karnych" w listopadzie 2022 r.: ponad 200 osób zarówno online, jak i osobiście. W przypadku większości naszych wydarzeń dołożyliśmy wszelkich starań, aby nadać im bardziej ekologiczny wymiar, dzięki korzystaniu z lokalnych usług gastronomicznych, unikaniu marnotrawienia żywności, pozyskiwaniu materiałów firmowych na szczeblu lokalnym z materiałów wielokrotnego użytku.

Komunikacja oparta na współpracy

W 2022 r. współpracowaliśmy z innymi instytucjami UE, podejmując wspólne działania w zakresie komunikacji. W październiku połączyliśmy siły z ENISA – Agencją Unii Europejskiej ds. Cyberbezpieczeństwa i Komisją Europejską, aby przedstawić kampanię na rzecz Europejskiego Miesiąca Cyberbezpieczeństwa (ECSM) z okazji jego 10. rocznicy. W innym przypadku służyliśmy pomysłami i wsparciem w zakresie ochrony danych na potrzeby międzyinstytucjonalnej komunikacji online. W szczególności w EU Voice i projekcie pilotażowym EU Video ściśle współpracowaliśmy w ramach międzyinstytucjonalnej komunikacji online, aby zapewnić wytyczne redakcyjne i politykę serwerów, a także pomóc instytucjom UE biorącym udział w projekcie.

3.8.
Rozwijająca się organizacja

Aby wesprzeć nasze cele, zwłaszcza te określone w strategii EIOD na lata 2020-2024, poszerzyliśmy naszą organizację i wprowadziliśmy inne zmiany, aby lepiej odzwierciedlić nasze metody pracy.

Dostosowaliśmy wewnętrzną organizację EIOD, tworząc specjalną służbę prawną oraz sektor zarządzania i zgodności wewnętrznej z przepisami, aby zapewnić niezbędną wiedzę fachową umożliwiającą wykonywanie niektórych zadań.

Osiągnięcie naszych celów oznacza również, że musimy rozważnie zarządzać naszymi zasobami. W związku z tym podjęto znaczne wysiłki w zakresie planowania, wykonania i kontroli budżetu.

Przeprowadziliśmy również niezbędne przygotowania do otwarcia biura łącznikowego EIOD w Strasburgu, które zostanie oficjalnie zainaugurowane na początku 2023 r., w celu zacieśnienia współpracy międzyinstytucjonalnej i międzynarodowej oraz zapewnienia dodatkowego wsparcia doradczego w kwestiach ochrony danych.

Kluczowe wskaźniki efektywności w 2022 r.

EIOD korzysta z szeregu kluczowych wskaźników efektywności (KPI), które są pomocne w monitorowaniu jego wyników w świetle głównych celów określonych w strategii EIOD. Dzięki nim EIOD ma w razie konieczności możliwość dostosowania działań oraz zwiększenia wpływu swojej pracy i efektywności wykorzystania zasobów.

Poniższa tabela zawiera krótki opis każdego kluczowego wskaźnika efektywności i wyniki według stanu na 31 grudnia 2022 r. Wyniki te mierzy się w stosunku do początkowych celów lub w porównaniu z wynikami z poprzedniego roku wykorzystywanymi jako wskaźnik.

W 2022 r. osiągnęliśmy lub przekroczyliśmy - w niektórych przypadkach znacznie - wyznaczone cele dla ośmiu z dziewięciu kluczowych wskaźników efektywności, przy czym wartość jednego wskaźnika - KPI 8 dotyczącego stopnia obsadzenia stanowisk przewidzianych w planie zatrudnienia - była tylko nieznacznie poniżej wyznaczonego celu. Wyniki te dobrze odzwierciedlają pozytywną ścieżkę osiągania naszych celów strategicznych w ciągu całego roku.

KLUCZOWE WSKAŹNIKI EFEKTYWNOŚCI (KPI)		Wyniki na 31.12.2021 r.	Cel na 2022 r.
KPI 1 Wskaźnik wewnętrzny	Liczba inicjatyw, w tym publikacji, dotyczących monitorowania i promowania technologii zwiększających ochronę prywatności i danych, zorganizowanych lub współorganizowanych przez EIOD	13 inicjatyw	10 inicjatyw
KPI 2 Wskaźnik wewnętrzny i zewnętrzny	Liczba działań ukierunkowanych na międzydyscyplinarne rozwiązania w zakresie polityki (wewnętrzne i zewnętrzne)	8 działań	8 działań
KPI 3 Wskaźnik wewnętrzny	Liczba spraw rozpatrywanych w kontekście współpracy międzynarodowej (Globalne Zgromadzenie ds. Prywatności, Rada Europy, OECD, Światowa Sieć Egzekwowania Przepisów o Ochronie Prywatności, Międzynarodowa Grupa Robocza ds. Ochrony Danych w Telekomunikacji, Wiosenna Konferencja Europejskich Organów Ochrony Danych, organizacje międzynarodowe), w które EIOD wniósł znaczący wkład w postaci pisemnych opracowań	27 spraw	5 spraw
KPI 4 Wskaźnik zewnętrzny	Liczba akt, w przypadku których EIOD wystąpił w charakterze głównego sprawozdawcy, sprawozdawcy lub członka zespołu sporządzającego dokumentację w kontekście EROD	21 przypadków	5 przypadków

KPI 5 **Wskaźnik zewnętrzny**	Liczba opinii na podstawie art. 42 oraz wspólnych opinii EIOD-EROD wydanych na wniosek Komisji Europejskiej o konsultacje w sprawie aktów ustawodawczych	4 wspólne opinie 27 opinii	Punktem odniesienia jest poprzedni rok
KPI 6 **Wskaźnik zewnętrzny**	Liczba audytów/wizyt przeprowadzonych fizycznie lub zdalnie	4 audyty 2 wizyty	3 różne audyty/ wizyty
KPI 7 **Wskaźnik zewnętrzny**	Liczba obserwujących konta EIOD w mediach społecznościowych YouTube (YT), LinkedIn (L), Twitter (T), EU Voice oraz EU Video	YT - 2 750 L - 63 000 T - 29 100 EU Voice - 5 100 EU Video - 690	Wyniki za poprzedni rok + 10%
KPI 8 **Wskaźnik wewnętrzny**	Stopień obsadzenia stanowisk przewidzianych w planie zatrudnienia	86,9%	90%
KPI 9 **Wskaźnik wewnętrzny**	Wykonanie budżetu	98,2%	85%

edps.europa.eu

Urząd Publikacji
Unii Europejskiej

EDPS