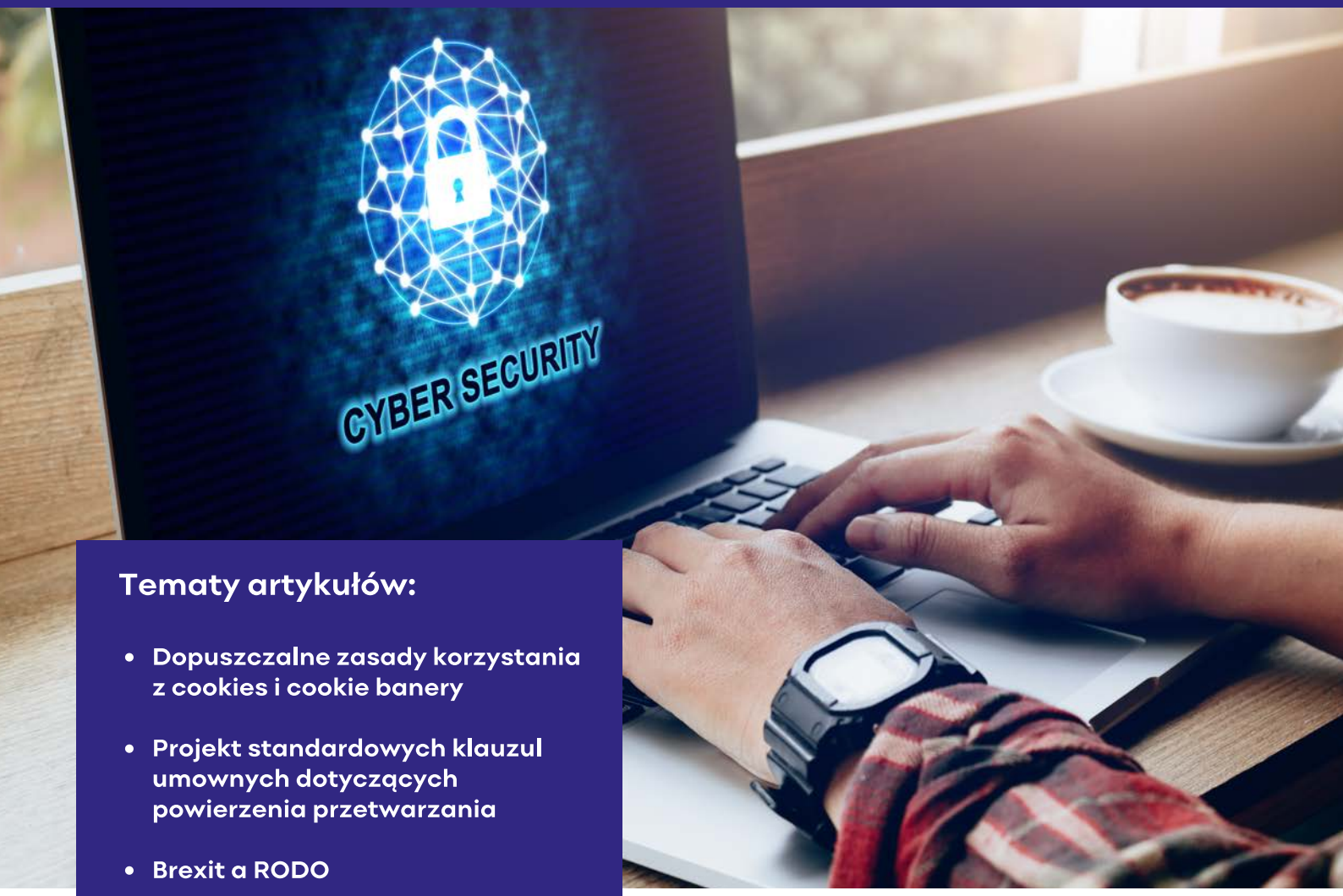
NR 1 - STYCZEŃ/LUTY 2021

NEWSLETTER RODO



Tematy artykułów:

- Dopuszczalne zasady korzystania z cookies i cookie banery
- Projekt standardowych klauzul umownych dotyczących powierzenia przetwarzania
- Brexit a RODO
- Wytyczne EROD w sprawie przykładów dotyczących zgłaszania naruszeń ochrony danych
- Projekt Data Governance Act
- Najnowsze naruszenia ochrony danych

Traple Konarski Podrecki & Wspólnicy

TKP

Dopuszczalne zasady korzystania z cookies – wnioski z decyzji CNIL

adw. Xawery Konarski, Senior Partner

W dniu 10 grudnia 2020 r. francuski organ ds. ochrony danych osobowych (CNIL) wydał dwie decyzje nakładające rekordowe kary pieniężne za nieprzestrzeganie zasad korzystania z cookies. Pierwsza z decyzji została wydana przeciwko spółkom Google LLC (60 mln euro kary) i Google Ireland (40 mln euro kary), a druga przeciwko Amazon Europe Core (35 mln euro kary).

Podstawa materialnoprawna i ustalenia w decyzjach CNIL

Podstawą prawną decyzji CNIL był art. 82 francuskiej ustawy o ochronie danych (Loi Informatique et libertés; LIL), stanowiący transpozycję do prawa francuskiego art. 5 ust. 3 dyrektywy UE 2002/58/WE w sprawie prywatności i łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej)[1].

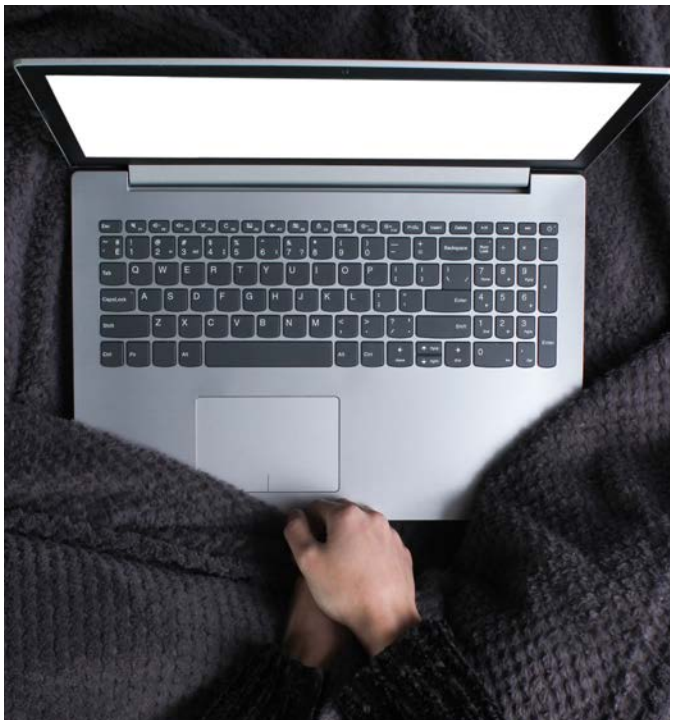
Artykuł 82 francuskiej ustawy LIL wymaga, aby w przypadku instalowania tzw. nieistotnych plików cookies, a więc cookies, które nie są niezbędne do świadczenia usługi, łącznie spełnione zostały dwa wymogi:

- realizacja obowiązku informacyjnego – obejmującego jasne i wyczerpujące podanie informacji dotyczących celów instalowania plików cookies oraz informacji o mechanizmach, za pomocą których użytkownik może się sprzeciwić wykorzystaniu cookies;
- uzyskanie od użytkownika uprzedniej zgody – która powinna zostać przez niego wyrażona po otrzymaniu informacji o celach wykorzystywania cookies.

Zdaniem CNIL zarówno Google, jak i Amazon naruszyły wyżej wymienione wymogi.

Podczas sprawdzania strony internetowej google.fr CNIL stwierdził, że na dole strony wyświetlany jest baner informacyjny z następującą adnotacją: „Przypomnienie o prywatności od Google" oraz dwa przyciski: „Przypomnij mi o tym później" i „Uzyskaj dostęp teraz". Według CNIL baner nie informował użytkowników o plikach cookies, które były już zainstalowane na ich urządzeniach – m.in. w celach reklamowych. Ponadto informacje te nie były podawane natychmiast po kliknięciu przez użytkownika na przycisk „Uzyskaj dostęp teraz".

Z kolei w trakcie kontroli strony internetowej amazon.fr CNIL ustalił, że informacje przekazywane użytkownikom nie były ani jasne, ani kompletne. Baner dotyczący plików cookies wyświetlany na stronie zawierał jedynie ogólny i przybliżony opis ich celów („aby oferować i ulepszać nasze usługi"). Ponadto link „Czytaj więcej" umieszczony w banerze nie wyjaśniał użytkownikom, że mogą oni odmówić przyjmowania cookies, nie zawierał też informacji, jak to zrobić. CNIL stwierdził, że niedostarczenie odpowiednich informacji przez Amazon Europe Core było jeszcze bardziej oczywiste w przypadku użytkowników odwiedzających stronę po kliknięciu na reklamę opublikowaną na innej stronie. W tym przypadku nie udzielono bowiem żadnych informacji.



[1] 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).

W podsumowaniu omówienia stanu faktycznego obu analizowanych decyzji należy podkreślić, że CNIL zwrócił szczególną uwagę na fakt, że pliki cookies były instalowane natychmiast po wejściu użytkownika na strony internetowe, przed przekazaniem odpowiednich informacji i przed wyrażeniem zgody przez użytkowników.

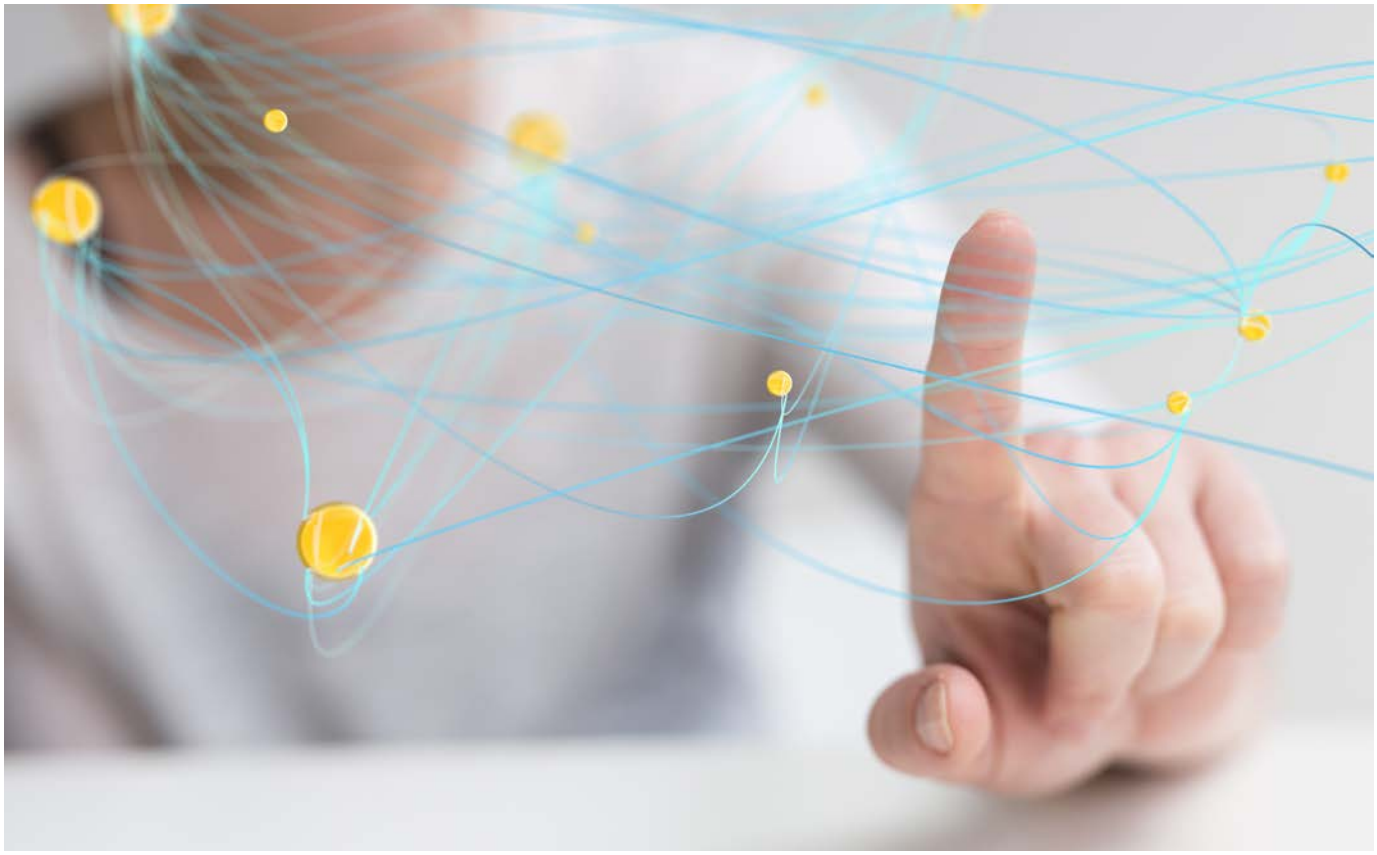
Kluczowe wnioski z decyzji CNIL

Po pierwsze, decyzje CNIL ponownie podkreśliły znaczenie przestrzegania unijnych zasad dotyczących obowiązku informacyjnego oraz zgody użytkownika na instalowanie plików cookies „innych niż niezbędne do świadczenia usługi" (np. cookies reklamowe). W przypadku prawa polskiego odpowiednikiem art. 82 francuskiej ustawy LIL jest art. 173 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (PT), ustanawiający wymogi tego samego rodzaju.

Po drugie, co budzi znacznie większe kontrowersje interpretacyjne, CNIL – a więc organ ds. ochrony danych osobowych – wydał decyzje na podstawie przepisów o e-Prywatności (a nie przepisów RODO). Jak się wydaje, przesądziła o tym specyfika implementacji art. 5 ust. 3 dyrektywy 2002/58/WE do francuskiego porządku prawnego, gdyż dokonano jej w ramach ustawy o ochronie danych osobowych.

Moim zdaniem, z uwagi na odmienny sposób transpozycji tego przepisu dyrektywy do prawa polskiego (w ramach art. 173 PT), polski organ ds. ochrony danych osobowych (PUODO) nie ma kompetencji do orzekania na podstawie odrębnych przepisów o e-Prywatności, a więc przepisów Prawa telekomunikacyjnego.

Po trzecie, CNIL – rozstrzygając sprawy Amazona i Google – odrzucił ich argumenty, że z uwagi na ustanowioną w RODO zasadę podlegania jednemu organowi nadzorczemu w Unii Europejskiej (one-stop-shop) francuski organ powinien był przekazać te sprawy do organów Unii Europejskiej, w których spółki te mają główne siedziby, tj. do Luksemburga (Amazon Europe Core) oraz Irlandii (Google Ireland). CNIL wyjaśnił, że mechanizm „pojedynczego punktu kontaktowego" GDPR nie miał zastosowania, ponieważ sprawa ta została wniesiona na mocy prawa francuskiego wdrażającego dyrektywę o prywatności i łączności elektronicznej – przepisy te nie zawierają takiej konstrukcji jak RODO. Przepisy o e-Prywatności są przy tym względniejsze, gdyż mają charakter lex specialis w stosunku do RODO.



Wytyczne LfD Niedersachsen ws. cookie banerów (Consent Layer)

Mateusz Kupiec

Administrator strony internetowej musi poinformować użytkownika o stosowaniu plików cookies, a także uzyskać jego zgodę na stosowanie (niektórych rodzajów) takich plików przed zapisaniem ich na urządzeniu końcowym. Co więcej, istnieją pewne dodatkowe wymagania, których należy przestrzegać, aby zgoda użytkownika była wyrażona skutecznie. Organ nadzorczy dla kraju związkowego Dolnej Saksonii (Die Landesbeauftragte für den Datenschutz Niedersachsen; LfD Niedersachsen) opublikował stanowisko dotyczące sposobów służących do pozyskiwania zgody na korzystanie z plików cookies.

Narzędzia do zarządzania zgodami

Organ w pierwszej kolejności zauważa, że w celu kompleksowego zarządzania zgodami na stosowanie plików cookies oraz narzędzi analitycznych podmiotów trzecich na stronach internetowych coraz częściej wdrażane i wykorzystywane są platformy do zarządzania zgodami (ang. consent management platform, CPM). Podmioty oferujące takie narzędzia nierzadko podkreślają w swoich materiałach promocyjnych, że za pomocą ich produktu pozyskuje się na stronie internetowej zgody spełniające wymogi wynikające z zasad ochrony danych osobowych. LfD Niedersachsen wskazuje, że wprawdzie korzystanie z platform do zarządzania zgodami może zasadniczo ułatwić uzyskanie oświadczenia woli użytkownika odwiedzającego daną stronę internetową, ale skuteczność konkretnego narzędzia zależy w dużej mierze od sposobu korzystania z niego przez podmiot zarządzający stroną. **Samo korzystanie z platform do zarządzania zgodami nie powoduje automatycznie uzyskania ważnej zgody w świetle RODO.**

Świadomość zgody

Zdaniem LfD Niedersachsen użytkownik wyrażający zgodę na zapisanie plików cookies na jego urządzeniu końcowym będzie działał świadomie jedynie wtedy, gdy **cele przetwarzania danych zostaną mu dokładnie wyjaśnione, w szczególności w przypadku tworzenia przez** administratora strony kompleksowych profili użytkowania. W związku z tym organ uznał za niewystarczające np. informacje, że pliki cookies są wykorzystywane, aby „dokonywać analiz i przeprowadzać działania promocyjne" lub „polepszyć jakość korzystania ze strony".

Moment wyrażenia zgody

LfD Niedersachsen podkreśla, że zgoda na stosowanie plików cookies musi być udzielona przed ich zapisaniem na urządzeniu końcowym użytkownika. Chociaż wymóg ten nie jest wyraźnie uregulowany, wynika on z funkcji zgody jako podstawy przetwarzania danych osobowych.

Wycofanie zgody

LfD Niedersachsen przypomina, że zgodnie z art. 7 ust. 3 zdanie 4 RODO[1] cofnięcie zgody musi być tak samo łatwe jak jej udzielenie. Tym samym, jeżeli zgoda na korzystanie z plików cookies jest udzielana bezpośrednio przy korzystaniu ze strony internetowej, musi istnieć również możliwość odwołania tej zgody w ten sam sposób. W przypadku korzystania z platformy do zarządzania zgodami na stronie internetowej użytkownik powinien mieć możliwość łatwego odnalezienia jej ponownie w dowolnym momencie i zmiany dokonanych wcześniej ustawień. Dobrą praktyką w ocenie organu jest np. umieszczenie w nagłówku lub stopce strony internetowej linku do platformy. Zdaniem organu **zgoda na stosowanie plików cookies nie powinna być wycofywana przy użyciu osobnego formularza kontaktowego, ponieważ wypełnienie go wymaga znacznie więcej wysiłku niż tylko kliknięcie na przycisk lub odznaczenie wyraźnej liczby pól na platformie.**

[1]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).

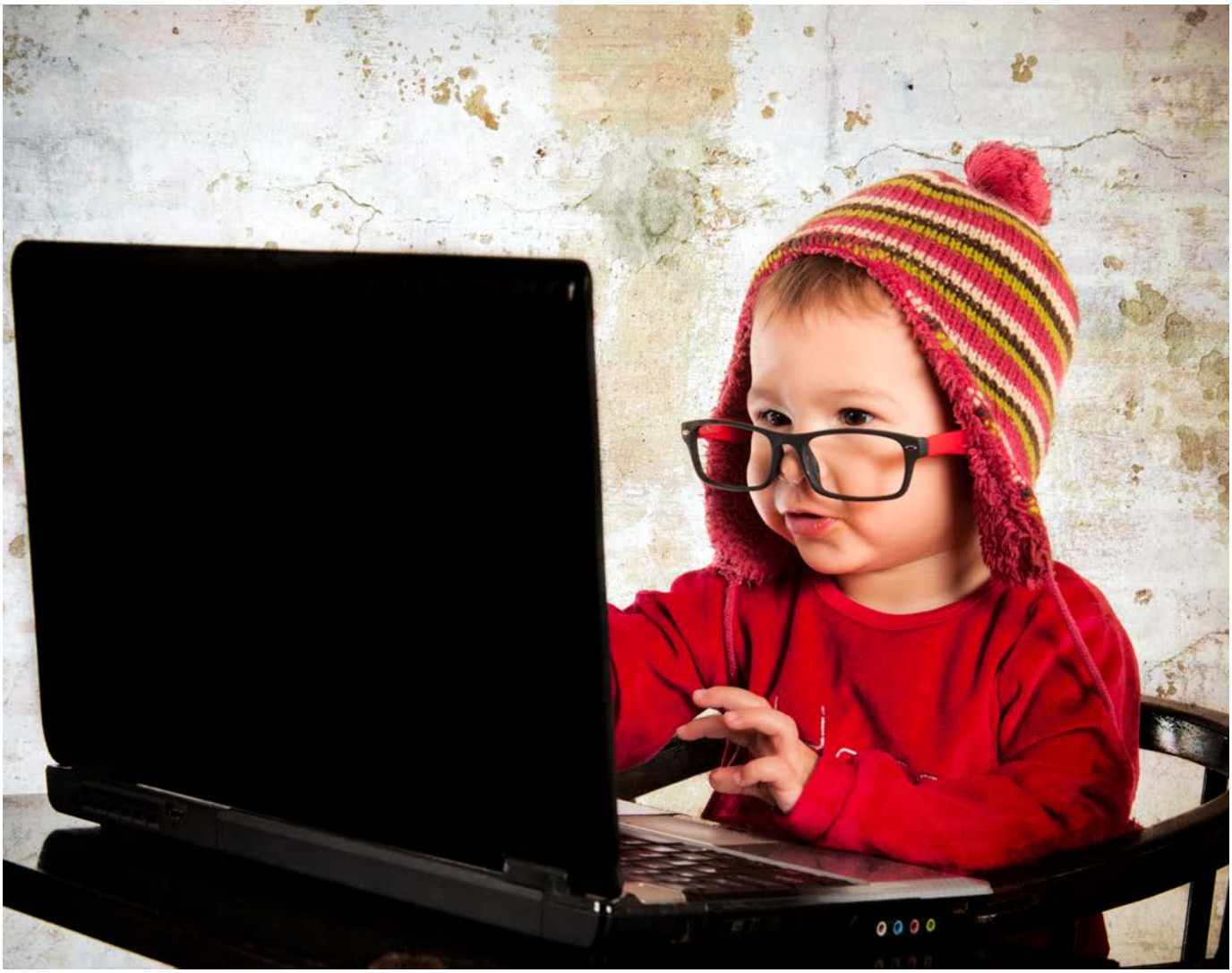
Zakaz wywierania wpływu na decyzję użytkownika o wyrażeniu zgody na stosowanie plików cookies

LfD Niedersachsen uznaje za niedopuszczalne wywieranie jakiegokolwiek wpływu na decyzję o wyrażeniu zgody na stosowanie plików cookies za pomocą technik manipulacji zachowaniem użytkownika (tzw. nudging). Organ wskazuje, że za nudging mogą również zostać uznane wszelkie praktyki podmiotu zarządzającego stroną, których celem jest wielokrotne zwracanie się do użytkownika z prośbą o wyrażenie zgody na stosowanie plików cookies, w przypadku gdy odmówił on jej udzielenia.

Pliki cookies na stronach przeznaczonych dla dzieci i młodzieży

Organ wskazuje, że jeżeli podmiot zarządza stroną internetową skierowaną (ze względu na jej wygląd oraz treść) do dzieci lub młodzieży i korzysta z plików cookies, to musi pamiętać, że w przypadku usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku, które nie ukończyło 16 lat, takie przetwarzanie jest zgodne z prawem tylko wtedy, gdy zgodę wyraziła lub zaaprobowała ją osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem oraz wyłącznie w zakresie wyrażonej zgody (art. 8 ust. 1 RODO). LfD Niedersachsen przypomina, że w celu realizacji tego wymogu na stronie internetowej konieczna jest najpierw weryfikacja wieku użytkownika wyrażającego zgodę w sposób ograniczający ryzyko nadużyć (kłamstwa co do swojego rzeczywistego wieku) ze strony osób poniżej 16 roku życia.

Wytyczne (wyłącznie w języku niemieckim) dostępne są pod adresem:
https://lfd.niedersachsen.de/startseite/themen/internet/datenschutzkonforme-einwilligungen-auf-webseiten-anforderungen-an-consent-layer-194906.html



Konsultacje wytycznych EROD w sprawie przykładów dotyczących zgłaszania naruszeń ochrony danych

Katarzyna Barszczewska-Mazur

14 stycznia 2021 r. odbyło się 44. posiedzenie plenarne, podczas którego Europejska Rada Ochrony Danych (EROD) przyjęła Wytyczne 01/2021 w sprawie przykładów dotyczących zgłaszania naruszeń ochrony danych. Wytyczne zostały przekazane do konsultacji publicznych, które potrwają do 2 marca 2021 r.

Uwagi wstępne

Podczas 1. posiedzenia plenarnego EROD zatwierdziła wytyczne dotyczące zgłaszania naruszeń ochrony danych osobowych wydane przez Grupę Roboczą Art. 29 (WP250rev.01)[1]. W zamyśle EROD Wytyczne 01/2021 mają uzupełniać ten dokument poprzez opracowanie bardziej praktycznych, bazujących na konkretnych przypadkach wskazówek i zaleceń, które uwzględnią również wnioski krajowych organów nadzoru z dotychczasowej praktyki stosowania RODO. EROD dostrzegła trudności, z jakimi mierzą się administratorzy danych w procesie zarządzania naruszeniami ochrony danych. Potrzeby administratorów dotyczą w szczególności sposobu postępowania w przypadku stwierdzenia naruszenia danych i określenia czynników, które należy uwzględnić w ocenie ryzyka.

Zasadność przyjęcia Wytycznych

Artykuł 33 ust. 1 RODO[2] zobowiązuje administratorów danych, aby bez zbędnej zwłoki, nie później niż w ciągu 72 godzin po stwierdzeniu naruszenia ochrony danych osobowych, zgłosili je właściwemu organowi nadzorczemu, chyba że jest mało prawdopodobne, by skutkowało ono ryzykiem naruszenia praw lub wolności osób fizycznych. Wskazanie terminu, co więcej – tak krótkiego, jest wyrazem przekonania, że przy braku odpowiedniej i szybkiej reakcji naruszenie ochrony danych osobowych może skutkować powstaniem uszczerbku fizycznego, szkód majątkowych lub niemajątkowych u osób fizycznych lub wszelkich innych szkód gospodarczych lub społecznych.

Typowe kategorie naruszeń zidentyfikowane i przeanalizowane przez EROD

Przykłady przedstawione w Wytycznych są fikcyjne, ale opierają się na typowych przypadkach naruszeń ochrony danych osobowych, z którymi w swojej praktyce zetknęły się organy nadzorcze. Omówienie tych sytuacji ma na celu wyjaśnienie, czy w konkretnych okolicznościach administrator danych powinien wykonać obowiązki, o których mowa w art. 33 ust. 1 oraz art. 34 RODO, tj. czy naruszenie powinno zostać zgłoszone organowi nadzoru i czy o tym naruszeniu należy poinformować osoby, których dane dotyczą.

Wytyczne analizują poszczególne przypadki według określonych kategorii naruszeń:

[1] Zob. https://edpb.europa.eu/our-work-tools/our-documents/guideline/personal-data-breach-notifications_pl (dostęp: 1.02.2020).
[2] 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).

1. Ataki ransomware

W tej kategorii naruszeń złośliwy kod szyfruje dane osobowe, uniemożliwiając ich odczyt, a następnie atakujący zwraca się do administratora danych o zapłatę okupu w zamian za przekazanie kodu deszyfrującego pliki. Ten rodzaj ataku zwykle klasyfikowany jest jako naruszenie dostępności, ale często może łączyć się z naruszeniem poufności. Wytyczne omawiają tę kategorię w modelach:

- **Ransomware z właściwą zapasową kopią danych i bez eksfiltracji (wycieku) danych** – w tym modelu uznano, że ryzyko naruszenia praw lub wolności osób fizycznych nie występuje.
- **Ransomware bez właściwej kopii zapasowej** – naruszenie powinno zostać zgłoszone organowi nadzoru, natomiast obowiązek poinformowania podmiotów danych należy ocenić z perspektywy długości okresu niedostępności danych i trudności, jakie może to spowodować w organizacji, np. opóźnienie wypłaty wynagrodzeń.
- **Ransomware z kopią zapasową i bez eksfiltracji, do którego doszło w szpitalnych bazach danych** – ten przypadek zaklasyfikowano jako wiążący się z wysokim ryzykiem naruszenia praw i wolności osób, których dane dotyczą. Decydujące znaczenie miały takie okoliczności jak szczególne kategorie danych osobowych oraz potencjalnie długi czas przywrócenia danych skutkujący opóźnieniami w opiece nad pacjentami. EROD rozróżniła sytuację podmiotów danych, które były leczone w szpitalu w ostatnich latach, od sytuacji osób leczonych 20 lat przed wystąpieniem naruszenia.
- **Ransomware bez właściwej kopii zapasowej, lecz z eksfiltracją** – uznano, że ten przypadek wiąże się z wysokim ryzykiem naruszenia praw i wolności osób fizycznych, ponieważ może prowadzić do szkód zarówno materialnych (np. straty finansowe spowodowane wyciekiem danych z kart kredytowych), jak i niemajątkowych (np. kradzież tożsamości lub oszustwo, ponieważ wyciekły dane z dowodów osobistych).

2. Ataki związane z eksfiltracją danych

Ataki te zwykle mają na celu skopiowanie, eksfiltrację i nieuprawnione używanie danych osobowych dla bezprawnych celów. W tej kategorii mieszczą się głównie naruszenia poufności i niekiedy również integralności danych. Wytyczne odnoszą się do poniższych przypadków:

- **Eksfiltracja danych z internetowych formularzy uzupełnianych przez kandydatów do pracy** – uznano, że ten przypadek może wiązać się z wysokim ryzykiem naruszenia praw i wolności osób fizycznych, pomimo że nie obejmował szczególnych kategorii danych osobowych. Decydujące znaczenie ma fakt, że doszło do ujawnienia znacznej ilości danych osobowych pochodzących z formularzy internetowych, a dane te mogą być nadużywane na wiele sposobów (kierowanie niezamówionych komunikatów marketingowych, kradzież tożsamości itp.).
- **Eksfiltracja zaszyfrowanego hasła ze strony internetowej** – w tym modelu uznano, że ryzyko naruszenia praw lub wolności osób fizycznych nie występuje. Powiadomienie podmiotów danych nie było obowiązkowe, ale administrator podjął takie działanie i Wytyczne wskazują, że w wielu przypadkach można to uznać za dobrą praktykę.
- **Atak dotyczący danych do logowania w witrynie bankowej** – EROD podkreśliła, że administratorzy przetwarzający informacje o tak wrażliwym charakterze jak dane finansowe ponoszą większą odpowiedzialność w zakresie zapewnienia odpowiedniego stopnia bezpieczeństwa danych. Przypadek zaklasyfikowano jako wiążący się z wysokim ryzykiem naruszenia praw i wolności wszystkich osób, których dane dotyczą.

3. Wewnętrzne źródło ryzyka w postaci czynnika ludzkiego

Wytyczne akcentują rolę i powszechność błędu ludzkiego w występowaniu naruszeń ochrony danych osobowych. Tego typu naruszenia mogą mieć charakter zarówno zamierzony, jak i niezamierzony, stąd administratorom danych bardzo trudno jest zidentyfikować luki w zabezpieczeniach i podjąć odpowiednie środki w celu ich uniknięcia. Wytyczne analizują modele eksfiltracji danych biznesowych przez byłego pracowni-ka oraz przypadkowego transferu danych do zaufanej strony trzeciej.

4. Zagubione lub skradzione urządzenia i dokumenty papierowe

Częstym przypadkiem naruszenia jest zgubienie lub kradzież urządzeń przenośnych. Administrator musi wtedy wziąć pod uwagę okoliczności przetwarzania, takie jak rodzaj danych przechowywanych w urządzeniu, a także środki podjęte przed naruszeniem w celu zapewnienia odpowiedniego poziomu bezpieczeństwa.

Ocena ryzyka przeprowadzana przy takich naruszeniach może nastręczać trudności, ponieważ urządzenie nie jest już dostępne. Tę kategorię naruszeń zazwyczaj uznaje się za naruszenia poufności. Jeśli jednak nie istnieje żadna kopia zapasowa skradzionej bazy danych, może dojść również do naruszenia dostępności i integralności.

Wytyczne omawiają takie warianty tego naruszenia jak:

- **Kradzież nośnika zawierającego zaszyfrowane lub niezaszyfrowane dane osobowe.**
- **Kradzież papierowych dokumentów zawierających szczególne kategorie danych osobowych.**

5. Błędy związane z przesyłaniem poczty

Jak wskazują Wytyczne, źródłem ryzyka w tej kategorii przypadków jest błąd ludzki, ale bez intencjonalnego działania i chęci doprowadzenia do naruszenia, gdyż najczęściej jest to wynik nieuwagi. Niewiele działań łagodzących skutki naruszenia może zostać podjętych, więc administratorzy powinni skupić się raczej na zapobieganiu. Możliwe przypadki:

- B**łąd w wysyłce pocztą tradycyjną („snail mail")** – polega on na tym, że przesyłka nie zostaje skierowana do właściwej osoby, np. klient otrzymuje zamówienie wraz z rachunkiem, na którym widnieją dane osobowe, dotyczącym zamówie-nia innego klienta.
- **Błędna wysyłka e-maila zawierającego wrażliwe lub zwykłe dane osobowe.**

6. Inne przypadki – inżynieria społeczna

Pod tą zbiorczą kategorią przypadków, powiązanych ze sobą wykorzystaniem inżynierii społecznej, kryją się takie zdarzenia jak:

- **Kradzież tożsamości** – na żądanie osoby podającej się za klienta firma telekomunikacyjna dokonała zmiany adresu e-mail, na który mają być przesyłane billingi. Zmianę przeprowadzono po potwierdzeniu tożsamości klienta, zgodnie z procedurami obowiązującymi w firmie. Osoba podająca się za klienta dysponowała danymi, których sprawdzenie obejmowała weryfikacja tożsamości. Pośród innych uwag EROD zwróciła szczególną uwagę na to, że statyczne uwierzytelnianie oparte na wiedzy (w ramach którego odpowiedź nie ulega zmianie i informacje nie są znane jedynie klientowi – jak w przypadku hasła) nie jest zalecane.
- Eksfiltracja e-maili – z wykorzystaniem danych pozyskanych z eksfiltracji e-maili atakujący, udając dostawcę, dokonał zmiany danych konta bankowego na swoje własne, a także wysłał kilka fałszywych faktur, które zawierały nowy numer konta bankowego. EROD uznała, że ten przypadek może się wiązać z wysokim ryzykiem naruszenia praw i wolności osób fizycznych.

Do każdego z przypadków zidentyfikowane zostały:

- **Uprzednie środki i ocena ryzyka** – EROD podkreśliła, że większości naruszeń można zapobiec, zapewniając odpowiednie organizacyjne, fizyczne i techniczne środki bezpieczeństwa. Wśród przykładów wskazano dysponowanie kopią zapasową danych, a także wdrożenie programu edukacji, szkolenia i podnoszenia świadomości pracowników (SETA).
- **Środki mające na celu zaradzenie naruszeniu i obowiązki, które należy wykonać w związku z wystąpieniem naruszenia.**

Z kolei do każdej kategorii naruszeń zaproponowano organizacyjne i techniczne środki, które mają służyć zapobieganiu naruszenia lub łagodzeniu jego skutków.

Komentarz

EROD stwierdza w Wytycznych, że naruszenia ochrony danych osobowych są problemami samymi w sobie, ale należy je postrzegać również jako symptomy podatnych na zagrożenia, niekiedy przestarzałych systemów bezpieczeństwa danych. Najlepszą praktyką jest zapobieganie naruszeniom, ale gdy już dojdzie do ich wystąpienia, administrator danych powinien podjąć starania, aby zebrać jak najwięcej informacji mówiących o słabości tego systemu.

Ta wiedza powinna następnie zostać wykorzystana w projektowaniu odpowiednich środków technicznych i organizacyjnych. Zadaniem administratora jest zapewnienie stopnia bezpieczeństwa danych przetwarzanych w swojej organizacji odpowiadającemu zidentyfikowanym rodzajom ryzyka naruszenia praw lub wolności osób fizycznych, których dane są przetwarzane. Nie ulega wątpliwości, że nie jest to zadanie łatwe, a z pewnością jest koszto- i czasochłonne, a co więcej – musi być powtarzane z biegiem czasu, wraz ze zmianami o charakterze nie tylko wewnętrznym (np. zmiana procesu przetwarzania danych osobowych w organizacji), lecz także zewnętrznym (np. zmiana stanu wiedzy technicznej).

Dokumenty takie jak Wytyczne należy docenić nie tylko dlatego, że wskazują na uznane przez EROD za wartościowe środki, które mają służyć zapobieganiu naruszenia lub łagodzeniu jego skutków, lecz także dlatego, że pomagają administratorom usprawnić proces zarządzania naruszeniami ochrony danych. Administratorzy muszą mieć świadomość, że celem Wytycznych jest jedynie zapewnienie pomocy w ocenie naruszeń, do których dojdzie w ich organizacji, a jakakolwiek zmiana w okolicznościach omówionych przypadków może skutkować innym wynikiem oceny ryzyka. Tekst Wytycznych, jaki zostanie ustalony w ostatecznym brzmieniu, po zakończeniu konsultacji, z pewnością będzie ważną pomocą w budowaniu efektywnego systemu ochrony danych osobowych w organizacji, ale – z powyższych względów – pomoc ta będzie miała nieco ograniczone zastosowanie.

Projekt standardowych klauzul umownych dotyczących powierzenia przetwarzania

adw. Katarzyna Syska

Komisja Europejska przedstawiła projekt decyzji ustanawiającej standardowe klauzule umowne między administratorami a podmiotami przetwarzającymi na podstawie art. 28 ust. 7 rozporządzenia 2016/679 (RODO)[1] i art. 29 ust. 7 rozporządzenia 2018/1725[2] (dotyczącego przetwarzania danych osobowych przez instytucje unijne). Standardowe klauzule umowne stanowią mechanizm zapewniania zgodności z warunkami powierzenia przetwarzania danych osobowych określonymi w art. 28 ust. 3–4 RODO.

Po opublikowaniu ostatecznej wersji decyzji administratorzy i podmioty przetwarzające będą więc mieli możliwość korzystania z ustalonego przez Komisję wzoru umowy, który oczywiście będzie wymagał dopasowania do okoliczności konkretnego przetwarzania.

Aktualny status klauzul

Komisja Europejska przedstawiła projekt decyzji ustanawiającej standardowe klauzule umowne między administratorami a podmiotami przetwarzającymi w listopadzie 2020 r.

Komisja Europejska ma uprawnienie do wydania decyzji określającej standardowe klauzule umowne na podstawie art. 28 ust. 7 RODO. Decyzja taka wydawana jest zgodnie z procedurą sprawdzającą wskazaną w art. 93 ust. 2 RODO, co oznacza, że projekt decyzji musi zostać pozytywnie zaopiniowany przez komitet złożony z przedstawicieli państw członkowskich.

Warto zwrócić uwagę, że opracowane przez Komisję standardowe klauzule umowne odnoszą się zarówno do przepisów RODO (zawierają postanowienia wymagane na podstawie art. 28 ust. 3–4 RODO), jak i do przepisów rozporządzenia 2018/1725, które dotyczy przetwarzania danych osobowych przez instytucje i organy unijne (klauzule zawierają postanowienia wymagane przez art. 29 ust. 3–4 tego rozporządzenia).

Co do projektu standardowych klauzul wypowiedzieli się Europejska Rada Ochrony Danych (EROD) oraz Europejski Inspektor Ochrony Danych (EDPS) – organy te wydały wspólną opinię w tej sprawie w połowie stycznia 2021 r. EROD i EDPS zarekomendowali wprowadzenie pewnych zmian do projektu standardowych klauzul umownych. Ponadto organy te podkreśliły, że postanowienia, które jedynie powtarzają przepisy art. 28 ust. 3–4 RODO oraz art. 29 ust. 3–4 rozporządzenia 2018/1725, nie są wystarczające, aby stanowić standardowe klauzule umowne. Stwierdzono też, że umowa powierzenia przetwarzania powinna dodatkowo określać, w jaki sposób obowiązki wskazane w art. 28 RODO lub w art. 29 rozporządzenia 2018/1725 mają być realizowane.

Należy się zatem spodziewać pewnych zmian w ostatecznej wersji standardowych klauzul umownych przyjętych przez Komisję.

Korzystanie ze standardowych klauzul umownych opracowanych przez Komisję nie będzie obowiązkowe – strony mogą wynegocjować własną umowę, przy czym musi ona oczywiście spełniać warunki art. 28 ust. 3–4 RODO.

[1] 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).
[2] 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.

Warto dodać, że standardowe klauzule umowne mogą być opracowywane także przez krajowe organy nadzorcze. Na razie jedynymi opracowanymi przez krajowy organ nadzorczy standardowymi klauzulami umownymi, które zostały opublikowane na stronie EROD, są standardowe klauzule umowne duńskiego organu nadzorczego. Zostały one opublikowane na stronie EROD po tym, jak duński organ nadzorczy wprowadził zmiany do ich projektu, zgodnie z rekomendacjami EROD.

Struktura klauzul

Projekt standardowych klauzul umownych opracowanych przez Komisję można podzielić na dwie części: ogólną i szczegółową.

Część ogólna zawiera postanowienia, które zasadniczo nie wymagają uzupełnień. Są to m.in. postanowienia dotyczące zobowiązania podmiotu przetwarzającego do działania zgodnie z poleceniami administratora, zwrotu lub usunięcia danych po rozwiązaniu umowy, korzystania z podwykonawców czy też ogólnie ujęte obowiązki pomagania administratorowi w wykonywaniu jego zadań.

Natomiast część szczegółowa składa się z siedmiu załączników (I–VII), które należy uzupełnić w taki sposób, aby odpowiadały one kontekstowi konkretnej sytuacji powierzenia przetwarzania danych.

W załącznikach należy wskazać:

- strony umowy;
- szczegółowe informacje o przetwarzaniu (jego przedmiot, cel, charakter, czas trwania, kategorie danych i kategorie podmiotów danych);
- środki służące zabezpieczeniu danych osobowych;
- dodatkowe polecenia administratora;
- szczególne ograniczenia lub środki bezpieczeństwa dotyczące przetwarzania szczególnych kategorii danych;
- dalsze podmioty przetwarzające;
- środki techniczne i organizacyjne, za pomocą których podmiot przetwarzający ma pomagać administratorowi w wywiązywaniu się z jego zadań.

Struktura ta jest zatem podobna do duńskich standardowych klauzul umownych, które również dzielą się na zasadniczo niewymagającą zmian część ogólną oraz załączniki wymagające uzupełnienia.

Stosowanie standardowych klauzul umownych opracowanych przez Komisję będzie zatem wymagało ich uzupełnienia przez strony i dostosowania do konkretnego przypadku powierzenia przetwarzania danych.

Standardowe klauzule umowne nie będą więc uniwersalnym wzorem umowy, który można by zastosować w każdej sytuacji, bez żadnych zmian czy uzupełnień. Takie podejście jest zgodne z opinią EROD i EDPS, którzy podkreślili, że umowa taka powinna uszczegóławiać obowiązki wskazane w art. 28 ust. 3–4 RODO.

Po przyjęciu przez Komisję decyzji w sprawie standardowych klauzul umownych dotyczących powierzenia przetwarzania z pewnością będą one cenną wskazówką co do tego, jak prawidłowo realizować poszczególne wymagania wynikające z art. 28 ust. 3–4 RODO.

Brexit a RODO – ochrona danych po wyjściu Wielkiej Brytanii z UE

dr Iga Małobęcka-Szwast

W ramach Umowy o handlu i współpracy między Unią Europejską i Europejską Wspólnotą Energii Atomowej z jednej strony a Zjednoczonym Królestwem Wielkiej Brytanii i Irlandii Północnej z drugiej strony (Trade and Cooperation Agreement, dalej: „TCA" lub „umowa o handlu i współpracy") wynegocjowanej pomiędzy UE a Wielką Brytanią 24 grudnia 2020 r. zdecydowano się na utrzymanie swobodnego przepływu danych między Europejskim Obszarem Gospodarczym (27 państw członkowskich UE oraz Islandia, Liechtenstein i Norwegia; dalej: „EOG") a Wielką Brytanią od 1 stycznia 2021 r. Dodatkowy okres przejściowy ma obowiązywać maksymalnie do 1 lipca 2021 r.

Wstęp

Dnia 31 stycznia 2020 r. Wielka Brytania opuściła Unię Europejską, ale na 11-miesięczny okres przejściowy określony w „Umowie o wystąpieniu" Wielka Brytania nie była traktowana jako państwo trzecie w rozumieniu przepisów RODO. W tym okresie administratorzy i podmioty przetwarzające dane nie musieli podejmować dodatkowych działań, o których mowa w art. 44 i n. RODO[1], a transfery danych do Wielkiej Brytanii były traktowane jak te dokonywane między państwami członkowskimi UE. Okres przejściowy dla wystąpienia Wielkiej Brytanii z Unii Europejskiej zakończył się 31 grudnia 2020 r.

Tuż przed jego upływem, dnia 24 grudnia 2020 r., UE i Wielka Brytania wynegocjowały umowę o handlu i współpracy, w której postanowieniach końcowych zawarto tzw. klauzulę pomostową. W ramach tej klauzuli UE zgodziła się opóźnić wprowadzenie ograniczeń transferu danych o kolejne cztery miesiące, z możliwością przedłużenia tego okresu do sześciu miesięcy (tzw. klauzula pomostowa), tj. do 1 lipca 2021 r. Postanowienie to umożliwia swobodny przepływ danych osobowych z EOG do Wielkiej Brytanii do czasu przyjęcia decyzji stwierdzającej odpowiedni stopień ochrony lub upływu uzgodnionego dodatkowego okresu przejściowego.

Umowa TCA została ostatecznie uzgodniona między UE i Wielką Brytanią 24 grudnia 2020 r. i obowiązuje tymczasowo od 1 stycznia 2021 r. Do 28 lutego 2021 r. TCA musi zostać jeszcze formalnie zatwierdzona przez Parlament Europejski.

Klauzula pomostowa

Artykuł FINPROV 10A umowy TCA, który określa przepisy przejściowe dotyczące przekazywania danych osobowych do Wielkiej Brytanii, przewiduje, że **transfery danych do tego państwa tymczasowo nie będą traktowane jako przekazywanie danych do państwa trzeciego.**

[1] 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).

W czasie trwania tego dodatkowego okresu przejściowego administratorzy i podmioty przetwarzające dane nie będą musieli spełniać dodatkowych wymogów, o których mowa w rozdziale V RODO.

Czas trwania okresu przejściowego

Podstawowy okres przejściowy określony w TCA, przez który transfer danych może się odbywać na dotychczasowych zasadach, to cztery miesiące. Okres ten może jednak zostać automatycznie przedłużony o kolejne dwa miesiące, tj. maksymalnie do 1 lipca 2021 r., chyba że jedna ze stron TCA się temu sprzeciwi.

Okres przejściowy może się zakończyć wcześniej, jeżeli Komisja Europejska wyda decyzje wykonawcze w sprawie odpowiedniego poziomu ochrony danych w odniesieniu do Zjednoczonego Królestwa zgodnie z art. 45 ust. 3 RODO i odpowiednio art. 36 ust. 3 dyrektywy 2016/680[2].

Co się stanie po zakończeniu okresu przejściowego?

Od 1 lipca 2021 r. Wielka Brytania będzie traktowana jako państwo trzecie, a do transferu danych do tego państwa zastosowanie znajdą postanowienia rozdziału V RODO (Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych).

Komisja Europejska zadeklarowała zamiar szybkiego rozpoczęcia formalnej procedury dotyczącej przyjęcia **decyzji w sprawie odpowiedniego poziomu ochrony w odniesieniu do Zjednoczonego Królestwa.**

Przed wydaniem takiej decyzji Komisja będzie musiała dokonać oceny brytyjskiego prawa ochrony danych osobowych i praktyki jego stosowania w świetle orzecznictwa Trybunału Sprawiedliwości UE. Zgodnie z art. 45 RODO przekazywanie danych na podstawie decyzji Komisji stwierdzającej odpowiedni stopień ochrony będzie możliwe bez konieczności spełnienia dodatkowych warunków.

Jeżeli jednak Komisja nie wyda w przewidzianym czasie decyzji w sprawie odpowiedniego poziomu ochrony, przekazywanie danych do Wielkiej Brytanii po upływie okresu przejściowego wymagać będzie zastosowania odpowiednich zabezpieczeń, o których mowa w art. 46 RODO (tj. m.in. standardowych klauzul umownych czy wiążących reguł korporacyjnych).

Na taką ewentualność zwraca uwagę również brytyjski organ nadzorczy – ICO. ICO zaleca, aby przed okresem przejściowym i w jego trakcie firmy współpracowały z podmiotami z UE i EOG, które przekazują im dane osobowe, w celu wprowadzenia alternatywnych mechanizmów transferu danych, aby zabezpieczyć się przed wszelkimi przerwami w swobodnym przepływie danych osobowych z UE do Wielkiej Brytanii.

Warunki swobodnego przepływu danych w okresie przejściowym

TCA uzależnia zastosowanie klauzuli pomostowej od spełnienia przez Wielką Brytanię określonych warunków. Swobodny przepływ danych w okresie przejściowym jest uzależniony od zachowania przez Wielką Brytanię obowiązujących w dniu 31 grudnia 2020 r. przepisów o ochronie danych osobowych opartych na prawie UE, tj. RODO i dyrektywie 2016/680. W okresie przejściowym Wielka Brytania nie będzie mogła również korzystać ze swoich kompetencji w zakresie międzynarodowych transferów danych.

Stanowiska organów nadzorczych w związku z Brexitem

W związku z Brexitem organy nadzorcze w różnych państwach wydały własne stanowiska, nie wprowadzają one jednak żadnych innych warunków transferu danych niż te, które wynikają wprost z TCA. Swoje stanowiska upubliczniły m.in. następujące organy nadzorcze:

1. Prezes UODO.
2. Brytyjski organ nadzorczy (ICO).
3. Konferencja Niezależnych Organów Ochrony Danych Federacji i Krajów Związkowych (Datenschutzkonferenz).
4. Francuski organ nadzorczy (CNIL).
5. Organ nadzorczy dla kraju związkowego Nadrenia-Palatynat (LfDI Rhineland-Palatinate).
6. Islandzki organ nadzorczy.
7. Irlandzki organ nadzorczy (DPC).
8. Duński organ nadzorczy.

Źródło:
https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:22020A1231(01)&from=EN

https://uodo.gov.pl/pl/138/1810

[2] 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 uchylająca decyzję ramową Rady 2008/977/WSiSW.

Raport Komisji Europejskiej dotyczący wdrażania niektórych przepisów RODO w przepisach krajowych

adw. dr hab. Grzegorz Sibiga, Partner

Komisja Europejska opublikowała raport dotyczący wdrażania niektórych przepisów RODO w przepisach krajowych. W artykule przedstawiamy najważniejsze wnioski wynikające z tego dokumentu.

Opublikowany przez Komisję Europejską dokument „Raport dotyczący wdrożenia szczególnych przepisów rozporządzenia 2018/679" dotyczy wykonania w prawie krajowym państw Unii Europejskiej niektórych upoważnień zawartych w RODO w:

- art. 8 ust. 1 (obniżenie granicy wieku dla zgody dziecka na przetwarzanie danych osobowych w usługach społeczeństwa informacyjnego oferowanych bezpośrednio dziecku);
- art. 9 ust. 4 (dalsze warunki w stosunku do art. 9 ust. 2 RODO dla przetwarzania danych genetycznych, danych biometrycznych lub danych o stanie zdrowia);
- art. 23 ust. 1 lit. c i e oraz art. 23 ust. 2 (ograniczenia praw i obowiązków przewidzianych w art. 5, 12–22 i art. 34 z powodu bezpieczeństwa publicznego oraz innych ważnych celów leżących w interesie publicznym, w szczególności ważnego interesu gospodarczego lub finansowego, w tym kwestii pieniężnych, budżetowych i podatkowych, zdrowia publicznego i zabezpieczenia społecznego);
- art. 85 ust. 1 i 2 (pogodzenie prawa do ochrony danych osobowych z wolnością wypowiedzi i informacji, w tym z potrzebami dziennikarskimi oraz do celów wypowiedzi akademickiej, artystycznej lub literackiej);
- art. 89 ust. 2, 3 i 4 (przetwarzanie danych osobowych do celów archiwalnych w interesie publicznym, do celów badań naukowych i historycznych lub do celów statystycznych).

Dobór przepisów uzupełniających

Pomimo że celem RODO była ścisła harmonizacja ochrony danych osobowych w państwach UE, to akt ten zawiera znaczną liczbę upoważnień dla prawodawców krajowych do uzupełniania regulacji RODO, ich uszczegóławiania oraz modyfikowania, w tym ograniczania stosowania niektórych rozwiązań zawartych w RODO. Raport Komisji Europejskiej omawia realizację tylko niektórych, wybranych upoważnień, przy czym nie zostały podane kryteria doboru właśnie tych upoważnień z RODO, które dotyczą odległych od siebie zagadnień kwestii umiejscowionych w różnych częściach RODO. To jednak pierwszy dokument analityczny na poziomie Unii Europejskiej, w którym dokonuje się przeglądu i porównania przepisów krajowych przyjętych na podstawie RODO, i to według określonej metodyki wraz z wnioskami wynikającymi z porównania. W sumie to 81 stron analizy wraz z załącznikami, przy czym znaczącą część tekstu zajmuje sam wykaz krajowych aktów prawnych.

Różnice i podobieństwa

Raport wskazuje na podobieństwa i różnice w prawie państw członkowskich, przy czym różnią się od siebie nawet daty przyjmowania przepisów przez poszczególne kraje; ostatnim państwem wykonującym RODO były Węgry, w których stosowna ustawa weszła w życie dopiero 26 kwietnia 2019 r.

Wykazanym w raporcie przykładem różnic jest podejście państw unijnych do ograniczenia wieku dzieci (niepełnoletnich) na wyrażanie zgody w przypadku oferowanych im bezpośrednio usług społeczeństwa informacyjnego. RODO przewiduje dopuszczalność zgody dziecka, które ukończyło 16 lat, a poniżej tego wieku przetwarzanie jest zgodne z prawem, gdy zgodę wyraziła lub zaaprobowała ją osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem. Państwa członkowskie mogą przewidzieć w swoim prawie niższą granicę wiekową, która musi jednakże wynosić co najmniej 13 lat. Okazuje się, że 9 krajów nie zmieniło przepisów, pozostawiając limit 16 lat (m.in. Polska, Węgry, Chorwacja), natomiast pozostałe państwa wprowadziły aż trzy różne limity wiekowe: 13 (np. Belgia), 14 (np. Włochy) lub 15 lat (np. Francja). W ten sposób dla usług świadczonych w sieci uzyskaliśmy w UE aż cztery granice wiekowe dla małoletnich wyrażających zgodę na przetwarzanie ich danych.

Dodatkowe warunki i ograniczenia praw

Większość państw skorzystała z możliwości wprowadzenia dodatkowych warunków, w tym ograniczeń, w zakresie przetwarzania danych o zdrowiu oraz danych genetycznych i biometrycznych. Chodzi tutaj głównie o przepisy przewidujące tajemnicę (poufność) danych medycznych wraz z ograniczoną kategorią osób mających dostęp do tajnych danych.

Część państw wykorzystała również możliwości ograniczenia praw osób, których dane dotyczą, z powołaniem się na generalne przesłanki z art. 23 ust. 1 („bezpieczeństwo publiczne” i „interes publiczny”). Raport przedstawia, że są to bardzo rozbudowane ograniczenia, w wielu przypadkach zależne od specyfiki krajowej. W generalnych wnioskach raportu stwierdzono jednak, że większość tych przepisów ograniczających nie wdraża w wystarczającym stopniu warunków i zabezpieczeń wymaganych w art. 23 ust. 2 RODO.

Źródło:
https://www.dataguidance.com/sites/default/files/160993017039 2.pdf

Projekt unijnego rozporządzenia w sprawie europejskiego zarządzania danymi (Data Governance Act)

dr Iga Małobęcka-Szwast oraz Mateusz Kupiec

Dnia 25 listopada 2020 r. Komisja Europejska (dalej: „KE", „Komisja") opublikowała projekt rozporządzenia w sprawie europejskiego zarządzania danymi (Data Governance Act, dalej: „DGA"). Projektowany akt prawny ma przyczynić się do zwiększenia wolumenu wymienianych danych i stworzenia nowych modeli biznesowych, a także rozwiązać najważniejsze problemy hamujące rozwój gospodarki opartej na danych w Unii Europejskiej. W tekście przedstawiamy główne cele i założenia projektu rozporządzenia.

Kontekst wniosku KE

W ramach *Europejskiej strategii w zakresie danych*, opublikowanej w lutym 2020 r., Komisja opisała wizję wspólnej **europejskiej przestrzeni danych – jednolitego rynku danych**, na którym dane mogłyby być wykorzystywane, zgodnie z obowiązującymi przepisami, bez względu na fizyczne miejsce ich przechowywania w UE.

Aby urzeczywistnić tę wizję, Komisja proponuje ustanowić wspólne **europejskie przestrzenie danych** w poszczególnych dziedzinach jako konkretne rozwiązania, w ramach których można będzie udostępniać i łączyć dane. Tego rodzaju wspólne europejskie przestrzenie danych mogą obejmować takie obszary, jak: zdrowie, mobilność, produkcja, usługi finansowe, energia lub rolnictwo, lub też obszary tematyczne, takie jak Europejski Zielony Ład czy wspólne europejskie przestrzenie danych dla administracji publicznej lub danych dotyczących umiejętności.

W ocenie Komisji działanie na poziomie UE jest konieczne w celu usunięcia barier dla dobrze funkcjonującej gospodarki opartej na danych oraz utworzenia ogólnounijnych ram zarządzania w zakresie dostępu do danych i ich wykorzystywania, w szczególności w odniesieniu do ponownego wykorzystywania niektórych rodzajów danych będących w posiadaniu sektora publicznego, świadczenia usług przez dostawców usług udostępniania danych na rzecz użytkowników biznesowych i osób, których dane dotyczą, jak również gromadzenia i przetwarzania danych udostępnianych z pobudek altruistycznych przez osoby fizyczne i prawne.

Cele DGA

Projektowany akt ma na celu zapewnienie większej dostępności danych na potrzeby ich wykorzystywania poprzez zwiększenie zaufania do pośredników w zakresie danych oraz wzmocnienie mechanizmów udostępniania danych w całej UE. Rozporządzenie będzie regulowało następujące sytuacje:

- Udostępnianie danych sektora publicznego do ponownego wykorzystywania w sytuacjach, w których dane te są objęte prawami innych osób.
- Udostępnianie danych między przedsiębiorstwami w zamian za wynagrodzenie w dowolnej postaci.
- Umożliwianie wykorzystywania danych osobowych z pomocą „pośrednika w udostępnianiu danych osobowych", który ma pomagać osobom fizycznym w wykonywaniu ich praw wynikających z ogólnego rozporządzenia o ochronie danych (RODO).
- Umożliwianie wykorzystywania danych z pobudek altruistycznych.

Zawartość projektu DGA

Projektowane rozporządzenie stworzy podstawę dla nowego europejskiego sposobu zarządzania danymi, który jest zgodny z wartościami i zasadami UE, takimi jak ochrona danych osobowych (RODO), ochrona konsumentów i zasady konkurencji.

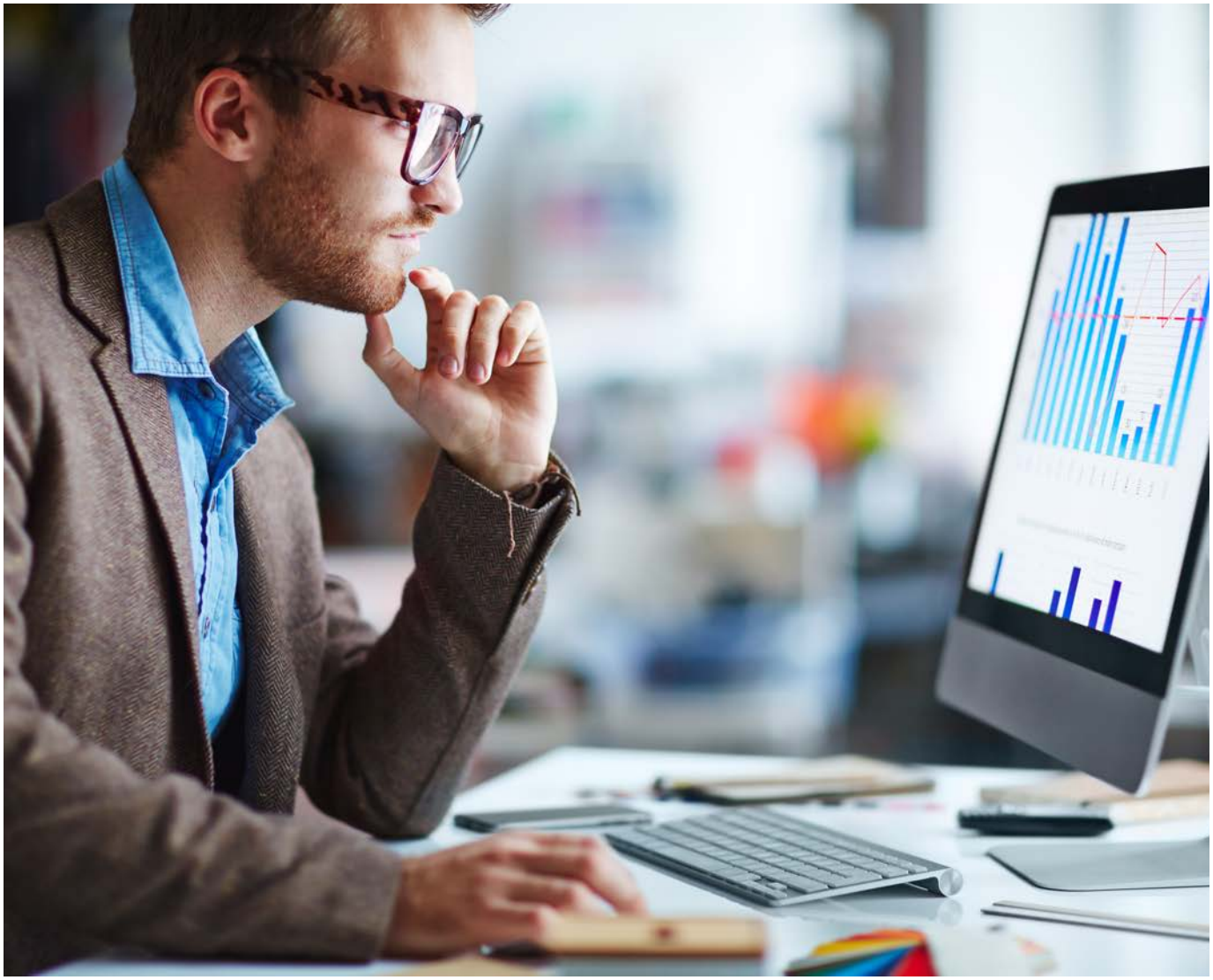
DGA stanowi alternatywny model dla praktyk w zakresie przetwarzania danych dużych platform technologicznych, które swoją siłę rynkową i modele biznesowe opierają na kontroli nad ogromną ilością danych.

Projekt Komisji zakłada model oparty na neutralności i przejrzystości pośredników w zakresie danych, którzy są organizatorami udostępniania lub łączenia danych, w celu zwiększenia zaufania do systemu wymiany danych. Aby zapewnić tę neutralność, pośrednik w wymianie danych nie może zajmować się nimi na własny rachunek (np. sprzedając je innej firmie lub wykorzystując je do opracowania własnego produktu na podstawie tych danych) i będzie musiał spełnić surowe wymagania, w szczególności te wynikające z RODO.

Przepisy projektowanego aktu prawnego przewidują m.in.:

- Ułatwienia w zakresie altruistycznego podejścia do danych, rozumianego jako dobrowolne udostępnianie danych przez osoby fizyczne lub przedsiębiorstwa dla wspólnego dobra. Proponowane przepisy mają umożliwić organizacjom zaangażowanym w altruizm danych rejestrację jako „organizacja o altruistycznym podejściu do danych" (*data altruism organisation*).
- Utworzenie mechanizmu ponownego wykorzystywania niektórych kategorii chronionych informacji sektora publicznego w celach komercyjnych i niekomercyjnych, przy poszanowaniu praw innych osób lub podmiotów (zwłaszcza ze względu na ochronę danych osobowych, ale także z uwagi na ochronę praw własności intelektualnej).
- Zwiększenie zaufania do wymiany danych osobowych i nieosobowych oraz obniżenie kosztów związanych z wymianą danych poprzez utworzenie systemu zgłaszania pośredników w udostępnianiu danych. Zgodnie z projektem DGA tacy pośrednicy będą musieli spełnić szereg wymogów, w szczególności wymóg zachowania neutralności w odniesieniu do wymienianych danych. Proponowane przepisy mają zapewnić ścisłe oddzielenie działalności konkretnego podmiotu w zakresie wymiany danych od jego działalności komercyjnej.
- Wyznaczenie organów właściwych do monitorowania i wdrażania ram zgłaszania dostawców usług udostępniania danych oraz podmiotów o altruistycznym podejściu do danych.

Projekt dostępny jest pod adresem: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767.
Źródło: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2102.



Projekt wytycznych irlandzkiego organu nadzorczego w przedmiocie ochrony danych osobowych dzieci

Mateusz Kupiec

Pierwsze kontakty dziecka ze światem cyfrowym mają obecnie miejsce już na bardzo wczesnym etapie jego rozwoju. Zdarza się, że dzieci w wieku przedszkolnym często wchodzą w interakcje z różnego rodzaju stronami internetowymi, aplikacjami za pośrednictwem telefonów komórkowych, inteligentnych zabawek oraz innych urządzeń. W celu zwiększenia poziomu bezpieczeństwa przetwarzania danych osobowych dzieci irlandzka Komisja ds. Ochrony Danych (Data Protection Commission, dalej: „DPC") opublikowała projekt wytycznych dotyczących tego zagadnienia pt.: „Fundamentals for a child-oriented approach to data processing". W tekście przedstawiamy ich wybrane elementy.

Realizacja praw dziecka jako podmiotu danych

Każdemu podmiotowi danych na gruncie RODO[1] przysługuje szereg uprawnień (art. 15–22 RODO), np. prawo dostępu do danych, prawo do wyrażenia sprzeciwu. Zdaniem DPC dziecka nie należy uznawać za kompetentne do zarządzania swoimi danymi osobowymi, jeżeli jest oczywiste, że działa ono wbrew własnemu interesowi. Z konsultacji przeprowadzonych przez organ wynika, że wśród młodszych dzieci istnieje ogólna tendencja do angażowania rodziców w pomoc w zarządzaniu ich danymi osobowymi; im starszy jest wiek respondentów, tym bardziej oddalają się oni od tego poglądu i dążą do większego nacisku na zarządzanie własnymi danymi osobowymi.

DPC uważa jednak, że nie należy ustalać jako jedynego punktu ogólnego progu wiekowego, po którego osiągnięciu dzieci powinny mieć możliwość korzystania ze swoich praw we własnym imieniu. Według DPC przy ocenie tego, czy dziecko powinno móc skutecznie korzystać z własnych praw do ochrony danych, należy wziąć pod uwagę m.in. takie czynniki, jak:

- Wiek i stopień dojrzałości dziecka.
- Rodzaj prawa, którego realizacji dziecko żąda.
- Kontekst przetwarzania i rodzaj usług oferowanych przez administratora (np. relacja lekarz – pacjent).
- Rodzaj danych osobowych, o których mowa.
- To, czy umożliwienie dziecku samodzielnego korzystania z prawa do ochrony danych osobowych leży w jego najlepszym interesie (np. czy rozumie ono konsekwencje usunięcia danych).
- To, czy dziecko stara się korzystać ze swoich praw z pomocą rodzica lub opiekuna.

Profilowanie dzieci i podejmowanie wobec nich zautomatyzowanych decyzji

W opublikowanych wytycznych DPC zwrócono również uwagę na zagadnienie wykorzystywania danych osobowych dzieci do ich profilowania oraz podejmowania wobec nich zautomatyzowanych decyzji. Organ stoi na stanowisku, że administratorzy danych nie powinni stosować takich praktyk wobec dzieci, o ile nie są w stanie wykazać, w jaki sposób i dlaczego jest to w najlepszym interesie najmłodszych. DPC uważa, że pokazywanie dzieciom spersonalizowanych reklam (opartych na profilowaniu) nie mieści się w zakresie pojęcia „najlepszego interesu dziecka".

[1] 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).

Działania w celu zwiększenia poziomu bezpieczeństwa danych osobowych dzieci

DPC zauważa, że nie istnieje jedno uniwersalne rozwiązanie w zakresie ochrony danych osobowych dzieci. W swoich wytycznych organ przedstawia jednak przykładową listę rozwiązań, które mogą umożliwić zapewnienie odpowiedniego poziomu bezpieczeństwa przetwarzanych danych osobowych dzieci. W ocenie DPC administratorzy danych powinni m.in.:

- Zrezygnować z systematycznego udostępniania danych osobowych dziecka podmiotom trzecim bez wyraźnej wiedzy, świadomości i kontroli ze strony jego rodziców. W szczególności nie należy udostępniać tożsamości dziecka lub informacji kontaktowych innym podmiotom trzecim.
- Domyślnie wyłączyć geolokalizację dla dzieci, chyba że świadczona przez nich usługa jest od niej zależna; w takim przypadku należy wyjaśnić dziecku (np. poprzez użycie symboli/ikon), że jego lokalizacja jest dostępna dla usługi lub może być widoczna dla innych użytkowników, oraz znacznie zmniejszyć poziom dokładności gromadzenia danych geolokalizacyjnych (z wyjątkiem sytuacji, w których jest to konieczne).
- W stosownych przypadkach umożliwić rodzicom dokonanie zmian ustawień konta dziecka, jeżeli ustawienia konkretnej usługi / konkretnego urządzenia pozwalają rodzicom na śledzenie lub monitorowanie sposobu, w jaki ich dziecko z nich korzysta.
- Powiadomić o ewentualnym naruszeniu ochrony danych osobowych rodzica, a nie wyłącznie dziecko, którego dotyczy naruszenie. **Ewidencja naruszeń prowadzona przez administratora powinna zawierać odniesienia do wszelkich przypadków naruszenia danych osobowych dzieci**.

Wszystkie zainteresowane podmioty mogą ustosunkować się do projektu wytycznych poprzez dostarczenie DPC swoich uwag i komentarzy do 31 marca 2021 r.

Projekt wytycznych dostępny jest pod adresem: https://www.dataprotection.ie/en/news-media/consultations/children-front-and-centre-fundamentals-child-oriented-approach-data-processing.

Biała księga CNIL dotycząca asystentów głosowych

Mateusz Kupiec

Liczba asystentów głosowych będących obecnie w użyciu na świecie liczona jest w miliardach. Asystenci głosowi mogą wykonywać różne czynności po usłyszeniu odpowiedniego słowa lub polecenia – np. kontrolować oświetlenie, odpowiadać na pytania, składać zamówienia online, umawiać na spotkania. Zagadnieniu asystentów głosowych z punktu widzenia ochrony danych osobowych przyjrzał się francuski organ nadzorczy (CNIL), który opublikował białą księgę dotyczącą asystentów głosowych. Przedstawiamy fragmenty opracowania organu.

Czym jest asystent głosowy?

Zdaniem CNIL pod pojęciem „asystenta głosowego" należy rozumieć oprogramowanie, które zapewnia możliwość prowadzenia ustnego dialogu z użytkownikiem w języku naturalnym. Kiedy użytkownik wypowiada hasło budzące (ang. *the wake word*), asystent „budzi się" i może rejestrować jego komendy, które przekształcane są z mowy na tekst. Przy wykorzystaniu technologii przetwarzania języka naturalnego słowa wypowiadane przez użytkownika są poddawane analizie. Organ zauważa, że asystent głosowy bywa nierzadko mylony z inteligentnym głośnikiem, który w rzeczywistości jest jedynie materialnym nośnikiem (korpusem) asystenta. W białej księdze wskazuje się również, że nie każde oprogramowanie będące osobistym asystentem (ang. *personal assistant*) będzie asystentem głosowym.

Głos a dane osobowe

CNIL zauważa, że głos jest kluczowym elementem budującym tożsamość jednostki. W praktyce głos przekazuje, oprócz samych słów mówiącego, wiele innych jego cech: emocje, intencje, stan fizyczny itp. Opierając się na mechanizmach percepcji, inni ludzie są w stanie zinterpretować te sygnały i odszyfrować te stany. Zdaniem organu głos danej osoby będzie mieścił się w pojęciu „danych osobowych" w rozumieniu art. 4 pkt 1 RODO[1], ale nie zawsze będzie należał on do szczególnej kategorii danych w rozumieniu art. 9 RODO.

Asystenci głosowi a RODO – scenariusze zastosowania

CNIL przedstawia trzy fikcyjne scenariusze korzystania z asystentów głosowych w kontekście realizacji zasad wynikających z RODO:

- Korzystanie z podstawowych funkcji asystenta głosowego.
- Korzystanie przez użytkownika z aplikacji bankowej za pośrednictwem asystenta głosowego.
- Ponowne wykorzystanie przez producenta (dostawcę) asystenta zebranych przez niego danych osobowych w celu poprawy jakości usług.

Analiza tych scenariuszy doprowadza do następujących wniosków:

- W przypadku korzystania przez osobę fizyczną z podstawowych funkcji asystenta głosowego administratorem jej danych będzie producent konkretnego asystenta, o ile określa on cele (świadczenie usługi pomocy głosowej) i środki (przetwarzanie za pośrednictwem asystenta powiązanego z kontem użytkownika) przetwarzania danych. W przypadku korzystania przez użytkownika z aplikacji bankowej za pośrednictwem asystenta głosowego administratorem danych osobowych będzie bank korzystający z takiego oprogramowania, podczas gdy jego producent będzie pełnił funkcję podmiotu przetwarzającego.
- Dostawcy asystentów głosowych mogą spełniać obowiązek informacyjny wynikający z art. 13 RODO wobec podmiotu danych przy wykorzystaniu różnych środków przekazu, w tym np. poprzez nagrania komunikatów informacyjnych, które są wysyłane do czasu potwierdzenia przez użytkownika zapoznania się z nimi podczas tworzenia konta, polityki prywatności dostępnej na stronie dostawcy. Bank może natomiast przekazać użytkownikowi informacje dotyczące przetwarzania jego danych osobowych za pomocą asystenta głosowego podczas parowania przez niego swojego konta bankowego z danym oprogramowaniem.
- Odpowiednią podstawą przetwarzania danych osobowych użytkownika w ramach korzystania przez niego zarówno z podstawowych funkcji asystenta głosowego, jak i z aplikacji bankowej za jego pośrednictwem będzie

[1] 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).

niezbędność przetwarzania do wykonania umowy, której stroną jest użytkownik (art. 6 ust. 1 lit. b RODO). W przypadku ponownego wykorzystania przez producenta asystenta zebranych danych w celu poprawy jakości usług właściwą podstawą przetwarzania będzie prawnie uzasadniony interes producenta asystenta lub zgoda użytkownika.

Asystenci głosowi a RODO – wybrane dobre praktyki

CNIL przedstawia również dobre praktyki, dzięki którym producenci asystentów głosowych oraz inne podmioty biorące udział w przetwarzaniu danych osobowych użytkownika mogą je skutecznie chronić. Zdaniem CNIL:

- Producenci asystentów głosowych powinni pozwalać użytkownikowi na zadawanie pytań dotyczących operacji przetwarzania danych osobowych przez asystenta głosowego.
- Podmioty korzystające z asystentów głosowych powinny przed wdrożeniem takiego oprogramowania ustalić, czy za jego pomocą będą przetwarzane informacje dotyczące szczególnie wrażliwych podmiotów danych.
- Należy pozwalać użytkownikom asystentów głosowych na wybranie ich własnych haseł budzących.
- Należy określać odrębne okresy retencji danych przetwarzanych przez asystenta głosowego w zależności od rodzaju gromadzonych informacji. Na przykład dane związane z kontem użytkownika mogą być przechowywane dłużej niż jednorazowe zapytania skierowane do asystenta głosowego.

Mity o asystentach głosowych

Autorzy białej księgi odnoszą się też do wybranych mitów dotyczących asystentów głosowych.
Wbrew niektórym opiniom asystenci głosowi:

- Nie nagrywają wszystkiego, co mówi się w ich obecności.
- Nie rozumieją użytkowników w sposób doskonały, są jedynie przykładem tzw. słabej sztucznej inteligencji (ang. weak AI).
- Nie zawsze wykorzystują zebrane dane w celu profilowania użytkowników.

Organ potwierdza jednak niektóre wątpliwości dotyczące asystentów głosowych:

- Asystenci głosowi (a właściwe urządzenia wyposażone w takie oprogramowanie) są rzeczywiście chętnie i często używani przez dzieci.
- Asystenci głosowi są podatni na ataki hakerskie.

Biała księga CNIL w języku angielskim jest dostępna pod adresem:
https://www.cnil.fr/sites/default/files/atoms/files/cnil_white-paper-on_the_record.pdf.

Strategia EROD na lata 2021–2023

Mateusz Kupiec

Podczas 43. posiedzenia Europejskiej Rady Ochrony Danych (EROD) przyjęto strategię organu na lata 2021–2023. W dokumencie tym określono najważniejsze założenia strategii EROD skupione wokół czterech filarów oraz zarys działań, które mają zostać podjęte w ramach każdego z nich. Przedstawiamy plany EROD na najbliższe trzy lata.

Filar 1: Pogłębienie harmonizacji i ułatwienie stosowania przepisów

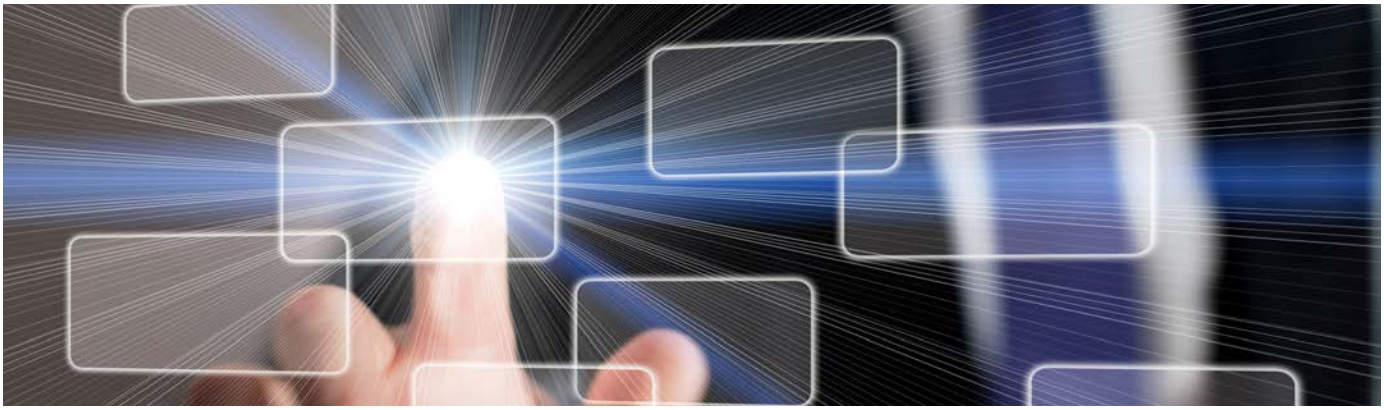
EROD zapowiada dalsze działania w celu zapewnienia spójności w stosowaniu przepisów z zakresu ochrony danych osobowych poprzez:

- Publikowanie kolejnych wytycznych dotyczących kluczowych pojęć unijnego prawa ochrony danych (np. pojęcia uzasadnionego interesu, zakresu praw osób, których dane dotyczą) oraz kontynuowanie współpracy z szerokim gronem zewnętrznych podmiotów zainteresowanych. EROD pragnie podjąć dodatkowe wysiłki w celu wyeliminowania potencjalnych luk lub rozbieżności w interpretacji i stosowaniu przepisów ochrony danych osobowych w państwach członkowskich.
- Dalszą popularyzację rozwoju i wdrażania mechanizmów zgodności dla administratorów i podmiotów przetwarzających – zwłaszcza poprzez prowadzenie odpowiednich warsztatów i szkoleń personelu w celu stymulowania narzędzi promujących zgodność, w szczególności kodeksów postępowania i certyfikacji.
- Wsparcie rozwoju narzędzi oraz podjęcie działań informacyjnych dostosowanych do potrzeb podmiotów nieposiadających wiedzy eksperckiej z zakresu ochrony danych osobowych (np. dla małych i średnich przedsiębiorstw).

Filar 2: Wsparcie skutecznego egzekwowania przepisów i współpracy pomiędzy organami nadzorczymi

EROD wyraża chęć zaangażowania się we wspieranie współpracy pomiędzy wszystkimi krajowymi organami nadzorczymi w egzekwowaniu unijnego prawa ochrony danych. Organ planuje nie tylko zapewnić skuteczniejsze funkcjonowanie mechanizmów współpracy i spójności, lecz także dążyć do wypracowania rzeczywistej wspólnej kultury egzekwowania prawa wśród organów nadzorczych. Zamiary te EROD planuje zrealizować poprzez:

- Zachęcanie do korzystania z pełnego zakresu narzędzi współpracy przewidzianych odpowiednio w rozdziale VII RODO i w rozdziale VII dyrektywy 2016/680, a także niwelowanie rozbieżności pomiędzy krajowymi procedurami dotyczącymi egzekwowania ochrony danych osobowych.
- Wdrożenie skoordynowanych ram egzekwowania prawa (ang. Coordinated Enforcement Framework, CEF) w celu ułatwienia wspólnych działań w elastyczny, ale skoordynowany sposób. CEF ma usprawnić koordynację działań w zakresie egzekwowania prawa na podstawie wspólnie określonych priorytetów i wspólnej metodologii.
- Utworzenie grupy ekspertów wspierających (ang. Support Pool of Experts, SPE) na podstawie projektu pilotażowego w celu zapewnienia wsparcia w formie wiedzy specjalistycznej przydatnej w dochodzeniach i działaniach związanych z egzekwowaniem przepisów oraz w celu wzmocnienia współpracy i solidarności pomiędzy wszystkimi organami nadzorczymi w UE.



Filar 3: Podejście do nowych technologii oparte na prawach podstawowych

EROD zapowiada stałe monitorowanie nowych technologii oraz ich potencjalnego wpływu na prawa podstawowe i codzienne życie jednostek. EROD zamierza:

- Dokonywać oceny nowych technologii poprzez m.in. ustalanie wspólnych stanowisk i wskazówek dotyczących rozwiązań w takich obszarach, jak: AI, biometria, technologie reklamowe, chmura obliczeniowa itp.
- Wzmocnić realizację zasad *privacy by design i privacy be default* poprzez m.in. przedstawienie odpowiednich wytycznych.
- Zintensyfikować współpracę z innymi organami regulacyjnymi i decydentami.

Filar 4: Wymiar globalny

EROD pragnie ustanawiać i popularyzować unijne i światowe standardy w przedmiocie międzynarodowego transferu danych. Organ chce promować na arenie międzynarodowej unijny model ochrony danych jako wzór do naśladowania. W tym celu EROD będzie:

- Upowszechniać (poprzez opracowywanie odpowiednich wytycznych) korzystanie z takich narzędzi transferu, które – biorąc pod uwagę m.in. ryzyko związane z dostępem organów publicznych państw trzecich do danych osobowych – zapewniają adekwatny poziom ochrony danych.
- Współpracować ze społecznością międzynarodową: EROD i jej członkowie będą dążyć do dialogu z organizacjami międzynarodowymi i sieciami instytucjonalnymi, aby pełnić rolę lidera w ochronie danych i promować wysokie standardy ochrony na całym świecie.
- Ułatwiać współpracę pomiędzy członkami EROD a organami nadzorczymi krajów trzecich w zakresie ochrony danych osobowych, skupiając się na kooperacji w sprawach dotyczących egzekwowania prawa z udziałem administratorów lub podmiotów przetwarzających zlokalizowanych poza EOG.

Komentarz

Opublikowany dokument pozwala zobaczyć, jakie obszary i cele będą najważniejsze dla EROD w nadchodzących trzech latach. Niemniej, jak wskazuje sam organ, strategia ma charakter jedynie poglądowy i nie stanowi wyczerpującej listy działań, tematów, którymi będzie się on zajmował.

Strategia EROD na lata 2021–2023 dostępna jest pod adresem: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_strategy2021-2023_en.pdf.

Prezes UODO nałożył administracyjną karę pieniężną za niezgłoszenie naruszenia ochrony danych

r.pr Dominika Nowak

Dnia 9 grudnia 2020 r. Prezes UODO wydał decyzję nakładającą na administratora: Towarzystwo Ubezpieczeń i Reasekuracji WARTA SA administracyjną karę pieniężną za niezgłoszenie naruszenia ochrony danych oraz za niezawiadomienie o zdarzeniu osób, których dotyczyło naruszenie.

Stan faktyczny

W maju 2020 r. do UODO wpłynęła informacja od osoby trzeciej o naruszeniu danych osobowych. Naruszenie to polegało na wysłaniu pocztą elektroniczną przez agenta ubezpieczeniowego polisy ubezpieczeniowej do nie-właściwego adresata. Agent był podmiotem przetwarzającym dla Towarzystwa Ubezpieczeń i Reasekuracji WARTA SA z siedzibą w Warszawie (dalej: „Warta"). Polisa zawierała następujące dane: imiona, nazwiska, adresy zamieszkania, numery PESEL, adresy e-mail, numery telefonu oraz informacje dotyczące samochodu, który był przedmiotem tej polisy. Doszło do naruszenia poufności danych. Osobą, która poinformowała UODO o naruszeniu, był nieuprawniony adresat wiadomości otrzymanej od agenta.

osobowych oraz że została przeprowadzona ocena pod kątem ryzyka naruszenia praw i wolności osób fizycznych. Na podstawie dokonanej analizy Warta uznała, że to naruszenie nie wymaga zgłoszenia do organu nadzorczego. Po wysłaniu przez organ nadzorczy pisma z prośbą o wyjaśnienia Warta nadal nie zgłosiła naruszenia ani nie powiadomiła osób, których ono dotyczyło. Warta zgłosiła naruszenie do organu nadzorczego oraz powiadomiła osoby, których dotyczyło naruszenie, po wszczęciu postępowania administracyjnego.

Decyzja

W konsekwencji Prezes UODO w decyzji z dnia 9 grudnia 2020 r. (DKN.5131.5.2020) stwierdził naruszenie przez Wartę następujących przepisów:

- art. 33 ust. 1 RODO[1], które polegało na niezgłoszeniu Prezesowi UODO naruszenia ochrony danych osobowych bez zbędnej zwłoki, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia;
- art. 34 ust. 1 UODO, które polegało na niezawiadomieniu o naruszeniu ochrony danych osobowych – bez zbędnej zwłoki – osób, których dane dotyczą.

Prezes UODO nałożył administracyjną karę pieniężną w wysokości 85 588 złotych (słownie: osiemdziesiąt pięć tysięcy pięćset osiemdziesiąt osiem złotych).

Praktyczne wnioski płynące z decyzji

Z uzasadnienia decyzji Prezesa UODO można wywnioskować kilka przydatnych wskazówek dla osób zajmujących się zarządzaniem naruszeniami ochrony danych w organizacji.

Po pierwsze, dokonując oceny powagi naruszenia ochrony danych, należy pamiętać o tym, że fakt, że klient sam podał błędny adres poczty elektronicznej, na który został wysłany dokument zawierający dane osobowe, nie może mieć wpływu na wynik oceny ryzyka naruszenia praw lub wolności. Na tę ocenę nie wpływa również to, że nieuprawniony odbiorca zwrócił się do administratora, przekazując informację o mającym miejsce naruszeniu, oraz że administrator zwrócił się z prośbą o trwałe usunięcie wiadomości i o informację zwrotną potwierdzającą to usunięcie, chyba że takiego odbiorcę można uznać za zaufanego.

[1] 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).

Ostrożnie należy jednak uznawać podmiot, który otrzymał dane osobowe bez uprawnienia, za odbiorcę zaufanego. Odbiorcę można uznać za zaufanego, jeżeli można racjonalnie oczekiwać, że ta osoba nie odczyta omyłkowo wysłanych danych lub nie uzyska do nich wglądu oraz że wypełni polecenie ich odesłania. Odbiorca w niniejszej sprawie nie został uznany przez Prezesa UODO za zaufanego.

Zdaniem Prezesa UODO podmiot dopuszczający możliwość wykorzystania do komunikacji z klientem poczty elektronicznej powinien mieć świadomość ryzyk związanych np. z nieprawidłowym podaniem przez klienta adresu poczty elektronicznej i w związku z tym powinien wdrożyć odpowiednie środki techniczne i organizacyjne.

W celu minimalizacji ryzyk z tym związanych można podjąć np. takie działania, jak: przyjęcie procedury weryfikacji podawanego adresu e-mail oraz szyfrowanie dokumentów zawierających dane osobowe wysyłanych pocztą elektroniczną (np. polis czy umów).

Jednocześnie należy zauważyć, że Prezes UODO w tej decyzji kwestionuje ocenę administratora co do wystąpienia ryzyka naruszenia praw lub wolności osób fizycznych, których dotyczy naruszenie. Zastrzeżenie budzi brak przedstawienia przez Prezesa UODO konkretnej oceny, z której wynika poziom ryzyka wymagający spełnienia obowiązku z art. 33 ust. 1 RODO i art. 34 ust. 1 RODO, oraz metodyki, z której korzysta do przeprowadzenia takiej oceny. W decyzji wyłącznie wskazano, że zakres danych osobowych objętych naruszeniem przesądza o tym, że wystąpiło wysokie ryzyko naruszenia praw i wolności osób fizycznych. W praktyce takie stanowisko Prezesa UODO jest niewystarczające i może prowadzić do sytuacji, w której administratorzy będą zgłaszać wszystkie naruszenia ochrony danych, bez względu na poziom ryzyka.

Źródło:
https://uodo.gov.pl/pl/138/1801
https://uodo.gov.pl/decyzje/DKN.5131.5.2020

Prezes UODO nałożył administracyjną karę pieniężną za opóźnioną reakcję na informację o lukach w systemie

r.pr Dominika Nowak

Dnia 17 grudnia 2020 r. Prezes UODO wydał decyzję nakładającą na administratora: ID Finance Poland Sp. z o.o., właściciela portalu pożyczkowego MoneyMan.pl, administracyjną karę pieniężną za opóźnioną reakcję na informację o lukach w systemie, co doprowadziło do naruszenia poufności, integralności i dostępności danych osobowych.

Stan faktyczny

Na decyzję podjętą przez organ nadzorczy miały wpływ następujące elementy stanu faktycznego. Administrator nie zareagował odpowiednio szybko na otrzymany sygnał o lukach w zabezpieczeniach na serwerze obsługiwanym przez podmiot przetwarzający. Luki te sprawiły, że dane klientów były dostępne dla osób nieuprawnionych. Z powodu braku reakcji osoba nieuprawniona skopiowała te informacje i usunęła z serwera. Za ich zwrot zażądano okupu. Te wydarzenia spowodowały, że administrator dokonał analizy zabezpieczeń oraz zgłosił naruszenie ochrony danych organowi nadzoru.

Naruszenie dotyczyło następujących danych osobowych: imię i nazwisko, poziom wykształcenia, adres e-mail, dane dotyczące zatrudnienia, adres e-mail osoby, której klient chce polecić pożyczkę, dane dotyczące zarobków, dane dotyczące stanu cywilnego, numery telefonu, numer PESEL, narodowość, numer NIP, miejsce urodzenia, adres korespondencyjny, adres zameldowania, numer telefonu do miejsca pracy oraz numer rachunku bankowego. **Doszło również do naruszenia poufności haseł, które – co należy podkreślić – nie były zaszyfrowane**.

Decyzja

W konsekwencji Prezes UODO w decyzji z dnia 17 grudnia 2020 r. (DKN.5130.1354.2020) stwierdził naruszenie przez ID Finance Poland sp. z o.o. w likwidacji z siedzibą w Warszawie przepisów **art. 5 ust. 1 lit. f, art. 25 ust. 1, art. 32 ust. 1 lit. b, art. 32 ust. 1 lit. d oraz art. 32 ust. 2 RODO**[1], polegające na niewdrożeniu, zarówno w fazie projektowania procesu przetwarzania, jak i w czasie samego przetwarzania, odpowiednich środków technicznych i organizacyjnych:

- odpowiadających ryzyku naruszenia zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemu przetwarzania danych osobowych;
- zapewniających zdolność skutecznego i szybkiego stwierdzenia naruszenia ochrony danych osobowych;
- zapewniających regularną ocenę skuteczności tych środków, co skutkowało uzyskaniem przez osoby trzecie nieuprawnionego dostępu do przetwarzanych danych osobowych.
- Prezes UODO nałożył na ID Finance Poland sp. z o.o. w likwidacji administracyjną karę pieniężną w wysokości 1 069 850 złotych (jeden milion sześćdziesiąt dziewięć tysięcy osiemset pięćdziesiąt złotych).

Komentarz

Biorąc pod uwagę analizowaną decyzję Prezesa UODO, należy zwrócić uwagę na dwie kwestie. Po pierwsze szyfrowanie haseł użytkowników do ich kont na portalach społecznościowych, w sklepach internetowych lub innych jest obecnie uznawane za standard przez organ nadzorczy. Administratorzy powinni uwzględniać ten sposób zabezpieczenia danych już na etapie projektowania zabezpieczeń technicznych zgodnie z art. 25 ust. 1 RODO.

Po drugie administrator powinien przyjąć środki techniczne i organizacyjne umożliwiające szybkie stwierdzenie naruszenia ochrony danych osobowych, a następnie wdrożenie środków zaradczych. W praktyce oznacza to np., że przyjęte przez administratora procedury powinny być wdrożone, a pracownicy przeszkoleni z wyznaczonego sposobu postępowania.

Po trzecie administrator powinien wdrożyć środki umożliwiające regularne sprawdzanie, czy wprowadzone rozwiązania działają i czy są stosowane.

Źródło:
https://uodo.gov.pl/pl/138/1809
https://uodo.gov.pl/decyzje/DKN.5130.1354.2020

[1] 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).

PUBLIKACJE

- **„Czy czeka nas konkurencyjny organ nadzorczy?”** – artykuł autorstwa dr Igi Małobęckiej-Szwast, w którym analizuje, czy organy ochrony konkurencji i konsumentów staną się konkurencyjnymi organami nadzorczymi. Artykuł ukazał się w nr 1/2021 kwartalnika ABI Expert.

- **„Zagrożenia przy korzystaniu ze służbowej poczty elektronicznej”** - artykuł autorstwa r.pr. Dominiki Nowak na temat zagrożeń dla służbowej poczty elektronicznej, zapobiegania naruszeniom oraz postępowaniu w razie wstąpienia naruszenia ochrony danych. Artykuł ukazał się w Rzeczpospolitej 15 stycznia 2020 r.

- **„Ochrona danych osobowych studentów w dobie rozwoju technologii biometrycznych wyzwaniem dla polskich uczelni”** – artykuł autorstwa Mateusza Kupca dotyczący zagadnienia przetwarzania danych biometrycznych studentów jako wrażliwych podmiotów danych przez uczelnie wyższe. Artykuł ukazał się w Zeszycie 25 nr 4 Białostockich Studiów Prawniczych.

- **"Ochrona danych wewnątrz związków zawodowych"** – artykuł autorstwa Mateusza Kupca dotyczący praktycznych problemów ochrony danych osobowych w związkach zawodowych. Artykuł ukazał się w nr 1/2021 kwartalnika ABI Expert.

- **"Podstawy prawne przetwarzania"** – artykuł autorstwa Mateusza Kupca stanowiący przegląd decyzji europejskich organów nadzorczych oraz wyroków sądów dotyczących zagadnienia legalności przetwarzania danych. Artykuł ukazał się w nr 1/2021 kwartalnika ABI Expert.

- **„Inspektor ochrony danych wobec działań władczych organu nadzorczego w sprawach indywidualnych”** – artykuł autorstwa dr hab. Grzegorza Sibiga na temat sytuacji prawnej i roli IOD w stosunku do organu nadzorczego. Artykuł ukazał się w dodatku do Monitora Prawniczego (nr 23/2020).

- **"Ocena odpowiedniości przepisów RODO do zapewnienia przejrzystości działania systemów AI – wybrane zagadnienia"** – artykuł autorstwa adw. Katarzyny Syski na temat stosowania przepisów RODO o przejrzystości, w tym przepisów dotyczących całkowicie zautomatyzowanych decyzji, do systemów sztucznej inteligencji. Artykuł ukazał się w dodatku do Monitora Prawniczego (nr 23/2020).

- **„Oddziaływanie prawa ochrony danych osobowych (RODO) na prawo ochrony konkurencji i konsumentów”** – artykuł autorstwa dr Igi Małobęckiej-Szwast na temat oddziaływania RODO na prawo ochrony konkurencji i konsumentów. Artykuł ukazał się w dodatku do Monitora Prawniczego (nr 23/2020).

- **„Podejście oparte na ryzyku w RODO w praktyce – wnioski po dwóch latach stosowania RODO”** – artykuł autorstwa r.pr. Dominiki Nowak na temat oceny stosowania podejścia opartego na ryzyku na podstawie RODO w praktyce oraz dwóch rozwiązań, które mogą być pomocne w jego stosowaniu: normy ISO/EIC 27701 oraz standardu Ramy Prywatności opublikowanego NIST. Artykuł ukazał się w Dodatku do Monitora Prawniczego nr 23/2020.

WYDARZENIA

10.02.2021
GODZ. 10:00-13:00

Pliki cookies – aspekty techniczne, najnowsze orzecznictwo i wytyczne organów regulacyjnych, aspekty proceduralne postępowań o naruszenie zasad korzystania z cookies

Prelegenci: adw. Xawery Konarski, adw. dr hab. Grzegorz Sibiga, dr inż. Andrzej Kaczmarek, r.pr. Dominika Nowak

W 2020 r. organy krajowe poszczególnych państw Unii Europejskiej wydały szereg decyzji nakładających wysokie kary pieniężne za naruszenie przepisów o korzystaniu z cookies. W sprawach tych orzekał również Trybunał Sprawiedliwości Unii Europejskiej oraz sądy krajowe. Podstawą materialnoprawną tych decyzji oraz orzeczeń były zarówno przepisy RODO, jak przepisy o e-Prywatności.

Podczas webinarium omówimy kwestie techniczne i prawne związane ze stosowaniem plików cookies w praktyce. W naszych prezentacjach uwzględnimy najnowsze decyzje i wytyczne organów nadzorczych, najistotniejsze orzecznictwo oraz projekt Prawa komunikacji elektronicznej.

Program webinarium

10.00 – 10.10 **Wstęp - Powitanie uczestników**

10.10 – 10.50 **Techniczne aspekty związane z plikami cookies - dr inż. Andrzej Kaczmarek**
- uporządkowanie terminologii dotyczącej plików cookies
- omówienie technologii działających podobnie jak pliki cookies
- rodzaje cookies
- przepływy informacji w związku z działaniem plików cookies

10.50 – 11.30 **Najważniejsze problemy prawne dotyczące korzystania z plików cookies na podstawie orzecznictwa, decyzji, oraz stanowisk organów nadzorczych - adw. Xawery Konarski**
- omówienie kluczowych wyroków TSUE dotyczących plików cookies
- identyfikacja najważniejszych problemów prawnych dotyczących korzystania z plików cookies w świetle decyzji i wytycznych organów nadzorczych państw UE
- elementy przesądzające o stwierdzeniu naruszenia przepisów i wysokości nakładanych kar na podstawie przepisów RODO i o e-Prywatności

11.30 – 12.10 **Zasady dopuszczalnego korzystania z cookies – aktualny i przyszły stan prawny - r.pr. Dominika Nowak**
- Praktyczne omówienie kluczowych wytycznych organów nadzorczych - jak stosować pliki cookies zgodnie z przepisami?
- Znaczenie prawne podziału na niezbędne, funkcjonalne i reklamowe cookies
- O czym należy pamiętać wdrażając regulacje dotyczące plików cookies?
- Regulacja cookies w projekcie Prawa komunikacji elektronicznej

12.10 – 12.50 **Kompetencje Prezes UODO i Prezesa UKE oraz ich wykonywanie w sprawach stosowania cookies - adw. dr hab. Grzegorz Sibiga**
- Kompetencje Prezesa UODO i Prezesa UKE w sprawach stosowania plików cookies – sankcje przewidziane za naruszenia przepisów
- Czy może dojść do kolizji kompetencji Prezesa UODO i Prezesa UKE ?
- Specyfika postępowań Prezesa UODO oraz Prezesa UKE.
- Przykłady spraw dotyczących cookies

12.50 – 13.00 **Zakończenie – sesja pytań i odpowiedzi**

Rejestracja >>

ZESPÓŁ RODO

Xawery Konarski
Adwokat, Senior Partner
xawery.konarski@traple.pl

dr hab. Grzegorz Sibiga
Adwokat, Partner
grzegorz.sibiga@traple.pl

Katarzyna Syska
Adwokat, Senior Associate
katarzyna.syska@traple.pl

Dominika Nowak
Radca prawny, Senior Associate
dominika.nowak@traple.pl

dr Iga Małobęcka-Szwast LL.M.
Senior Associate
iga.malobecka@traple.pl

Katarzyna Barszczewska-Mazur
Associate
katarzyna.barszczewska@traple.pl

Mateusz Kupiec
Trainee
mateusz.kupiec@traple.pl

Redaktor newslettera:
dr Iga Małobęcka-Szwast

Pytania prosimy kierować na adres:
rodo@traple.pl