GP Partners
Gawroński, Biernatowski Sp.K.
info@gppartners.pl
al. Jana Pawła II 12
00-124 Warszawa

Warszawa, 25 sierpnia 2023 r.

Skarżący:
Łukasz Olejnik

reprezentowany przez:
r. pr. Macieja Gawrońskiego
GP Partners Gawroński, Biernatowski Sp.K.
al. Jana Pawła II 12, 00-124 Warszawa

Prezes Urzędu Ochrony Danych Osobowych
ul. Stawki 2
00-193 Warszawa

SKARGA
NA NIEZGODNE Z PRAWEM PRZETWARZANIE DANYCH OSOBOWYCH

Działając w imieniu skarżącego, Pana Łukasza Olejnika (pełnomocnictwo wraz z dowodem uiszczenia opłaty skarbowej w załączeniu) niniejszym

składam skargę

na niezgodne z prawem[1] przetwarzanie danych osobowych **Pana Łukasza Olejnika** przez **OpenAI OpCo, LLC**, 3180 18th Street, San Francisco, CA, USA, w ramach narzędzia ChatGPT

polegające na przetwarzaniu danych z naruszeniem zasady zgodności z prawem, rzetelności i przejrzystości, tj. z naruszeniem art. 5 ust. 1 lit. a RODO, niewykonaniu prawa dostępu do danych osobowych i informacji o przetwarzaniu danych osobowych zgodnie z art. 15 w zw. z art. 12 RODO, niewykonaniu prawa do sprostowania danych osobowych zgodnie z art. 16 w zw. z art. 12 RODO, a także przetwarzaniu w sposób sprzeczny z zasadą data protection by design, tj. z naruszeniem art. 25 ust. 1 RODO

oraz wnoszę:

1) o wszczęcie postępowania administracyjnego w sprawie przetwarzania danych osobowych Pana Łukasza Olejnika niezgodnie z prawem przez OpenAI OpCo, LLC,

2) o zobowiązanie OpenAI OpCo, LLC do wykonania zgodnie z art. 15 i 16 w zw. z art. 12 RODO praw Pana Łukasza Olejnika, tj. prawa dostępu do danych osobowych oraz do informacji o przetwarzaniu danych osobowych oraz prawa do sprostowania danych osobowych,

3) o zobowiązanie OpenAI do przedłożenia Prezesowi Urzędu Ochrony Danych Osobowych dokumentu oceny skutków dla ochrony danych (DPIA) dotyczącej przetwarzania danych osobowych w celach związanych z udostępnianiem narzędzia ChatGPT.

W niniejszej sprawie zastosowania nie znajduje zasada *one-stop-shop* wynikająca z art. 56 w zw. z art. 60 RODO (wynika to z logiki przedstawionej przez francuski organ nadzorczy, tj. CNIL w decyzji z dnia 21 stycznie 2019 r. o nałożeniu kary na Google[2]) – szerzej w pkt 2.2. skargi.

UZASADNIENIE

[1] Tj. niezgodnie z przepisami Rozporządzenia 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), („**RODO**").

[2] Délibération de la formation restreinte n° SAN – 2019-001 du 21 janvier 2019 prononçant une sanction pécuniaire à l'encontre de la société X, https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000038032552/

1. **STAN FAKTYCZNY**

1.1. OpenAI i ChatGPT

OpenAI. OpenAI OpCo, LLC („**OpenAI**") jest organizacją prowadzącą badania nad rozwojem sztucznej inteligencji i wdrażaniem narzędzi opartych o sztuczną inteligencję. OpenAI powstało w 2015 r. jako centrum badawcze działające non-profit w celu promowania sztucznej inteligencji przyjaznej dla człowieka. Od 2019 r. istnieje także spółka OpenAI LP, która rozwija narzędzia sztucznej inteligencji w celach komercyjnych.

ChatGPT. Do najbardziej znanych i popularnych pod względem liczby użytkowników narzędzi OpenAI należy **Chat Generative Pre-Trained Transformer**, w skrócie ChatGPT. ChatGPT to aplikacja chatbot służąca do generowania odpowiedzi na dane wprowadzone do chatu przez użytkownika w formie podpowiedzi, komunikatów (*prompt, input*). ChatGPT to narzędzie o uniwersalnym zastosowaniu, służące głównie do generowania treści, prowadzenia konwersacji o różnorodnych tematach i odpowiadania na pytania użytkowników.

ChatGPT wykorzystuje obecnie model językowy Generative Pre-trained Transformer 3,5 i 4 (GPT-3,5 i GPT-4). Modele GPT-3,5 i GPT-4 zostały opracowane za pomocą techniki uczenia maszynowego, przy użyciu dużych zbiorów danych (*big data sets*). Modele umożliwiają kompilowanie przez ChatGPT dużej ilości dostępnych powszechnie danych w celu generowania treści adekwatnych do podpowiedzi, zapytań użytkowników. Podstawowy schemat działania ChatGPT wygląda następująco:

> *Generuje on* [Chat-GPT] *teksty za pomocą techniki obliczeniowej zwanej „siecią neuronową typu transformer", a parametry sieci zostały ustalone poprzez wcześniejsze jej „trenowanie" na przykładach z olbrzymiej bazy danych tekstowych. Generalnie na wejściu program otrzymuje fragment tekstu w języku naturalnym, na przykład zapytanie, i ma za zadanie wygenerować inny tekst, sensowny i poprawny gramatycznie, który najbardziej pasuje jako kontynuacja danego fragmentu. Dopasowanie określone jest przez bazę danych tekstowych, na której program był trenowany. Można powiedzieć, że program generuje najbardziej prawdopodobną kontynuację tekstu na podstawie tekstów występujących w bazie*[3].

Wyniki generowane przez ChatGPT (w tym ich poprawność i aktualność) są w dużej mierze zależne od danych, którymi ChatGPT został zasilony, jak też od skuteczności modeli językowych. Bazy danych, z których korzysta ChatGPT w celu generowania tekstów pochodzą z wielu różnych źródeł i obejmują różnorodne kategorie danych, w tym także dane osobowe.

1.2. Przetwarzanie danych Pana Łukasza Olejnika przez OpenAI

Skarżący w niniejszej sprawie, Pan Łukasz Olejnik jest niezależnym badaczem zajmującym się m.in. cyberbezpieczeństwem, prywatnością i ochroną danych i autorem prac w tych obszarach.

Pan Łukasz Olejnik skierował do ChatGPT pytanie w celu wygenerowania swojej własnej biografii. W odpowiedzi ChatGPT wygenerował tekst z krótką biografią i opisem kariery zawodowej Pana Łukasza Olejnika. W tekście wygenerowanym przez ChatGPT znajdowały się częściowo nieprawdziwe informacje. Między innymi, ChatGPT wskazał:

> *Lukasz Olejnik has done extensive research on web browsing history and related topics such as online tracking, user privacy, and web security. He has written numerous articles and academic papers on the subject, and has been recognized for his contributions to the field. For example, in 2020, he co-authored a paper titled "What Web Browser History Tells Us About User Activity and Privacy"*

W powyższym fragmencie ChatGPT wskazał błędny tytuł i datę artykułu autorstwa Pana Łukasza Olejnika. W innym wygenerowanym fragmencie ChatGPT przypisał błędnie Panu Łukaszowi Olejnikowi autorstwo kilku artykułów.

Dowód 1: Zrzut fragmentu konwersacji Pana Łukasza Olejnika z ChatGPT

Pan Łukasz Olejnik, w uzupełnieniu pytań o swoją biografię skierował do ChatGPT dodatkowo pytanie o swoją płeć. ChatGPT odpowiedział, że Pan Łukasz Olejnik jest mężczyzną. W celu zrozumienia sposobu ustalenia i wygenerowania tej informacji Pan Łukasz Olejnik zapytał jak ChatGPT stwierdził jego płeć. ChatGPT w odpowiedzi opisał proces, który doprowadził do

---

[3] A. Kisielewicz, Bajki o sztucznej inteligencji i prawdziwe zagrożenia, https://wszystkoconajwazniejsze.pl/andrzej-kisielewicz-bajki-o-sztucznej-inteligencji-i-prawdziwe-zagrozenia/ (dostęp: 03.08.2023).

wygenerowania odpowiedzi. Z opisu wynika m.in., że ChatGPT przeanalizował dostępne informacje, w tym zdjęcia, informacje biograficzne, w tym dotyczące płci pochodzące z kilku różnych źródeł.

Dowód 2: Zrzut fragmentu konwersacji Pana Łukasza Olejnika z ChatGPT

1.3. Żądanie wykonania praw jednostki przez Pana Łukasza Olejnika i wymiana korespondencji z OpenAI[4]

Żądanie wykonania praw jednostki. W związku ze zidentyfikowanymi błędami w informacjach wygenerowanych przez ChatGPT Pan Łukasz Olejnik w dniu 27 marca 2023 r. skierował do OpenAI wiadomość mailową z prośbą:

1) o wskazanie wszelkich informacji dotyczących Łukasza Olejnika będących w posiadaniu OpenAI zgodnie z art. 12, 14 i 15 RODO,
2) o sprostowanie jego danych dotyczących artykułu, który według ChatGPT jest zatytułowany „What Web Browser History Tells Us About User Activity and Privacy".

W korespondencji z OpenAI Pan Łukasz Olejnik wskazał wyraźnie przepisy art. 12, 14 i 15 RODO jako podstawę prawną żądania, o którym mowa w pkt 1 powyżej. W uzupełnieniu Pan Łukasz Olejnik wymienił art. 13.2.f), 14.2.g) i 15.1.h) RODO jako przykład informacji, którą w szczególności chciałby uzyskać od OpenAI w odpowiedzi na swoje żądanie.

> *I would kindly **ask about all the information you have concerning Lukasz Olejnik** (the user in your system identified via email lukasz.w3c@gmail.com, but also the external data that you used). Concretely, since I am a citizen of the EEA, specifically the EU, please consider the principles as drawn directly from the GDPR. **With a specific attention to article 12, article 14, article 15.***
>
> *I would also ask you **to change the following bio**: "Lukasz Olejnik has done extensive research on web browsing history and related topics such as online tracking, user privacy, and web security. He has written numerous articles and academic papers on the subject, and has been recognized for his contributions to the field. For example, in 2020,"he co-authored a paper titled "What Web Browser History Tells Us A"out User Activity and Privacy""*
>
> *The mentioned title of the paper is incorrect, as well as the date.*
>
> *(…)*
>
> *I expect you to provide me the appropriate "logic involved in any automatic personal data processing", and the provisions of article 13(2)(f), not to mention 14(2)(g), and 15(1)(h).*

Dowód 3: Korespondencja e-mail Pana Łukasza Olejnika z OpenAI w sprawie przetwarzania danych osobowych w ramach ChatGPT.

Odpowiedź OpenAI. OpenAI nie wykonało żądań Pana Łukasza Olejnika zgłoszonych w korespondencji z dnia 27 marca 2023 r. W pierwszej wiadomości OpenAI poinformowało, że uznaje żądanie zgłoszone przez Pana Łukasza Olejnika za wykonane poprzez ogólne zablokowanie możliwości odpowiadania przez ChatGPT na pytania zawierające jego imię. W następnej odpowiedzi zawartej w wiadomości mailowej z dnia 18 kwietnia 2023 r. OpenAI wskazało, że nie ma możliwości skorygowania informacji o Panu Łukaszu Olejniku zawartej we fragmencie tekstu wygenerowanego przez ChatGPT.

---

[4] W celu przedstawienia rzeczywistej wymiany korespondencji w treści skargi przytaczane są fragmenty wiadomości w języku angielskim. W załączeniu do skargi przekazujemy zapis oryginalnej korespondencji (po angielsku) oraz dodatkowo tłumaczenie maszynowe całej korespondencji.

Poniżej fragment korespondencji od OpenAI:

> (…) *As some background, ChatGPT is designed to produce conversational text by predicting and outputting the next most likely word in response to a user's request. In some cases the next most likely word may also not be the most accurate one. We are working to improve the accuracy of our models, but we warn users that ChatGPT output may be false or factually inaccurate in the ChatGPT UI as well as Section 3(d) of our Terms of Use. Although* ***we are unable to change the information in the statement you have flagged****, we can address the issue by preventing your name from being generated by ChatGPT. Please let us know if you would like us to do this.*

W uzupełnieniu do powyższych informacji OpenAI wkleiło także do korespondencji link do Polityki Prywatności oraz załączyło dokument w formacie PDF zatytułowany „*OPENAI DATA SUBJECT ACCESS REQUEST RESPONSE*". Dokument zawierał informacje o przetwarzaniu danych przez OpenAI w odpowiedzi na żądanie dostępu do danych.

Dowód 3: Korespondencja e-mail Pana Łukasza Olejnika z OpenAI w sprawie przetwarzania danych osobowych w ramach ChatGPT.

Dalsza wymiana korespondencji. W odpowiedzi na powyższe informacje uzyskane od OpenAI z dnia 19 kwietnia 2023 r. Pan Łukasz Olejnik wskazał uzupełniająco jakie dodatkowe informacje o przetwarzaniu swoich danych przez OpenAI chciałby uzyskać (m.in. kategorie przetwarzanych danych oraz źródła, z których OpenAI uzyskało dane oraz kategorie odbiorców danych).

W korespondencji z dnia 6 maja 2023 r. OpenAI wskazało, że przetwarzało dane osobowe Pana Łukasza Olejnika w sposób zautomatyzowany. Choć odpowiedź OpenAI była częściowo myląca, zgodnie z informacją przekazaną w korespondencji „*OpenAI does process any personal data using automated decisions with a legal or similarly significant effect*." W dalszej części wiadomości OpenAI wskazuje:

> *This is due to the fact that ChatGPT is designed to provide a response to a prompt provided by a human user, and therefore there is always human involvement. As a result, Article 22 of the GDPR is not applicable to OpenAI's processing activities, so there is no requirement to notify data subjects of the information described in Articles 13(2)(f), 14(2)(g) and 15(1)(h) of the GDPR.*

Z tego drugiego fragmentu wynikałoby, że nie dochodzi do przetwarzania danych polegającego na podejmowaniu zautomatyzowanych decyzji przez OpenAI. Informacja przekazana przez OpenAI była zatem wewnętrznie sprzeczna i mogła prowadzić do różnych, przeciwnych wniosków. Powyższą informację OpenAI następnie skorygowało.

W tym samym mailu OpenAI przekazało dodatkowe informacje dotyczące podmiotów podprzetwarzających dane na zlecenie OpenAI (subprocessors) oraz dodatkowe mechanizmy bezpieczeństwa przetwarzanych danych (additional data controls), poprzez wklejenie linków do stron internetowych w domenie OpenAI.

W późniejszym mailu OpenAI z dnia 7 czerwca 2023 r., w odpowiedzi na dodatkowe pytania Pana Łukasza Olejnika, OpenAI przekazało kolejne ogólne informacje dotyczące sposobu funkcjonowania modeli GPT-3.5 i GPT-4, źródeł danych osobowych oraz podmiotów stowarzyszonych z OpenAI. Wiadomość z dnia 7 czerwca 2023 r. była ostatnią z wiadomości, którą Pan Łukasz Olejnik uzyskał od OpenAI w odpowiedzi na swoje pierwotne żądanie z dnia 27 marca 2023 r.

Dowód 3: Korespondencja e-mail Pana Łukasza Olejnika z OpenAI w sprawie przetwarzania danych osobowych w ramach ChatGPT.

1.4. Wątpliwości związane z poziomem ochrony danych osobowych przetwarzanych przez OpenAI

Istotnym kontekstem faktycznym sprawy przetwarzania danych osobowych Pana Łukasza Olejnika przez OpenAI są pojawiające się wątpliwości związane z poziomem ochrony danych osobowych przetwarzanych w ramach narzędzi sztucznej inteligencji, w szczególności ChatGPT.

Przejawem tych wątpliwości są liczne działania europejskich organów sprawujących nadzór w obszarze przetwarzania danych osobowych[5], podejmowane w celu zrozumienia i przeciwdziałania zagrożeniom, jakie ChatGPT i inne podobne narzędzia stwarzają dla danych osobowych i prywatności osób fizycznych. Niepokój związany z bezpieczeństwem danych osobowych przetwarzanych przez ChatGPT jest wywołany w szczególności lawinowym wzrostem zainteresowania tym narzędziem i szerokimi możliwościami jego zastosowania, jak też masowym zakresem danych gromadzonych w celu trenowania modeli w ramach ChatGPT przez OpenAI.

Przykładowe działania i stanowiska organów nadzorczych:

- Włoski organ nadzorczy Garante per la Protezione dei Dati Personali, który początkowo zablokował ogólny dostęp do ChatGPT wskazywał, m.in. że OpenAI nie ma podstawy prawnej do masowego gromadzenia i przechowywania danych osobowych na potrzeby trenowania ChatGPT, przetwarzane dane nie są prawidłowe, jak też OpenAI nie dokonuje sprawdzenia wieku użytkowników ChatGPT[6]. ChatGPT został później odblokowany ze względu na pewne ulepszenia wprowadzone przez OpenAI w zakresie prywatności i przetwarzania danych osobowych[7].
- Francuski organ nadzorczy CNIL zapowiedział, że zintensyfikuje w 2023 r. swoją aktywność w obszarze ochrony danych osobowych w związku z narzędziami *generative AI.* W swoim czteropunktowym planie działania w zakresie sztucznej inteligencji wskazał, że najważniejszym wyzwaniem przy projektowaniu i wykorzystywaniu takich narzędzi jak ChatGPT jest zapewnienie ochrony danych osobowych[8].
- Z kolei heski komisarz ds. ochrony danych w Niemczech zwrócił się bezpośrednio do OpenAI z szeregiem pytań, w których zwrócił uwagę na niejasny cel przetwarzania danych przez ChatGPT oraz niejasne źródła, z których ChatGPT czerpie swoją wiedzę[9].
- Brytyjski organ nadzorczy ICO w swojej ogólnej komunikacji z dnia 3 kwietnia 2023 r. zaznaczył, że:

  > *Organizacje opracowujące lub wykorzystujące generatywną sztuczną inteligencję powinny od samego początku brać pod uwagę swoje obowiązki w zakresie ochrony danych, przyjmując podejście privacy by design oraz privacy by default. Nie jest to opcjonalne - jeśli przetwarzasz dane osobowe, takie jest prawo[10].*

---

[5] ChatGPT is entering a world of regulatory pain in Europe, https://www.politico.eu/article/chatgpt-world-regulatory-pain-eu-privacy-data-protection-gdpr/ (dostęp: 04.08.2023).

[6] Oryginalna decyzja z dnia 30 marca 2023 r. wydana przez Garante per la protezione dei dati personali (https://garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870832, dostęp: 01.08.2023 r.).

[7] ChatGPT: OpenAI riapre la piattaforma in Italia garantendo più trasparenza e più diritti a utenti e non utenti europei, https://garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9881490 (dostęp: 01.08.2023 r.).

[8] Artificial intelligence: the action plan of the CNIL, 16 May 2023, https://www.cnil.fr/en/artificial-intelligence-action-plan-cnil, (dostęp: 01.08.2023 r.).

[9] Pressemitteilung, Anhörung, Hessischer Datenschutzbeauftragter fordert Antworten zu ChatGPT https://datenschutz.hessen.de/presse/hessischer-datenschutzbeauftragter-fordert-antworten-zu-chatgpt, (dostęp: 01.08.2023 r.).

[10] Generative AI: eight questions that developers and users need to ask, tłum. własne, https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/04/generative-ai-eight-questions-that-developers-and-users-need-to-ask/, (dostęp: 01.08.2023 r.).

- Ponadto, państwa należące do grupy G7 wypracowały wspólne stanowisko w sprawie sztucznej inteligencji. W oświadczeniu określono szereg obszarów, w których organy regulacyjne ds. ochrony danych uważają, że generatywne narzędzia sztucznej inteligencji mogą stwarzać ryzyko. Do wspomnianych obszarów należą: podstawa prawna przetwarzania danych osobowych, bezpieczeństwo danych osobowych, transparentność przetwarzania, rozliczalność administratorów oraz minimalizacja przetwarzania danych[11].

Przywołane stanowiska organów nadzorczych w przedmiocie zgodnego z prawem przetwarzania danych osobowych w ramach narzędzi generatywnej sztucznej inteligencji potwierdzają wątpliwości, które powstają w związku z przetwarzaniem danych osobowych Pana Łukasza Olejnika przez OpenAI.

2. UZASADNIENIE PRAWNE

2.1. Zastosowanie przepisów RODO do przetwarzania danych osobowych Pana Łukasza Olejnika przez OpenAI

Do przetwarzania danych osobowych Pana Łukasza Olejnika przez OpenAI w zakresie opisanym w punkcie 1 skargi mają zastosowanie przepisy RODO.

Materialny zakres zastosowania. Zgodnie z art. 2 ust. 1 RODO:

> *Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych*

Jak wynika z opisu stanu faktycznego w punkcie 1 – OpenAI przetwarzało i przetwarza dane osobowe Pana Łukasza Olejnika.

Jednocześnie do przetwarzania danych osobowych Pana Łukasza Olejnika przez OpenAI nie ma zastosowania żadne z wyłączeń opisanych w art. 2 ust. 2 RODO.

Terytorialny zakres zastosowania. Zgodnie z art. 3 ust. 2 RODO:

> *Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego w Unii, niezależnie od tego, czy przetwarzanie odbywa się w Unii.*

Jak wynika z Polityki prywatności udostępnionej na stronie internetowej OpenAI[12], OpenAI posiada także jednostkę organizacyjną z siedzibą w Irlandii. Wskazuje to, że do przetwarzania danych osobowych Pana Łukasza Olejnika doszło w związku z działalnością prowadzoną przez jednostkę organizacyjną OpenAI w Unii, choć administratorem danych osobowych decydującym o tym przetwarzaniu jest OpenAI z siedzibą w USA.

Przetwarzanie danych osobowych Pana Łukasza Olejnika jest objęte terytorialnym zakresem zastosowania RODO.

2.2. Wyłączenie zastosowania zasady *one-stop-shop*

Mimo tego, że OpenAI posiada reprezentanta, jednostkę organizacyjną w UE – do transgranicznego przetwarzania danych przez OpenAI nie ma zastosowania mechanizm *one-stop-shop* opisany w art. 56 RODO, w zw. z art. 60 RODO.

W niniejszej sprawie analogiczne zastosowanie znajduje logika przedstawiona przez francuski organ nadzorczy, tj. CNIL w decyzji z dnia 21 stycznie 2019 r. o nałożeniu kary na Google[13]. Francuski organ, wydając decyzję w sprawie Google wskazał, że chociaż Google ma siedzibę główną w Irlandii, to podmiot z siedzibą w Irlandii w rzeczywistości "nie miał uprawnień decyzyjnych" w odniesieniu do celów i sposobów transgranicznego przetwarzania danych. Z tego

---

[11] Roundtable of G7 Data Protection and Privacy Authorities Statement on Generative AI, 21 June 2023, https://www.ppc.go.jp/files/pdf/G7roundtable_202306_statement.pdf, (dostęp: 01.08.2023 r.).

[12] OpenAI Privacy policy, https://openai.com/policies/privacy-policy (dostęp: 04.08.2023).

[13] Délibération de la formation restreinte n° SAN – 2019-001 du 21 janvier 2019 prononçant une sanction pécuniaire à l'encontre de la société X, https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000038032552/

powodu CNIL zdecydował, że mechanizm *one-stop-shop* nie ma zastosowania, a zatem CNIL był właściwy do podjęcia decyzji[14].

Powyższa logika odpowiada okolicznościom niniejszej sprawy – w rzeczywistości to OpenAI z siedzibą w USA decyduje o sposobach i celach przetwarzania, w szczególności w odniesieniu do przetwarzania danych w ramach narzędzia Chat-GPT, które zostało opracowane przez podmiot amerykański. Z tego powodu w sprawie nie będzie miał zastosowania mechanizm *one-stop-shop*, a PUODO będzie właściwy do rozstrzygnięcia o zasadności niniejszej skargi.

2.3. Nieprawidłowości w przetwarzaniu danych osobowych Pana Łukasza Olejnika

Pan Łukasz Olejnik identyfikuje nieprawidłowości w przetwarzaniu jego danych osobowych przez OpenAI w następujących obszarach:

1) naruszenie podstawowej zasady przetwarzania danych zawartej w art. 5 ust. 1 lit. a RODO, tj. zasady przetwarzania danych zgodnie z prawem, rzetelnie oraz przejrzyście,
2) nieprawidłowe wykonanie praw osoby, której dane dotyczą, w tym prawa dostępu do danych oraz prawa do sprostowania danych,
3) niezapewnienie wystarczającego poziomu bezpieczeństwa przetwarzanych danych osobowych oraz naruszenie zasady data protection by design (privacy by design).

2.4. Naruszenie zasady zgodności z prawem, rzetelnie i w sposób przejrzysty (art. 5 ust. 1 lit. a RODO)

Podstawowym aspektem nieprawidłowości w przetwarzaniu danych osobowych Pana Łukasza Olejnika przez OpenAI jest naruszenie zasady zgodności z prawem, rzetelności i przejrzystości przetwarzania danych osobowych. Zasada ta ma charakter fundamentalny dla wszystkich obowiązków wynikających z RODO. Zgodnie z art. 5 ust. 1 lit. a RODO:

> *1. Dane osobowe muszą być:*
>
> *a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość");*

Zasada rzetelności oznacza w praktyce, że dane należy przetwarzać w sposób lojalny i uczciwy w stosunku do podmiotu danych[15]. Ze stanu faktycznego sprawy wynika, że OpenAI systemowo ignoruje przepisy RODO w zakresie przetwarzania danych na potrzeby trenowania modeli w ramach Chat-GPT, przez co m.in. nie doszło do prawidłowego poinformowania Pana Łukasza Olejnika o przetwarzaniu jego danych osobowych. Szczegółowe nieprawidłowości związane z podaniem informacji o przetwarzaniu Pana Łukasza Olejnika zostały opisane w dalszej części pisma.

---

[14] Argumentację CNIL zdaje się potwierdzać także pośrednio praktyka Europejskiej Rady Ochrony Danych Osobowych, która w zaktualizowanych Wytycznych 9/2022 w sprawie zawiadamiania o naruszeniach ochrony danych osobowych wskazała, że niezależnie od tego, że administrator poza UE posiada przedstawiciela w UE (tak jak jest to w przypadku OpenAI), to ten administrator będzie odpowiedzialny za zgłoszenie naruszenia do każdego z organów sprawujących nadzór w państwie, w którym mieszkają osoby, których dotyczyło naruszenie. Takiego postanowienia w poprzednich wytycznych nie było co wskazuje na częściową zmianę kierunku w rozumieniu mechanizmu one-stop-shop (https://cowprawiepiszczy.com/2022/11/naruszenie-ochrony-danych-osobowych-najwazniejsze-nowe-wskazowki-uodo-i-erod/, dostęp: 11.08.2023).
Link do wytycznych EROD:
https://edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf
Oryginalny tekst wytycznych: *However, the mere presence of a representative in a Member State does not trigger the one-stopshop system. For this reason the breach will need to be notified to every supervisory authority for which affected data subjects reside in their Member State. This (These) notification(s) shall be the responsibility of the controller.*

[15] M. Gawroński (red.) Ochrona danych osobowych. Przewodnik po ustawie i RODO ze wzorami, Warszawa 2018, str. 94.

Ze stanu faktycznego sprawy wynika, że:

1) OpenAI **naruszyło zasadę zgodności z prawem (legalności)** przetwarzania, ponieważ ze sposobu podejścia OpenAI do przetwarzania danych Pana Łukasza Olejnika, jak też wykonania obowiązków związanych z przetwarzaniem jego danych wynika, że OpenAI w rzeczywistości zignorowało przepisy RODO w zakresie przetwarzania do celów (i) trenowania modeli w ramach Chat-GPT, jak też (ii) generowania treści przez Chat-GPT (na podstawie pytań użytkowników).

   Co więcej, OpenAI odpowiadało na żądania Pana Łukasza Olejnika w sposób **fasadowy**, przekazując szereg informacji, które jednak nie zawierały konkretnej treści i wyjaśnień dotyczących przetwarzania danych Pana Łukasza Olejnika, w tym w ramach trenowania modeli, w zakresie wymaganym przepisami RODO.

2) OpenAI **naruszyło zasadę rzetelności przetwarzania danych**, ponieważ dane Pana Łukasza Olejnika były i są przetwarzane przez OpenAI w sposób niebudzący zaufania, nieuczciwy, a być może też niesumienny, skoro OpenAI nie jest w stanie wyczerpująco poinformować o tym przetwarzaniu.

   W tym kontekście celowe byłoby, aby organ, mając na uwadze powyższe naruszenia, najprawdopodobniej mające charakter systemowy, zażądał przedłożenia przez OpenAI dokumentu oceny skutków dla ochrony danych (DPIA). Dokument ten może stanowić istotny element oceny, czy przetwarzanie danych przez OpenAI w ramach narzędzi Chat-GPT odbywa się zgodnie z RODO. DPIA sporządzone przez OpenAI powinno obejmować historię wersji, tak aby możliwe było zweryfikowanie jakie zmiany były wprowadzane i jaki miały one wpływ na ocenę skutków dla ochrony danych.

3) OpenAI **naruszyło zasadę przejrzystości przetwarzania** – świadczy o tym przede wszystkim to, że Pan Łukasz Olejnik jako podmiot danych, wbrew swoim prawom, nie był w stanie uzyskać wyczerpującej i wiarygodnej informacji o tym, jak przetwarzane są jego dane osobowe. Co więcej.

Powyższe naruszenia dotyczą w szczególności danych przetwarzanych w celu trenowania modeli stosowanych przez ChatGPT. Jak wynika z informacji publicznie dostępnych ChatGPT bazuje na danych źródłowych (z różnych źródeł), jednak dane te „kończą się" na 2021 r.[16]. Musi to oznaczać, że OpenAI, w celu późniejszego korzystania z tych danych – wykonało ich kopię, co oznacza, że doszło do ich przetwarzania.

2.5. Nieprawidłowe wykonanie praw Pana Łukasza Olejnika jako osoby, której dane dotyczą

Żądanie wykonania praw. W korespondencji mailowej do OpenAI z dnia 27 marca 2023 r. Pan Łukasz Olejnik zażądał wykonania przez OpenAI następujących praw:

1) prawa dostępu do danych osobowych (art. 15 RODO),

2) prawa do sprostowania danych osobowych (art. 16 RODO),

2.5.A. Prawo dostępu do danych osobowych

Prawo dostępu do danych osobowych. Zgodnie z art. 15 ust. 1 RODO:

> *1. Osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji:*
>
> *a) cele przetwarzania;*
>
> *b) kategorie odnośnych danych osobowych;*
>
> *c) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;*

---

[16] https://rodoradar.pl/chat-gpt-i-sztuczna-inteligencja-a-przepisy-o-ochronie-danych-osobowych/

(„*Obecnie ChatGPT stanowi zamknięty model językowy, z bazą danych (w wersji bezpłatnej) aktualną na wrzesień 2021 r. Oznacza to, że model ten został wytrenowany na podstawie informacji dostępnych w sieci, i nie tylko, wyłącznie w tym właśnie okresie*.").

d) w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;

e) informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;

f) informacje o prawie wniesienia skargi do organu nadzorczego;

g) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą - wszelkie dostępne informacje o ich źródle;

h) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz - przynajmniej w tych przypadkach - istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Prawo dostępu do danych regulowane w art. 15 RODO obejmuje trzy aspekty – prawo do uzyskania potwierdzenia, że dane osobowe są przetwarzane, prawo do uzyskania określonych informacji o przetwarzaniu danych oraz prawo do uzyskania dostępu do przetwarzanych danych osobowych.

Sposób wykonania prawa przez OpenAI. OpenAI w celu wykonania prawa Pana Łukasza Olejnika przekazało w załączeniu do korespondencji mailowej z dnia 18 kwietnia 2023 r. dokument zatytułowany „OPENAI DATA SUBJECT ACCESS REQUEST RESPONSE". W dokumencie OpenAI przekazało informacje obejmujące:

a) cele przetwarzania danych,

b) kategorie przetwarzanych danych,

c) kategorie odbiorców danych,

d) okres retencji danych,

e) informacje o źródle danych, jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą,

f) informacje o zautomatyzowanych decyzjach

g) informacja o transferach danych

h) informacja o prawach osoby, której dane dotyczą

Dodatkowo w osobnej sekcji dokumentu OpenAI przekazało informację o sposobach uzyskania kopii danych osobowych, wskazując w tym zakresie następujące kategorii danych, do których Pan Łukasz Olejnik może uzyskać dostęp:

- nazwa i informacje o koncie użytkownika,
- informacje o rozliczeniach,
- adres IP,
- historia czatów, informacje o użytkownikach i dane dotyczące logowań,
- dane przesyłane przez użytkowników (tzw. *uploads*),
- komunikacja z działem wsparcia,
- aktywność na forach,

Nieprawidłowości. Jakkolwiek opisany zakres informacji, których OpenAI udzieliło Panu Łukaszowi Olejnikowi sprawia wrażenie odpowiadającego wymogom z art. 15 RODO, to w rzeczywistości żądanie Pana Łukasza Olejnika nie zostało wykonane prawidłowo, przez co doszło do naruszenia art. 15 RODO.

Brak informacji o przetwarzaniu i kopii danych przetwarzanych w celu trenowania modeli. Przede wszystkim OpenAI pomija w ramach podawanych informacji, także w Polityce prywatności dostępnej online[17] informacje o przetwarzaniu danych osobowych wykorzystywanych do trenowania modeli językowych stosowanych przez ChatGPT. Mimo tego, że we fragmencie

[17] OpenAI Privacy policy, https://openai.com/policies/privacy-policy (dostęp: 04.08.2023).

dotyczącym źródeł pochodzenia informacji OpenAI wskazuje, że dane wykorzystywane do trenowania modeli obejmują dane osobowe, tak naprawdę **OpenAI nie podaje żadnych informacji o operacjach przetwarzania obejmujących te dane**. OpenAI narusza tym samym podstawowy element prawa z art. 15 RODO, tj. obowiązek potwierdzenia, że dane osobowe są przetwarzane.

W szczególności OpenAI nie uwzględniło przetwarzania danych osobowych w związku z trenowaniem modeli w informacjach o kategoriach danych osobowych ani kategoriach odbiorców danych. Przekazanie kopii danych także nie obejmowało danych osobowych przetwarzanych na potrzeby trenowania modeli językowych. Jak się wydaje fakt przetwarzania danych osobowych w celu trenowania modeli OpenAI ukrywa lub co najmniej kamufluje intencjonalnie. Wynika to także z Polityki prywatności OpenAI, która w części merytorycznej pomija procesy związane z przetwarzaniem danych osobowych w zakresie trenowania modeli językowych.

OpenAI informuje, że nie wykorzystuje danych tzw. „treningowych" do identyfikacji osób ani zapamiętywania ich informacji i pracuje nad zmniejszeniem ilości danych osobowych przetwarzanych w zbiorze danych „treningowych". Jakkolwiek mechanizmy te korzystnie wpływają na poziom ochrony danych osobowych i są zgodne z zasadą minimalizacji (art. 5 ust. 1 lit. c RODO) to ich zastosowanie nie zmienia faktu, że **dane „treningowe" są przetwarzane i obejmują dane osobowe**. Do operacji przetwarzania tych danych mają zastosowanie przepisy RODO, w tym obowiązek udzielenia osobie, której dane dotyczą dostępu do danych oraz przekazania informacji wskazanych w art. 15 ust. 1 RODO.

Brak wystarczających informacji o odbiorcach danych. W informacji przekazanej Panu Łukaszowi Olejnikowi przez OpenAI na temat odbiorców jego danych osobowych wskazano wyłącznie ogólnie ujęte kategorie odbiorców (m.in. sprzedawcy i dostawcy usług, podmioty powiązane z OpenAI, podmioty trzecie). Taki sposób poinformowania o odbiorcach danych nie odpowiada wymogom art. 15 ust. 1 lit. c RODO, z którego wynika, że administrator powinien przekazać:

> *informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione*

Wprawdzie z samego przepisu nie wynika wprost, czy administrator powinien wskazać konkretnych odbiorców z oznaczeniem ich tożsamości (jeśli jest to możliwe) – jednak takie rozumienie art. 15 ust. 1 lit. c RODO jest przyjęte, a ostatnio zostało potwierdzone w orzeczeniu Trybunału Sprawiedliwości Unii Europejskiej z dnia 12 stycznia 2023 r. w sprawie C-154/21[18]. W odpowiedzi na pytanie prejudycjalne Trybunał wskazał, że:

> *Artykuł 15 ust. 1 lit. c) rozporządzenia 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)*
>
> *należy interpretować w ten sposób, że:*
>
> *przewidziane w tym przepisie prawo dostępu osoby, której dane dotyczą, do dotyczących jej danych osobowych oznacza, w przypadku gdy dane te zostały lub zostaną ujawnione odbiorcom, że na administratorze danych ciąży obowiązek podania tej osobie dokładnej tożsamości tych odbiorców, chyba że nie jest możliwe zidentyfikowanie tych odbiorców lub tenże administrator danych wykaże, że wnioski o uzyskanie dostępu złożone przez osobę, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne w rozumieniu art. 12 ust. 5 rozporządzenia 2016/679, w których to przypadkach administrator ten może wskazać tej osobie wyłącznie kategorie odnośnych odbiorców.*

Z powyższego wyroku wynika, że OpenAI powinno było wskazać w odpowiedzi na żądanie Pana Łukasza Olejnika **tożsamość wszystkich odbiorców danych, których OpenAI może zidentyfikować**. Dlatego wskazanie przez OpenAI wyłącznie kategorii wybranych odbiorców np. w przypadku dostawców usług dla OpenAI lub podmiotów powiązanych z OpenAI musiało stanowić naruszenie obowiązków nałożonych na OpenAI jako administratora danych osobowych. OpenAI ma możliwość zidentyfikowania tych odbiorców, zatem informacja przekazana Panu Łukaszowi Olejnikowi była zbyt ogólna.

[18] Wyrok TS z 12.01.2023 r., C-154/21, RW PRZECIWKO ÖSTERREICHISCHE POST AG., LEX nr 3454592.

Co więcej, OpenAI nie wskazało wśród kategorii odbiorców danych osobowych **osób korzystających z ChatGPT**. Osoby kierujące do ChatGPT pytanie o Pana Łukasza Olejnika mogą otrzymać od OpenAI jego dane osobowe (osoby te byłyby zatem odbiorcami danych, o których należałoby poinformować w ramach prawa dostępu). W tym przypadku zresztą właściwe byłoby wskazanie wyłącznie kategorii odbiorców danych, jako że nie byłoby możliwe zidentyfikowanie konkretnych odbiorców.

Powyższe naruszenia są tym bardziej ewidentne, uwzględniając że Pan Łukasz Olejnik wskazał wprost w korespondencji z dnia 19 kwietnia 2023 r. do OpenAI, że chciałby uzyskać konkretną informację o odbiorcach swoich danych osobowych. Nie mogło być zatem wątpliwości co do zakresu informacji żądanych przez Pana Łukasza Olejnika. Natomiast OpenAI, w odpowiedzi na dodatkowe pytania dotyczące odbiorców danych wskazało na listę podmiotów podprzetwarzających dane osobowe (tzw. *subprocessors*) na zlecenie OpenAI. Niewątpliwie informacja o podmiotach podprzetwarzających (art. 28 ust. 2 RODO) jest informacją inną niż informacja o odbiorcach danych osobowych i to ten drugi element jest objęty prawem dostępu zgodnie z art. 15 RODO. Informacje podane przez OpenAI były w tym zakresie niezgodne z treścią żądania, a w dodatku mylące.

Brak wystarczających informacji o źródłach danych. Wątpliwości budzi także sposób wykonania przez OpenAI prawa dostępu do danych w zakresie przekazania informacji dotyczącej źródeł danych osobowych, w przypadku gdy dane osobowe nie zostały zebrane od osoby, której dane dotyczą. Zgodnie z art. 15 ust. 1 lit. g RODO:

> *1. Osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji:*
>
> (…)
>
> *g) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą - **wszelkie dostępne informacje o ich źródle**;*

Z powyższego przypisu wynika wprost, że administrator powinien podać wszelkie dostępne informacje o źródle danych osobowych zebranych nie od osoby, której dane dotyczą. W tym zakresie OpenAI wskazało:

> *Aby rozwijać i ulepszać nasze usługi, pozyskujemy i analizujemy zbiory danych z publicznie dostępnych źródeł, takich jak Internet, lub od stron trzecich które wcześniej zweryfikowaliśmy.*

Przytoczony fragment to całość informacji, które OpenAI przekazało Panu Łukaszowi Olejnikowi w wykonaniu prawa dostępu do danych w zakresie, o którym mowa w art. 15 ust. 1 lit. g RODO. Trudno uznać, że tak podany zakres informacji obejmuje *wszelkie dostępne informacje* o źródle danych osobowych. W szczególności należałoby wskazać przynajmniej z jakich kategorii źródeł OpenAI korzysta w celu zbierania danych potrzebnych do trenowania modeli, jak też od jakich stron trzecich pochodzą dane. Sposób sformułowania art. 15 ust. 1 lit. g RODO daje uzasadnione podstawy, aby oczekiwać od administratora podania co najmniej powyższych informacji o źródłach danych osobowych.

Wnioski. Przedstawione okoliczności świadczą o tym, że OpenAI naruszyło art. 15 RODO ze względu na nieprawidłową realizację prawa dostępu do danych. W literaturze[19] wskazuje się, że:

> *Brak jednego z obowiązkowych elementów jakiejkolwiek komunikacji z podmiotem danych będzie uznany za naruszenie przepisów o ochronie danych.*

Naruszenie art. 15 RODO przez OpenAI stanowiło jednocześnie naruszenie podstawowej zasady zgodności z prawem, rzetelność i przejrzystości przetwarzania zapisanej w **art. 5 ust. 1 lit. a RODO**.

2.5.B. Prawo do sprostowania danych osobowych

Prawo do sprostowania danych osobowych. Zgodnie z art. 16 RODO:

> *Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia*

[19] M. Gawroński (red.) Ochrona danych osobowych. Przewodnik po ustawie i RODO ze wzorami, Warszawa 2018, str. 206.

niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

Z prawem do sprostowania danych ściśle związana jest zasada prawidłowości danych wyrażona w art. 5 ust. 1 lit. d RODO. W literaturze[20] wskazuje się, że:

Prawidłowość danych wymaga od nas wdrożenia procedur weryfikacji jakości danych i dbałości o jakość danych osobowych oraz umożliwienia realizacji prawa do sprostowania i aktualizacji danych (art. 16 RODO).

Sposób wykonania prawa przez OpenAI. W odpowiedzi na żądanie sprostowania danych osobowych zgłoszone przez Pana Łukasza Olejnika OpenAI wskazało, że nie ma możliwości sprostowania nieprawidłowych danych osobowych objętych żądaniem.

Zamiast wykonania żądania sprostowania danych osobowych OpenAI, mimo braku takiego wniosku, ograniczyło przetwarzanie danych osobowych (art. 18 RODO) poprzez zablokowanie możliwości generowania odpowiedzi na pytania kierowane do ChatGPT dotyczące Pana Łukasza Olejnika.

Działanie OpenAI nie stanowiło usunięcia danych (wykonania prawa do bycia zapomnianym), ponieważ dane osobowe Pana Łukasza Olejnika nie zostały przez OpenAI usunięte, a jedynie doszło do ograniczenia przetwarzania poprzez zaprzestanie operacji przetwarzania polegającej na udostępnianiu danych osobowych Pana Łukasza Olejnika użytkownikom ChatGPT. Wątpliwe jest zresztą czy w ogóle istnieje możliwość wykonania przez OpenAI prawa do usunięcia danych przetwarzanych w celu trenowania modeli GPT.

Nieprawidłowości. Prawidłowość przetwarzanych danych osobowych jest podstawową zasadą przetwarzania oraz obowiązkiem każdego administratora danych osobowych. Zgodnie z art. 5 ust. 1 lit. d RODO:

Dane osobowe muszą być:

(…)

prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane ("prawidłowość");

Z powyższego przepisu wynika, że w przypadku gdy dane osobowe nie są prawidłowe w świetle celów ich przetwarzania – administrator powinien podjąć **wszelkie rozsądne działania**, aby te dane usunąć lub sprostować. W literaturze[21] wskazuje się, że:

Dbałość o jakość przetwarzanych danych służyć ma ochronie osób, których dane dotyczą. Przetwarzanie danych nieaktualnych, błędnych czy też w inny sposób nieprawidłowych może pociągać za sobą negatywne konsekwencje dla osób, których dane dotyczą, a także dla podmiotów, które te dane przetwarzają, dlatego prawodawca unijny uznaje za kwestię zasadniczą wymóg zapewnienia, aby przetwarzane dane były prawidłowe, tzn. zgodne ze stanem faktycznym, aktualne i nie zawierały błędów.

Prawidłowość danych jest zasadą, ale zgodnie z art. 5 ust. 1 lit. d RODO zasada ta nie jest bezwzględna. Nieprawidłowość danych osobowych jest naturalnie występującym zjawiskiem – istotą zasady prawidłowości danych jest jednak dążenie administratora, w ramach wszelkich rozsądnych działań, do prawidłowości lub prostowanie danych błędnych. Zgodnie z przyjętym w doktrynie stanowiskiem[22]:

Zasada prawidłowości danych nie powinna być jednak interpretowana jako nałożony na administratora obowiązek systematycznego poszukiwania danych nieprawidłowych. W praktyce takie podejście byłoby niezwykle trudne do realizacji, nie tylko ze względu na ilość przetwarzanych danych, ale także na problemy dotyczące weryfikacji ich poprawności. Dlatego też komentowany przepis rozporządzenia nakłada na administratora obowiązek

---

[20] Tamże, str. 98-99.

[21] P. Fajgielski [w:] Komentarz do rozporządzenia nr 2016/679 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) [w:] Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, wyd. II, Warszawa 2022, art. 5.

[22] Tamże.

uaktualnienia danych „w razie potrzeby". Oznacza to, że administrator powinien reagować na sygnały dotyczące nieprawidłowości (…)

Prawidłowość danych powinna być zapewniana w szczególności w razie wystąpienia przez podmiot danych z żądaniem skorygowania danych osobowych zgodnie z art. 16 RODO. Przepis ten stanowi praktyczną formę realizacji zasady prawidłowości danych.

W przypadku OpenAI i przetwarzania danych w celu trenowania modeli zasada ta jest w praktyce **całkowicie pomijana**. Świadczy o tym odpowiedź OpenAI na żądanie Pana Łukasza Olejnika, zgodnie z którą OpenAI nie było w stanie skorygować przetwarzanych danych. Systemowy brak możliwości korygowania danych OpenAI zakłada jako element modelu funkcjonowania ChatGPT.

Zgodnie z Polityką prywatności (tłumaczenie maszynowe):

Uwaga dotycząca dokładności: Usługi takie jak ChatGPT generują odpowiedzi, odczytując żądanie użytkownika i w odpowiedzi przewidując słowa, które najprawdopodobniej pojawią się w następnej kolejności. W niektórych przypadkach słowa, które najprawdopodobniej pojawią się w następnej kolejności, mogą nie być najbardziej dokładne. Z tego powodu nie należy polegać na faktycznej dokładności danych wyjściowych z naszych modeli. Jeśli zauważysz, że dane wyjściowe ChatGPT zawierają niedokładne informacje o Tobie i chcesz, abyśmy poprawili tę niedokładność, możesz przesłać prośbę o korektę na adres dsar@openai.com. Biorąc pod uwagę złożoność techniczną działania naszych modeli, ***możemy nie być w stanie poprawić niedokładności w każdym przypadku****. W takim przypadku możesz poprosić o usunięcie Twoich Danych Osobowych z danych wyjściowych ChatGPT, wypełniając ten formularz.*

Biorąc pod uwagę ogólny i niejasny opis mechanizmów zapewniających prawidłowość danych w ChatGPT, istnieje wysokie prawdopodobieństwo, że brak możliwości skorygowania danych jest w przypadku przetwarzania danych przez OpenAI **zjawiskiem występującym systemowo**, a nie wyłącznie w ograniczonych przypadkach.

Powyższe okoliczności mogą wywołać uzasadnione wątpliwości co do ogólnej zgodności z przepisami o ochronie danych osobowych narzędzia, którego istotnym elementem jest systemowa nieprawidłowość przetwarzanych danych. Wątpliwości te wzmacnia skala przetwarzanych danych w ramach ChatGPT oraz skala potencjalnych odbiorców danych osobowych, które wpływają na ryzyka dla praw i wolności związane z nieprawidłowością danych osobowych.

Znaczenie dla oceny opisanych zagadnień ma także to, że przetwarzanie danych osobowych w ramach ChatGPT nie sprowadza się wyłącznie do prezentowania danych źródłowych, którymi zasilane są modele (tak jak np. jest w przypadku klasycznych wyszukiwarek). Istotą nieprawidłowości danych osobowych przetwarzanych przez OpenAI jest nie tylko nieprawidłowość danych źródłowych. W przypadku narzędzi typu ChatGPT nieprawidłowość danych wynika także z przetworzenia danych (w ramach uczenia maszynowego) w celu wygenerowania treści i odnosi się w tym przypadku do **danych „wyjściowych".** Ryzyko związane z tą nieprawidłowością wzmaga także sposób podania danych przez ChatGPT, które często prezentowane są jako fakty, niezależnie od dokładności tych danych.

Dlatego w celu wykonania obowiązków z art. 5 ust. 1 lit. d RODO i art. 16 RODO OpenAI powinno dążyć do korygowania błędów powstałych wskutek generowania treści w odpowiedzi na pytania użytkowników. OpenAI powinno opracować i wprowadzić mechanizm korygowania danych w oparciu o odpowiedni filtr/moduł, który weryfikowałby i korygowałby treści generowane przez ChatGPT (np. w oparciu o bazę wyników skorygowanych). Zasadnym w kontekście zakresu obowiązku zapewnienia prawidłowości danych jest oczekiwanie od OpenAI, że korygowane będą przynajmniej dane zgłoszone lub oflagowane przez użytkowników jako nieprawidłowe. Taka sytuacja wystąpiła w przypadku żądania Pana Łukasza Olejnika.

Wierzymy, że możliwe jest opracowanie przez OpenAI adekwatnych i zgodnych z RODO mechanizmów korygowania danych nieprawidłowych (możliwe jest już teraz blokowanie generowania określonych treści wskutek nałożonej przez OpenAI blokady). W przypadku gdyby jednak w ocenie OpenAI opracowanie takich mechanizmów nie było możliwe – należałoby skonsultować zagadnienie z odpowiednimi organami nadzoru, w tym np. w trybie uprzednich konsultacji opisanym w art. 36 RODO.

Wnioski. W ocenie Pana Łukasza Olejnika doszło do naruszenia jego prawa do sprostowania danych – prawo to nie zostało wykonane, a zamiast niego, wbrew żądaniu, doszło do ograniczenia przetwarzania danych.

Co więcej, z informacji przekazanych w korespondencji mailowej, jak też z informacji dostępnych online wynika, że brak możliwości korygowania danych (wykonywania praw jednostek) w przypadku OpenAI ma charakter systemowy, przez co przetwarzanie danych przez OpenAI narusza zasadę prawidłowości danych zawartą w art. 5 ust. 1 lit. d RODO.

2.5.C. Inne naruszenia związane z nieprawidłowym wykonaniem praw Pana Łukasza Olejnika

Niezależnie od nieprawidłowości w wykonaniu konkretnych praw Pana Łukasza Olejnika opisanych w punktach 2.3.1 i 2.3.2 – także ogólny sposób wykonania tych praw wskazuje na przetwarzanie niezgodne z art. 12 RODO.

Model odpowiadania OpenAI na żądania podmiotu danych świadczy o **fasadowym wykonaniu praw**, wbrew obowiązkom OpenAI jako administratora danych osobowych. Oznacza to, że OpenAI działa w sposób mający sprawić wrażenie działania zgodnego z RODO (w zakresie wykonania praw jednostki), ale w rzeczywistości prawa te wykonuje z naruszeniem przepisów.

Zgodnie z art. 12 ust. 1 i 2 RODO:

> *1. Administrator podejmuje odpowiednie środki, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem - w szczególności gdy informacje są kierowane do dziecka - udzielić osobie, której dane dotyczą, wszelkich informacji, o których mowa w art. 13 i 14, oraz prowadzić z nią wszelką komunikację na mocy art. 15-22 i 34 w sprawie przetwarzania.* (…)
>
> *2. Administrator ułatwia osobie, której dane dotyczą, wykonanie praw przysługujących jej na mocy art. 15-22.*
>
> (…)

W korespondencji wymienionej przez Pana Łukasza Olejnika z OpenAI, administrator przekazał szereg różnych informacji, częściowo niezwiązanych z żądaniem Pana Łukasza Olejnika. Co więcej, komplet podanych informacji (mimo obszerności) nie obejmował konkretnych informacji zgodnie z zakresem art. 15 ust. 1 RODO. Do wykonania prawa nie doszło także mimo przesłania przez Pana Łukasza Olejnika większej liczby wiadomości mailowych, w części mających na celu wyjaśnienie żądania, dopytanie o konkretne zagadnienia, wskazanie, że odpowiedzi OpenAI nie dotyczyły zagadnień objętych żądaniem.

Wątpliwości budzi ponadto treść odpowiedzi OpenAI oraz sposób podania określonych informacji. Wyjaśnienia OpenAI zawierały liczne linki, odesłania do innych stron w domenie OpenAI. Odesłanie dotyczyło m.in. zagadnienia przetwarzania danych w celu trenowania modeli przez OpenAI – można twierdzić, że OpenAI utrudnia dostęp do informacje w tym zakresie. Ponadto, rzeczywiste doprowadzenie do wykonania praw (uzyskanie konkretnych informacji) wymagałoby często skierowania przez użytkownika dodatkowych pytań, w zależności od zagadnienia, przez różne kanały i do różnych adresatów. W korespondencji z OpenAI można zidentyfikować także błędnie podane informacje (np. wstępne stwierdzenie, że dochodzi do podejmowania zautomatyzowanych decyzji lub wskazanie listy podmiotów podprzetwarzajacych w odpowiedzi na pytanie o odbiorców danych osobowych).

Taki sposób wykonania prawa dostępu do danych przez OpenAI nie odpowiada obowiązkowi wykonania praw podmiotu danych **w zwięzłej, ani tym bardziej przejrzystej i zrozumiałej formie**. Działanie OpenAI narusza także w ocenie Pana Łukasza Olejnika art. 12 ust. 2 RODO zobowiązujący administratora do ułatwiania osobie, której dane dotyczą, wykonania przysługujących jej praw. W literaturze[23] wskazuje się, że:

> *Wśród naczelnych reguł dotyczących przetwarzania danych wprowadzonych przepisami rozporządzenia ogólnego znalazła się zasada przejrzystości, którą statuuje art. 5 ust. 1 lit. a tego aktu. Komentowany artykuł* [art. 12 RODO] *odnosi ją do trybu wykonywania określonych*

[23] J. Łuczak [w:] RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018, art. 12.

w rozdziale III praw osób, których dane dotyczą, wyznaczając spójne ramy postępowania dla wszystkich podmiotów przetwarzających dane objętych przepisami rozporządzenia ogólnego.

(…)

Słuszność przyjęcia zasady przejrzystości wydaje się nie budzić zastrzeżeń. Stanowi ona w istocie wyraz troski, jaką prawodawca europejski przywiązuje do wzmocnienia ***pozycji podmiotu danych*** *poprzez zapewnienie należytej realizacji przysługujących mu uprawnień, w tym także tych o charakterze informacyjnym.* (…) *Komunikaty pochodzące od administratora mają zatem nie tylko być dla podmiotu danych czytelne, ale również stanowić swego rodzaju* ***przewodnik****.*

Wnioski. Dlatego opisany sposób działania OpenAI w wykonaniu praw Pana Łukasza Olejnika naruszał art. 12 ust. 1 i 2 RODO jak też zasadę przejrzystości zapisaną w art. 5 ust. 1 lit. a RODO.

2.6. Naruszenie zasad data protection by design (privacy by design)

Naruszenie zasady data protection by design. W ocenie Pana Łukasza Olejnika, OpenAI, tworząc i udostępniając Chat-GPT, zupełnie **zignorowało zasadę data protection by design**.

Zasadę data protection by design opisuje art. 25 ust. 1 RODO, zgodnie z którym:

Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze wynikające z przetwarzania, administrat–r - zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania -wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, ***zaprojektowane w celu skutecznej realizacji zasad ochrony danych,*** *takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą.*

Privacy by design (inaczej projektowanie prywatności) to koncepcja, której istotą jest uwzględnianie ochrony prywatności w fazie projektowania. Podstawowe założenia tej zasady to w szczególności[24]:

1) ***Podejście proaktywne, nie reaktywne****; prewencyjne, a nie naprawcze. Podejście PbD przewiduje wydarzenia naruszające ochronę prywatności, zanim się wydarzą, i im zapobiega.* (…)
2) ***Ochrona prywatności jako wartość domyślna****. Koncepcja PbD bazuje na założeniu, że możemy być wszyscy pewni jednej rzeczy — domyślnych zasad. Privacy by Design dąży do zapewnienia maksymalnego stopnia ochrony prywatności, zapewniając, że dane osobowe są automatycznie chronione w każdym systemie informatycznym lub praktyce biznesowej. Jeżeli osoba nie zrobi nic, jej prywatność i tak pozostanie nienaruszona.* (…)
3) ***Ochrona prywatności wbudowana w projekt****. Koncepcja PbD jest wbudowana w projekt i architekturę systemów informatycznych i praktyk biznesowych. Nie jest dołączona jako dodatek, po fakcie.* (…)
4) ***Bezpieczeństwo od początku do końca*** *— ochrona przez cały cykl życia informacji. Koncepcja PbD wbudowana do systemu przed zgromadzeniem pierwszej informacji rozkłada się bezpiecznie na cały cykl życia przedmiotowych danych — solidne środki bezpieczeństwa są niezbędne dla ochrony prywatności, od początku do końca.* (…)
5) ***Widoczność i transparentność****. Koncepcja PbD dąży do zapewnienia wszystkich interesariuszy, że niezależnie od zastosowanej praktyki biznesowej czy technologii, w rzeczywistości działa zgodnie ze wskazanymi obietnicami i celami, podlegając niezależnej weryfikacji. Jej części składowe i operacje pozostają widoczne i przejrzyste, na równi dla użytkowników i dostawców.* (…)

---

[24] Na podstawie: P. Fajgielski [w:] Komentarz do rozporządzenia nr 2016/679 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) [w:] Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, wyd. II, Warszawa 2022, art. 25 oraz przytoczonego tam materiału źródłowego: Privacy by Design, The 7 Foundational Principles, Ann Cavoukian, Ph.D., https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf (dostęp: 04.08.2023).

6) ***Respektowanie prywatności użytkownika**. Koncepcja PbD wymaga przede wszystkim, aby architekci i operatorzy traktowali interesy osoby priorytetowo, oferując takie środki, jak solidne domyślne ustawienia prywatności i odpowiednie zawiadomienie, oraz zapewniając przyjazne dla użytkownika opcje. Użytkownik ma być w centrum uwagi*[25].

Sposób zaprojektowania narzędzia ChatGPT, uwzględniając także nieprawidłowości opisane w pkt 3.3 skargi (w szczególności brak możliwości wykonania prawa do sprostowania danych, lekceważenie operacji przetwarzania danych w celu trenowania modeli GPT) – **stoi w sprzeczności z wszystkimi wskazanymi założeniami zasady data protection by design**. W praktyce w przypadku przetwarzania danych przez OpenAI dochodzi do testowania narzędzia ChatGPT przy wykorzystaniu danych osobowych, nie w fazie projektowania, ale w środowisku produkcyjnym (tj. po udostępnieniu narzędzia).

OpenAI zdaje się akceptować, że wypracowany model narzędzia ChatGPT jest po prostu niezgodny z przepisami RODO i na ten stan się godzi. Świadczy to o zupełnym pominięciu celów, które stoją u podstaw zasady data protection by design.

3. Uwagi końcowe

Okoliczności faktyczne oraz prawne opisane w niniejszej skardze potwierdzają, że doszło do niezgodnego z prawem przetwarzania danych osobowych Pana Łukasza Olejnika przez OpenAI. Działanie OpenAI naruszało:

- **art. 5 ust. 1 lit. a RODO** – OpenAI przetwarzało dane Pana Łukasza Olejnika niezgodnie z prawem, nierzetelnie oraz w sposób nieprzejrzysty,
- **art. 12 i 15 RODO** – OpenAI nieprawidłowo wykonało prawo Pana Łukasza Olejnika dostępu do danych osobowych oraz do informacji o przetwarzaniu danych osobowych,
- **art. 12 i 16 RODO –** OpenAI nie wykonało prawa Pana Łukasza Olejnika do sprostowania jego nieprawidłowych danych,
- **art. 25 ust. 1 RODO** – OpenAI, projektując i wdrażając narzędzie ChatGPT, naruszyło zasadę data protection by design.

Wobec tych naruszeń zasadne jest aby zobowiązać OpenAI do wykonania zgodnie z art. 12, 15 i 16 RODO praw Pana Łukasza Olejnika, tj. prawa dostępu do danych osobowych oraz do informacji o przetwarzaniu danych osobowych oraz prawa do sprostowania danych osobowych.

Celowe byłoby także, aby organ, mając na uwadze powyższe naruszenia, najprawdopodobniej mające charakter systemowy, zażądał przedłożenia przez OpenAI dokumentu oceny skutków dla ochrony danych (DPIA). Dokument ten może stanowić istotny element oceny, czy przetwarzanie danych przez OpenAI w ramach narzędzi Chat-GPT odbywa się zgodnie z RODO.

Nowe rozwiązania technologiczne, w szczególności narzędzia tak innowacyjne i skomplikowane technologicznie jak narzędzia generatywnej sztucznej inteligencji o uniwersalnym zastosowaniu i powszechnym dostępie, a takim narzędziem jest ChatGPT – powinny być tworzone z uwzględnieniem modeli *right-based approach* (podejście oparte o indywidualne prawa podmiotów danych) i *risk-based approach* (podejście oparte o ryzyko, z jakim wiąże się przetwarzanie danych, w szczególności dla praw i wolności jednostki)[26]. Jak słusznie wskazał brytyjski organ ochrony danych osobowych:

> *Organizacje opracowujące lub wykorzystujące generatywną sztuczną inteligencję powinny od samego początku brać pod uwagę swoje obowiązki w zakresie ochrony danych, przyjmując podejście privacy by design oraz privacy by default. Nie jest to opcjonalne - jeśli przetwarzasz dane osobowe, takie jest prawo*[27].

---

[25] Oznacza to także, że należy projektować uwzględniając możliwość wykonania praw jednostek w związku z przetwarzaniem danych osobowych, tak: M. Gawroński (red.) Ochrona danych osobowych. Przewodnik po ustawie i RODO ze wzorami, Warszawa 2018, str. 341-342.

[26] The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, Study of the Panel for the Future of Science and Technology, European Parliamentary Research Service, czerwiec 2020, https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf (dostęp: 04.08.2023).

[27] Generative AI: eight questions that developers and users need to ask, tłum. własne, https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/04/generative-ai-eight-questions-that-developers-and-users-need-to-ask/, (dostęp: 01.08.2023 r.).

Z powyższych względów wnoszę jak we wstępie.

_____

Maciej Gawroński
radca prawny

Załączniki:

(1) Odpis pełnomocnictwa dla radcy prawnego Macieja Gawrońskiego,

(2) Dowód opłaty skarbowej od pełnomocnictwa,

(3) Zrzut fragmentu konwersacji Pana Łukasza Olejnika z ChatGPT,

(4) Zrzut fragmentu konwersacji Pana Łukasza Olejnika z ChatGPT,

(5) Korespondencja e-mail Pana Łukasza Olejnika z OpenAI w sprawie przetwarzania danych osobowych w ramach ChatGPT.

(6) Tłumaczenie maszynowe korespondencji e-mail Pana Łukasza Olejnika z OpenAI w sprawie przetwarzania danych osobowych w ramach ChatGPT.