

# Oświadczenie



## Oświadczenie 3/2024 w sprawie roli organów ochrony danych w ramach aktu w sprawie sztucznej inteligencji

Przyjęte 16 lipca 2024 r.

Europejska Rada Ochrony Danych przyjęła następujące oświadczenie:

### 1 KONTEKST I CEL NINIEJSZEGO OŚWIADCZENIA

1. W dniu 12 lipca 2024 r. rozporządzenie (UE) 2024/1689 w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji (akt w sprawie sztucznej inteligencji, zwany dalej „aktem w sprawie AI”) oraz zmiany niektórych aktów prawnych Unii zostało opublikowane w Dzienniku Urzędowym<sup>1</sup>.
2. Akt w sprawie AI ustanawia zharmonizowane przepisy dotyczące wprowadzania do obrotu, oddawania do użytku i wykorzystywania sztucznej inteligencji (zwanej dalej „AI”) zgodnie z nowymi ramami prawnymi i wymaga nadzoru rynku w rozumieniu rozporządzenia (UE) 2019/1020<sup>2</sup>. Jak stwierdzono w art. 1 ust. 1, celem aktu w sprawie AI jest poprawa funkcjonowania rynku wewnętrznego i wspieranie innowacji przy jednoczesnym promowaniu upowszechnienia zorientowanej na człowieka i godnej zaufania sztucznej inteligencji oraz zapewnieniu zdrowia, bezpieczeństwa i wysokiego poziomu ochrony praw podstawowych zapisanych w Karcie praw podstawowych Unii Europejskiej (zwanej dalej „Kartą”), w tym w odniesieniu do podstawowych praw do prywatności i ochrony danych osobowych (odpowiednio w art. 7 i 8 Karty).

---

<sup>1</sup> Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) (Tekst mający znaczenie dla EOG), Dz.U. L, 2024/1689 z 12.7.2024, ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>.

<sup>2</sup> Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/1020 z dnia 20 czerwca 2019 r. w sprawie nadzoru rynku i zgodności produktów oraz zmieniające dyrektywę 2004/42/WE oraz rozporządzenia (WE) nr 765/2008 i (UE) nr 305/2011 (Tekst mający znaczenie dla EOG).

3. Z tej perspektywy akt w sprawie AI i unijne przepisy dotyczące ochrony danych (w szczególności RODO<sup>3</sup>, rozporządzenie UE o ochronie danych<sup>4</sup> i dyrektywa o ochronie danych w sprawach karnych<sup>5</sup>, jak również dyrektywa o prywatności i łączności elektronicznej<sup>6</sup>) muszą być co do zasady<sup>7</sup> traktowane (i konsekwentnie interpretowane) jako instrumenty uzupełniające i wzajemnie się wzmacniające. Należy tak czynić zarówno pod względem celów prawa, jak i pod względem zapewnianej ochrony, w tym praw osób, których dane dotyczą (które można również zakwalifikować jako „osoby, których dane dotyczą” zgodnie z RODO). Ponadto należy podkreślić, że unijne prawo ochrony danych ma pełne zastosowanie do przetwarzania danych osobowych związanych z cyklem życia systemów AI, jak wyraźnie uznano w art. 2 ust. 7 aktu w sprawie AI (zob. również motywy 9 i 10).
4. W rzeczywistości przetwarzanie danych osobowych (które często jest ściśle powiązane z danymi nieosobowymi) w całym cyklu życia systemów AI – a w szczególności w całym cyklu życia tych systemów AI, które stwarzają wysokie zagrożenie dla praw podstawowych<sup>8</sup> – wyraźnie stanowi (i nadal będzie stanowił) kluczowy element różnych technologii objętych zakresem definicji AI, jak zapisano w art. 3 ust. 1 aktu w sprawie AI. Z tych powodów krajowe organy ochrony danych (zwane dalej „organami ochrony danych”) podejmowały działania w związku z tymi zmianami technologicznymi<sup>9</sup>, a EROD, która uważnie śledziła proces legislacyjny dotyczący aktu w sprawie AI<sup>10</sup>, zaczęła już badać wzajemne, wieloaspektowe powiązania tego aktu z unijnym prawem o ochronie danych.

---

<sup>3</sup> Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Tekst mający znaczenie dla EOG), Dz.U. L 119 z 4.5.2016, s. -881.

<sup>4</sup> Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Tekst mający znaczenie dla EOG) Dz.U. L 295 z 21.11.2018, s. 39-98.

<sup>5</sup> Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylenia decyzji ramowej Rady 2008/977/WSiSW, Dz.U. L 119 z 4.5.2016, s. 89-131.

<sup>6</sup> Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej), Dz.U. L 201 z 31.7.2002, s. 37-47.

<sup>7</sup> W szczególności w odniesieniu do zdalnej identyfikacji biometrycznej akt w sprawie AI stanowi *lex specialis* w stosunku do dyrektywy o ochronie danych w sprawach karnych (art. 5 ust. 1 lit. h) aktu w sprawie AI).

<sup>8</sup> W tym względzie zob. największą część systemów AI wymienionych w załączniku III do aktu w sprawie AI.

<sup>9</sup> Było to widoczne w unijnych jurysdykcjach za pośrednictwem stanowisk, konsultacji publicznych, wysłuchań parlamentarnych, wytycznych, opinii związanych z ocenami skutków dla ochrony danych, dochodzeń, środków naprawczych i (czasami) sankcji. Organy ochrony danych uczestniczą również w różnych piaskownicach regulacyjnych.

<sup>10</sup> Zob. w szczególności Wspólną opinię EROD-EIOD nr 5/2021 w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji), 18 czerwca 2021 r. (zwaną dalej „Wspólną opinią EROD i EIOD nr 5/2021”); Oświadczenie EROD w sprawie pakietu usług cyfrowych i strategii w zakresie danych przyjęte 18 listopada 2021 r.

5. W niniejszym oświadczeniu EROD pragnie dodatkowo zwrócić uwagę na kwestie nadzoru i koordynacji, które mogą pojawić się w związku z wyznaczaniem przez państwa członkowskie właściwych organów<sup>11</sup> w obszarach, które są tak ściśle powiązane z kwestiami ochrony danych osobowych. Należy wziąć pod uwagę, że na poziomie krajowym ramy egzekwowania aktu w sprawie AI będą musiały zostać sporządzone w przyszłym roku po wejściu w życie aktu w sprawie AI w ścisłej współpracy z jednym lub większą liczbą ustanowionych lub wyznaczonych „właściwych organów krajowych” (zwanym dalej „właściwymi organami krajowymi”), w szczególności organów nadzoru rynku (zwanym dalej „organami nadzoru rynku”)<sup>12</sup>, współdziałających zarówno ze sobą, jak i z organami ochrony danych i innymi organami zajmującymi się ochroną praw podstawowych.<sup>13</sup> EROD jest świadoma, że niektóre państwa członkowskie podjęły już decyzję o wyznaczeniu organów nadzoru rynku. W takich przypadkach niektóre zalecenia zawarte w niniejszym oświadczeniu mogą już nie być w pełni aktualne.
6. Jak już stwierdzono we Wspólnej opinii EROD i EIOD<sup>14</sup>, nowe ramy egzekwowania przepisów powinny zawierać uznanie znaczącej roli organów ochrony danych na szczeblu krajowym, w szczególności ze względu na ich doświadczenie i wiedzę fachową zdobytą przy opracowywaniu wytycznych i najlepszych praktyk oraz prowadzeniu działań w zakresie egzekwowania prawa w kwestiach związanych z AI w odniesieniu do przetwarzania danych osobowych zarówno na szczeblu krajowym, jak i międzynarodowym<sup>15</sup>. Organy ochrony danych okazały się i wciąż okazują się podmiotami niezbędnymi do tego, aby wdrożenie systemów AI w różnych sektorach odbywało się w sposób bezpieczny, oparty na poszanowaniu praw i pewny.
7. Należy również podkreślić, że wyznaczenie organów ochrony danych jako organów nadzoru rynku przyniosłoby korzyści wszystkim zainteresowanym stronom w łańcuchu wartości AI, dzięki istnieniu pojedynczego punktu kontaktowego i ułatwianiu interakcji między różnymi organami regulacyjnymi, których dotyczy zarówno akt w sprawie AI, jak i unijne przepisy o ochronie danych.
8. Ponadto, w świetle aktu w sprawie AI, EROD postrzega następujące kwestie jako szczególnie ważne:
  - organy ochrony danych, oprócz swej wiedzy fachowej w zakresie technologii AI, posiadają też kwalifikacje w wielu obszarach, o których mowa w art. 70 ust. 3 aktu w sprawie AI, takich jak przetwarzanie danych i bezpieczeństwo danych, oraz w zakresie oceny zagrożeń dla praw podstawowych stwarzanych przez nowe technologie;
  - organy ochrony danych, ze względu na swoją pełną niezależność<sup>16</sup>, mogą zapewnić skuteczny niezależny nadzór nad systemami AI, zgodnie z wymogami art. 70 ust. 1 aktu w sprawie AI<sup>17</sup>;
  - Zgodnie z art. 74 ust. 8 aktu w sprawie AI organy ochrony danych – lub inne organy spełniające te same wymogi dotyczące niezależności (na warunkach określonych w art. 41–44 dyrektywy

---

<sup>11</sup> Zob. motyw 153 aktu w sprawie AI.

<sup>12</sup> Zob. art. 3 ust. 48 aktu w sprawie AI.

<sup>13</sup> Zob. art. 77 i motyw 157 aktu w sprawie AI.

<sup>14</sup> Zob. w szczególności pkt 47 i nast. Wspólnej opinii EROD i EIOD nr 5/2021.

<sup>15</sup> Organy ochrony danych od dłuższego czasu są aktywne oraz współpracują ze sobą w zakresie różnych tematów związanych z systemami AI na różnych forach międzynarodowych (Okrągły Stół Organów Ochrony Danych i Prywatności grupy G7, międzynarodowa organizacja Global Privacy Assembly (GPA), Międzynarodowa Grupa Robocza ds. Ochrony Danych w Technologii, Rada Europy, międzynarodowe organizacje normalizacyjne itp.) oraz poprzez swoich przedstawicieli na forum OECD. To zintegrowanie działań jest szczególnie ważne w obecnym kontekście, w którym regulacje dotyczące AI są przedmiotem szeroko zakrojonych dyskusji na całym świecie, zwłaszcza w odniesieniu do opracowywania norm.

<sup>16</sup> Zob. art. 8 ust. 3 Karty oraz art. 16 ust. 2 Traktatu o funkcjonowaniu Unii Europejskiej (zwanego dalej „TFUE”).

<sup>17</sup> Zob. również motywy 79 i 80 aktu w sprawie AI.

(UE) 2016/680) – muszą zostać wyznaczone jako organy nadzoru rynku w odniesieniu do systemów AI wysokiego ryzyka wymienionych w pkt 1 załącznika III do aktu w sprawie AI, w zakresie, w jakim są wykorzystywane do celów ścigania przestępstw, kontroli granicznej oraz w kontekście wymiaru sprawiedliwości i demokracji, a także w odniesieniu do systemów AI wysokiego ryzyka wymienionych w pkt 6, 7 i 8 załącznika III do aktu w sprawie AI, które są kluczowymi elementami porządku demokratycznego;

- z perspektywy systematyki szczególnie cenne jest również to, że w przypadku, gdy unijne instytucje, organy, urzędy i agencje wchodzi w zakres aktu w sprawie AI, EIOD działa jako organ właściwy do ich nadzoru, jak przewidziano w art. 70 ust. 9 aktu w sprawie AI<sup>18</sup>;
- Ponadto w świetle przepisów zawartych w art. 26 ust. 9, art. 27 ust. 4 i załączniku VIII sekcja C pkt 5 aktu w sprawie AI oczekuje się ścisłego związku między oceną skutków dla ochrony danych a oceną wpływu na prawa podstawowe<sup>19</sup>.

## 2 ZALECENIA

9. EROD zaleca, aby państwa członkowskie wyznaczyły organy ochrony danych jako organy nadzoru rynku w odniesieniu do systemów AI wysokiego ryzyka, o których mowa w art. 74 ust. 8 aktu w sprawie AI. Ponadto EROD zaleca, aby biorąc pod uwagę opinie krajowych organów ochrony danych, państwa członkowskie rozważyły wyznaczenie organów ochrony danych jako organów nadzoru rynku w odniesieniu do pozostałych systemów AI wysokiego ryzyka wymienionych w załączniku III, w szczególności gdy takie systemy AI wysokiego ryzyka znajdują się w sektorach, które mogą mieć wpływ na prawa i wolności osób fizycznych w odniesieniu do przetwarzania danych osobowych, chyba że dla tych sektorów wyznaczenie jest obowiązkowe na mocy aktu w sprawie AI (np. sektor finansowy).
10. Biorąc pod uwagę powyższe, ponieważ pojedynczym punktem kontaktowym na mocy aktu w sprawie AI powinien być organ nadzoru rynku, jak określono w art. 70 ust. 2 aktu w sprawie AI, organy ochrony danych (działające w charakterze organów nadzoru rynku) powinny zostać wyznaczone jako pojedyncze punkty kontaktowe dla społeczeństwa i partnerów na szczeblu państw członkowskich i całej Unii. Pozostaje to bez wpływu na przedstawicieli państw członkowskich w Europejskiej Radzie ds. Sztucznej Inteligencji, którzy mogą być inni, jak wskazano w art. 65 ust. 4 lit. b) aktu w sprawie AI. Umożliwiłoby to również stosowanie jednolitego, spójnego i skutecznego podejścia w różnych sektorach.
11. Patrząc z szerszej perspektywy, istnieje potrzeba rozsądnej współpracy między organami nadzoru rynku a innymi podmiotami, których zadaniem jest nadzór nad systemami AI<sup>20</sup>, w tym organami ochrony danych, i należy ustanowić w tym zakresie jasne procedury w oparciu o art. 74 ust. 10 aktu w sprawie AI<sup>21</sup>. Procedury takie należy tworzyć i rozwijać zgodnie z zasadą lojalnej współpracy, przewidzianą w art. 4 ust. 3 Traktatu o Unii Europejskiej, jak podkreślił Trybunał Sprawiedliwości w

---

<sup>18</sup> Zob. również art. 3 ust. 48, art. 74 ust. 9 i art. 43 ust. 1 aktu w sprawie AI.

<sup>19</sup> Zob. art. 26 ust. 9, art. 27 ust. 4 i załącznik VIII pkt 5 aktu w sprawie AI.

<sup>20</sup> W szczególności w dziedzinie bezpieczeństwa produktów (np. w przypadku inteligentnych zabawek, zob. również załącznik I), konkurencyjności, usług cyfrowych i medialnych, usług finansowych, ochrony konsumentów oraz ochrony praw podstawowych.

<sup>21</sup> Zob. również w odniesieniu do działalności prowadzonej w ramach piaskownic regulacyjnych, art. 57 ust. 10 aktu w sprawie AI.

sprawie *Bundeskartellamt*<sup>22</sup>. W ten sposób można zapobiec niespójnościom między decyzjami podejmowanymi przez różne władze i organy nadzoru w ekosystemie cyfrowym oraz czerpać synergię generowaną przez spójne, skuteczne i uzupełniające się działania w zakresie egzekwowania prawa, z korzyścią dla osób fizycznych i pewności prawa.

12. Chociaż nadawanie nowych zadań i uprawnień w odniesieniu do nadzoru nad systemami AI może przebiegać sprawniej dzięki umiejętnościom prawnym i technicznym już obecnym w organach ochrony danych, sam fakt, że przewiduje się nowe zadania i uprawnienia dla organów ochrony danych, w tym w ramach ich funkcji jako organów nadzoru rynku, pociąga za sobą potrzebę zapewnienia przez państwa członkowskie odpowiednich dodatkowych zasobów ludzkich i finansowych.
13. Uwagi poczynione do tej pory dotyczące stosunków między krajowymi organami ochrony danych a organami nadzoru rynku na mocy aktu w sprawie AI mają analogiczne zastosowanie do działań nadzorczych prowadzonych przez Urząd ds. AI<sup>23</sup> w odniesieniu do modeli AI ogólnego przeznaczenia, które mogłyby być również odpowiednio trenowane pod kątem danych osobowych<sup>24</sup> i których wyniki mogą mieć wpływ na prywatność osób fizycznych i ich prawa do ochrony danych. W tym względzie akt w sprawie AI nie określa obecnie wyraźnej koordynacji działań Urzędu ds. AI i organów ochrony danych/EROD.
14. EROD podkreśla, że w każdym przypadku, gdy model lub system AI ogólnego przeznaczenia wiąże się z przetwarzaniem danych osobowych, może on – podobnie jak każdy inny system AI – wchodzić w zakres kompetencji nadzorczych, w stosownych przypadkach, odpowiednich krajowych organów ochrony danych (również współpracujących zgodnie z rozdziałem VII RODO) i EIOD (gdzie wchodzi w zakres rozporządzenia UE o ochronie danych). W związku z tym krajowe organy ochrony danych i EIOD muszą być odpowiednio zaangażowane w nadzór nad tymi systemami w przypadku pojawienia się pytań dotyczących kwestii wchodzących w zakres unijnych przepisów o ochronie danych. Jest to konieczne do zapewnienia zgodności z art. 8 Karty i art. 16 TFUE, w tym w odniesieniu do procesu oceny kodeksów praktyk, o których mowa w art. 56 aktu w sprawie AI.
15. W związku z tym EROD zwraca uwagę Komisji Europejskiej i unijnego Urzędu ds. AI, który jest jej częścią, na potrzebę współpracy z krajowymi organami ochrony danych i EROD oraz na potrzebę ustanowienia, w porozumieniu z nimi, odpowiednich zasad wzajemnej współpracy<sup>25</sup> w możliwie najbardziej skutecznym sposób i w pełnej zgodności z zasadą lojalnej współpracy przywołaną przez Trybunał Sprawiedliwości<sup>26</sup>.

W imieniu Europejskiej Rady Ochrony Danych

Przewodnicząca

(Anu Talus)

---

<sup>22</sup> Wyrok Trybunału Sprawiedliwości z dnia 4 lipca 2023 r., *Meta Platforms i in.* (Conditions générales d'utilisation d'un réseau social, C-252/21, ECLI:EU:C:2023:537), w szczególności pkt 53-63.

<sup>23</sup> Urząd ds. AI, o którym mowa w art. 64 aktu w sprawie AI, został ustanowiony decyzją Komisji z dnia 24 stycznia 2024 r. ustanawiającą Europejski Urząd ds. Sztucznej Inteligencji, C/2024/390, OJ C, C/2024/1459 z 14.2.2024.

<sup>24</sup> Zob. również załącznik XI, sekcja 1 ust. 1 lit. e) i ust. 2 lit. c) aktu w sprawie AI.

<sup>25</sup> Również w świetle art. 2 ust. 3 lit. c) i d), art. 3 i 6 decyzji Komisji z dnia 24 stycznia 2024 r. ustanawiającej Europejski Urząd ds. Sztucznej Inteligencji, C/2024/1459.

<sup>26</sup> Zob. przypis 22 do niniejszego oświadczenia.