GRUPA ROBOCZA ARTYKUŁU 29 DS. OCHRONY DANYCH

17/PL

WP260

Wytyczne dotyczące przejrzystości na mocy rozporządzenia 2016/679

GRUPA ROBOCZA DS. OCHRONY OSÓB FIZYCZNYCH W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH

powołana na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r.,

uwzględniając art. 29 i art. 30 ust. 1 lit. a) oraz ust. 3 wspomnianej dyrektywy,

uwzględniając swój regulamin wewnętrzny,

PRZYJMUJE NINIEJSZY DOKUMENT:

Spis treści

Wprowadzenie

1. Niniejsze wytyczne zapewniają praktyczne wskazówki oraz pomoc w interpretacji nowego obowiązku zapewnienia przejrzystości przetwarzania danych osobowych na mocy ogólnego rozporządzenia o ochronie danych[1] ("**RODO**"). Przejrzystość stanowi nadrzędny wymóg na mocy RODO mający zastosowanie do trzech głównych obszarów: (1) zapewniania informacji osobom, których dane dotyczą, związanych z rzetelnym przetwarzaniem; (2) sposobów, w jakie administratorzy danych komunikują się z osobami, których dane dotyczą, w związku z ich prawami wynikającymi z RODO; oraz (3) sposobów umożliwiania przez administratorów danych wykonywania swoich praw przez osoby, których dane dotyczą[2]. O ile zgodność z zasadą przejrzystości jest wymagana w odniesieniu do przetwarzania danych na mocy dyrektywy (UE) 2016/680[3], wytyczne te mają również zastosowanie do interpretacji tej zasady.[4]

2. Przejrzystość to od dawna ustanowiona cecha prawa UE[5]. Dotyczy ona budowania zaufania wobec procedur, które mają wpływ na obywatela, umożliwiając mu zrozumienie, oraz gdy to konieczne, podważenie tych procedur. Jest ona również wyrazem zasady rzetelności w odniesieniu do przetwarzania danych osobowych wyrażonej w artykule 8 Karty Praw Podstawowych Unii Europejskiej. Zgodnie z RODO (artykuł 5 ust. 1 lit. a)[6]), dodatkowo do wymogów, zgodnie z którymi dane muszą być przetwarzane zgodnie z prawem i rzetelnie, przejrzystość jest obecnie wskazana jako podstawowy aspekt tych zasad.[7] Przejrzystość jest nierozerwalnie związana z rzetelnością i nową zasadą rozliczalności na mocy RODO. Z artykułu 5 ust. 2 wynika również, że administrator musi być w stanie wykazać, że dane osobowe są przetwarzane w sposób przejrzysty dla osoby, której dane dotyczą.[8] Powiązana z tym zasada rozliczalności wymaga przejrzystości operacji przetwarzania, aby administratorzy

[1] Rozporządzenie (UE) 2016/679 Parlamentu Europejskiego i Rady 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.

[2] Wytyczne te określają ogólne zasady w odniesieniu do wykonywania praw przez osoby, których dane dotyczą, zamiast rozważać konkretne procedury dla każdego z praw osoby, której dane dotyczą, na mocy RODO.

[3] Dyrektywa (UE) 2016/680 Parlamentu Europejskiego i Rady 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.

[4] Podczas gdy przejrzystość jest jedną z zasad dotyczących przetwarzania danych osobowych określonych w artykule 4 dyrektywy (UE) 2016/680, motyw 26 stanowi, że wszelkie przetwarzanie danych osobowych musi być "zgodne z prawem, rzetelne i przejrzyste" dla osób fizycznych, których sprawa dotyczy.

[5] Artykuł 1 TUE odnosi się do decyzji podejmowanych "*z możliwie najwyższym poszanowaniem zasady otwartości i jak najbliżej obywateli";* artykuł 11 ust. 2 stanowi, że "*instytucje utrzymują otwarty, przejrzysty i regularny dialog ze stowarzyszeniami przedstawicielskimi i społeczeństwem obywatelskim";* oraz artykuł 15 TFUE dotyczy między innymi obywateli Unii mających prawo dostępu do dokumentów instytucji, organów i jednostek organizacyjnych Unii oraz wymogów tych instytucji, organów i jednostek organizacyjnych Unii w celu zapewnienia przejrzystości ich prac.

[6] "Dane osobowe muszę być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą".

[7] W dyrektywie 95/46/WE, do przejrzystości odniesiono się w motywie 38 tylko poprzez wymóg, aby przetwarzanie było rzetelne, ale nie odniesiono się do niej w odpowiadającym mu artykule 6 ust. 1 lit. a).

[8] Artykuł 5 ust. 2 RODO zobowiązuje administratora danych do wykazania przejrzystości (wraz z pięcioma innymi zasadami dotyczącymi przetwarzania danych określonymi w artykule 5 ust. 1) zgodnie z zasadą rozliczalności.

danych byli w stanie wykazać przestrzeganie obowiązków wynikających z RODO[9]. Zgodnie z motywem 171 RODO, gdy przetwarzanie przed 25 maja 2018 r. już się toczy, administrator powinien zapewnić przestrzeganie obowiązków w zakresie przejrzystości z dniem 25 maja 2018 r. (wraz z wszystkimi innymi obowiązkami wynikającymi z RODO). Oznacza to, że przed 25 maja 2018 r. administratorzy danych powinni zrewidować wszystkie informacje przekazywane osobom, których dane dotyczą, odnoszące się do przetwarzania ich danych osobowych (na przykład oświadczeń / informacji dotyczących prywatności, etc.) w celu zapewnienia, że przestrzegają wymogów w odniesieniu do przejrzystości, które są omawiane w tych wytycznych.

3. Gdy przejrzystość jest zapewniana przez administratorów danych, uprawnia ona osoby, których dane dotyczą, do rozliczania administratorów danych i podmiotów przetwarzających oraz do realizacji kontroli nad ich danymi osobowymi, na przykład poprzez udzielenie lub wycofanie świadomej zgody oraz wykonanie ich praw osób, których dane dotyczą[10]. Pojęcie przejrzystości w RODO jest raczej ukierunkowane na użytkownika, a nie legalistyczne, i jest realizowane poprzez konkretne praktyczne wymogi nałożone na administratorów danych i podmioty przetwarzające w szeregu artykułów. Praktyczne wymogi (informacyjne) są określone w artykułach 12-14 RODO. Jednak jakość, dostępność i zrozumiałość informacji są tak ważne jak rzeczywista treść informacji dotyczących przejrzystości, które muszą być zapewnione osobom, których dane dotyczą.

4. Wymogi w zakresie przejrzystości zawarte w RODO mają zastosowanie niezależnie od podstawy prawnej przetwarzania i przez cały cykl przetwarzania. Wynika to wyraźnie z artykułu 12, który stanowi, że przejrzystość ma zastosowanie na następujących etapach cyklu przetwarzania danych:

- przed lub na początku cyklu przetwarzania danych, tj. gdy dane osobowe są zbierane czy to od osoby, której dane dotyczą, czy też pozyskiwane w inny sposób;

- przez cały okres przetwarzania, tj. podczas komunikowania się z osobami, których dane dotyczą, na temat ich praw; oraz

- w określonych momentach, gdy przetwarzanie trwa, na przykład gdy występują naruszenia danych lub w przypadku istotnych zmian w przetwarzaniu.

Znaczenie przejrzystości

5. Przejrzystość nie jest zdefiniowana w RODO. Motyw 39 RODO informuje o znaczeniu i skutkach zasady przejrzystości w kontekście przetwarzania danych:

> *„Dla osób fizycznych powinno być przejrzyste, że dotyczące ich dane osobowe są zbierane, wykorzystywane, przeglądane lub w inny sposób przetwarzane oraz w jakim*

[9] Nałożony na administratorów danych obowiązek wdrożenia środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z RODO i aby móc to wykazać, jest określony w artykule 24 ust. 1.

[10] Patrz na przykład opinia rzecznika generalnego Cruz Villalón przedstawiona (9 lipca 2015 r.) w sprawie Bara (sprawa C-201/14), par. 74: „*wymóg informowania osób, których dotyczy przetwarzanie ich danych osobowych, który gwarantuje przejrzystość wszelkich czynności przetwarzania, jest tym ważniejszy, iż uzależnione jest od niego wykonywanie przez osoby zainteresowane ich prawa dostępu do przetwarzanych danych, przewidzianego w art. 12 dyrektywy 95/46, oraz ich prawa sprzeciwu wobec przetwarzania tych danych, zdefiniowanego w art. 14 tej dyrektywy”.*

stopniu te dane osobowe są lub będą przetwarzane. Zasada przejrzystości wymaga, by wszelkie informacje i wszelkie komunikaty związane z przetwarzaniem tych danych osobowych były łatwo dostępne i zrozumiałe oraz sformułowane jasnym i prostym językiem. Zasada ta dotyczy w szczególności informowania osób, których dane dotyczą, o tożsamości administratora i celach przetwarzania oraz innych informacji mających zapewnić rzetelność i przejrzystość przetwarzania w stosunku do osób, których sprawa dotyczy, a także prawa takich osób do uzyskania potwierdzenia i informacji o przetwarzanych danych osobowych ich dotyczących."

Elementy przejrzystości na mocy RODO

6. Kluczowe artykuły odnoszące się do przejrzystości w RODO, mające zastosowanie do praw osoby, której dane dotyczą, znajdują się w Rozdziale III (Prawa osoby, której dane dotyczą). Artykuł 12 określa ogólne zasady dotyczące: zapewniania informacji osobom, których dane dotyczą (na mocy artykułów 13-14); komunikowania się z osobami, których dane dotyczą w kwestiach wykonania ich praw (na mocy artykułów 15-22); oraz komunikowania się w kwestii naruszeń ochrony danych (artykuł 34). Artykuł 12 wymaga w szczególności, że przedmiotowe informacje lub komunikacja muszą być zgodne z następującymi zasadami:

- muszą być zwięzłe, przejrzyste, zrozumiałe i łatwo dostępne (artykuł 12 ust. 1);

- musi być użyty jasny i prosty język (artykuł 12 ust. 1);

- wymóg użycia jasnego i prostego języka ma szczególne znaczenie przy udzielaniu informacji dzieciom (artykuł 12 ust. 1);

- muszą być udzielone na piśmie „*lub w inny sposób, w tym w stosownych przypadkach – elektronicznie"* (artykuł 12 ust. 1);

- jeżeli osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie (artykuł 12 ust. 1); oraz

- muszą być wolne od opłat (artykuł 12 ust. 5).

„Zwięzłe, przejrzyste, zrozumiałe i łatwo dostępne"

7. Wymóg, aby podawać informacje osobom, których dane dotyczą, oraz aby prowadzić z nimi komunikację w „*zwięzły i przejrzysty*" sposób oznacza, że administratorzy danych powinni przedstawiać informacje / prowadzić komunikację skutecznie i zwięźle w celu uniknięcia zmęczenia informacyjnego. Informacje te powinny być wyraźnie odróżnione od innych informacji niezwiązanych z ochroną prywatności, takich jak przepisy umowne. W kontekście online wykorzystanie warstwowych oświadczeń / informacji o prywatności umożliwi osobie, której dane dotyczą, przejście do konkretnej części takich oświadczeń / informacji, do których osoby raczej chcą uzyskać natychmiastowy dostęp zamiast musieć przewijać duże ilości tekstu w poszukiwaniu określonych kwestii.

8. Wymóg, aby informacje były „zrozumiałe" oznacza, że powinny być zrozumiane przez przeciętnego docelowego odbiorcę. Oznacza to, że administrator musi najpierw zidentyfikować grupę docelową oraz ocenić poziom zrozumienia przeciętnego odbiorcy. Jednak w związku z tym, że grupa docelowa może różnić się od rzeczywistej grupy odbiorców, administrator powinien również regularnie sprawdzać, czy informacje / komunikacja są nadal dostosowane do rzeczywistej grupy odbiorców (w szczególności, gdy należą do niej dzieci), oraz dokonywać dostosowań, gdy to konieczne. Administratorzy mogą wykazać zgodność z zasadą

przejrzystości, sprawdzając zrozumiałość informacji i skuteczność interfejsów / informacji / polityk dla użytkownika, etc., poprzez panele użytkownika.

9. Głównym aspektem zasady przejrzystości określonym w tych postanowieniach jest to, że osoba, której dane dotyczą, powinna być w stanie określić z góry, jaki zakres i jakie konsekwencje wiążą się z przetwarzaniem. GR Art. 29 stoi na stanowisku, że w ramach dobrych praktyk, w szczególności w przypadku kompleksowego, technicznego lub nieoczekiwanego przetwarzania danych administratorzy powinni nie tylko udzielić informacji przewidzianych w artykułach 13 i 14, ale również odrębnie sprecyzować, używając jednoznacznego języka, jakie będą najważniejsze *konsekwencje* przetwarzania; innymi słowy, jakiego rodzaju wpływ określone przetwarzanie opisane w oświadczeniu / informacjach dotyczących prywatności będzie rzeczywiście miało na osobę, której dane dotyczą? Taki opis konsekwencji przetwarzania nie powinien po prostu opierać się na nieszkodliwych i przewidywalnych przykładach „najlepszych przypadków" przetwarzania danych, lecz powinien zapewnić przegląd rodzajów przetwarzania, które mogłyby mieć największy wpływ na podstawowe prawa i wolności osób, których dane dotyczą, w odniesieniu do przetwarzania ich danych osobowych.

10. Element „łatwo dostępne" oznacza, że osoba, której dane dotyczą, nie powinna być zmuszona do poszukiwania informacji; powinno być dla niej natychmiast oczywiste, gdzie można uzyskać dostęp do tych informacji, na przykład można je jej bezpośrednio przekazać, podać link do nich, wyraźnie je oznaczając lub wskazać w odpowiedzi na pytanie w języku naturalnym (na przykład w warstwowym dostępnym online oświadczeniu / informacjach dotyczących prywatności, w często zadawanych pytaniach, w formie kontekstowych wyskakujących okienek, które się uaktywniają, gdy osoba, której dane dotyczą, wypełnia formularz online, bądź też w interaktywnym kontekście cyfrowym poprzez interfejs chatbota, etc.).

Przykład

Każda organizacja, która prowadzi stronę internetową, powinna publikować oświadczenie / informacje dotyczące prywatności na stronie internetowej. Link to tego oświadczenia / informacji powinien być wyraźnie widoczny na każdej stronie tej strony internetowej pod powszechnie używanym hasłem (takim jak „ochrona prywatności", „polityka prywatności" czy „informacje dotyczące ochrony danych"). Umiejscowienie lub kolorystyka, które powodują, że tekst lub link jest mniej zauważalny lub trudny do znalezienia na stronie internetowej, nie stanowią spełnienia wymogu łatwej dostępności.

W przypadku aplikacji niezbędne informacje powinny być również udostępnione ze sklepu online przed pobraniem. Gdy aplikacja już jest zainstalowana, informacje nigdy nie powinny być dostępne dalej niż „po dwóch dotknięciach urządzenia". Ogólnie mówiąc, oznacza to, że funkcjonalność menu często wykorzystywana w aplikacjach zawsze powinna obejmować opcję „ochrona prywatności" / „ochrona danych".

GR Art. 29 zaleca jako dobrą praktykę, aby w momencie zbierania danych osobowych w kontekście online zapewniać link do oświadczenia / informacji dotyczących prywatności lub aby informacje te były udostępnione na tej samej stronie, na której zbierane są dane osobowe.

„Jasny i prosty język”

11. W przypadku informacji *na piśmie* (oraz gdy informacji udziela się ustnie lub przy użyciu metod audio / audiowizualnych, w tym dla osób, których dane dotyczą, z dysfunkcją wzroku) należy stosować dobre praktyki w zakresie jasnego pisania.[11] Podobny wymóg językowy („prostego, zrozumiałego języka”) został wcześniej wprowadzony przez ustawodawcę UE[12] i motyw 42 RODO zawiera wyraźne odniesienie do niego w kontekście zgody[13]. Wymóg używania jasnego i prostego języka oznacza, że informacje powinny być zapewniane tak jasnym i prostym językiem jak to możliwe, unikając złożonych zdań i struktur językowych. Informacje powinny być konkretne i ostateczne; nie powinny być sformułowane w sposób abstrakcyjny lub ambiwalentny, ani nie powinny pozostawiać miejsca na różne interpretacje. W szczególności cele i podstawa prawna przetwarzania danych osobowych powinny być jasne.

Przykład

Następujące zdania nie są wystarczająco jasne w odniesieniu do celów przetwarzania:

- *„Możemy wykorzystywać Twoje dane osobowe na potrzeby rozwijania nowych usług”* (ponieważ nie jest jasne, jakie są to usługi lub w jaki sposób dane pomogą w ich rozwinięciu);

- *„Możemy wykorzystywać Twoje dane osobowe na potrzeby badań” (*ponieważ nie jest jasne, do jakiego rodzaju badań się to odnosi); oraz

- „*Możemy wykorzystywać Twoje dane osobowe w celu oferowania spersonalizowanych usług”* (ponieważ nie jest jasne, co pociąga za sobą personalizacja).

12. Należy również unikać określeń językowych takich jak „może”, „mógłby”, „jakiś”, „często” oraz „możliwy”. Akapity i zdania powinny być dobrze skonstruowane, z użyciem punktorów i tiret w celu zasygnalizowania relacji hierarchicznej. Należy używać formy czynnej zamiast biernej oraz unikać używania zbyt wielu rzeczowników. Informacje zapewniane osobie, której dane dotyczą, nie powinny zawierać zbyt legalistycznego, technicznego lub specjalistycznego języka lub terminologii. Gdy informacje są tłumaczone na jeden lub więcej innych języków, administrator danych powinien zapewnić, aby wszystkie tłumaczenia były prawidłowe oraz aby składnia miała sens w innym języku (językach), tak aby przetłumaczony tekst nie musiał być rozszyfrowywany czy reinterpretowany. (Powinno być zapewnione tłumaczenie na jeden lub więcej innych języków, gdy grupą docelową administratora są osoby, których dane dotyczą, mówiące tymi językami).

[11] Patrz publikacja Komisji Europejskiej Jak pisać zrozumiale (2011), dostępna pod adresem: https://publications.europa.eu/en/publication-detail/-/publication/c2dab20c-0414-408d-87b5-dd3c6e5dd9a5.
[12] Artykuł 5 dyrektywy Rady 93/13/EWG w sprawie nieuczciwych warunków w umowach konsumenckich.
[13] Motyw 42 stanowi, że oświadczenie o wyrażeniu zgody przygotowane przez administratora powinno mieć zrozumiałą i łatwo dostępną formę, być sformułowane jasnym i prostym językiem i nie powinno zawierać nieuczciwych warunków.

Zapewnianie informacji dzieciom

13. Gdy grupą docelową administratora danych są dzieci bądź jest on lub powinien być świadomy faktu, że jego produkty / usługi są w szczególności wykorzystywane przez dzieci (i potencjalnie podstawą jest zgoda dziecka)[14], powinien on zapewnić, że słownictwo, ton lub styl używanego języka jest odpowiedni dla dzieci i tak do nich dostosowany, że dziecko będące adresatem informacji rozpozna, że wiadomość / informacja jest skierowana do niego[15]. Przydatny przykład języka ukierunkowanego na dzieci wykorzystywanego jako alternatywa wobec oryginalnego języka prawnego znajduje się w „Konwencji ONZ o prawach dziecka w języku przyjaznym dzieciom"[16]. Podobnie, jeżeli administrator danych wie, że z jego produktów / usług korzystają inni słabsi członkowie społeczeństwa, w tym osoby niepełnosprawne lub osoby, które mogą mieć trudności z dostępem do informacji (lub te produkty / usługi są do nich skierowane), administratorzy danych muszą wziąć pod uwagę słabości takich osób, których dane dotyczą, podczas dokonywania oceny, jak zapewnić, aby przestrzegać obowiązków dotyczących przejrzystości w odniesieniu do takich osób, których dane dotyczą[17]. Dotyczy to konieczności zidentyfikowania odbiorców przez administratora danych, jak to omówiono w punkcie 8.

„Na piśmie lub w inny sposób"

14. Zgodnie z artykułem 12 ust. 1 udzielanie informacji osobom, których dane dotyczą, lub komunikacja z nimi powinny odbywać się na piśmie[18]. (Artykuł 12 ust. 7 przewiduje również, że informacje, których się udziela, można opatrzyć standardowymi znakami graficznymi, i kwestia ta jest omówiona w części dotyczącej narzędzi wizualizacji w punktach 42-45). Jednak RODO pozwala również na używanie innych, nieokreślonych „środków", w tym środków elektronicznych. Stanowisko GR Art. 29 w odniesieniu do środków elektronicznych do przekazywania informacji na piśmie jest takie, że gdy administrator danych utrzymuje stronę internetową (lub, częściowo lub w pełni, działa za jej pośrednictwem), GR Art. 29 zaleca wykorzystywanie warstwowych oświadczeń / informacji dotyczących prywatności, co umożliwia odwiedzającym stronę internetową przejście do tych konkretnych aspektów określonego oświadczenia / informacji dotyczących prywatności, które ich najbardziej interesują (więcej informacji na temat warstwowych oświadczeń / informacji dotyczących prywatności – patrz punkt 30). Oczywiście stosowanie warstwowych oświadczeń / informacji dotyczących prywatności to niejedyny spośród środków elektronicznych do przekazywania informacji na piśmie, które mogą wykorzystać administratorzy. Do innych środków elektronicznych należą wyskakujące „w odpowiednim czasie" powiadomienia kontekstowe, „3D touch" lub powiadomienia pojawiające się po najechaniu kursorem, oraz panele kontroli

[14] Tj. dzieci w wieku 16 lat lub starsze (lub, gdy jest to zgodne z artykułem 8 ust. 1 RODO prawo krajowe państwa członkowskiego określiło wiek, w którym dzieci mogą wyrazić zgodę na propozycję świadczenia usług społeczeństwa informacyjnego, konkretnie między 13 a 16 rokiem życia, dla dzieci, które są w tym określonym na poziomie krajowym wieku umożliwiającym wyrażenie zgody.

[15] Motyw 38 stanowi że „Szczególnej ochrony danych osobowych wymagają dzieci, gdyż mogą one być mniej świadome ryzyka, konsekwencji, zabezpieczeń i praw przysługujących im w związku z przetwarzaniem danych osobowych". Motyw 58 stanowi że „Zważywszy że dzieci zasługują na szczególną ochronę, wszelkie informacje i komunikaty – gdy przetwarzanie dotyczy dziecka – powinny być sformułowane tak jasnym i prostym językiem, by dziecko mogło je bez trudu zrozumieć".

[16] https://www.unicef.org/rightsite/files/uncrcchilldfriendlylanguage.pdf

[17] Na przykład Konwencja ONZ o prawach osób niepełnosprawnych wymaga zapewniania odpowiedniej formy pomocy i wsparcia dla osób niepełnosprawnych w celu zapewnienia im dostępu do informacji.

[18] Artykuł 12 ust. 1 odnosi się do „języka" i stanowi, że informacji udziela się na piśmie lub w inny sposób, w tym w stosownych przypadkach – elektronicznie.

prywatności (ang. „privacy dashboard"). Do dodatkowych nietekstowych środków elektronicznych, które można zapewnić *dodatkowo* obok warstwowych oświadczeń / informacji dotyczących prywatności, można zaliczyć filmy wideo oraz ostrzeżenia głosowe smartfonów lub Internetu rzeczy[19]. Inne środki, niekoniecznie elektroniczne, mogą obejmować na przykład komiksy, infografiki lub schematy.

15. Niezbędne jest, aby metoda lub metody wybrane do udzielania informacji były dostosowane do określonych okoliczności, tj. sposobu, w jaki administrator danych i osoba, której dane dotyczą, się komunikują, lub sposobu zbierania informacji od osoby, której dane dotyczą. Na przykład przekazanie informacji jedynie na piśmie w formie elektronicznej, np. w oświadczeniu /informacji o prywatności online, może nie być odpowiednie / wykonalne w przypadku, gdy urządzenie, które zbiera dane osobowe, nie posiada ekranu (np. urządzenia Internetu rzeczy / urządzenia inteligentne) umożliwiającego dostęp do strony internetowej / wyświetlenie takich informacji. W takich przypadkach należy rozważyć odpowiednie alternatywne dodatkowe środki, na przykład zapewnienie oświadczenia / informacji dotyczących prywatności na piśmie w formie instrukcji lub podanie adresu URL strony internetowej (tj. konkretnej strony na stronie internetowej), na której znajduje się oświadczenie / informacje dotyczące prywatności w instrukcji na piśmie lub w opakowaniu. Dodatkowo można też przewidzieć zapewnienie informacji audio (ustnie), jeżeli urządzenie niemające ekranu posiada funkcje audio. GR Art. 29 wydała wcześniej zalecenia odnoszące się do przejrzystości i zapewniania informacji osobom, których dane dotyczą, w Opinii w sprawie ostatnich postępów w dziedzinie Internetu Przedmiotów[20] (jak np. stosowanie kodów QR drukowanych na przedmiotach Internetu rzeczy, tak aby podczas skanowania kodu QR wyświetlane były wymagane informacje w zakresie przejrzystości). Zalecenia te nadal będą miały zastosowanie na mocy RODO.

„… informacji można udzielić ustnie"

16. Artykuł 12 ust. 1 stanowi, że informacji można udzielić ustnie osobie, której dane dotyczą, na jej wniosek, o ile innymi sposobami (tj. nie ustnie) potwierdzi się informacje dotyczące tożsamości osoby, której dane dotyczą. Wymóg weryfikacji tożsamości osoby, której dane dotyczą, przed udzieleniem informacji ustnie ma zastosowanie tylko do informacji dotyczących wykonania praw osoby, której dane dotyczą, jak określono w artykułach 15-22 i 34. Ten warunek wstępny udzielenia informacji ustnych nie może mieć zastosowania do udzielania ogólnych informacji dotyczących prywatności, jak określono w artykułach 13 i 14, ponieważ informacje wymagane na mocy artykułów 13 i 14 muszą zawsze być udostępniane *przyszłym* użytkownikom / klientom (których tożsamości administrator danych nie byłby w stanie zweryfikować). W związku z tym informacje, które mają być zapewnione na mocy artykułów 13 i 14, mogą być udzielone ustnie bez wymagania przez administratora potwierdzenia tożsamości osoby, której dane dotyczą.

17. Ustne udzielenie informacji wymagane na mocy artykułów 13 i 14 niekoniecznie oznacza informacje ustne udzielone jednej osobie przez drugą osobę (tj. osobiście lub telefonicznie). Możliwe jest automatyczne udzielanie informacji ustanych, dodatkowo to udzielania informacji na piśmie. Na przykład może to mieć zastosowanie w kontekście osób z dysfunkcją wzroku w przypadku komunikacji z dostawcami usług społeczeństwa informacyjnego, lub w kontekście urządzeń inteligentnych nieposiadających ekranu, jak wskazano powyżej w punkcie 15. W przypadku gdy administrator danych postanowił ustnie udzielić informacji osobie, której dane

[19] Te przykłady środków elektronicznych mają jedynie charakter ilustracyjny i administratorzy danych mogą opracować nowe innowacyjne metody służące zapewnieniu zgodności z artykułem 12.
[20] Opinia GR Art. 29 8/2014, przyjęta 16 września 2014 r.

dotyczą, lub gdy osoba, której dane dotyczą, żąda udzielenia informacji ustnej lub komunikacji ustnej, GR Art. 29 uważa, że administrator danych powinien pozwolić osobie, której dane dotyczą, na ponowne odsłuchanie wcześniej nagranych wiadomości. Jest to konieczne, gdy wniosek o udzielenie informacji ustnych dotyczy osób, których dane dotyczą, z dysfunkcją wzroku lub innych osób, których dane dotyczą, które mogą mieć trudności z dostępem do informacji w formie pisemnej lub z ich zrozumieniem. Administrator danych powinien również zapewnić posiadanie zapisu i możliwość wykazania (w celu przestrzegania wymogu przejrzystości): (i) wniosku o informacje ustne, (ii) metody, za pomocą której dokonano weryfikacji tożsamości osoby, której dane dotyczą (gdy to właściwe – patrz punkt 16 powyżej) oraz (iii) faktu, że udzielono informacji osobie, której dane dotyczą.

„Wolne od opłat"

18. Na mocy artykułu 12 ust. 5 administratorzy danych nie mogą pobierać od osób, których dane dotyczą, opłat za udzielanie informacji na mocy artykułów 13 i 14 ani za komunikację i działania podejmowane na mocy artykułów 15-22 (dotyczących praw osób, których dane dotyczą) oraz artykułu 34 (zawiadamianie osób, której dane dotyczą, o naruszeniach ochrony danych osobowych). Ten aspekt przejrzystości oznacza również, że wszelkie informacje zapewniane zgodnie z wymogami w zakresie przejrzystości nie mogą być uzależnione od transakcji finansowych, na przykład od płatności za usługi lub produkty bądź od zakupu usług lub produktów.[21]

Informacje podawane osobie, której dane dotyczą – artykuły 13 i 14

Treść

19. RODO wymienia kategorie informacji, które muszą być przekazane osobie, której dane dotyczą w odniesieniu do przetwarzania jej danych osobowych, gdy dane są zbierane od osoby, której dane dotyczą (artykuł 13) lub pozyskiwane z innego źródła (artykuł 14). W **tabeli zawartej w wykazie** do niniejszych wytycznych podsumowano kategorie informacji, które muszą być podane na mocy artykułów 13 i 14. Wzięto również w niej pod uwagę charakter, zakres i treść tych wymogów. Dla jasności, GR Art. 29 stoi na stanowisku, że nie ma różnicy między statusem informacji, które mają być podane odpowiednio na mocy ustępu 1 i 2 artykułu 13 oraz 14. Wszystkie informacje w tych ustępach są równie ważne i muszą być zapewnione osobie, której dane dotyczą.

„Odpowiednie środki"

20. Podobnie jak treść, ważne są również forma i sposób, w jakich wymaga się podania informacji na mocy artykułów 13 i 14 osobie, której dane dotyczą. Zestawienie takich informacji często określa się jako informacje o ochronie danych, informacje o ochronie prywatności, politykę prywatności, oświadczenie dotyczące prywatności lub informacje

[21] Tytułem przykładu, jeżeli dane osobowe osoby, której dane dotyczą, są zbierane w związku z zakupem, informacje, których podanie wymagane jest na mocy artykułu 13, powinny być zapewnione raczej przed dokonaniem płatności i w chwili, gdy informacje są zbierane, a nie po dokonaniu transakcji. Podobnie, nawet jeżeli osobie, której dane dotyczą, świadczone są usługi wolne od opłat, informacje z artykułu 13 muszą być podane raczej przed niż po zarejestrowaniu się, zważywszy że artykuł 13 ust. 1 wymaga podania informacji „podczas pozyskiwania danych osobowych".

dotyczące rzetelnego przetwarzania. RODO nie przewiduje formatu i metody podania informacji osobie, której dane dotyczą, ale wyraźnie wskazuje, że obowiązkiem administratora danych jest podjęcie „odpowiednich środków" w odniesieniu do zapewnienia wymaganych informacji do celów przejrzystości. Oznacza to, że administrator danych powinien wziąć pod uwagę wszystkie okoliczności zbierania i przetwarzania danych przy podejmowaniu decyzji o odpowiedniej metodzie i formacie podania informacji. W szczególności należy ocenić odpowiednie środki w świetle doświadczeń użytkownika związanych z korzystaniem z usługi/produktu. Oznacza to wzięcie pod uwagę używanego urządzenia (jeżeli to właściwe), rodzaju interfejsów/interakcji użytkownika z administratorem danych („podróży" użytkownika) oraz ograniczeń, jakie pociągają za sobą te czynniki. Jak wskazano w punkcie 14 powyżej, GR Art. 29 zaleca, że przypadku, gdy administrator danych jest obecny online, powinno być zapewnione warstwowe oświadczenie / informacje dotyczące prywatności.

21. Aby pomóc w określeniu najodpowiedniejszego sposobu zapewnienia informacji, przed rozpoczęciem działania administratorzy danych mogą chcieć przetestować różne metody poprzez testy z udziałem użytkowników (np. testy typu hall) w celu uzyskania informacji zwrotnych na temat tego, na ile proponowane środki są dostępne, zrozumiałe i łatwe w użyciu dla użytkowników. Dokumentowanie tego podejścia powinno także pomóc administratorom danych w wypełnianiu ich obowiązków w zakresie rozliczalności poprzez wykazanie, dlaczego narzędzie /podejście wybrane do przekazania informacji jest najodpowiedniejsze w danych okolicznościach.

22. Zapewnienie rozliczalności w zakresie przejrzystości odnosi się nie tylko do momentu zbierania danych osobowych, ale do całego cyklu przetwarzania, niezależnie od przekazywanych informacji lub komunikatów. Ma to na przykład miejsce w przypadku zmiany treści / warunków istniejących oświadczeń / informacji dotyczących prywatności. Administrator powinien przestrzegać tych samych zasad przy przekazywaniu zarówno wstępnego oświadczenia / informacji dotyczących prywatności, jak i przy informowaniu o dalszych zmianach w oświadczeniu. Jako że większość obecnych klientów lub użytkowników tylko spojrzy na komunikat o zmianach w oświadczeniach / informacjach dotyczących prywatności, administrator powinien podjąć wszelkie środki konieczne do zapewnienia poinformowania o tych zmianach w taki sposób, aby zapewnić, że większość odbiorców rzeczywiście je zauważy. Oznacza to na przykład, że powiadomienie o zmianach powinno zawsze być przekazane w odpowiedni sposób (np. w formie wiadomości elektronicznej / listu w formie papierowej, etc.) mający zastosowanie konkretnie w przypadku tych zmian (np. nie może być przekazane wraz z komunikatami marketingu bezpośredniego), przy czym takie powiadomienie musi spełniać wymogi artykułu 12, czyli informacje muszą być zwięzłe, zrozumiałe, łatwo dostępne oraz udzielone jasnym i prostym językiem. Wskazanie w oświadczeniu / informacjach dotyczących prywatności, że osoba, której dane dotyczą, powinna regularnie sprawdzać zmiany lub aktualizacje w oświadczeniu / informacjach dotyczących prywatności, uznawane jest nie tylko za niewystarczające, ale również za nierzetelne w kontekście artykułu 5 ust. 1 lit. a). Dalsze wytyczne w odniesieniu do czasu powiadomienia o zmianach osób, których dane dotyczą, omówiono poniżej w punkcie 26.

Termin udzielenia informacji

23. Artykuły 13 i 14 określają informacje, które muszą być podane osobie, której dane dotyczą, na etapie rozpoczęcia cyklu przetwarzania. Artykuł 13 dotyczy sytuacji, w której dane są zbierane bezpośrednio od osoby, której dane dotyczą. Chodzi tu o dane osobowe, które:

- osoba, której dane dotyczą, świadomie podaje administratorowi danych (np. podczas wypełniania formularza online); lub

- administrator danych zbiera od osoby, której dane dotyczą, w ramach obserwacji (np. używając automatycznych urządzeń do pobierania danych lub oprogramowania do pobierania danych, takich jak na przykład kamery, urządzenia sieciowe, śledzenie wifi, RFID lub inne rodzaje czujników).

Artykuł 14 ma zastosowanie w przypadku pozyskiwania danych w sposób inny niż od osoby, której dane dotyczą. Dotyczy to danych osobowych, które administrator danych pozyskał ze źródeł takich jak:

- administratorzy danych będący stronami trzecimi;

- publicznie dostępne źródła;

- brokerzy danych; lub

- inne osoby, których dane dotyczą.

24. Jeżeli chodzi o termin udzielenia informacji, udzielenie ich we właściwym czasie jest istotnym elementem obowiązku zapewnienia przejrzystości i obowiązku rzetelnego przetwarzania danych. Gdy zastosowanie ma artykuł 13, na mocy artykułu 13 ust. 1 informacje muszą być podane „*podczas pozyskiwania danych osobowych*". W przypadku danych pozyskanych pośrednio na mocy artykułu 14 ramy czasowe, w jakich wymagane informacje muszą być udzielone osobie, której dane dotyczą, określone są w artykule 14 ust. 3 lit. a) do c), jak poniżej:

- Ogólny wymóg jest taki, że informacje muszą być podane w „rozsądnym terminie" po pozyskaniu danych osobowych - najpóźniej w ciągu miesiąca – „*mając na uwadze konkretne okoliczności przetwarzania danych osobowych"* (artykuł 14 ust. 3 lit. a)).

- Ogólny termin jednego miesiąca wskazany w artykule 14 ust. 3 lit. a) może być skrócony na mocy artykułu 14 ust. 3 lit. b)[22], który przewiduje sytuację, w której dane są wykorzystywane do komunikacji z osobą, której dane dotyczą. W takim przypadku informacje muszą być podane najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą. Jeżeli pierwsza komunikacja ma miejsce przed upłynięciem jednomiesięcznego terminu po pozyskaniu danych osobowych, wówczas informacje muszą być podane *najpóźniej* przy pierwszej komunikacji z osobą, której dane dotyczą, niezależnie od tego, że termin jednego miesiąca od momentu pozyskania danych nie minął. Jeżeli pierwsza komunikacja z osobą, której dane dotyczą, ma miejsce ponad miesiąc po pozyskaniu danych osobowych, wówczas artykuł 14 ust. 3 lit. a) nadal ma zastosowanie, tak że informacje z artykułu 14 muszą być podane osobie, której dane dotyczą, najpóźniej w ciągu miesiąca od ich pozyskania.

- Ogólny termin jednego miesiąca wskazany w artykule 14 ust. 3 lit. a) może być również skrócony na mocy artykułu 14 ust. 3 lit. c)[23], który przewiduje sytuację, w której dane są ujawniane innemu odbiorcy (czy to stronie trzeciej czy też nie)[24]. W takim przypadku informacje muszą być podane najpóźniej przy ich pierwszym ujawnieniu. W tym przypadku,

[22] Użycie słów *„jeżeli dane osobowe mają być stosowane do …*" w artykule 14 ust. 3 lit. b) wskazuje ogólne stanowisko odnoszące się do maksymalnego okresu określonego w artykule 14 ust. 3 lit. a), ale nie zastępuje go.
[23] Użycie słów *„jeżeli planuje się ujawnić dane osobowe innemu odbiorcy…*" w artykule 14 ust. 3 lit. c) podobnie wskazuje ogólne stanowisko odnoszące się do maksymalnego okresu określonego w artykule 14 ust. 3 lit. a), ale nie zastępuje go.
[24] Artykuł 4 ust. 9 definiuje „odbiorcę" i wyjaśnia, że odbiorca, któremu ujawnia się dane osobowe, nie musi być stroną trzecią. W związku z tym odbiorca może być administratorem danych, współadministratorem lub podmiotem przetwarzającym.

jeżeli ujawnienie ma miejsce przed upłynięciem jednomiesięcznego terminu, wówczas informacje muszą być podane *najpóźniej* przy ich pierwszym ujawnieniu, niezależnie od tego, że termin jednego miesiąca od momentu pozyskania danych nie minął. Podobnie do stanowiska wyrażonego w artykule 14 ust. 3 lit. b), jeżeli ujawnienie danych osobowych ma miejsce ponad miesiąc po pozyskaniu danych osobowych, wówczas artykuł 14 ust. 3 lit. a) nadal ma zastosowanie, tak że informacje z artykułu 14 muszą być podane osobie, której dane dotyczą, najpóźniej w ciągu miesiąca od ich pozyskania.

25. W związku z tym w każdym przypadku maksymalne ramy czasowe, w jakich informacje z artykułu 14 muszą być podane osobie, której dane dotyczą, to jeden miesiąc. Jednakże wymogi rzetelności i rozliczalności na mocy RODO wymagają, aby administratorzy danych zawsze uwzględniali rozsądne oczekiwania osób, których dane dotyczą, wpływ, jaki przetwarzanie może na nie mieć, oraz możliwość wykonania ich praw w odniesieniu do tego przetwarzania, przy podejmowaniu decyzji na temat tego, w jakim momencie przekazać informacje z artykułu 14. Rozliczalność wymaga od administratorów wykazania uzasadnienia ich decyzji oraz uzasadnienia, dlaczego informacje podano w danym czasie. W praktyce trudne może być spełnienie tych wymogów przy zapewnianiu informacji w 'ostatnim momencie'. W tym zakresie motyw 39 stanowi, między innymi, że osobom, których dane dotyczą, „*należy uświadomić ryzyka, zasady, zabezpieczenia i prawa związane z przetwarzaniem danych osobowych oraz sposoby wykonywania praw przysługujących im w związku z takim przetwarzaniem*". Z tych wszystkich względów GR Art. 29 stoi na stanowisku, że administratorzy danych powinni udzielać informacji osobom, których dane dotyczą, odpowiednio wcześniej przed upływem przewidzianego terminu. Dalsze uwagi co do tego, czy czas pomiędzy powiadomieniem osób, których dane dotyczą, o czynnościach przetwarzania, a faktycznym wprowadzeniem w życie tych czynności przetwarzania, przedstawiono w poniższym akapicie.

Termin powiadomienia o zmianach w informacjach z artykułu 13 i 14

26. RODO nie odnosi się do wymogów dotyczących terminu (i metod) mających zastosowanie do powiadomienia o zmianach w informacjach, których wcześniej udzielono osobie, której dane dotyczą, na mocy artykułu 13 lub 14 (z wyjątkiem planowanego dalszego celu przetwarzania, w którym to przypadku informacje dotyczące tego dalszego celu muszą być przekazane przed rozpoczęciem tego dalszego przetwarzania zgodnie z artykułem 13 ust. 3 i artykułem 14 ust. 4 – patrz punkt 41 poniżej). Jednak, jak zauważono powyżej w kontekście terminu udzielenia informacji z artykułu 14, administrator danych musi uwzględniać zasady rzetelności i rozliczalności pod względem rozsądnych oczekiwań osoby, której dane dotyczą, lub potencjalnego wpływu tych zmian na osobę, której dane dotyczą. Jeżeli zmiana w informacjach wskazuje na zasadniczą zmianę charakteru przetwarzania (np. poszerzenie kategorii odbiorców lub wprowadzenie przekazywania do kraju trzeciego) lub zmianę, która może nie mieć zasadniczego znaczenia dla czynności przetwarzania, ale może być istotna dla osoby, której dane dotyczą, i mieć na nią wpływ, wówczas informacje takie powinny być zapewnione osobie, której dane dotyczą, odpowiednio wcześniej przed faktycznym wprowadzeniem zmiany a metoda zastosowana do podania tych zmian do wiadomości osoby, której dane dotyczą, powinna być wyraźna i skuteczna. Ma to zapewnić, że osoba, której dane dotyczą, nie „przeoczy" zmiany, oraz zapewnić jej rozsądne ramy czasowe na (a) rozważenie charakteru i wpływu zmiany oraz (b) wykonanie jej praw na mocy RODO w odniesieniu do zmiany (np. wycofanie zgody lub wyrażenie sprzeciwu wobec przetwarzania).

27. Administratorzy danych powinni dokładnie rozważyć okoliczności i kontekst każdej sytuacji, w której wymagana jest aktualizacja informacji w zakresie przejrzystości, w tym możliwy wpływ zmian na osobę, której dane dotyczą, i metodę użytą do powiadomienia o zmianach, oraz być w stanie wykazać, na ile czas pomiędzy powiadomieniem o zmianach a wprowadzeniem w życie zmiany jest zgodny z zasadą rzetelności wobec osoby, której dane dotyczą. Ponadto stanowisko GR Art. 29 jest takie, że, zgodnie z zasadą rzetelności, przy powiadamianiu o takich zmianach osób, których dane dotyczą, administrator danych powinien również wyjaśnić, jaki będzie prawdopodobny wpływ tych zmian na osoby, których dane dotyczą. Jednak zgodność z wymogami dotyczącymi przejrzystości nie „wybieli" sytuacji, w której zmiany w przetwarzaniu danych są tak znaczące, że charakter przetwarzania staje się zupełnie inny od tego, jaki był wcześniej. GR Art. 29 podkreśla, że wszystkie inne zasady zawarte w RODO, w tym te dotyczące niezgodnego dalszego przetwarzania, nadal mają zastosowanie niezależnie od przestrzegania obowiązków w zakresie przejrzystości.

28. Dodatkowo, gdy informacje w zakresie przejrzystości (np. zawarte w oświadczeniu / informacjach dotyczących prywatności) nie zmieniają się w istotny sposób, istnieje prawdopodobieństwo, że osoby, których dane dotyczą, które korzystały z usługi przez znaczny okres, nie będą pamiętały informacji udzielonych im na początku na mocy artykułów 13 i/lub 14. W sytuacjach, w których przetwarzanie danych odbywa się stale, w celu zapewnienia rzetelności przetwarzania administrator powinien ponownie informować osoby, których dane dotyczą, o zakresie przetwarzania danych, na przykład w formie przypomnienia oświadczenia/informacji dotyczących prywatności przekazywanego w odpowiednich odstępach czasowych.

Tryb – format, w jakim mają być podane informacje

29. Zarówno artykuł 13, jak i 14 odnoszą się do nałożonego na administratora danych obowiązku „*podania osobie, której dane dotyczą, wszystkich następujących informacji…"*. Znaczącym słowem jest tu „podaje". Oznacza to, że administrator danych musi podjąć aktywne działania w celu zapewnienia przedmiotowych informacji osobie, której dane dotyczą. Osoba, której dane dotyczą, nie musi podejmować aktywnych działań w celu uzyskania informacji, o których mowa w tych artykułach, lub znalezienia ich wśród innych informacji, takich jak regulamin korzystania ze strony internetowej lub aplikacji. Ilustruje to przykład w punkcie 10.

Warstwowe oświadczenia / informacje dotyczące prywatności

30. W kontekście cyfrowym, w świetle ilości informacji, których podanie osobie, której dane dotyczą, jest wymagane, GR Art. 29 zaleca, iż powinny być raczej wykorzystywane warstwowe oświadczenia / informacje dotyczące prywatności[25] w celu odesłania do różnych kategorii informacji, które muszą być udzielone osobie, której dane dotyczą, zamiast wyświetlania wszystkich takich informacji w pojedynczych informacjach na ekranie, aby uniknąć zmęczenia informacyjnego. Warstwowe oświadczenia / informacje dotyczące prywatności mogą pomóc w rozwiązaniu napięcia między kompletnością a zrozumieniem, poprzez umożliwienie użytkownikom bezpośredniego przejścia do tych części informacji, które chcą przeczytać. Należy zauważyć, że warstwowe oświadczenia / informacje dotyczące prywatności to nie jedynie strony zagnieżdżone, które wymagają kilku kliknięć w celu uzyskania określonych informacji. Projekt i układ pierwszej warstwy oświadczenia / informacji dotyczących

[25] Jak zauważono powyżej, administratorzy danych mogą również opracować nowe innowacyjne metody zapewnienia zgodności z artykułem 12.

prywatności powinien być taki, aby osoba, której dane dotyczą, miała jasny przegląd dostępnych dla niej informacji na temat przetwarzania jej danych osobowych oraz tego, gdzie/jak może znaleźć te szczegółowe informacje wśród warstw oświadczenia / informacji dotyczących prywatności. Ważne jest, aby informacje zawarte w różnych warstwach warstwowych informacji były spójne i aby te warstwy nie zapewniały sprzecznych informacji. W odniesieniu do istotnych informacji, które mogą być zawarte w pierwszej warstwie oświadczenia / informacji dotyczących prywatności, stanowisko GR Art. 29 jest takie, że powinny one zawsze zawierać informacje dotyczące przetwarzania, które ma największy wpływ na osobę, której dane dotyczą, oraz przetwarzania, które mogłoby zaskoczyć osobę, której dane dotyczą. W związku z tym osoba, której dane dotyczą, powinna być w stanie zrozumieć z informacji zawartych w pierwszej warstwie, jakie będą konsekwencje przedmiotowego przetwarzania dla osoby, której dane dotyczą (patrz punkt 9 powyżej).

31. W kontekście cyfrowym, obok zapewnienia online warstwowego oświadczenia / informacji dotyczących prywatności administratorzy danych mogą również postanowić wykorzystać dodatkowe narzędzia w zakresie przejrzystości (patrz dalsze przykłady poniżej), które zapewniają indywidualnej osobie, której dane dotyczą, dostosowane informacje, które są charakterystyczne dla sytuacji określonej indywidualnej osoby, której dane dotyczą, oraz produktów/usług, z których korzysta osoba, której dane dotyczą.

Informacje typu „push" i „pull

32. Innym sposobem zapewnienia informacji w zakresie przejrzystości jest wykorzystanie informacji typu „push" i „pull". W przypadku informacji typu „push" podanie informacji w zakresie przejrzystości ma miejsce „w odpowiednim czasie", podczas gdy informacje typu „pull" ułatwiają dostęp do informacji za pomocą metod, takich jak zarządzanie zgodą, panele kontroli przejrzystości oraz samouczki „dowiedz się więcej". Zapewnia to osobie, której dane dotyczą, doświadczenia w zakresie przejrzystości bardziej przyjazne użytkownikowi.

- panel kontroli prywatności to jeden punkt, w którym osoby, których dane dotyczą, mogą przeglądać 'informacje dotyczące prywatności' oraz zarządzać swoimi preferencjami dotyczącymi prywatności, pozwalając na lub uniemożliwiając wykorzystywanie ich danych przez konkretną usługę na określone sposoby. Jest to szczególnie użyteczne, gdy osoby, których dane dotyczą, korzystają z tej samej usługi na szeregu różnych urządzeń, ponieważ zapewnia im dostęp do ich danych osobowych i kontrolę nad nimi, niezależnie od tego, w jaki sposób korzystają z usługi. Umożliwienie osobom, których dane dotyczą, manualnego dostosowania ich ustawień prywatności za pośrednictwem panelu kontroli prywatności może również ułatwić personalizację oświadczenia / informacji dotyczących prywatności poprzez odzwierciedlenie tylko rodzajów przetwarzania mających miejsce w odniesieniu do tej konkretnej osoby, której dane dotyczą. Preferowane jest wbudowanie panelu kontroli prywatności w istniejącą architekturę usługi (np. poprzez użycie tego samego projektu i marki jak w przypadku pozostałej części usługi), ponieważ zapewni to, iż dostęp i korzystanie będą intuicyjne, oraz może pomóc w zachęceniu użytkowników do zainteresowania się tym informacjami, tak samo jak zainteresowaliby się innymi aspektami usługi. Może być to skuteczny sposób pokazania, że 'informacje dotyczące prywatności' to raczej niezbędna i integralna część usługi, a nie długa lista w prawniczym żargonie.

- Informacje podane w odpowiednim czasie wykorzystywane są w celu zapewnienia określonych 'informacji dotyczących prywatności' ad hoc, w momencie gdy najważniejsze jest ich przeczytanie przez osobę, której dane dotyczą. Metoda ta jest przydatna do podawania

informacji w różnych momentach w trakcie całego procesu zbierania danych; umożliwia podzielenie informacji na łatwo przyswajalne fragmenty i rozłożenie ich udzielania w czasie, oraz ogranicza poleganie na jednym oświadczeniu / informacjach dotyczących prywatności, które są trudne do zrozumienia bez kontekstu. Na przykład, jeżeli osoba, której dane dotyczą, kupuje produkt online, można podać krótkie informacje wyjaśniające w wyskakujących okienkach towarzyszącym określonym polom tekstowym. Informacje pojawiające się obok pola, w którym osoba, której dane dotyczą, proszona jest o podanie numeru telefonu, mogłyby wyjaśniać na przykład, że dane te są zbierane tylko na potrzeby kontaktu związanego z zakupem i że będą ujawniane tylko firmie odpowiedzialnej za dostawę.

Inne rodzaje „odpowiednich środków"

33. Zważywszy na bardzo wysoki poziom dostępu do Internetu w UE i fakt, że osoby, których dane dotyczą, mogą wejść do sieci w każdym momencie, z wielu lokalizacji i przy użyciu różnych urządzeń, jak wskazano powyżej, stanowisko GR Art. 29 jest takie, że „odpowiednim środkiem" do zapewnienia informacji w zakresie przejrzystości w przypadku administratorów danych, którzy są obecni w świecie cyfrowym / online, jest uczynienie tego za pomocą elektronicznego oświadczenia / informacji dotyczących prywatności. Jednak, uwzględniając okoliczności zbierania i przetwarzania danych, administrator danych może dodatkowo (lub alternatywnie, gdy administrator danych nie jest obecny w świecie cyfrowym / online) wykorzystać inne metody i formaty do zapewnienia informacji. Inne możliwe sposoby udzielenia informacji osobie, której dane dotyczą, pojawiające się w następujących różnych środowiskach danych osobowych mogą obejmować:

a. Środowisko 'w formie papierowej', na przykład w przypadku zawierania umowy za pośrednictwem poczty: pisemne wyjaśnienia, ulotki, informacje w dokumentacji umownej, komiksy, infografika, schematy;

b. Środowisko telefoniczne: ustne wyjaśnienia przez rzeczywistą osobę, aby umożliwić interakcję i odpowiedzi na pytania, automatyczne lub wcześniej nagrane informacje z możliwością odsłuchania dalszych bardziej szczegółowych informacji;

c. Środowisko bezekranowej inteligentnej technologii / Internetu przedmiotów, jak np. analiza śledzenia wifi: znaki graficzne, kody QR, ostrzeżenia głosowe, informacje pisemne zawarte w papierowej instrukcji konfiguracji lub filmy wideo zawarte w cyfrowej instrukcji konfiguracji, informacje pisemne w urządzeniu mobilnym, wiadomości wysyłane SMS-em lub pocztą elektroniczną, widoczne tablice/panele zawierające informacje, znaki informacyjne/oznakowanie (ang. public signage), publiczne kampanie informacyjne;

d. Środowisko „od osoby do osoby", jak np. odpowiadanie na badania opinii publicznej, osobista rejestracja w usłudze: pisemne wyjaśnienia przekazywane w formie papierowej lub elektronicznej;

e. Środowisko „rzeczywiste" z telewizją przemysłową / nagrywaniem przez drony: widoczne tablice/panele zawierające informacje, znaki informacyjne/oznakowanie (ang. public signage), publiczne kampanie informacyjne, informacje w gazetach / mediach.

Informacje dotyczące profilowania i zautomatyzowanego podejmowania decyzji

34. Informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz istotne informacje o zasadach ich podejmowania, a także o

znaczących i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą, stanowią część obowiązkowych informacji, które muszą być zapewnione osobie, której dane dotyczą, na mocy art. 13 ust. 2 lit. f) i art. 14. ust. 2 lit. g). GR Art. 29 opracowała również wytyczne dotyczące zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania[26], w których można znaleźć dalsze wytyczne odnoszące się do wprowadzania w życie przejrzystości w określonych okolicznościach profilowania.

Pozostałe kwestie – ryzyko, przepisy i zabezpieczenia

35. Motyw 39 RODO również odnosi się do zapewniania określonych informacji, które nie są wyraźnie objęte artykułami 13 i 14 (patrz tekst motywu powyżej w punkcie 25). Wskazanie w tym motywie, że osobom fizycznym należy uświadomić ryzyka, zasady i zabezpieczenia związane z przetwarzaniem danych osobowych, powiązane jest z szeregiem innych kwestii, do których należy ocena skutków dla ochrony danych. Jak określono w wytycznych GR Art. 29 dotyczących oceny skutków dla ochrony danych[27], administratorzy danych mogą rozważyć publikację oceny skutków dla ochrony danych (lub jej części), w ramach budowania zaufania wobec czynności przetwarzania oraz wykazania przejrzystości i rozliczalności, mimo że taka publikacja nie jest obowiązkowa. Ponadto przestrzeganie kodeksu postępowania (przewidziane w artykule 40) może iść w kierunku wykazania przejrzystości, ponieważ kodeksy postępowania mogą być opracowywane w celu sprecyzowania stosowania RODO w odniesieniu m.in. do rzetelnego i przejrzystego przetwarzania, informacji podawanych opinii publicznej i osobom, których dane dotyczą, i informacji zapewnianych dzieciom i ochrony dzieci.

36. Inną istotną kwestią dotyczącą przejrzystości jest ochrona danych w fazie projektowania i domyślna ochrona danych (co jest wymagane na mocy artykułu 25). Zasady te wymagają, aby administratorzy danych od początku wbudowali elementy ochrony danych w swoje czynności przetwarzania i systemy, a nie w ostatniej chwili uwzględniali kwestię zapewniania zgodności z ochroną danych. Motyw 78 dotyczy wdrażania przez administratorów danych środków, które spełniają wymogi uwzględniania ochrony danych w fazie projektowania i domyślnej ochrony danych, w tym środków polegających na zapewnianiu przejrzystości co do funkcji i przetwarzania danych osobowych.

37. Odrębnie, kwestia współadministratorów jest również związana z uświadamianiem osobom fizycznym ryzyk, zasad i zabezpieczeń. Artykuł 26 ust. 1 wymaga, aby współadministratorzy w przejrzysty sposób określali odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO, w szczególności w odniesieniu do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw, oraz ich obowiązków w odniesieniu do podawania informacji, o których mowa w art. 13 i 14. Artykuł 26 ust. 2 wymaga, aby zasadnicza treść uzgodnień była udostępniana osobom, których dane dotyczą. Innymi słowy, dla osoby, której dane dotyczą, musi być całkowicie jasne, do którego administratora danych może się zwrócić, gdy zamierza wykonać jedno lub więcej ze swoich praw przysługujących jej na mocy RODO[28].

[26] Wytyczne dotyczące zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania na potrzeby rozporządzenia 2016/679, WP251.

[27] Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679 WP248 rev.01

[28] Na mocy artykułu 26 ust. 3, niezależnie od uzgodnień między współadministratorami, o których mowa w ust. 1, osoba, której dane dotyczą, może wykonywać przysługujące jej prawa wynikające z RODO wobec każdego ze współadministratorów.

Informacje dotyczące dalszego przetwarzania

38. Zarówno artykuł 13, jak i 14, zawiera przepis[29], który wymaga, aby administrator danych poinformował osobę, której dane dotyczą, jeżeli zamierza dalej przetwarzać jej dane osobowe w celu innym niż cel, w którym zostały one zebrane/pozyskane. Jeżeli tak, *„przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji, o których mowa w ust. 2”*. Przepisy te w szczególności wprowadzają w życie zasadę z artykułu 5 ust. 1 lit. b), zgodnie z którą dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach, a ich dalsze przetwarzanie w sposób *niezgodny* z tymi celami jest zakazane[30]. W przypadku, gdy dane osobowe są dalej przetwarzane w celach, które są *niezgodne* z pierwotnymi celami (artykuł 6 ust. 4 informuje o tej kwestii[31]), zastosowanie mają artykuły 13 ust. 3 i 14 ust. 4. Wskazane w tych artykułach wymogi informowania osoby, której dane dotyczą, o dalszym przetwarzaniu, propagują stanowisko zawarte w RODO, że w czasie i w kontekście, w którym zbierane są dane osobowe, osoba, której dane dotyczą, ma rozsądne przesłanki by spodziewać się, że może nastąpić przetwarzanie danych w tym celu[32]. Innymi słowy, osoby, której dane dotyczą, nie powinno się zaskakiwać celem przetwarzania jej danych osobowych.

39. Artykuły 13 ust. 3 i 14 ust. 4, w zakresie w jakim odnoszą się do udzielenia „*wszelkich innych stosownych informacji, o których mowa w ust. 2”*, można na pierwszy rzut oka zinterpretować w ten sposób, że pozostawiają administratorowi danych pewien stopień uznania co do zakresu i konkretnych kategorii informacji z właściwego ustępu 2 (tj. artykuł 13 ust. 2 lub artykuł 14 ust. 2, gdy to właściwe), które powinny zostać udzielone osobie, której dane dotyczą. (Motyw 61 określa to mianem „*innych niezbędnych informacji”*). Jednakże domyślne stanowisko jest takie, że wszystkie tego typu informacje określone w tym właściwym ustępie powinny być zapewnione osobie, której dane dotyczą, o ile nie istnieje lub nie ma zastosowania jedna lub więcej kategorii informacji.

40. Stanowisko GR Art. 29 jest takie, że zgodnie z zasadą przejrzystości wyrażoną w artykule 12 oraz niezbędnymi warunkami wstępnymi rozliczalności i rzetelności na mocy RODO, administratorzy danych powinni udzielić osobom, których dane dotyczą, dalszych informacji dotyczących analizy zgodności przeprowadzonej na mocy artykułu 6 ust. 4[33], gdy dla nowego celu przetwarzania bazują na podstawie prawnej innej niż zgoda lub prawo krajowe/UE (innymi słowy wyjaśnienie, w jaki sposób przetwarzanie w innym celu (celach) jest zgodne z pierwotnym celem). Ma to zapewnić osobom, których dane dotyczą, możliwość rozważenia zgodności dalszego przetwarzania i przewidzianych zabezpieczeń oraz zdecydowania, czy wykonywać swoje prawa, np. m.in. prawo ograniczenia przetwarzania lub prawo wyrażenia sprzeciwu wobec przetwarzania.[34]

---

[29] W artykułach 13 ust. 3 i 14 ust. 4, które są identyczne z wyjątkiem słowa „zebrane”, które jest użyte w artykule 13, które jest zastąpione w artykule 14 słowem „pozyskane”.

[30] Patrz, na przykład w kwestii tej zasady, motywy 47, 50, 61, 156, 158; artykuły 6 ust. 4 i 89.

[31] Artykuł 6 ust. 4 określa, w sposób niewyczerpujący, czynniki, które mają być wzięte pod uwagę w celu ustalenia, czy przetwarzanie w innym celu jest zgodne z celem, w którym dane osobowe są pierwotnie zbierane, mianowicie: powiązanie między celami; kontekst, w którym dane osobowe zebrano; charakter danych osobowych (w szczególności, czy obejmują one szczególne kategorie danych osobowych lub dane osobowe dotyczące czynów zabronionych lub skazań); możliwe konsekwencje planowanego dalszego przetwarzanie dla osób, których dane dotyczą; oraz istnienie odpowiednich zabezpieczeń.

[32] Motywy 47 i 50.

[33] Odnosi się do tego również motyw 50.

[34] Jak wskazano w motywie 63, umożliwi to osobie, której dane dotyczą, wykonanie jej prawa dostępu, by mieć świadomość przetwarzania i móc zweryfikować zgodność przetwarzania z prawem.

41. Kwestia terminu powiązana jest z wykonaniem praw osoby, której dane dotyczą. Jak podkreślono powyżej, terminowe udzielenia informacji jest istotnym elementem wymogów przejrzystości na mocy artykułów 13 i 14 oraz jest nierozerwalnie związane z koncepcją rzetelnego przetwarzania. Informacje odnoszące się do *dalszego przetwarzania* muszą być udzielone „przed tym dalszym przetwarzaniem". Stanowisko GR Art. 29 jest takie, że między poinformowaniem a rozpoczęciem przetwarzania powinien upłynąć rozsądny okres, zamiast natychmiastowego rozpoczęcia przetwarzania po otrzymaniu informacji przez osobę, której dane dotyczą. Zapewnia to osobom, których dane dotyczą, praktyczne korzyści związane z zasadą przejrzystości, dając im istotną możliwość rozważenia (i potencjalnie wykonania ich praw w odniesieniu do) dalszego przetwarzania. To, czym jest rozsądny okres, zależeć będzie od konkretnych okoliczności. Zasada rzetelności wymaga, że im bardziej naruszające (lub mniej oczekiwane) jest dalsze przetwarzanie, tym dłuższy powinien być powyższy okres. Podobnie, zasada rozliczalności wymaga, że administratorzy danych muszą być w stanie wykazać, jak w określonych okolicznościach są uzasadnione podjęte przez nich postanowienia co do terminu udzielenia tych informacji oraz na ile generalnie termin jest sprawiedliwy dla osób, których dane dotyczą. (Patrz również poprzednie uwagi dotyczące ustalenia rozsądnych ram czasowych powyżej w punktach 26-28).

Narzędzia służące do wizualizacji

42. Co istotne, zasada przejrzystości w RODO nie jest ograniczona do wprowadzenia jej w życie po prostu poprzez komunikację językową (czy to pisemną czy ustną). RODO przewiduje narzędzia służące do wizualizacji (wskazując w szczególności na znaki graficzne, mechanizmy certyfikacji oraz znaki jakości i oznaczenia w zakresie ochrony danych), gdy to właściwe. Motyw 58[35] wskazuje, że dostępność informacji kierowanych do ogółu społeczeństwa lub osób, których dane dotyczą, jest szczególnie ważna w środowisku online.[36]

Znaki graficzne

43. Motyw 60 przewiduje możliwość przekazania informacji osobie, której dane dotyczą „w połączeniu" ze standardowymi znakami graficznymi, co pozwoli na podejście wielowarstwowe. Jednak użycie znaków graficznych nie powinno po prostu zastąpić informacji niezbędnych do wykonania praw osoby, której dane dotyczą, nie powinny one również być wykorzystywane w celu zastąpienia przestrzegania obowiązków administratora danych wynikających z artykułów 13 i 14. Artykuł 12 ust. 7 przewiduje użycie takich znaków graficznych, stanowiąc że:

„Informacje, których udziela się osobom, których dane dotyczą, na mocy art. 13 i 14, można opatrzyć standardowymi znakami graficznymi, które w widoczny, zrozumiały i czytelny sposób przedstawią sens zamierzonego przetwarzania. Jeżeli znaki te są przedstawione elektronicznie, muszą się nadawać do odczytu maszynowego".

[35] „Informacje te mogą być przekazywane w formie elektronicznej, na przykład za pomocą strony internetowej, gdy są kierowane do ogółu społeczeństwa. Dotyczy to w szczególności sytuacji, gdy duża liczba podmiotów i złożoność technologiczna działań sprawiają, że osobie, której dane dotyczą, trudno jest dowiedzieć się i zrozumieć, czy dotyczące jej dane osobowe są zbierane, przez kogo oraz w jakim celu, na przykład w przypadku reklamy w Internecie".

[36] W tym kontekście administratorzy powinni brać pod uwagę osoby, których dane dotyczą, z dysfunkcją wzroku (np. daltonistów).

44. Jako że artykuł 12 ust. 7 stanowi, że: „. *Jeżeli znaki te są przedstawione elektronicznie, muszą się nadawać do odczytu maszynowego”,* sugeruje to, iż mogą mieć miejsce sytuacje, w których znaki graficzne nie są przedstawione elektronicznie[37], na przykład znaki graficzne na fizycznej dokumentacji papierowej, urządzeniach Internetu przedmiotów lub opakowaniu urządzenia Internetu przedmiotów, informacje w miejscach publicznych na temat śledzenia wifi, kody QR oraz powiadomienia telewizji przemysłowej.

45. Ewidentnie celem używania znaków graficznych jest zwiększenie przejrzystości dla osób, których dane dotyczą, poprzez potencjalne zmniejszenie potrzeby przedstawienia dużych ilości pisemnych informacji osobie, której dane dotyczą. Jednakże przydatność znaków graficznych do skutecznego przekazywania informacji wymaganych na mocy artykułów 13 i 14 osobom, których dane dotyczą, zależy od standaryzacji symboli/obrazów, które mają być uniwersalnie wykorzystywane i rozpoznawane w całej UE jako skrót odnoszący się do tych informacji. W tym zakresie RODO przypisuje odpowiedzialność za opracowanie kodeksu znaków graficznych Komisji, ale docelowo Europejska Rada Ochrony Danych może, albo na wniosek Komisji, albo z własnej inicjatywy, przedstawić Komisji opinię na temat takich znaków graficznych[38]. GR Art. 29 zauważa że, zgodnie z motywem 166, opracowanie kodeksu znaków graficznych powinno koncentrować się na podejściu opartym na materiałach dowodowych oraz przed taką standaryzacją konieczne będzie przeprowadzenie obszernych badań dotyczących skuteczności znaków graficznych w tym kontekście w połączeniu z branżą oraz szerszą opinią publiczną.

Mechanizmy certyfikacji, znaki jakości i oznaczenia

46. Oprócz używania standardowych znaków graficznych, RODO (artykuł 42) przewiduje również wykorzystywanie mechanizmów certyfikacji oraz znaków jakości i oznaczeń w zakresie ochrony danych osobowych mających świadczyć o zgodności z RODO operacji przetwarzania prowadzonych przez administratorów i podmioty przetwarzające oraz mających zwiększyć przejrzystość dla osób, których dane dotyczą[39]. GR Art. 29 wyda wytyczne dotyczące mechanizmów certyfikacji w odpowiednim czasie.

---

[37] RODO nie zawiera definicji terminu „przeznaczony do odczytu maszynowego”, ale motyw 21 dyrektywy 2013/37/UE17 definiuje ten termin jako:
„ ... format pliku zorganizowany tak, aby aplikacje komputerowe mogły łatwo zidentyfikować, rozpoznać i uzyskać określone dane, w tym poszczególne stwierdzenia faktów, i ich wewnętrzną strukturę. Dane zakodowane w plikach zorganizowanych w formacie przeznaczonym do odczytu komputerowego to dane przeznaczone do odczytu komputerowego. Formaty przeznaczone do odczytu komputerowego mogą być otwarte lub zastrzeżone; mogą one występować jako standardy formalne lub nie. Dokumentów zakodowanych w formacie pliku ograniczającym przetwarzanie automatyczne z powodu niemożności pozyskania danych lub utrudnień w ich pozyskaniu z tych dokumentów nie należy uznawać za sporządzone w formacie przeznaczonym do odczytu komputerowego. Państwa członkowskie powinny w stosownych przypadkach zachęcać do korzystania z formatów otwartych przeznaczonych do odczytu komputerowego.”

[38] Artykuł 12 ust. 8 przewiduje, że Komisji przysługuje prawo przyjmowania aktów delegowanych zgodnie z art. 92 w celu określenia informacji przedstawianych za pomocą znaków graficznych i procedur ustanowienia standardowych znaków graficznych. Motyw 166 (dotyczący aktów delegowanych Komisji ogólnie) wskazuje, że Komisja musi prowadzić odpowiednie konsultacje podczas swoich prac przygotowawczych, w tym na szczeblu eksperckim. Jednakże Europejska Rada Ochrony Danych również ma do odegrania ważną rolę konsultacyjną w odniesieniu do standaryzacji znaków graficznych, ponieważ artykuł 70 ust. 1 stanowi, że EROD z własnej inicjatywy lub w stosownych przypadkach na wniosek Komisji udziela Komisji opinii w sprawie znaków graficznych.

[39] Patrz wskazanie w motywie 100.

Wykonanie praw osób, których dane dotyczą

47. Przejrzystość nakłada na administratorów danych potrójny obowiązek, jeżeli chodzi o prawa osób, których dane dotyczą, wynikające z RODO, muszą oni bowiem[40]:

- udzielać osobom, których dane dotyczą, informacji na temat przysługujących im praw[41] (zgodnie z wymogami artykułów 13 ust. 2 lit. b) oraz 14 ust. 2 lit. c);

- przestrzegać zasady przejrzystości (tj. dotyczącej jakości komunikacji, jak określono w artykule 12 ust. 1) w przypadku komunikowania się z osobami, których dane dotyczą, w kwestii przysługujących im praw na mocy artykułów 15-22 i 34; oraz

- ułatwiać osobom, których dane dotyczą, wykonanie praw przysługujących im na mocy artykułów 15-22.

48. Wymogi RODO w odniesieniu do wykonania tych praw i charakteru wymaganych informacji są tak skonstruowane, aby *zapewnić znaczącą pozycję* osobom, których dane dotyczą, tak aby mogły egzekwować swoje prawa i rozliczać administratorów danych z przetwarzania ich danych osobowych. Motyw 59 podkreśla, że *„należy przewidzieć procedury ułatwiające osobie, której dane dotyczą, wykonywanie praw”* oraz że administrator danych powinien *„zapewnić możliwość wnoszenia odnośnych żądań także drogą elektroniczną, w szczególności gdy dane osobowe są przetwarzane drogą elektroniczną”*. Procedura zapewniona osobom, których dane dotyczą, przez administratora danych do wykonania ich praw powinna być odpowiednia do kontekstu i charakteru relacji i interakcji między administratorem a osobą, której dane dotyczą. W tym celu administrator danych może zdecydować o zapewnieniu różnych procedur do wykonania praw, które odzwierciedlają różne sposoby, w jakie odbywa się interakcja osób, których dane dotyczą, z tym administratorem danych.

Przykład dobrych praktyk

Dostawca usług opieki zdrowotnej wykorzystuje elektroniczny formularz na swojej stronie internetowej w celu umożliwienia osobom, których dane dotyczą, składania wniosków online o dostęp do ich danych osobowych. Ponadto zapewnia formularze papierowe w recepcjach swoich przychodni, tak aby osoby, których dane dotyczą, mogły również składać wnioski osobiście.

Przykład niewłaściwych praktyk

Dostawca usług opieki zdrowotnej zamieścił na swojej stronie internetowej oświadczenie informujące, że wszystkie osoby, których dane dotyczą, powinny kontaktować się z jego działem obsługi klienta w celu żądania dostępu do danych osobowych.

[40] W sekcji RODO „Przejrzystość i korzystanie z praw” dotyczącej praw osób, których dane dotyczą (Sekcja 1, Rozdział III, mianowicie artykuł 12).

[41] Prawo dostępu, sprostowania, usunięcia, ograniczenia przetwarzania, wniesienia sprzeciwu wobec przetwarzania, przenoszenia.

Wyłączenia od obowiązku podania informacji

Wyłączenia z artykułu 13

49. Jedyne wyłączenie od obowiązków informacyjnych administratora danych wynikających z artykułu 13 w przypadku, gdy zebrał dane osobowe bezpośrednio od osoby, której dane dotyczą, występuje „*gdy – i w zakresie, w jakim – osoba, której dane dotyczą, dysponuje już tymi informacjami*”[42]. Zasada rozliczalności wymaga od administratorów danych wykazania (i udokumentowania), jakie informacje osoba, której dane dotyczą, już posiada, w jaki sposób i kiedy je otrzymała, oraz że od tamtego czasu nie miały miejsce zmiany w tych informacjach, które spowodowałyby ich nieaktualność. Ponadto użycie sformułowania „w zakresie, w jakim” w artykule 13 ust. 4 wyraźnie wskazuje, że nawet jeżeli osoba, której dane dotyczą, wcześniej otrzymała określone kategorie z wykazu informacji wymienionych w artykule 13, administrator danych nadal ma obowiązek uzupełnienia tych informacji w celu zapewnienia, że osoba, której dane dotyczą, będzie miała kompletny zestaw informacji wymienionych w artykułach 13 ust. 1 i ust. 2. Poniżej zaprezentowano przykład najlepszych praktyk dotyczący ograniczonego sposobu, w jaki powinno być skonstruowane wyłączenie wskazane w artykule 13 ust. 4.

Przykład

Osoba fizyczna rejestruje się w usłudze poczty elektronicznej online i otrzymuje wszystkie informacje wymagane na mocy artykułu 13 ust. 1 i ust. 2 w momencie rejestracji. Sześć miesięcy później osoba, której dane dotyczą, aktywuje funkcję komunikatora internetowego za pośrednictwem dostawcy usługi poczty elektronicznej oraz podaje w tym celu numer swojego telefonu komórkowego. Dostawca usługi zapewnia osobie, której dane dotyczą, określone informacje z artykułu 13 ust. 1 i ust. 2 na temat przetwarzania numeru telefonu (np. cele i podstawa prawna przetwarzania, odbiorcy, okres przechowywania), ale nie podaje innych informacji, które osoba fizyczna już posiada od 6 miesięcy i które nie zmieniły się od tamtego czasu (np. tożsamość i dane kontaktowe administratora i inspektora ochrony danych, informacje dotyczące praw osoby, której dane dotyczą, i prawa wniesienia skargi do organu nadzorczego). Jednak w ramach najlepszych praktyk, wszystkie te informacje powinny być ponownie przekazane osobie, której dane dotyczą. Nowe przetwarzanie do celów usługi komunikatora internetowego mogą mieć wpływ na osobę, której dane dotyczą, w sposób, który skłoni ją do usiłowania wykonania prawa, o którym mogła zapomnieć, od czasu otrzymania informacji 6 miesięcy wcześniej. Przekazanie wszystkich informacji ponownie pozwala zapewnić, że osoba, której dane dotyczą, będzie dobrze poinformowana o tym, jak są wykorzystywane jej dane oraz o przysługujących jej prawach.

Wyłączenia z artykułu 14

50. Artykuł 14 określa znacznie szerszy zestaw wyłączeń od obowiązku informacyjnego nałożonego na administratora danych, w przypadku pozyskiwania danych w sposób inny niż od osoby, której dane dotyczą. Wyłączenia te powinny, co do zasady, być interpretowane i stosowane w sposób zawężający. Dodatkowo do okoliczności, w których osoba, której dane

[42] Artykuł 13 ust. 4.

dotyczą, dysponuje już tymi informacjami (artykuł 14 ust. 5 lit. a)), artykuł 14 ust. 5 pozwala również na następujące wyłączenia:

- udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku lub może uniemożliwić lub poważnie utrudnić realizację celów takiego przetwarzania;

- administrator danych podlega wynikającemu z prawa krajowego lub prawa UE wymogowi pozyskania lub ujawnienia danych osobowych i prawo przewiduje odpowiednią ochronę prawnie uzasadnionych interesów osoby, której dane dotyczą; lub

- obowiązek zachowania tajemnicy zawodowej (w tym statutowy obowiązek zachowania tajemnicy), który jest uregulowany prawem krajowym lub prawem UE, oznacza że dane osobowe muszą pozostać poufne.

Okazuje się niemożliwe, niewspółmiernie duży wysiłek i poważne utrudnienie realizacji celów

51. Artykuł 14 ust. 5 lit. b) pozwala na 3 odrębne sytuacje, w których obowiązek udzielenia informacji określony w artykułach 14 ust. 1, 2 i 4 jest zniesiony:

i) gdy okazuje się to niemożliwe (w szczególności do celów archiwalnych, badań naukowych/historycznych lub statystycznych);

ii) jeżeli wymagałoby to niewspółmiernie dużego wysiłku (w szczególności do celów archiwalnych badań naukowych/historycznych lub statystycznych); lub

iii) jeżeli udzielenie informacji wymaganych na mocy artykułu 14 ust. 1 może uniemożliwić lub poważnie utrudnić realizację celów takiego przetwarzania.

"Okazuje się niemożliwe"

52. Sytuacja, w której udzielenie informacji „okazuje się niemożliwe" na mocy artykułu 14 ust. 5 lit. b), to sytuacja typu „wszystko albo nic", ponieważ coś jest albo niemożliwe albo nie jest; niemożliwość nie jest stopniowalna. Zatem jeżeli administrator danych chciałby opierać się na tym wyłączeniu, musi wykazać czynniki, które rzeczywiście *uniemożliwiają* mu udzielenie przedmiotowych informacji osobom, których dane dotyczą. Jeżeli, po pewnym czasie, czynniki, które przyczyniły się do „niemożliwości" już nie istnieją, i udzielenie informacji osobom, których dane dotyczą, staje się możliwe, wówczas administrator danych powinien niezwłocznie to uczynić. W praktyce będzie niewiele sytuacji, w których administrator danych może wykazać, że rzeczywiście niemożliwe jest udzielenie informacji osobom, których dane dotyczą. Ilustruje to poniższy przykład.

Przykład

Osoba, której dane dotyczą, rejestruje się w usłudze subskrypcji online płatnej z dołu. Po rejestracji administrator danych zbiera dane kredytowe dotyczące osoby, której dane dotyczą, z biura informacji kredytowej, w celu podjęcia decyzji, czy świadczyć tę usługę. Zgodnie ze swoimi zasadami postępowania, administrator informuje osoby, których dane dotyczą, o zbieraniu takich danych kredytowych w ciągu trzech dni od ich pozyskania, zgodnie z artykułem 14 ust. 3 lit. a). Jednakże adres i numer telefonu osoby, której dane dotyczą, nie

jest zarejestrowany w publicznych rejestrach (w rzeczywistości osoba, której dane dotyczą, mieszka za granicą). Osoba, której dane dotyczą, nie podała adresu poczty elektronicznej podczas rejestrowania się w usłudze lub adres poczty elektronicznej jest nieaktualny. Administrator ustala, że nie ma sposobu bezpośredniego skontaktowania się z osobą, której dane dotyczą. Jednak w tym przypadku administrator może podać informacje na temat zbierania informacji kredytowych na swojej stronie internetowej, przed rejestracją. W tym przypadku udzielenie informacji zgodnie z artykułem 14 nie byłoby niemożliwe.

Niemożliwe podanie źródła pochodzenia danych

53. Motyw 61 stanowi, że „*Jeżeli osobie, której dane dotyczą, nie można podać pochodzenia danych osobowych, ponieważ korzystano z różnych źródeł, informacje należy przedstawić w sposób ogólny*". Zniesienie wymogu udzielenia osobom, których dane dotyczą, informacji o źródle pochodzenia ich danych osobowych, ma zastosowanie tylko, jeżeli nie jest to możliwe, ponieważ różnych elementów danych osobowych dotyczących tej samej osoby, której dane dotyczą, nie można przypisać do określonego źródła. Na przykład sam fakt, że baza danych zawierająca dane osobowe licznych osób, których dane dotyczą, została opracowana przez administratora danych przy wykorzystaniu więcej niż jednego źródła, nie jest wystarczający do zniesienia tego wymogu, jeżeli możliwe jest (choć czasochłonne lub uciążliwe) określenie źródła pochodzenia danych osobowych indywidualnych osób, których dane dotyczą. Zważywszy na wymogi uwzględniania ochrony danych w fazie projektowania i domyślnej ochrony danych[43], mechanizmy przejrzystości powinny być wbudowane w systemy przetwarzania od samego początku, tak aby wszystkie źródła pochodzenia danych osobowych otrzymanych przez organizację można było śledzić i dotrzeć do ich źródła pochodzenia w każdym momencie cyklu przetwarzania danych (patrz punkt 36 powyżej).

„Niewspółmiernie duży wysiłek"

54. Na mocy artykułu 14 ust. 5 lit. b), jak w przypadku sytuacji „okazuje się niemożliwe", „niewspółmiernie duży wysiłek" również może mieć zastosowanie, w szczególności w przypadku przetwarzania „*do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem zabezpieczeń, o których mowa w artykule 89 ust. 1*". Motyw 62 również wskazuje te cele jako przypadki, w których udzielenie informacji osobie, której dane dotyczą, wymagałoby niewspółmiernie dużego wysiłku, oraz stanowi, że należy przy tym uwzględnić liczbę osób, których dane dotyczą, okres przechowywania danych oraz wszelkie przyjęte odpowiednie zabezpieczenia.

55. Podczas ustalania, co może stanowić niemożliwość lub niewspółmiernie duży wysiłek na mocy artykułu 14 ust. 5 lit. b), istotne jest, że nie ma porównywalnych wyłączeń na mocy artykułu 13 (w przypadku zbierania danych od osoby, której dane dotyczą). Jedyna różnica między sytuacją z artykułu 13 a sytuacją z artykułu 14 jest taka, że w tej ostatniej dane osobowe nie są zbierane od osoby, której dane dotyczą. Wynikają z tego dwie konsekwencje:

[43] Artykuł 25.

- na wyłączeniu nie mogą *rutynowo* opierać się administratorzy danych, którzy nie przetwarzają danych osobowych do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych[44]; oraz

- wynika z tego, że niemożliwość lub niewspółmiernie duży wysiłek pojawiają się tylko w okolicznościach, które nie mają zastosowania, jeżeli dane osobowe są zbierane od osoby, której dane dotyczą. Innymi słowy, niemożliwość lub niewspółmiernie duży wysiłek muszą być bezpośrednio związane z faktem, że dane osobowe pozyskano w sposób inny niż od osoby, której dane dotyczą.

56. Czynniki, o których mowa powyżej w ustępie 62 (liczba osób, których dane dotyczą, okres przechowywania danych oraz wszelkie przyjęte odpowiednie zabezpieczenia) mogą wskazywać na rodzaje kwestii, które przyczyniają się do konieczności podjęcia przez administratora danych niewspółmiernie dużego wysiłku w celu udzielenia osobie, której dane dotyczą, istotnych informacji z artykułu 14.

Przykład

Badacze historyczni, którzy chcą ustalić pochodzenie na podstawie nazwisk, uzyskują ogromny zbiór danych dotyczący 20 000 osób, których dane dotyczą. Jednakże dane zebrano 50 lat temu i od tamtego czasu ich nie aktualizowano, i nie obejmują one danych kontaktowych. Zważywszy na rozmiar bazy danych, a szczególnie okres przechowywania danych, znalezienie indywidualnych osób, których dane dotyczą, w celu udzielenia im informacji z artykułu 14 wymagałoby od badaczy niewspółmiernie dużego wysiłku.

57. W przypadku gdy administrator danych chciałby oprzeć się na wyłączeniu zawartym w artykule 14 ust. 5 lit. b) na podstawie, że udzielenie informacji wymagałoby niewspółmiernie dużego wysiłku, powinien przeprowadzić test bilansujący w celu oceny wysiłku wymaganego do udzielenia informacji osobie, której dane dotyczą, przez administratora danych, oraz skutków i konsekwencji niepodania informacji dla osoby, której dane dotyczą. Ocena ta powinna być udokumentowana przez administratora danych zgodnie z jego obowiązkami w zakresie rozliczalności. W takim przypadku artykuł 14 ust. 5 lit. b) określa, że administrator musi podjąć odpowiednie środki, by chronić prawa i wolności oraz prawnie uzasadnione interesy osoby, której dane dotyczą, w tym udostępnić informacje publicznie. Ponadto mogą mieć miejsce sytuacje, w których administrator danych przetwarza dane osobowe, w których nie jest wymagana identyfikacja osoby, której dane dotyczą (np. dane poddane pseudonimizacji). (W takich przypadkach istotny może być również artykuł 11 ust. 1, ponieważ stanowi, że administrator danych nie ma obowiązku zachowania, uzyskania ani przetworzenia dodatkowych informacji w celu zidentyfikowania osoby, której dane dotyczą, wyłącznie po to, by zastosować się do RODO).

[44] W przypadku gdy dane osobowe są przetwarzane do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, musi być to z zastrzeżeniem zabezpieczeń, o których mowa w art. 89 ust. 1.

Poważne utrudnienie realizacji celów

58. Ostatnia sytuacja, o której mowa w artykule 14 ust. 5 lit. b), to sytuacja, w której udzielenie informacji osobie, której dane dotyczą, na mocy artykułu 14 ust. 1 może uniemożliwić lub poważnie utrudnić realizację celów takiego przetwarzania. Aby móc oprzeć się na tym wyłączeniu, administratorzy danych muszą wykazać, że udzielenie tylko informacji określonych w artykule 14 ust. 1 unieważniłoby cele przetwarzania. Szczególnie bazowanie na tym aspekcie z artykułu 14 ust. 5 lit. b) zakłada, że przetwarzanie danych jest zgodne z zasadami określonymi w artykule 5, i że, co najważniejsze, w każdych okolicznościach, przetwarzanie danych osobowych jest rzetelne i że ma podstawę prawną.

Przykład

Bank A podlega na mocy ustawodawstwa dotyczącego przeciwdziałania praniu brudnych pieniędzy obowiązkowemu wymogowi zgłaszania podejrzanych działań dotyczących rachunków prowadzonych w tym banku do właściwego organu finansowego ds. egzekwowania prawa. Bank A otrzymuje informacje od Banku B (w innym państwie członkowskim), że posiadacz rachunku zlecił mu przekazanie pieniędzy na inny rachunek posiadany w Banku A, co wydaje się podejrzane. Bank A przekazuje te dane dotyczące posiadacza rachunku oraz informacje na temat podejrzanych działań właściwemu organowi finansowemu ds. egzekwowania prawa. Przedmiotowe ustawodawstwo dotyczące przeciwdziałania praniu brudnych pieniędzy uznaje za przestępstwo ostrzeżenie przez bank zgłaszający posiadacza rachunku, że może być on przedmiotem dochodzeń. W tej sytuacji zastosowanie ma artykuł 14 ust. 5 lit. b), ponieważ udzielenie osobie, której dane dotyczą (posiadaczowi rachunku w Banku A) informacji z artykułu 14 dotyczących przetwarzania danych osobowych posiadacza rachunku otrzymanych z Banku B poważnie utrudniłoby realizację celów ustawodawstwa, w tym zapobiegania ostrzeżeniom. Jednakże podczas otwierania rachunku wszystkim posiadaczom rachunków w Banku A powinny być udzielone ogólne informacje, że ich dane osobowe mogą być przetwarzane w celach zapobiegania praniu brudnych pieniędzy.

Uzyskanie lub ujawnienie jest wyraźnie określone w prawie

59. Artykuł 14 ust. 5 lit. c) pozwala na zniesienie wymogów informacyjnych przewidzianych w artykułach 14 ust. 1, ust. 2 i ust. 4, gdy – i w zakresie, w jakim – pozyskiwanie lub ujawnianie danych osobowych *„jest wyraźnie uregulowane prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator”*. To wyłączenie uwarunkowane jest przedmiotowym prawem przewidującym „*odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą”*. Takie prawo musi bezpośrednio dotyczyć administratora danych a przedmiotowe pozyskiwanie lub ujawnianie danych osobowych powinno być obowiązkowe dla administratora danych. W związku z tym administrator danych musi być w stanie wykazać, jak przedmiotowe prawo ma do niego zastosowanie i wymaga od niego pozyskiwania lub ujawniania przedmiotowych danych osobowych. Podczas gdy zadaniem Unii lub państwa członkowskiego jest takie sformułowanie prawa, aby przewidywało „*odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą”,* administrator danych powinien zapewnić (i być w stanie wykazać), że jego pozyskiwanie lub ujawnianie danych osobowych jest zgodne z tymi środkami. Ponadto administrator danych powinien

wyraźnie wskazać osobom, których dane dotyczą, że pozyskuje lub ujawnia dane osobowe zgodnie z przedmiotowym prawem, chyba że istnieje prawny zakaz uniemożliwiający administratorowi danych uczynienie tego. Jest to zgodne z motywem 41 RODO, który stanowi, że podstawa prawna lub akt prawny powinny być jasne i precyzyjne, a ich zastosowanie przewidywalne dla osób im podlegających – jak wymaga tego orzecznictwo Trybunału Sprawiedliwości Unii Europejskie i Europejskiego Trybunału Praw Człowieka. Jednak artykuł 14 ust. 5 lit. c) nie będzie miał zastosowania w sytuacji, gdy administrator danych podlega obowiązkowi uzyskania danych bezpośrednio od osoby, której dane dotyczą, w którym to przypadku zastosowanie będzie miał artykuł 13 i jedynym wyłączeniem na mocy RODO mającym zastosowanie do udzielania osobie, której dane dotyczą, informacji dotyczących przetwarzania będzie to przewidziane w artykule 13 ust. 4 (tj. gdy – i w zakresie, w jakim – osoba, której dane dotyczą, dysponuje już tymi informacjami).

Przykład

Organ podatkowy podlega na mocy prawa krajowego obowiązkowemu wymogowi pozyskiwania informacji dotyczących wynagrodzeń pracowników od ich pracodawców. Dane osobowe nie są pozyskiwane od osób, których dane dotyczą, i w związku z tym organ podatkowy podlega wymogom artykułu 14. Jednak jako że pozyskanie od pracodawców danych osobowych przez organ podatkowy jest wyraźnie określone prawem, wymogi informacyjne wskazane w artykule 14 nie mają w tym przypadku zastosowania do organu podatkowego.

Poufność wynikająca z obowiązku zachowania tajemnicy

60. Artykuł 14 ust. 5 lit. d) przewiduje wyłączenie od obowiązku informacyjnego nałożonego na administratorów danych, gdy dane osobowe *„muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii lub w prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy”*. W przypadku gdy administrator danych chce oprzeć się na tym wyłączeniu, musi być w stanie wykazać, że odpowiednio zidentyfikował to wyłączenie, oraz wykazać, jak obowiązek zachowania tajemnicy zawodowej bezpośrednio odnosi się do administratora danych, tak że uniemożliwia administratorowi danych udzielenie osobie, której dane dotyczą, wszystkich informacji określonych w artykułach 14 ust. 1, ust. 2 i ust. 4.

Przykład

Lekarz (administrator danych) podlega obowiązkowi zachowania tajemnicy zawodowej w odniesieniu do informacji medycznych swoich pacjentów. Pacjentka (w przypadku której ma zastosowanie obowiązek zachowania tajemnicy zawodowej) podaje lekarzowi informacje na temat swojego zdrowia dotyczące choroby genetycznej, którą ma również szereg jej bliskich krewnych. Pacjentka podaje również lekarzowi określone dane osobowe jej krewnych (osób, których dane dotyczą), które cierpią na tę samą chorobę. Lekarz nie jest zobowiązany do udzielenia tym krewnym informacji z artykułu 14, ponieważ ma zastosowanie wyłączenie przewidziane w artykule 14 ust. 5 lit. d). Jeżeli lekarz miałby udzielić informacji z artykułu

14 krewnym, naruszony zostałby obowiązek zachowania tajemnicy zawodowej, którego musi przestrzegać wobec swojej pacjentki.

Ograniczenia praw osoby, której dane dotyczą, na mocy artykułu 23

61. Artykuł 23 przewiduje dla państw członkowskich (lub UE) możliwość dalszego ograniczenia aktem prawnym zakresu praw osób, których dane dotyczą[45], w odniesieniu do przejrzystości i istotnych praw osób, których dane dotyczą, jeżeli ograniczenie takie nie narusza istoty podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym, służącym jednemu lub większej liczbie spośród dziesięciu celów określonych w artykule 23 ust. 1 lit a) do j). Jeżeli taki akt zmniejsza ogólne obowiązki w zakresie przejrzystości, które w przeciwnym przypadku miałyby zastosowanie do administratorów danych na mocy RODO, administrator danych powinien być w stanie wykazać, jak krajowy przepis miałby do niego zastosowanie. Jak określono w artykule 23 ust. 2 lit. h), administrator danych powinien poinformować osoby, których dane dotyczą, że opiera się na takim krajowym prawnym ograniczeniu obowiązku w zakresie przejrzystości, o ile nie narusza to celu ograniczenia.

Przejrzystość i naruszenia ochrony danych

62. GR Art. 29 opracowała wytyczne dotyczące naruszeń ochrony danych[46], ale na potrzeby niniejszych wytycznych, obowiązki administratora danych w zakresie informowania osoby, której dane dotyczą, o naruszeniach ochrony danych muszą w pełni uwzględniać wymogi w zakresie przejrzystości określone w artykule 12. Powiadomienie o naruszeniu ochrony danych musi być zgodne z tymi samymi wymogami, opisanymi powyżej (w szczególności w zakresie używania jasnego i prostego języka), które mają zastosowanie do każdej innej komunikacji z osobą, której dane dotyczą, w odniesieniu do jej praw oraz w związku z udzielaniem informacji na mocy artykułów 13 i 14.

[45] Jak określono w artykułach 12-22 i 34 oraz artykule 5, o ile jego przepisy odpowiadają prawom i obowiązkom przewidzianym w art. 12–22.
[46] Wytyczne dotyczące zgłoszeń naruszeń ochrony danych na mocy Rozporządzenia 2016/679 WP250.

Wykaz

Informacje, które muszą być udzielone osobie, której dane dotyczą, na mocy artykułu 13 lub artykułu 14

Rodzaj wymaganych informacji	**Właściwy artykuł (w przypadku zbierania danych bezpośrednio od osoby, której dane dotyczą**	**Właściwy artykuł (w przypadku zbierania danych osobowych w sposób inny niż od osoby, której dane dotyczą)**	**Uwagi GR Art. 29 dotyczące wymogu informacyjnego**
Tożsamość i dane kontaktowe administratora danych oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe jego przedstawiciela[47]	Artykuł 13 ust. 1 lit. a)	Artykuł 14 ust. 1 lit. a)	Informacje powinny umożliwić łatwą identyfikację administratora i najlepiej różne formy komunikacji z administratorem danych (np. numer telefonu, adres e-mail, adres pocztowy, etc.)
Gdy ma to zastosowanie – dane kontaktowe inspektora ochrony danych	Artykuł 13 ust. 1 lit. b)	Artykuł 14 ust. 1 lit. b)	Patrz wytyczne dotyczące inspektorów ochrony danych[48]
Cele przetwarzania danych osobowych	Artykuł 13 ust. 1 lit. c)	Artykuł 14 ust. 1 lit. c)	Dodatkowo do celów przetwarzania, do których mają posłużyć dane osobowe, należy określić właściwą podstawę prawną przetwarzania, na której się opiera administrator, zgodnie z artykułem 6 lub 9
Jeżeli podstawą prawną przetwarzania są prawnie uzasadnione interesy (artykuł 6 ust. 1 lit. f), prawnie uzasadnione	Artykuł 13 ust. 1 lit. d)	Artykuł 14 ust. 2 lit. b)	Należy określić dany interes na rzecz osoby, której dane dotyczą. W ramach najlepszych praktyk, administrator danych

[47] Zgodnie z definicją z artykułu 4 ust. 17 RODO (oraz jak wskazano w motywie 80), „przedstawiciel" oznacza osobę fizyczną lub prawną mającą miejsce zamieszkania lub siedzibę w Unii, która została wyznaczona na piśmie przez administratora lub podmiot przetwarzający na mocy art. 27 do reprezentowania administratora lub podmiotu przetwarzającego w zakresie ich obowiązków wynikających z RODO. Obowiązek ten ma zastosowanie, gdy, zgodnie z artykułem 3 ust. 2, administrator lub podmiot przetwarzający nie mają jednostek organizacyjnych w Unii, ale przetwarzanie dotyczy oferowania towarów lub usług osobom, których dane dotyczą, w Unii, lub monitorowania ich zachowania.

[48] Wytyczne dotyczące inspektorów ochrony danych, WP243 rev.01, ostatnio zmienione i przyjęte 5 kwietnia 2017 r.

interesy realizowane przez administratora lub przez stronę trzecią			powinien również podać osobie, której dane dotyczą, informacje wynikające z testu bilansującego, który powinien był być przeprowadzony przez administratora danych, aby umożliwić opieranie się na artykule 6 ust. 1 lit. f) jako podstawie prawnej przetwarzania, przed każdym zbieraniem danych osobowych osób, których dane dotyczą.
Kategorie odnośnych danych osobowych	Niewymagany	Artykuł 14 ust. 1 lit. d)	Informacje są wymagane w sytuacji z artykułu 14, ponieważ dane osobowe pozyskano z innego źródła niż od osoby, której dane dotyczą, która w związku z tym nie jest świadoma tego, jakie kategorie jej danych osobowych pozyskał administrator danych.
Informacje o odbiorcach[49] danych osobowych (lub o kategoriach odbiorców)	Artykuł 13 ust. 1 lit. e)	Artykuł 14 ust. 1 lit. e)	Pojęcie „odbiorcy" zdefiniowano w artykule 4 ust. 9 w taki sposób, że odbiorca nie musi być stroną trzecią. W związku z tym administratorzy danych, współadministratorzy i podmioty przetwarzające, którym dane są przekazywane lub ujawniane, objęci są terminem „odbiorca" i informacje o takich odbiorcach powinny być udzielone dodatkowo do informacji o odbiorcach będących stronami trzecimi. Zgodnie z zasadą rzetelności, domyślne stanowisko jest takie, że administrator danych powinien zapewnić informacje o rzeczywistych

[49] Jak określono w artykule 4 ust. 9 RODO i wskazano w motywie 31

			(z podaniem nazwy/nazwiska) odbiorcach danych osobowych. Jeżeli administrator danych postanawia podać tylko informacje o kategoriach odbiorców, administrator danych musi być w stanie wykazać, dlaczego przyjęcie tego podejścia jest dla niego rzetelne. W takich okolicznościach informacje o kategoriach odbiorców powinny być jak najbardziej konkretne, wskazując rodzaj odbiorcy (tj. odnosząc się do działań prowadzonych przez administratora), branżę, sektor i podsektor oraz lokalizację odbiorców.
Informacje o przekazywaniu danych do państw trzecich, fakt takiego przekazania i informacje o właściwych zabezpieczeniach[50] (w tym o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony[51]) oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych.	Artykuł 13 ust. 1 lit. f)	Artykuł 14 ust. 1 lit. f)	Musi być wskazany właściwy artykuł RODO pozwalający na przekazywanie i odpowiedni mechanizm (np. decyzja stwierdzająca odpowiedni stopień ochrony na mocy artykułu 45 / wiążące reguły korporacyjne na mocy artykułu 47 / standardowe klauzule ochrony danych na mocy artykułu 46 ust. 2 / wyjątki i zabezpieczenia na mocy artykułu 49, etc.). Gdy to możliwe, powinien być również podany link do użytego mechanizmu lub informacji o tym, gdzie i w jaki sposób można uzyskać dostęp do właściwego dokumentu lub go uzyskać. Zgodnie z zasadą rzetelności informacje powinny wyraźnie

[50] Jak określono w artykule 46 ust. 2 i ust. 3.
[51] Zgodnie z artykułem 45.

			wskazywać wszystkie państwa trzecie, do których będą przekazywane dane.
Okres przechowywania (lub jeżeli to niemożliwe, kryteria wykorzystane do określenia tego okresu)	Artykuł 13 ust. 2 lit. a)	Artykuł 14 ust. 2 lit. a)	Jest to związane z wymogiem minimalizacji danych przewidzianym w artykule 5 ust. 1 lit c) i wymogiem ograniczenia przechowania z artykułu 5 ust. 1 lit. e). Okres przechowywania (lub kryteria jego określenia) może być podyktowany czynnikami takimi jak wymogi ustawowe lub wytyczne branżowe, ale powinien być sformułowany w taki sposób, który pozwala osobie, której dane dotyczą, na ocenę, na podstawie jej własnej sytuacji, jaki będzie okres przechowywania dla określonych danych/celów. Nie jest wystarczające ogólne stwierdzenie przez administratora danych, że dane osobowe będą przechowywane tak długo, jak to niezbędne do prawnie uzasadnionych celów przetwarzania. W stosownym przypadku, powinny być przewidziane różne okresy przechowywania dla różnych kategorii danych osobowych i/lub różnych celów, w tym, gdy to właściwe, okresów archiwizacji.
Prawa osoby, której dane dotyczą, do: - dostępu; - sprostowania; - usunięcia;	Artykuł 13 ust. 2 lit. b)	Artykuł 14 ust. 2 lit. c)	Informacje te powinny obejmować streszczenie tego, co to prawo obejmuje i jakie kroki może podjąć osoba, której dane dotyczą, w celu wykonania tego prawa. W szczególności prawo do wniesienia

- ograniczenia przetwarzania; - wniesienia sprzeciwu wobec przetwarzania oraz - przenoszenia.			sprzeciwu wobec przetwarzania musi być wyraźnie podane do wiadomości osoby, której dane dotyczą, najpóźniej przy pierwszej komunikacji z osobą, której dane dotyczą, oraz musi być przedstawione jasno i odrębnie od innych informacji[52]. W odniesieniu do prawa do przenoszenia patrz Wytyczne GR Art. 29 dotyczące prawa do przenoszenia danych[53].
Jeżeli przetwarzanie odbywa się na podstawie zgody (lub wyraźnej zgody), prawo do cofnięcia zgody w dowolnym momencie	Artykuł 13 ust. 2 lit. c)	Artykuł 14 ust. 2 lit. d)	Informacje te powinny obejmować informacje, jak można wycofać zgodę, biorąc pod uwagę, że wycofanie zgody przez osobę, której dane dotyczą, musi być równie łatwe jak jej wyrażenie[54].
Prawo wniesienia skargi do organu nadzorczego	Artykuł 13 ust. 2 lit. d)	Artykuł 14 ust. 2 lit. e)	Informacje te powinny wyjaśniać, że zgodnie z artykułem 77 osoba, której dane dotyczą, ma prawo wnieść skargę do organu nadzorczego, w szczególności w państwie członkowskim swojego zwykłego pobytu, swojego miejsca pracy lub miejsca popełnienia domniemanego naruszenia RODO.
Informacje, czy istnieje wymóg ustawowy lub umowny podania informacji, lub czy niezbędne jest zawarcie umowy lub czy jest obowiązek podania informacji i jakie są	Artykuł 13 ust. 2 lit. e)	Niewymagany	Na przykład w kontekście zatrudnienia podanie określonych informacji obecnemu lub potencjalnemu pracodawcy może być wymogiem ustawowym.

[52] Artykuł 21 ust. 4 i motyw 70 (który ma zastosowanie w przypadku marketingu bezpośredniego).
[53] Wytyczne dotyczące prawa do przenoszenia danych, WP242 rev.01, ostatnio zmienione i przyjęte 5 kwietnia 2017 r.
[54] Artykuł 7 ust. 3.

ewentualne konsekwencje niepodania danych			Formularze online powinny wyraźnie określać, jakie pola są „wymagane", jakie nie i jakie będą konsekwencje niewypełnienia wymaganych pól.
Źródło pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych	Niewymagany	Artykuł 14 ust. 2 lit. f)	Informacje powinny obejmować: charakter źródeł (tj. źródła publiczne / prywatne; rodzaje organizacji / branży / sektora; oraz gdzie przechowywano informacje (UE lub poza UE), etc.). Należy podać konkretne źródło pochodzenia danych, chyba że uczynienie tego nie jest możliwe – patrz dalsze wytyczne w punkcie 53.
Informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, oraz – w stosownych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą	Artykuł 13 ust. 2 lit. f)	Artykuł 14 ust. 2 lit. g)	Patrz Wytyczne GR Art. 29 dotyczące zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania[55].

[55] Wytyczne dotyczące zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania na potrzeby Rozporządzenia 2016/679, WP251.