Warszawa, 12.05.2017r.

STANOWISKO OMNI MODO W RAMACH KONSULTACJI DOKUMENTÓW DOTYCZĄCYCH GDPR (PROFILOWANIE / ZGODA/ ZGŁOSZENIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH)

Przygotowali:

Marta Bargiel-Kaflik

Marcin Cwener

Mirosław Gumularz

PROFILOWANIE

1. Relacja pojęcia zautomatyzowanego podejmowania decyzji (w tym profilowania) z art. 22 GDPR[1] i profilowania z art. 21 ust. 1–2 GDPR

Z jednej strony GDPR w art. 21 ust. 1–2 (w kontekście prawa sprzeciwu) zdaje się przesądzać, iż w przypadku profilowania wykorzystywanego w celu marketingu bezpośredniego możliwe jest powołanie się na prawnie uzasadniony interes administratora lub strony trzeciej (czyli bez odrębnej zgody na profilowanie/o ile ten interes zachodzi). Z drugiej jednak strony, art. 21 ust. 1–2 GDPR w odróżnieniu od innych przepisów (np. art. 22 GDPR) nie mówi o profilowaniu w kontekście zautomatyzowanego podejmowania decyzji.

W tym zakresie możliwe są dwa warianty interpretacyjne:

a. przyjęcie, że każde profilowanie w celach marketingu bezpośredniego może potencjalnie opierać się na usprawiedliwionym interesie administratora danych lub strony

[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).

trzeciej – niezależnie od kwalifikacji jako zautomatyzowane podejmowanie decyzji (decyzji w rozumieniu motywu 71 GDPR);

b. przyjęcie, że tylko profilowanie (w celach marketingu bezpośredniego), które nie jest jednocześnie zautomatyzowanym podejmowaniem decyzji może być oparte na uzasadnionym interesie (a nie na przesłankach z art. 22 GDPR). Przyjmując drugi wariant, konieczność zebrania dodatkowej zgody na profilowanie (na podstawie art. 22 ust. 2 GDPR) na potrzeby marketingu bezpośredniego uzależniona byłaby każdorazowo od ustalenia czy w danym stanie faktycznym takie profilowanie polega na wywoływaniu skutków prawnych lub czy wpływa znacząco na podmiot danych (np. dyskryminująco). W praktyce istotny będzie ten drugi element. Przyjęcie drugiego stanowiska prowadziłoby ad absurdum, ponieważ stosowanie art. 22 GDPR oznacza m.in. umożliwienie „odwołania się" od podejmowanej decyzji, co w przypadku marketingu wydaje się nieracjonalne (art. 22 ust. 3 GDPR – prawo do uzyskania interwencji ludzkiej ze strony administratora, do wyrażenia własnego stanowiska i do zakwestionowania tej decyzji).

Pytania:

– czy prawnie uzasadniony interes administratora danych (o ile ta przesłanka zostanie wykazana) uzasadnia kierowanie marketingu bezpośredniego (np. reklamy behawioralnej, mailing) bez konieczności badania przesłanki „podejmowania decyzji" tj. bez konieczności zbierania zgody, o której mowa w art. 22 GDPR?[2]

– czy w ogóle kierowanie marketingu bezpośredniego (na podstawie profilowania) może zostać zakwalifikowane jako zautomatyzowane podejmowanie decyzji?

– czy – przyjmując, że marketing bezpośredni może być kwalifikowany w pewnych sytuacjach jako zautomatyzowane podejmowanie decyzji w rozumieniu art. 22 GDPR – możliwe jest przetwarzanie danych na potrzeby wysyłania informacji handlowych na podstawie jednej zgody? np. wyrażam zgodę na przetwarzanie przez X moich danych osobowych polegające na profilowaniu, w celu marketingu bezpośredniego realizowanego poprzez przesyłanie informacji handlowych drogą elektryczną. Czy w takiej sytuacji zgoda z art. 22 ust. 2 GDPR zawsze powinna być odrębnym oświadczeniem?

[2] Natomiast to czy należy zbierać zgodę marketingową z art. 10 ustawy o świadczeniu usług drogą elektroniczną należy uznać za odrębną kwestię.

2. Pojęcie profilowania i zautomatyzowanego podejmowania decyzji, a obowiązki informacyjne

Zgodnie z treścią z art. 13 ust. 1 GDPR:

„Jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, administrator podczas pozyskiwania danych osobowych podaje jej wszystkie następujące informacje:

(…)

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.

Literalne brzmienie tego przepisu wskazuje, iż obowiązek informacyjny dotyczy wyłącznie zautomatyzowanego podejmowania decyzji. Profilowanie niebędące zautomatyzowanym podejmowaniem decyzji nie podlega tej regulacji i nie wymaga spełnienia obowiązku informacyjnego z art. 13 GDPR.

Pytanie:

czy kierowanie informacji handlowych drogą elektroniczną (np. przez administratora danych na podstawie zgody z art. 10 ustawy o świadczeniu usług drogą elektroniczną i przy spełnieniu przesłanek legalizujących z art. 6 GDPR) wymaga spełnienia obowiązku informacyjnego wskazanego powyżej?

ZGODA

1. Czy cofnięcie zgody w związku z uprawnieniem określonym w art. 17 ust. 1 lit b GDPR, powinno skutkować usunięciem danych również z kopii zapasowych systemów informatycznych?

Zgodnie z art. 17 ust. 1 lit. b GDPR „osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli (…) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie (…) i nie ma innej podstawy prawnej przetwarzania”. Przy założeniu, że nie zachodzi żadna przesłanka określona w ust. 3 ww. przepisu, literalna wykładania przemawia za przyjęciem stanowiska, zgodnie z którym usunięcie danych powinno być całkowite i nieodwracalne.

PYTANIA:

– czy w takim przypadku administrator będzie zobowiązany również do usunięcia danych z kopii bezpieczeństwa (backup)?

– czy możliwe jest przechowanie danych na potrzeby wewnętrznej listy robinsona (w celu nie pozyskiwania zgody od osoby, która ją cofnęła?

2. Możliwość zbierania zgody w formie jednego oświadczenia obejmującego kilka celów

W myśl art. 6 ust.1 lit a GDPR, zgoda może być wyrażona na przetwarzanie danych w jednym lub większej liczbie określonych celów. Literalna wykładania przepisu zdaje się sugerować możliwość wyrażenia za pomocą jednego oświadczenia woli (np. w formie jednej klauzuli) zgody na przetwarzanie danych w kilku celach. Jednakże stanowisko takie byłoby sprzeczne z wnioskami zawartymi w motywach GDPR. W motywie 32 podkreślono bowiem, że zgoda powinna dotyczyć wszystkich czynności przetwarzania dokonywanych w tym samym celu lub w tych samych celach. Jeżeli przetwarzanie służy różnym celom, potrzebna jest zgoda na wszystkie te cele. Dodatkowo zgodnie z motywem 43 zgody nie uważa się za dobrowolną, jeżeli nie można jej wyrazić z osobna na różne operacje przetwarzania danych osobowych, mimo że w danym przypadku byłoby to stosowne, lub jeżeli od zgody uzależnione jest wykonanie umowy – w tym świadczenie usługi – mimo że do jej wykonania zgoda nie jest niezbędna. Połączenie w jednej klauzuli kilku oświadczeń bezwzględnie wyłącza dobrowolność wyrażenia zgody.

PYTANIE:

Czy na gruncie GDPR dopuszczalne będzie zbieranie w jednej klauzuli kilku oświadczeń, których przedmiotem jest wyrażenie zgody na przetwarzanie danych? Jeśli nie, w jaki sposób należy rozumieć przepis 6 ust.1 lit a GDPR?

3. Wyraźne działanie potwierdzające a opcja double opt-in

Zgodnie z art. 4 pkt 11 GDPR zgoda osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych. Ustalenie bezpiecznego (zgodnego z przepisami GDPR) sposobu wyrażenia zgody w formie wyraźnego działania potwierdzającego ma zatem doniosłe znaczenie praktyczne dla administratorów. W przypadku zbierania zgody za pomocą formularzy internetowych, wydaje się, że wyraźnym działaniem potwierdzającym może być wprowadzenie adresu poczty e-mail, a następnie potwierdzenie dyspozycji przy wykorzystaniu linku przesłanego na wskazany w formularzu adres e-mail.

PYTANIE:

Czy na gruncie GDPR wyraźne działanie potwierdzające w przypadku zgód zbieranych za pomocą formularzy internetowych, powinno być realizowane z wykorzystaniem opcji double opt-in, czy też wystarczającym jest zastosowanie opcji single opt-in (na wzór rozwiązania określonego w art. 10 ušude – pozostawienie adresu e-mail w celu otrzymywania informacji handlowej drogę elektroniczną)

4. Podstawa prawna przetwarzania danych przez podmioty, którym udostępniono dane na podstawie zgody

Na gruncie obecnie obowiązujących przepisów, w przypadku udostępnienia danych osobowych podmiotom trzecim na podstawie zgody (np. udostępnienie danych w celach marketingowych na rzecz podmiotów trzecich), przyjąć można dwie koncepcje w kontekście podstawy prawnej przetwarzania danych przez odbiorcę danych, tj. że przetwarza dane na podstawie zgody (tzw. zgoda przechodząca), lub przetwarza dane na podstawie prawnie usprawiedliwionego celu.

PYTANIE:

Czy odbiorca danych, któremu udostępniono dane na podstawie zgody udzielonej przez osobę, której dane dotyczącą, przetwarza dane na podstawie zgody, czy też innej przesłanki określonej w art. 6 GDPR?

ZGŁASZANIE NARUSZEŃ OCHRONY DANYCH OSOBOWYCH

1. Stwierdzenie naruszenia ochrony danych

Zgodnie z art. 33 ust. 1 GDPR, „w przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin **po stwierdzeniu naruszenia** – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia".

PYTANIA:

– Czy zgłoszenie naruszenia ochrony danych zakłada uprzednie zgromadzenie dowodów jednoznacznie potwierdzających, że do naruszenia doszło? Czy ratio legis obowiązku notyfikacyjnego polega również na zgłaszaniu wysokiego prawdopodobieństwa, że do naruszenia mogło dojść (np. w sytuacji, w której administrator dowiaduje się o takiej sytuacji z mediów)?

– Czy przed zgłoszeniem naruszenia ochrony danych administrator danych musi dysponować dowodami jednoznacznie potwierdzającymi, że do naruszenia doszło czy też uzyskanie wysokiego prawdopodobieństwa, że do naruszenia mogło dojść, powoduje konieczność zgłoszenia naruszenia.

2. Skutki zgłoszenia naruszenia

Przepis art. 32 GDPR stanowi, iż 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 zagrożenia, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku (…).

PYTANIE:

Czy w przypadku zastosowania przez administratora danych – przy uprzednim uwzględnieniu stanu wiedzy technicznej, kosztu wdrażania oraz charakteru, zakresu,

kontekstu i celu przetwarzania oraz ryzyka naruszenia praw lub wolności osób fizycznych – środków technicznych i organizacyjnych, które jednak okazały się niewystarczające do ochrony przetwarzanych danych, co doprowadziło do naruszenia tej ochrony oraz notyfikowania tego faktu do organu nadzorczego, na administratora danych może zostać nałożona administracyjna kara pieniężna?

3. Rola Inspektora Ochrony Danych przy zgłaszaniu naruszeń ochrony danych

Zgodnie z art. 39 ust. 1 GDPR, inspektor ochrony danych ma następujące zadania:

a) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;

b) monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;

c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35;

d) **współpraca z organem nadzorczym;**

e) **pełnienie funkcji punktu kontaktowego dla organu nadzorczego** w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz **w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.**

W myśl natomiast przepisu art. 33 ust. 3 GDPR, zgłoszenie, o którym mowa w ust. 1, musi **co najmniej**:

a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;

b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;

c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;

d) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

PYTANIE:

Przepisy GDPR nie precyzują kto powinien podpisać zgłoszenie o zaistnieniu naruszenia ochrony danych osobowych. Na gruncie orzecznictwa TSUE oraz wypracowanej reguły Rewe/Comet, doprecyzowanie przez ustawodawstwo krajowe pełnej formy zgłoszenia może pozostawać w sprzeczności z tą zasadą, jako że nie można stwierdzić, aby brak w przepisach GDPR pełnej informacji o kształcie zgłoszenia utrudniał wykonywanie przepisów unijnych.

Czy zatem wobec braku precyzyjnej informacji o tym kto obowiązany jest do podpisania notyfikacji, w sytuacji braku zgodności oceny administratora danych z oceną dokonaną przez inspektora ochrony danych osobowych co do zajścia naruszenia ochrony danych decydujące jest stanowisko administratora danych czy też inspektora ochrony danych? Czy notyfikacja naruszenia powinna być podpisana przez administratora danych czy przez inspektora ochrony danych? W jaki sposób inspektor ochrony danych powinien zachować się w sytuacji, w której administrator danych, który go wyznaczył, nie podejmuje kroków zmierzających do notyfikowania naruszenia ochrony danych?

4. Zakres przedmiotowy rejestru naruszeń ochrony danych

W myśl art. 33 ust. 5 GDPR, administrator dokumentuje **wszelkie** naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić **organowi nadzorczemu** weryfikowanie przestrzegania niniejszego artykułu.

PYTANIE:

Czy dokumentowanie naruszeń ochrony danych osobowych obejmować ma naruszenia, które zostały notyfikowane organowi nadzorczemu, czy też obejmować ma także naruszenia, co do których brak było obowiązku prawnego zgłoszenia organowi nadzorczemu?