FUNDACJA PANOPTYKON

Warszawa, 12 grudnia 2025 r.

Szanowny Pan
Dariusz Standerski
Sekretarz Stanu
Ministerstwo Cyfryzacji

Szanowny Panie Ministrze,

Dziękujemy za zaproszenie do złożenia uwag do propozycji tzw. omnibusów cyfrowych. Nasze stanowisko przedstawiamy poniżej.

Ze względu na napięty harmonogram prac, ograniczamy się do podkreślenia najważniejszych kwestii, które powinny zaalarmować polski rząd. W razie potrzeby pogłębionej analizy, odsyłamy Państwa do obszernych opracowań przygotowanych przez ekspertów z naszej sieci: European Digital Rights i noyb.

W razie pytań lub wątpliwości, zapraszamy do kontaktu.

Z poważaniem,

Szymielewicz

.....

Katarzyna Szymielewicz
Prezeska Fundacji

FUNDACJA PANOPTYKON

Opinia Fundacji Panoptykon dotycząca propozycji uproszczenia prawa unijnego tzw. omnibusów cyfrowych

I. Zarzuty natury fundamentalnej

Przedstawione propozycje nie zostały oparte na dowodach – a przynajmniej takie dowody nie zostały wraz z nimi opublikowane. Tymczasem decyzja o zmianie podstawowych zasad dotyczących ochrony prywatności i danych osobowych wymaga solidnych dowodów i rygorystycznej analizy. Komisja nie opublikowała oceny skutków proponowanych regulacji dla praw podstawowych ani nie przedstawiła danych wskazujących, że obecne przepisy szkodzą odpowiedzialnie działającym firmom. Nie wyjaśniła również, dlaczego trudności w egzekwowaniu prawa miałyby uzasadniać jego osłabienie. Co więcej, Komisja proponuje zastosowanie uproszczonej procedury, która nie pozostawia miejsca na demokratyczną debatę w Parlamencie Europejskim.

Pomimo obietnic Komisji, że reforma unijnych regulacji dotyczących cyfryzacji nie osłabi podstawowych praw i wolności obywateli, kluczowe fragmenty tego projektu zmieniają *zasady* przyjęte w ogólnym rozporządzeniu o ochronie danych (RODO) i dyrektywie o e-prywatności – dwóch aktach prawnych stanowiących fundament dla ochrony naszej prywatności w sieci.

Właśnie dlatego 470 organizacji społeczeństwa obywatelskiego, związków zawodowych i grup interesu publicznego wyraziło zaniepokojenie planami Komisji Europejskiej dotyczącymi wprowadzenia drastycznych zmian w przepisach chroniących prawa pracownicze i socjalne, prawa człowieka, prawa cyfrowe i środowisko. Już sam ten głos powinien być wystarczającym powodem, aby polski rząd ponownie rozważył swoje stanowisko.

Ponadto, na podstawie dogłębnej analizy, nie jesteśmy przekonani, że zmiany proponowane przez Komisję przyniosą korzyści małym i średnim przedsiębiorstwom. Mniejsze firmy zainwestowały już znaczne środki, aby dostosować się do RODO. Apelowały one o praktyczne wsparcie: szablony, standardowe formularze, spójne wytyczne oraz przewidywalne egzekwowanie przepisów. Większość z nich nie domagała się nowych podstaw prawnych, dodatkowych wyjątków ani zmienionych definicji. MŚP oczekiwały przede wszystkim jasności i spójnego egzekwowania prawa.

Tymczasem, propozycja Komisji wprowadza jeszcze większą złożoność prawną. Mniejsze firmy będą zatem musiały zmierzyć się z wypracowaniem nowej dokumentacji i nowych procedur,

podczas gdy większe podmioty zyskają szersze pole do interpretacji przepisów. Jest to sprzeczne z deklarowanym celem wspierania europejskich przedsiębiorstw i pomija wiele istotnych czynników leżących u podstaw braku konkurencyjności UE.

Prawdziwe uproszczenie nie wymaga zmian w przepisach, ale jaśniejszego określenia wymogów zgodności z prawem i spójnego ich egzekwowania. Dlatego uważamy, że Komisja Europejska powinna:

- zapewnić spójne stosowanie regulacji cyfrowych w państwach członkowskich;
- wspierać organy ochrony danych i innych regulatorów oraz zapewnić im zasoby, aby mogły działać skutecznie i w sposób skoordynowany;
- zapewnić, aby sygnały pochodzące z urządzeń końcowych były interoperacyjne i wiążące (w zakresie ochrony danych), bez wyjątków, które osłabiłyby ich skuteczność.

II. Szczegółowe uwagi

1. Proposal for Regulation on simplification of the digital legislation

1.1. Zmiana definicji danych osobowych

Projekt Komisji zmienia sposób rozumienia danych osobowych, ponieważ uzależnia poziom ochrony od oceny samego administratora (tj. od tego, czy biorąc pod uwagę swoje możliwości techniczne, może on zidentyfikować osobę, której dane dotyczą). Istnieje przypuszczenie, że chodzi o wyłączenie niektórych danych pseudonimizowanych (zob. art. 4 ust. 5 RODO) z zakresu stosowania RODO – wbrew obecnemu rozumieniu, zgodnie z którym są one objęte tym rozporządzeniem.

Wprowadziłoby to uznaniowość w interpretacji, które dane administratorzy uznają za „osobowe", co przełożyłoby się również na to, które z nich będą chronione zgodnie z RODO, a które nie. Ponieważ jest to podstawowa definicja RODO, jej zmiana będzie mieć poważne konsekwencje (np. w zakresie współpracy między administratorami a podmiotami przetwarzającymi, międzynarodowego przekazywania danych, wymogów bezpieczeństwa zgodnie z art. 32 RODO, dostępności praw i ochrony osób, których dane dotyczą) oraz – co stanowiłoby zagrożenie dla całej konstrukcji prawnej – rozszczelnienia fundamentów RODO.

Kluczową wadą tej definicji wydaje się być to, że opiera się ona wyłącznie na roli administratora danych oraz dostępnej mu wiedzy, podczas gdy jego partnerzy biznesowi, osoby, których dane dotyczą, oraz organy nadzorcze nie mają dostępu do odpowiednich informacji, które pozwoliłyby im ustalić, jakie możliwości łączenia danych ma administrator i – w związku z tym – jakiego standardu ich ochrony powinni oczekiwać.

W połączeniu z już i tak niespójnym egzekwowaniem przepisów i niskim poziomem zgodności z RODO taka zmiana definicji danych stworzyłaby nie tylko kolejną ogromną lukę, umożliwiającą nieuczciwym podmiotom nieprzestrzeganie praw wynikających z RODO, lecz także spowodowała niepewność co do prawa u wszystkich zainteresowanych podmiotów.

Dla szerszego grona administratorów taka zmiana prawdopodobnie nie doprowadziłaby do istotnego uproszczenia, ponieważ większość z nich nie będzie w stanie w znaczący sposób wykorzystać pseudonimizacji. W wielu przypadkach fakt, że te same dane mogą kilkakrotnie przechodzić między stanem objętym a nieobjętym przepisami, może dodatkowo skomplikować zarządzanie nimi.

Dla osób, których dane dotyczą, oraz organów nadzorczych rosnąca niepewność co do tego, czy przetwarzanie danych (w nieprzejrzystym systemie informatycznym) podlega przepisom RODO czy nie, sprawiłaby, że zarządzanie uprawnieniami wynikającymi z rozporządzenia stałoby się niezwykle skomplikowane.

1.2. Nowa podstawa do przetwarzania danych wrażliwych w systemach AI

Proponowany wyjątek od zasady wyrażonej w art. 9 RODO (przetwarzanie danych wrażliwych) otwiera szeroką furtkę do wykorzystywania tych danych w procesie tworzenia i trenowania systemów AI. Do tej pory firmy, które chciały wykorzystywać dane wrażliwe (np. wyniki badań lekarskich) do takich celów, musiały uzyskać wyraźne zgody. Dodatkowo tego rodzaju zgodę osoba, której dane dotyczą, zawsze mogła wycofać.

Komisja proponuje stworzenie nowej podstawy prawnej, umożliwiającej firmom zbieranie i późniejsze przetwarzanie danych wrażliwych do trenowania lub testowania systemów AI. Zgodnie z tą podstawą administratorzy mogliby przetwarzać wrażliwe dane osobowe w celu opracowywania i obsługi systemów sztucznej inteligencji. Jedyne, co przedsiębiorca musiałby wykazać, to to, że nie zbierał takich danych celowo, a ich usunięcie z wykorzystywanych zbiorów wymagałoby od niego „nieproporcjonalnego wysiłku".

Proponowane przepisy tworzą „przywilej" dla sztucznej inteligencji, który wykracza poza samo trenowanie („rozwijanie") systemów i obejmuje również ich „działanie". Może to oznaczać, że przetwarzanie danych będzie łatwiej uzasadnić prawnie, gdy będzie się odbywało za pośrednictwem systemu sztucznej inteligencji (podczas gdy to samo przetwarzanie w „tradycyjnej" bazie danych nie miałoby podstawy prawnej zgodnie z art. 9 ust. 2 RODO).

Obawiamy się, że w takim scenariuszu administratorzy danych zaczną wybierać technologię sztucznej inteligencji do przetwarzania wrażliwych danych osobowych, właśnie ze względu na niższy standard ochrony przewidziany w zmienionym art. 9 RODO.

1.3. Uzasadniony interes jako podstawa dla trenowania modeli AI

Projekt Komisji umożliwia trenowanie modeli AI na danych osobowych bez wyraźnej zgody użytkownika, opierając się jedynie na „uzasadnionym interesie" administratora. Jeśli ta zmiana wejdzie w życie, firmy rozwijające systemy AI będą mogły legalnie funkcjonować w modelu *opt-out*, czyli wykorzystywać potrzebne im dane, o ile podmiot danych się temu wyraźnie nie sprzeciwi.

Stwarza to ryzyko masowych naruszeń prawa do prywatności i ochrony danych, ponieważ osoby, których dane będą w ten sposób wykorzystywane, mogą nawet nie być tego świadome, co uniemożliwi im skuteczne zgłoszenie sprzeciwu.

Propozycja Komisji ani nie upraszcza, ani rozwiązuje problemy oceny, czy administratorzy danych mogą powołać się na prawnie uzasadniony interes w celu trenowania systemów AI. Nowy przepis w dużej mierze powiela art. 6 ust. 1 lit. f) RODO, a zawarte w nim dodatkowe elementy (np. niedookreślone zabezpieczenia) nie wydają się upraszczać stosowania art. 88c RODO. A przecież problem z trenowaniem sztucznej inteligencji nie wynikał z braku podstawy prawnej, (już teraz może nią być uzasadniony interes), ale na spełnieniu warunków przewidzianych w art. 6 ust. 1 lit. f) RODO, w tym przeprowadzenia testu równowagi. Oba etapy tego testu nie zostały w żaden sposób doprecyzowane ani uproszczone w art. 88c.

Kluczowa będzie zatem interpretacja tego przepisu. Jeśli uznamy, że przeszukiwanie całego Internetu i wszelkich dostępnych baz danych w celach – zasadniczo – komercyjnych (firmy zajmujące się sztuczną inteligencją są obecnie wyceniane na biliony dolarów) mieści się w pojęciu uzasadnionego interesu, trudno będzie odmówić tej samej podstawy prawnej innym podmiotom, na przykład w kontekście profilowania i zbierania danych behawioralnych użytkowników sieci.

Biorąc pod uwagę, że administratorzy mogą nie mieć bezpośredniego kontaktu z osobami, których dane dotyczą, a osoby te mogą nigdy nie dowiedzieć się o konkretnym administratorze, nie jest jasne, w jaki sposób „bezwarunkowe prawo do sprzeciwu" powinno być wdrażane w praktyce.

Ponadto, z punktu widzenia osób, których dane dotyczą, rezygnacja z setek lub tysięcy systemów sztucznej inteligencji poszczególnych administratorów również nie wydaje się stanowić uproszczenia.

1.4. Zautomatyzowane podejmowanie decyzji: nowa norma?

Art. 22 RODO daje podmiotom danych prawo do niepodlegania zautomatyzowanemu (tj. bez udziału człowieka) podejmowaniu decyzji, które wywołują skutki prawne lub podobne (np. zwolnienie z pracy, przyznanie kredytu, odmowa wizy etc.), a jednocześnie przewiduje wyjątki od tej zasady (np. gdy przetwarzanie jest niezbędne do zawarcia umowy, wymagane przez przepis prawa lub gdy osoba wyraziła zgodę).

Propozycja Komisji łączy ustępy 1 i 2 art. 22 RODO w jeden ustęp. Na pierwszy rzut oka wydaje się, że ust. 1 nie został znacząco zmieniony, a jedynie inaczej sformułowany. Jedyna istotna zmiana dotyczy zezwolenia na stosowanie zautomatyzowanego podejmowania decyzji w przypadku „konieczności" zawarcia lub wykonania umowy, niezależnie od oceny, czy *sama decyzja* mogłaby zostać podjęta w inny sposób niż w pełni zautomatyzowany.

Obecna wersja art. 22 ust. 2 lit. a) RODO stanowi, że „administrator musi być w stanie wykazać, że tego rodzaju przetwarzanie jest konieczne, biorąc pod uwagę, czy można zastosować metodę mniej ingerującą w prywatność" (zob. Wytyczne do Art. 29, s. 23). Proponowana zmiana wydaje się odchodzić od tej zasady. W przyszłości przy ocenie konieczności nie powinno mieć znaczenia, czy decyzja mogłaby zostać podjęta również przy użyciu środków innych niż wyłącznie zautomatyzowane.

Obawiamy się, że ta zmiana usankcjonuje szeroko praktykowane zawieranie umów z konsumentami bez udziału człowieka. Zautomatyzowane podejmowanie decyzji (np. zawieszenie konta, odmowa zawarcia umowy) staje się coraz częstsze i jest postrzegane przez osoby, których dane dotyczą, jako niezwykle frustrujące. Proponowana zmiana może przyspieszyć ten proces, ponieważ administratorzy danych będą mieli większą swobodę decydowania o tym, czy stosować zautomatyzowane podejmowanie decyzji przy zawieraniu lub wykonywaniu umowy.

1.5. Nowe zasady zgłaszania incydentów organom nadzorczym

Dotychczas administrator był zobowiązany do zgłaszania każdego naruszenia bezpieczeństwa przetwarzania danych, chyba że (w jego ocenie) istniało małe prawdopodobieństwo naruszenia praw osób, których dane dotyczą. Zgodnie z propozycją Komisji, przedsiębiorcy musieliby zgłaszać jedynie te incydenty, które *w ich ocenie* „prawdopodobnie spowodują wysokie ryzyko naruszenia danych osobowych", co znacząco podniesie próg dla obowiązkowych zgłoszeń.

Krótko mówiąc, dotychczasowy obowiązek zgłaszania organowi nadzorczemu

niemal każdego incydentu zostałby zastąpiony rozwiązaniem, w którym większość incydentów nie wymagałaby takiego zgłoszenia. Propozycja Komisji przewiduje ponadto wydłużenie terminu zgłaszania z 72 do 92 godzin.

Chociaż wydłużenie terminu zgłoszenia zmniejsza pilność w przypadku naruszenia danych, administrator nadal będzie zobowiązany do dokumentowania każdego incydentu (zob. art. 33 ust. 5 RODO), jego oceny i podjętych działań naprawczych.

Nawet jeśli powiadamianie organu nadzorczego nie będzie konieczne, nie jest jasne, czy taka zmiana faktycznie uprości procesy (poza odciążeniem organów przyjmujących zgłoszenia).

Z drugiej strony organy nadzorcze utraciłyby kluczowe informacje na temat szerszych zagrożeń dla cyberbezpieczeństwa, które mogłyby zostać wykorzystane do ograniczenia dalszych naruszeń oraz do lepszego zrozumienia skali i charakteru takich ataków.

Z punktu widzenia osób, których dane dotyczą, zmiana ta byłaby szczególnie odczuwalna w przypadkach, w których administratorzy (niesłusznie) twierdzą, że nie ma wysokiego ryzyka. Wówczas organy nadzorcze utraciłyby możliwość niezgodzenia się z tą oceną i nakazania administratorom powiadomienia o naruszeniu osób, których dane dotyczą.

1.6. Dostęp do danych osobowych na urządzeniu końcowym: bez ograniczeń?

Celem obecnego art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej jest ograniczanie dostępu do danych przechowywanych na urządzeniu końcowym, niezależnie od ich charakteru. Ten przepis zapewnia „integralność urządzenia", realizując art. 7 i 8 Karty Praw Podstawowych. Chodzi o każdy przypadek uzyskania dostępu do danych osobowych i nieosobowych znajdujących się na smartfonie, komputerze, telewizorze smart lub urządzeniu IoT. Ta norma dotyczy administratorów, którzy mają faktyczną możliwość „pobrania" danych z urządzenia lub przechowywania ich na nim, a nie tylko umieszczenia plików *cookie*.

Projekt Komisji zakłada włączenie zasady zgody, zawartej w dyrektywie o prywatności i łączności elektronicznej, do RODO. Zamiast wymagać uprzedniej zgody użytkownika przed przechowywaniem lub odczytywaniem informacji na urządzeniu, przedsiębiorstwa mogłyby powoływać się na uzasadniony interes lub niejasne podstawy, takie jak „bezpieczeństwo" lub„pomiar oglądalności". W efekcie stosowany byłby bardziej liberalny (nowy) art. 88a RODO w odniesieniu do danych osobowych, podczas gdy obecne (bardziej restrykcyjne) podejście zostałoby utrzymane w odniesieniu do dostępu do danych nieosobowych.

Sytuacja, w której mielibyśmy dwa podobne, ale różne systemy prawne w art. 5 ust. 3 e-prywatności i art. 88c RODO, jest z natury rzeczy myląca. Tym bardziej że różnica między nimi opierałaby się na (również niejasnej) definicji „danych osobowych" w zmienionym art. 4 ust. 1 i art. 41a RODO (omówionych powyżej), co potęgowałoby zamieszanie.

Osoby, których dane dotyczą, miałyby jeszcze większe trudności niż dostawcy usług internetowych w ustaleniu, czy w ich sytuacji ma zastosowanie przepis art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej (lub odpowiedni przepis prawa krajowego).

2. Proposal for Regulation on simplification for AI rules

2.1. Brak obowiązku zgłaszania systemu, jeśli jego dostawca uzna, że system „nie stwarza znaczącego ryzyka szkody dla zdrowia, bezpieczeństwa lub praw podstawowych", mimo że podpada pod Aneks III AI Act (tj. listę obszarów wysokiego ryzyka)

Obecnie w takim przypadku AI Act zobowiązuje dostawcę do rejestrowania systemu w unijnej bazie. Chodzi o to, żeby organy nadzorcze mogły taki przypadek wyłapać i zbadać. Usunięcie tego obowiązku stworzy lukę pozwalającą dostawcom systemów AI omijać nadzór i unikać transparentności. Organy nadzorcze dowiedzą się o istnieniu takich systemów dopiero w przypadku skargi lub ujawnionego incydentu. W efekcie systemy naruszające prawa człowieka mogą trafić na rynek bez jakiejkolwiek wcześniejszej kontroli, zwiększając ryzyko dyskryminacji, błędnych decyzji i naruszeń prywatności.

2.2. Osłabienie uprawnień krajowych organów ochrony praw podstawowych

Komisja proponuje odebranie organom ochrony praw podstawowych (takim jak PIP, RPD, PUODO) bezpośredniego dostępu do dokumentacji systemów AI wysokiego ryzyka. Byłyby one zmuszone korzystać z pośrednictwa krajowego organu nadzoru rynku, a to może spowolnić i utrudnić ich działania.

2.3. Opóźnienie wejścia w życie przepisów AIA dot. systemów wysokiego ryzyka

Komisja proponuje wydłużenie okresu przejściowego (w którym przepisy AI Act nie stosują się do systemów wysokiego ryzyka), jednocześnie zostawiając sobie furtkę do skrócenia tych terminów, jeśli uzna, że „rynek jest gotowy". Taka konstrukcja wprowadza niepewność dla organów nadzoru, przedsiębiorców i użytkowników systemów AI, utrudniając im zaplanowanie wdrożenia nowych procedur.