17/PL

GR260 rev.01

Grupa Robocza Art. 29

# Wytyczne w sprawie przejrzystości na podstawie rozporządzenia 2016/679

**Przyjęte dnia 29 listopada 2017 r.**

**Ostatnio zmienione i przyjęte w dniu 11 kwietnia 2018 r.**

**GRUPA ROBOCZA DS. OCHRONY OSÓB FIZYCZNYCH W ZAKRESIE**

**PRZETWARZANIA DANYCH OSOBOWYCH**

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

uwzględniając art. 29 i 30 tej dyrektywy,

uwzględniając swój regulamin wewnętrzny,

**PRZYJMUJE NINIEJSZE WYTYCZNE:**

Grupa Robocza została powołana na podstawie art. 29 dyrektywy 95/46/WE. Jest ona niezależnym europejskim organem doradczym w zakresie ochrony danych i prywatności. Zadania Grupy zostały określone w przepisach art. 30 dyrektywy 95/46/WE i art. 15 dyrektywy 2002/58/WE.

Obsługę sekretariatu zapewnia Komisja Europejska, Dyrekcja C (Prawa Podstawowe i Obywatelstwo Unii Europejskiej) Dyrekcji Generalnej ds. Sprawiedliwości, B-1049 Bruksela, Belgia, biuro nr MO-59 02/013.

Strona internetowa: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936

Spis treści

Wprowadzenie ..... 4
Znaczenie przejrzystości ..... 6
Elementy przejrzystości w świetle RODO ..... 6
*Zwięzła, przejrzysta, zrozumiała i łatwo dostępna forma* ..... 7
*Jasny i prosty język* ..... 9
*Udzielanie informacji dzieciom i innym osobom wymagającym szczególnego traktowania* ..... 10
*Na piśmie lub w inny sposób* ..... 12
*....informacji można udzielić ustnie...* ..... 13
*Wolne od opłat* ..... 14
Informacje udzielane osobie, której dane dotyczą – art. 13 i 14 ..... 15
*Treść* ..... 15
*Odpowiednie środki* ..... 15
*Czas podawania informacji* ..... 15
*Zmiany w informacjach, o których mowa w art. 13 i 14* ..... 18
*Terminy powiadamiania o zmianach w informacjach, o których mowa w art. 13 i 14* ..... 18
*Tryb i format udzielania informacji* ..... 19
*Warstwowe podejście w otoczeniu cyfrowym i warstwowe oświadczenia o ochronie prywatności / warstwowe informacje o polityce prywatności* ..... 20
*Warstwowe podejście w otoczeniu innym niż cyfrowe* ..... 21
*Powiadomienia typu „push" i „pull"* ..... 22
*Inne rodzaje „odpowiednich środków"* ..... 23
*Informacje dotyczące profilowania i zautomatyzowanego podejmowania decyzji* ..... 24
*Inne kwestie – ryzyko, zasady i zabezpieczenia* ..... 24
Informacje związane z dalszym przetwarzaniem ..... 25
Narzędzia wizualizacyjne ..... 27
*Znaki graficzne* ..... 27
*Mechanizmy certyfikacji, znaki jakości i oznaczenia* ..... 28
Wykonywanie uprawnień przysługujących osobom, których dane dotyczą ..... 29
Wyjątki od obowiązku udzielenia informacji ..... 30
*Wyjątki określone w art. 13* ..... 30
*Wyjątki określone w art. 14* ..... 31

*Okazuje się niemożliwe, niewspółmiernie duży wysiłek oraz poważne utrudnienie realizacji celów* ..... 31
„Okazuje się niemożliwe” ..... 31
*Niemożność podania źródła danych* ..... 32
„Niewspółmiernie duży wysiłek” ..... 33
*Poważne utrudnienie realizacji celów* ..... 34
*Pozyskiwanie lub ujawnianie jest wyraźnie uregulowane w prawie* ..... 35
*Poufność wynikająca z obowiązku zachowania tajemnicy* ..... 36
**Ograniczenia praw osoby, której dane dotyczą ..... 37**
**Przejrzystość oraz naruszenie ochrony danych ..... 38**
**Załącznik ..... 39**

Wprowadzenie

1. Niniejsze wytyczne Grupy Roboczej Art. 29 (GR29) zapewniają praktyczne wskazówki i pomoc w interpretacji w zakresie nowego obowiązku zachowania przejrzystości w odniesieniu do przetwarzania danych osobowych na podstawie ogólnego rozporządzenia o ochronie danych[1] („**RODO**"). Przejrzystość stanowi nadrzędny obowiązek wynikający z RODO, który ma zastosowanie do trzech głównych obszarów: 1) informowania osób, których dane dotyczą, w odniesieniu do rzetelności przetwarzania; 2) sposobu, w jaki administratorzy danych kontaktują się z osobami, których dane dotyczą, w związku z ich prawami wynikającymi z RODO; oraz 3) sposobu, w jaki administratorzy danych ułatwiają wykonywanie praw osobom, których dane dotyczą[2]. W zakresie, w jakim spełnienie wymogu przejrzystości jest konieczne w odniesieniu do przetwarzania danych na podstawie dyrektywy (UE) 2016/680[3], niniejsze wytyczne mają zastosowanie również do wykładni tej zasady[4]. Podobnie jak w przypadku wszystkich wytycznych GR29 również te wytyczne mają mieć ogólne zastosowanie i znaczenie dla administratorów bez względu na specyfikę sektorów, branż lub przepisów, z którymi mają do czynienia administratorzy danych. Ze względu na charakter wytycznych nie można w nich było uwzględnić niuansów i wielu zmiennych, które mogą wystąpić w kontekście obowiązków zapewnienia przejrzystości w danym sektorze, branży lub obszarze podlegającym regulacjom. Celem tych wytycznych jest jednak umożliwienie administratorom zrozumienia – na ogólnym poziomie – sposobu, w jaki GR29 interpretuje praktyczne skutki obowiązków zapewnienia przejrzystości, i wskazanie podejścia, które – zdaniem GR29 – administratorzy powinni przyjąć, aby wprowadzić przejrzystość, a ich działania opierały się na rzetelności i rozliczalności.

2. Przejrzystość od wielu lat jest stałym elementem prawa Unii[5]. Jej celem jest zapewnienie zaufania do procesów, które mają wpływ na obywatela, dzięki umożliwieniu mu ich

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.

[2] W niniejszych wytycznych określono ogólne zasady dotyczące wykonywania praw przez osoby, których dane dotyczą. Nie omówiono w nich natomiast szczególnych warunków związanych z poszczególnymi prawami osób fizycznych, których dane dotyczą, wynikającymi z RODO.

[3] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW.

[4] Chociaż przejrzystość nie jest jedną z zasad dotyczących przetwarzania danych osobowych, które określono w art. 4 dyrektywy (UE) 2016/680, w motywie 26 stwierdzono, że przetwarzanie danych osobowych musi być „zgodne z prawem, rzetelne i przejrzyste" względem zainteresowanej osoby fizycznej.

[5] W art. 1 TUE odniesiono się do podejmowania decyzji „z możliwie najwyższym poszanowaniem zasady otwartości i jak najbliżej obywateli"; w art. 11 ust. 2 stwierdzono, że „instytucje utrzymują otwarty, przejrzysty i regularny dialog ze

zrozumienia, a w razie konieczności również zgłoszenia wobec nich sprzeciwu. Stanowi również wcielenie zasady rzetelności w odniesieniu do przetwarzania danych osobowych, o którym mowa w art. 8 Karty praw podstawowych Unii Europejskiej. Na podstawie RODO (art. 5 ust. 1 lit. a)[6]) fundamentalnym aspektem tych zasad stała się – obok wymogu zgodnego z prawem i rzetelnego przetwarzania danych – także przejrzystość[7]. Przejrzystość jest nierozerwalnie związana z rzetelnością i nową zasadą rozliczalności w świetle RODO. Ponadto z art. 5 ust. 2 wynika, że administrator musi zawsze 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 danych byli w stanie wykazać, że przestrzegają swoich obowiązków wynikających z RODO[9].

3. Zgodnie z motywem 171 RODO, jeżeli przetwarzanie ma już miejsce w dniu 25 maja 2018 r., administrator danych powinien zapewnić, by od dnia 25 maja 2018 r. odbywało się ono zgodnie z obowiązkami zapewnienia przejrzystości (i ze wszystkimi innymi obowiązkami wynikającymi z RODO). Oznacza to, że przed dniem 25 maja 2018 r. administratorzy danych powinni zrewidować wszystkie informacje podawane osobom, których dane dotyczą, na temat przetwarzania ich danych osobowych (np. w oświadczeniach o ochronie prywatności / informacjach o polityce prywatności itd.), aby zapewnić ich zgodność z wymogami w zakresie przejrzystości omówionymi w niniejszych wytycznych. Jeżeli takie informacje są zmieniane lub uzupełniane, administratorzy powinni wyraźnie poinformować osoby, których dane dotyczą, że zmian tych dokonano w celu zapewnienia zgodności z przepisami RODO. GR29 zaleca czynne powiadamianie o takich zmianach lub uzupełnieniach osób, których dane dotyczą, a przynajmniej publiczne udostępnianie takich informacji przez administratorów (np. na swoich stronach internetowych). Jeżeli jednak zmiany lub uzupełnienia są istotne lub znaczne, wówczas zgodnie z pkt 29–32 poniżej osoba, której dane dotyczą, musi zostać o nich czynnie powiadomiona.

4. Przejrzystość (o ile jest przestrzegana przez administratorów danych) uprawnia osoby, których dane dotyczą, do pociągania do odpowiedzialności administratorów lub podmiotów przetwarzających i do sprawowania kontroli nad swoimi danymi osobowymi, np. poprzez udzielenie lub wycofanie świadomej zgody i wykonywanie praw przysługujących osobom, których dane dotyczą[10]. Koncepcja przejrzystości w RODO

---

stowarzyszeniami przedstawicielskimi i społeczeństwem obywatelskim"; w art. 15 TFUE mowa jest m.in. o prawie obywateli Unii do dostępu do dokumentów instytucji, organów i jednostek organizacyjnych Unii oraz o wymogach, zgodnie z którymi te instytucje, organy i jednostki organizacyjne Unii mają obowiązek zapewnić przejrzystość swoich prac.

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

[7] W dyrektywie 95/46/WE do przejrzystości nawiązano tylko w motywie 38, wspominając o warunku zapewnienia rzetelności przetwarzania danych, ale w odpowiadających temu motywowi przepisach art. 6 ust. 1 lit. a) nie ma wyraźnego odniesienia do przejrzystości.

[8] Zgodnie z art. 5 ust. 2 RODO administrator danych ma obowiązek wykazać przejrzystość (wraz z pięcioma pozostałymi zasadami dotyczącymi przetwarzania danych, o których mowa w art. 5 ust. 1) zgodnie z zasadą rozliczalności.

[9] W art. 24 ust. 1 przewidziano obowiązek, zgodnie z którym administrator danych ma wdrażać odpowiednie środki techniczne i organizacyjne, aby wykazać, że przetwarzanie odbywało się zgodnie z RODO.

[10] Zob. np. opinia rzecznika generalnego Cruza Villalóna (9 lipca 2015 r.) w sprawie C-201/14 Bara, pkt 74: „ten wymóg informowania osób, których dotyczy przetwarzanie ich danych osobowych, który gwarantuje przejrzystość wszelkich

skupia się w większym stopniu na użytkowniku niż na aspektach prawnych i jest realizowana za pomocą szczególnych wymogów praktycznych, które wiążą administratorów danych lub podmioty przetwarzające i są określone w wielu artykułach. Wymogi praktyczne (dotyczące informowania) wyszczególniono w art. 12–14 RODO. Jakość, dostępność i zrozumiałość informacji jest jednak tak samo ważna jak rzeczywista treść informacji dotyczących przejrzystości, którą należy udostępnić osobom, których dane dotyczą.

5. Ustanowione w RODO wymogi przejrzystości mają zastosowanie bez względu na podstawę prawną przetwarzania i na każdym etapie przetwarzania. Wynika to wyraźnie z art. 12, który stanowi, że przejrzystość należy zapewnić na następujących etapach cyklu przetwarzania danych:

- przed rozpoczęciem cyklu przetwarzania danych lub w chwili jego rozpoczęcia, tj. w momencie zbierania danych osobowych od osoby, której dane dotyczą, lub uzyskiwania ich w inny sposób;
- przez cały czas przetwarzania, tj. w momencie informowania osób, których dane dotyczą, o ich prawach; oraz
- w poszczególnych momentach przetwarzania, tj. kiedy występują naruszenia ochrony danych lub w przetwarzaniu zachodzą istotne zmiany.

## Znaczenie przejrzystości

6. RODO nie zawiera definicji przejrzystości. Motyw 39 RODO zawiera informacje na temat znaczenia i skutków 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 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 w świetle RODO

7. Artykuły, które mają największe znaczenie w zakresie przejrzystości w RODO, ponieważ mają zastosowanie do praw osób, których dane dotyczą, znajdują się w rozdziale III („Prawa osoby, której dane dotyczą”). W art. 12 ustanowiono ogólne zasady, które mają

---

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”.

zastosowanie do: udzielania informacji osobom, których dane dotyczą (na podstawie art. 13–14); powiadamiania osób, których dane dotyczą, o wykonywaniu ich praw (na podstawie art. 15–22); oraz powiadamiania o naruszeniach ochrony danych (art. 34). W szczególności w art. 12 wymaga się, by dane informacje lub komunikacja były zgodne z następującymi zasadami:

- muszą być w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie (art. 12 ust. 1);
- należy używać jasnego i prostego języka (art. 12 ust. 1);
- wymóg jasnego i prostego języka ma szczególne znaczenie, jeżeli informacje są kierowane do dziecka (art. 12 ust. 1);
- informacje są udzielane na piśmie „lub w inny sposób, w tym w stosownych przypadkach – elektronicznie" (art. 12 ust. 1);
- jeżeli osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie (art. 12 ust. 1); oraz
- informacje i komunikacja są zasadniczo wolne od opłat (art. 12 ust. 5).

*Zwięzła, przejrzysta, zrozumiała i łatwo dostępna forma*

8. Wymóg, zgodnie z którym podawanie informacji osobom, których dane dotyczą, i komunikacja z nimi odbywa się w „zwięzłej, przejrzystej, zrozumiałej i łatwo przystępnej formie", oznacza, że administratorzy danych powinni przekazywać informacje / komunikować się w sposób efektywny i zwięzły, tak aby nie przytłoczyć odbiorcy informacjami. Informacje te należy wyraźnie odróżnić od innych informacji niezwiązanych z prywatnością, np. postanowień umownych lub ogólnych warunków korzystania. W kontekście internetu zastosowanie warstwowego oświadczenia / warstwowej informacji o ochronie prywatności umożliwi osobie, której dane dotyczą, przejście do konkretnej części oświadczenia o ochronie prywatności / informacji o polityce prywatności, do której chce się natychmiast dostać, w związku z czym nie będzie musiała przewijać długiego tekstu w poszukiwaniu konkretnych kwestii.

9. Wymóg „zrozumiałości" informacji oznacza, że powinien ją zrozumieć przeciętny przedstawiciel grupy docelowych odbiorców. Zrozumiałość ma ścisły związek z wymogiem stosowania jasnego i prostego języka. Odpowiedzialny administrator danych będzie posiadał wiedzę na temat osób, o których zbiera informację, i będzie mógł ją wykorzystać, aby określić, jakie sformułowania będą najprawdopodobniej zrozumiałe dla odbiorców. Przykładowo, administrator zbierający dane osobowe wysoko wykwalifikowanych specjalistów może założyć wyższy stopień zrozumienia odbiorców niż administrator, który zbiera dane osobowe dzieci. Jeżeli administratorzy nie mają pewności co do stopnia zrozumiałości i przejrzystości informacji oraz skuteczności interfejsów użytkownika / powiadomień / polityk itd., mogą zbadać te kwestie, np. wykorzystując mechanizmy takie jak panele użytkowników, testy czytelności, interakcje formalne i nieformalne oraz dialog z grupami branżowymi, grupami reprezentującymi konsumentów i organami regulacyjnymi, stosownie do przypadku.

10. Najważniejszym aspektem zasady przejrzystości, którą określono we wspomnianych przepisach, jest to, że osoba, której dane dotyczą, powinna zawsze być w stanie z wyprzedzeniem określić zakres i skutki przetwarzania i że nie powinna zostać później

zaskoczona informacją, w jaki sposób wykorzystano jej dane osobowe. Jest to również ważny aspekt zasady rzetelności, o której mowa w art. 5 ust. 1 RODO, o czym świadczy związek tych przepisów z motywem 39, zgodnie z którym „[o]sobom fizycznym należy uświadomić ryzyka, zasady, zabezpieczenia i prawa związane z przetwarzaniem danych osobowych". Szczególnie w przypadku złożonego, technicznego lub niespodziewanego przetwarzania danych GR29 uważa, że poza zapewnieniem informacji wymaganych zgodnie z art. 13 i 14 (o których mowa w dalszej części niniejszych wytycznych) administratorzy powinni również oddzielnie i w sposób jednoznaczny wyjaśnić, jakie będą najważniejsze *skutki* przetwarzania: innymi słowy, jaki rzeczywisty wpływ na osobę, której dane dotyczą, będzie miało konkretne przetwarzanie opisane w oświadczeniu o ochronie prywatności / informacji o polityce prywatności. Zgodnie z zasadą rozliczalności i motywem 39 administratorzy danych powinni oceniać, czy istnieją szczególne zagrożenia dla osób fizycznych zaangażowanych w tego rodzaju przetwarzanie, o których należy powiadomić osoby, których dane dotyczą. Może to być pomocne w uzyskaniu ogólnego obrazu rodzajów przetwarzania, które mogą mieć największy wpływ na podstawowe prawa i wolności osób, których dane dotyczą, w związku z ochroną ich danych osobowych.

11. Element „łatwej dostępności" oznacza, że osoba, której dane dotyczą, nie powinna być zmuszona do wyszukiwania informacji; miejsce i sposób dostępu do informacji powinien od razu być dla niej oczywisty, co można zapewnić np. dzięki bezpośredniemu udzieleniu jej informacji, podaniu linków, wyraźnemu oznakowaniu takich informacji lub podaniu ich w formie odpowiedzi na pytanie sformułowanej w przystępny sposób (np. w internetowym warstwowym oświadczeniu o ochronie prywatności / warstwowej informacji o polityce prywatności, w FAQ, za pośrednictwem kontekstowych wyskakujących okien, które uruchamiają się podczas wypełniania internetowego formularza przez osobę, której dane dotyczą, lub – w interaktywnym kontekście cyfrowym – za pośrednictwem interfejsu chatbota itd. Mechanizmy te omówiono poniżej, w tym w pkt 33–40).

**Przykład**

Każda organizacja, która prowadzi stronę internetową, powinna opublikować na niej oświadczenie o ochronie prywatności / informację o polityce prywatności. Na każdej podstronie tej strony należy umieścić bezpośredni link do oświadczenia o ochronie prywatności / informacji o polityce prywatności, używając powszechnie stosowanego hasła (np. „Ochrona prywatności", „Polityka ochrony prywatności" lub „Informacja o polityce prywatności"). Pozycjonowanie lub schematy kolorystyczne, które sprawiają, że tekst lub link są mniej widoczne lub trudniejsze do zlokalizowania na stronie internetowej, nie są uważane za łatwo dostępne.

W przypadku aplikacji niezbędne informacje należy udostępnić również z poziomu sklepu internetowego przed pobraniem. Łatwą dostępność informacji należy zapewnić również z poziomu aplikacji po jej zainstalowaniu. Jednym ze sposobów spełnienia tego wymogu jest zapewnienie, by informacja była zawsze dostępna najwyżej po dwóch „kliknięciach" (np. poprzez dodanie opcji „Ochrona prywatności" / „Ochrona danych osobowych" w menu aplikacji). Ponadto omawiane informacje dotyczące prywatności powinny być opracowane indywidualnie dla danej aplikacji; generyczna informacja o polityce ochrony prywatności stosowanej przez przedsiębiorstwo będące właścicielem lub dystrybutorem

aplikacji jest niewystarczająca.

Jako najlepszą praktykę GR29 zaleca, by w momencie zbierania danych osobowych w środowisku online podawano link do oświadczenia o ochronie prywatności / informacji o polityce prywatności lub by udostępniano te informacje na tej samej stronie, na której zbiera się dane osobowe.

*Jasny i prosty język*

12. W przypadku informacji *pisemnych* (oraz gdy informacje pisemne są udzielane ustnie lub metodami dźwiękowo / audiowizualnymi, w tym osobom dotkniętym zaburzeniami widzenia) należy przestrzegać najlepszych praktyk w zakresie zrozumiałego stylu tekstu[11]. Podobny wymóg stylistyczny (dotyczący „prostego i zrozumiałego języka") był już wcześniej stosowany przez prawodawcę Unii[12] i został również wyraźnie wskazany w kontekście zgody w motywie 42 RODO[13]. Wymóg stosowania jasnego i prostego języka oznacza, że informacji należy udzielać w możliwie najprostszy sposób, bez stosowania złożonych struktur zdaniowych i językowych. Informacje powinny być konkretne i jednoznaczne; nie należy ich formułować przy pomocy pojęć abstrakcyjnych lub wieloznacznych ani pozostawiać dowolności interpretacji. Należy zwłaszcza jednoznacznie określić cele i podstawę prawną przetwarzania danych osobowych.

**Przykłady złych praktyk**

Poniższe zdania nie są wystarczająco jasne do celów przetwarzania:

- „Możemy wykorzystywać Twoje dane osobowe do opracowywania nowych usług" (nie wskazano wyraźnie, czym są „usługi", ani w jaki sposób dane pomogą ich w opracowaniu);
- „Możemy wykorzystywać Twoje dane osobowe do celów badawczych" (nie wskazano wyraźnie, o jakiego typu „badania" chodzi); oraz
- „Możemy wykorzystywać Twoje dane osobowe do oferowania spersonalizowanych usług" (nie wskazano wyraźnie, na czym polega „personalizacja").

**Przykłady dobrych praktyk[14]**

[11] Zob. wytyczne Komisji Europejskiej pt. „Jak pisać zrozumiale" (2011), dostępne pod adresem: https://publications.europa.eu/en/publication-detail/-/publication/c2dab20c-0414-408d-87b5-dd3c6e5dd9a5.

[12] Art. 5 dyrektywy Rady 93/13/EWG z dnia 5 kwietnia 1993 r. w sprawie nieuczciwych warunków w umowach konsumenckich.

[13] Zgodnie z motywem 42 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.

[14] Wymóg przejrzystości funkcjonuje zupełnie niezależnie od obowiązku upewnienia się przez administratorów danych o istnieniu właściwej podstawy prawnej przetwarzania zgodnie z art. 6.

- „Będziemy przechowywać historię Twoich zakupów i wykorzystywać szczegółowe informacje na temat produktów, które kupiłeś w przeszłości, aby proponować Ci inne produkty, którymi naszym zdaniem możesz być zainteresowany" (wyraźnie wskazano, jakie rodzaje danych będą przetwarzane oraz że osoba, której dane dotyczą, będzie otrzymywać ukierunkowane reklamy produktów i że dane tej osoby będą wykorzystywane w tym celu);

- „Będziemy przechowywać i badać informacje na temat Twoich ostatnich wizyt na naszej stronie i sposobu, w jaki poruszasz się po różnych sekcjach naszej strony, do celów analitycznych, aby dowiedzieć się, w jaki sposób użytkownicy korzystają z naszej strony, i uczynić ją bardziej intuicyjną" (wyraźnie wskazano, jakie rodzaje danych będą przetwarzane, oraz rodzaj analizy, którą administrator ma zamiar przeprowadzać); oraz

- „Będziemy rejestrować, na które artykuły na naszej stronie kliknąłeś, i wykorzystamy te informacje do tworzenia na tej stronie reklam przeznaczonych dla Ciebie, które będą dopasowane do Twoich zainteresowań, zidentyfikowanych przez nas na podstawie przeczytanych przez Ciebie artykułów" (wyraźnie wskazano, co obejmuje personalizacja i w jaki sposób określono zainteresowania osoby, której dane dotyczą).

13. Należy również unikać takich wyrazów określających jak „może", „niektóre", „często" i „możliwe". Jeżeli administratorzy danych postanowią używać bardziej wieloznacznych sformułowań, zasada rozliczalności wymaga, aby byli w stanie wykazać, dlaczego nie można było uniknąć stosowania takich sformułowań i że nie wpływają one na rzetelność przetwarzania. Należy zadbać o właściwą strukturę akapitów i zdań, stosując wypunktowania i wcięcia w tekście, aby wskazać związki hierarchiczne. Należy używać strony czynnej, a nie biernej, oraz unikać zbyt wielu rzeczowników. Informacje podawane osobie, której dane dotyczą, nie powinny być napisane zbyt prawniczym, technicznym lub specjalistycznym językiem ani zawierać słów o takim charakterze. Jeżeli informacje są tłumaczone na język obcy, administrator danych powinien zapewnić, by wszystkie tłumaczenia były wierne oraz by frazeologia i składnia tekstów w języku obcym były zrozumiałe, tak by nie trzeba było rozszyfrowywać znaczenia przetłumaczonego tekstu lub dokonywać jego reinterpretacji. (Jeżeli administrator kieruje informacje[15] do osób, których dane dotyczą i które posługują się innym językiem lub innymi językami, należy zapewnić tłumaczenie w tym języku lub tych językach.)

*Udzielanie informacji dzieciom i innym osobom wymagającym szczególnego traktowania*

14. Jeżeli administrator danych kieruje informacje do dzieci[16] lub wie / powinien wiedzieć, że jego towary/usługi są często wykorzystywane przez dzieci (również w przypadku, gdy

[15] Na przykład, jeżeli administrator prowadzi stronę internetową w danym języku lub oferuje opcje dla poszczególnych państw lub umożliwia płatność za towary i usługi w walucie danego państwa członkowskiego, może to wskazywać, że kieruje informacje do osób, których dane dotyczą, w konkretnym państwie członkowskim.
[16] W RODO nie zdefiniowano pojęcia „dziecka", jednak GR29 uznaje, że zgodnie z Konwencją ONZ o prawach dziecka, którą ratyfikowały wszystkie państwa członkowskie UE, dziecko jest osobą w wieku poniżej 18 lat.

administrator opiera się na zgodzie udzielonej przez dziecko)[17], powinien zapewnić, by stosowane słownictwo oraz ton i styl wypowiedzi były właściwe i dobrze zrozumiałe dla dzieci, tak aby dziecko będące odbiorcą informacji wiedziało, że wiadomość/informacja jest skierowana do niego[18]. Użytecznym przykładem języka kierowanego głównie do dziecka jako alternatywy dla pierwotnego języka prawniczego jest Konwencja ONZ o prawach dziecka w języku przyjaznym dla dzieci („UN Convention on the Rights of the Child in Child Friendly Language")[19].

15. Zdaniem GR29 prawo do przejrzystości jest samodzielnym prawem, które ma zastosowanie w takim samym stopniu do dzieci, jak do dorosłych. GR29 podkreśla w szczególności, że dzieci jako osoby, których dane dotyczą, nie tracą swoich praw do przejrzystości tylko dlatego, że zgodę wyraziła lub zaaprobowała osoba posiadająca odpowiedzialność rodzicielską w sytuacji, do której zastosowanie ma art. 8 RODO. W wielu przypadkach osoba posiadająca odpowiedzialność rodzicielską wyraża lub aprobuje zgodę jednorazowo, ale dziecko (podobnie jak każda inna osoba, której dane dotyczą) ma stale prawo do przejrzystości przez cały okres trwania relacji z administratorem danych. Jest to zgodne z art. 13 Konwencji ONZ o prawach dziecka, który stanowi, że dziecko ma prawo do swobodnej wypowiedzi, w tym prawo poszukiwania, otrzymywania i przekazywania informacji oraz idei wszelkiego rodzaju[20]. Należy podkreślić, że co prawda w art. 8 przewidziano możliwość wyrażenia zgody w imieniu dziecka przed osiągnięciem przez nie odpowiedniego wieku[21], ale *nie przewidziano w nim* środków zapewnienia przejrzystości kierowanych do osoby posiadającej odpowiedzialność rodzicielską, która wyraża taką zgodę. Zgodnie z konkretnymi wzmiankami o kierowanych do dzieci środkach zapewnienia przejrzystości, o których mowa w art. 12 ust. 1 (oraz w motywach 38 i 58), administratorzy danych, którzy kierują informacje do dzieci albo wiadomo im, że z ich towarów lub usług korzystają często dzieci w wieku, w którym prawdopodobnie umieją czytać, mają w związku z tym obowiązek zapewnić, by wszelkie informacje i komunikaty były przekazywane w jasnym i prostym języku lub w formie, którą dzieci mogą łatwo zrozumieć. Aby uniknąć wątpliwości, GR29 uznaje jednak, że w przypadku bardzo małych dzieci lub dzieci będących w wieku, w którym prawdopodobnie nie umieją czytać, można również wdrożyć środki zapewnienia przejrzystości skierowane do osób posiadających odpowiedzialność rodzicielską, ponieważ w większości przypadków takie dzieci prawdopodobnie nie będą w stanie zrozumieć nawet najbardziej podstawowych wiadomości dotyczących przejrzystości, czy to pisemnych, czy też w innej formie.

---

[17] Tj. przez dziecko w wieku co najmniej 16 lat (albo – jeżeli zgodnie z art. 8 ust. 1 RODO państwa członkowskie przewidziały w swoim prawie, że granica wiekowa do celów udzielenia zgody na oferowanie świadczenia usług społeczeństwa informacyjnego przypada między 13. a 16. rokiem życia – przez dziecko, które przekroczyło granicę wiekową przewidzianą w prawie krajowym).

[18] W motywie 38 stwierdzono, 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". W motywie 58 stwierdzono, 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".

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

[20] Art. 13 Konwencji ONZ o prawach dziecka stanowi, że: „Dziecko będzie miało prawo do swobodnej wypowiedzi; prawo to ma zawierać swobodę poszukiwania, otrzymywania i przekazywania informacji oraz idei wszelkiego rodzaju, bez względu na granice, w formie ustnej, pisemnej bądź za pomocą druku, w formie artystycznej lub z wykorzystaniem każdego innego środka przekazu według wyboru dziecka".

[21] Zob. przypis 17 powyżej.

16. Analogiczna sytuacja ma miejsce, gdy administratorowi danych jest wiadomo, że jego docelowymi klientami lub użytkownikami jego towarów lub usług są inni członkowie społeczeństwa wymagający szczególnego traktowania, w tym osoby niepełnosprawne lub osoby, które mogą mieć trudności z dostępem do informacji – wówczas administrator danych powinien uwzględnić ich trudności, oceniając możliwości wypełnienia przez niego obowiązków zapewnienia przejrzystości wobec osób, których dane dotyczą[22]. Dotyczy to konieczności dokonania przez administratora danych oceny prawdopodobnego poziomu zrozumienia przez grupę docelową, co zostało omówione powyżej w pkt 9.

*Na piśmie lub w inny sposób*

17. Zgodnie z art. 12 ust. 1 domyślną formą udzielania informacji lub komunikacji z osobami, których dane dotyczą, jest udzielanie informacji na piśmie[23]. (W art. 12 ust. 7 przewidziano również, że informacje można opatrzyć standardowymi znakami graficznymi; kwestię tę poruszono w sekcji poświęconej narzędziom wizualizacyjnym w pkt 49–53). W RODO przewidziano jednak możliwość korzystania z innych, nieokreślonych „środków", w tym drogi elektronicznej. Jeżeli chodzi o pisemne środki elektroniczne, GR29 uważa, że jeżeli administrator danych prowadzi stronę internetową (lub prowadzi całość lub część swojej działalności za pośrednictwem strony internetowej), GR29 zaleca stosowanie warstwowych oświadczeń o ochronie prywatności / warstwowych informacji o polityce prywatności, dzięki których osoby odwiedzające stronę internetową mogą zapoznać się z najbardziej interesującymi dla nich fragmentami danego oświadczenia o ochronie prywatności / informacji o polityce prywatności (więcej informacji na temat oświadczeń o ochronie prywatności / informacji o polityce prywatności znajduje się w pkt 35–37)[24]. Osoby, których dane dotyczą, powinny mieć jednak dostęp do wszystkich skierowanych do nich informacji również w jednym miejscu lub w ramach jednego dokumentu (elektronicznego lub papierowego), który powinien być łatwo dostępny dla takiej osoby, jeżeli zechce ona zapoznać się ze wszystkimi skierowanymi do niej informacjami. Należy podkreślić, że stosowanie warstwowej struktury nie ogranicza się wyłącznie do pisemnych środków elektronicznych stosowanych w celu udzielania informacji osobom, których dane dotyczą. Jak omówiono w pkt 35–36 i 38 poniżej, warstwową strukturę informacji udzielanych osobom, których dane dotyczą, można również zastosować przez połączenie kilku *metod* w celu zapewnienia przejrzystości przetwarzania.

18. Oczywiście stosowanie warstwowych oświadczeń o ochronie prywatności / warstwowych informacji o polityce prywatności w formie elektronicznej nie stanowi jedynego pisemnego środka elektronicznego, który mogą stosować administratorzy. Inne środki elektroniczne obejmują wyskakujące powiadomienia kontekstowe typu „just-in-time", powiadomienia za pomocą funkcji 3D Touch lub powiadomienia wyświetlające się po najechaniu kursorem oraz pulpity nawigacyjne prywatności. Niepisemne środki elektroniczne, które można

[22] Przykładowo w Konwencji o prawach osób niepełnosprawnych istnieje wymóg zapewnienia odpowiednich form pomocy i wsparcia dla osób niepełnosprawnych w celu zapewnienia im dostępu do informacji.

[23] W art. 12 ust. 1 pojawia się pojęcie „języka"; ponadto artykuł ten stanowi, że informacji udziela się na piśmie lub w inny sposób, w tym w stosownych przypadkach – elektronicznie.

[24] GR29 uznała już korzyści wynikające z warstwowej struktury informacji w opinii 10/2004 w sprawie bardziej ujednoliconych przepisów dotyczących informacji i w opinii 02/2013 w sprawie aplikacji na urządzenia inteligentne.

wykorzystać *oprócz* warstwowego oświadczenia o ochronie prywatności / warstwowej informacji o polityce prywatności, mogą obejmować filmy wideo oraz powiadomienia na smartfon lub powiadomienia głosowe w technologii internetu rzeczy[25]. „Inne środki", które nie muszą być środkami elektronicznymi, mogą obejmować np. komiksy, infografiki lub schematy blokowe. Jeżeli informacje dotyczące przejrzystości są kierowane do dzieci, administratorzy powinni rozważyć, jakie rodzaje środków mogą być szczególnie przystępne dla dzieci (m.in. komiksy/kreskówki, piktogramy, animacje itd.).

19. Najważniejsze jest, aby wybrane metody udzielania informacji były dostosowane do konkretnej sytuacji, tj. do sposobu komunikacji między administratorem danych a osobą, której dane dotyczą, lub sposobu zbierania informacji odnoszących się do tej osoby. Przykładowo udzielanie informacji wyłącznie w pisemnym formacie elektronicznym, np. w formie internetowego oświadczenia o ochronie prywatności / informacji o polityce prywatności, może być niewłaściwe/niepraktyczne, gdy urządzenie rejestrujące dane osobowe nie ma ekranu (np. urządzenia połączone za pośrednictwem internetu rzeczy / urządzenia inteligentne), na którym mogą być wyświetlane strony internetowe / takie pisemne informacje. W takich przypadkach należy rozważyć zastosowanie odpowiednich *dodatkowych* środków alternatywnych, np. umieszczenie oświadczenia o ochronie prywatności / informacji o polityce prywatności w papierowych instrukcjach lub podanie adresu URL strony internetowej (tzn. jej konkretnej podstrony), pod którym można znaleźć internetowe oświadczenie o ochronie prywatności / informację o polityce prywatności, w papierowej instrukcji lub na opakowaniu. Można również dodatkowo przekazać informacje w formie dźwiękowej (ustnej), jeżeli urządzenie bez ekranu może odtwarzać dźwięk. GR29 sformułowała wcześniej zalecenia dotyczące przejrzystości i przekazywania informacji osobom, których dane dotyczą, w opinii na temat ostatnich postępów w dziedzinie internetu rzeczy[26] (np. stosowania kodów QR wydrukowanych na obiektach w technologii internetu rzeczy, tak aby po zeskanowaniu kodu QR wyświetliły się wymagane informacje dotyczące przejrzystości). Zalecenia te mają zastosowanie również w zakresie RODO.

*....informacji można udzielić ustnie...*

20. W art. 12 ust. 1 przewidziano w szczególności, że na żądanie osoby, której dane dotyczą, informacji można udzielić ustnie, o ile innymi sposobami potwierdzi się jej tożsamość. Innymi słowy, sposób potwierdzenia tożsamości nie powinien opierać się wyłącznie na zapewnieniu danej osoby, że jest ona osobą o danym imieniu i nazwisku, oraz powinien umożliwiać administratorowi weryfikację tożsamości osoby, której dane dotyczą, dającą wystarczającą pewność. Wymóg weryfikacji tożsamości osoby, której dane dotyczą, przed przekazaniem informacji ustnie, ma zastosowanie tylko do tych informacji, które dotyczą wykonywania przez osobę, której dane dotyczą, jej praw przewidzianych w art. 15–22 i 34. Ten warunek wstępny dotyczący przekazywania informacji ustnie nie może mieć zastosowania do przekazywania ogólnych informacji na temat ochrony prywatności, o których mowa w art. 13 i 14, ponieważ informacje wymagane na podstawie art. 13 i 14 muszą być udostępniane również *przyszłym* użytkownikom/klientom (których tożsamości

[25] Powyższe przykłady środków elektronicznych mają jedynie charakter orientacyjny, a administratorzy danych mogą opracować nowe innowacyjne metody, aby zapewnić zgodność z art. 12.
[26] Opinia GR29 8/2014 przyjęta w dniu 16 września 2014 r.

administrator danych nie jest w stanie zweryfikować). W związku z tym informacje, których należy udzielić na podstawie art. 13 i 14, mogą zostać przekazane ustnie bez konieczności potwierdzenia przez administratora tożsamości osoby, której dane dotyczą.

21. Ustne udzielanie informacji, o których mowa w art. 13 i 14, niekoniecznie oznacza udzielenie informacji ustnie w formie bezpośredniego kontaktu z daną osobą (np. osobiście lub telefonicznie). Poza środkami pisemnymi można zapewnić automatyczne przekazywanie ustnych informacji. Taka sytuacja może mieć miejsce np. w kontekście osób słabowidzących, gdy kontaktują się one z dostawcami usług społeczeństwa informacyjnego, lub w kontekście urządzeń inteligentnych bez ekranów, o których wspomniano powyżej w pkt 19. GR29 jest zdania, że jeżeli administrator danych postanowi ustnie przekazać informacje osobie, której dane dotyczą, lub jeżeli osoba, której dane dotyczą, zażąda ustnego udzielenia informacji lub ustnej komunikacji, administrator danych powinien umożliwić osobie, której dane dotyczą, ponowne odsłuchanie nagranych wiadomości. Jest to konieczne, jeżeli żądanie ustnego udzielenia informacji dotyczy osób słabowidzących, których dane dotyczą, lub innych osób, których dane dotyczą, mających problemy z dostępem do informacji w formie pisemnej lub z ich zrozumieniem. Administrator danych powinien również upewnić się, że prowadzona jest dokumentacja w odniesieniu do poniższych elementów i że może ją przedstawić (do celów spełnienia wymogu rozliczalności): (i) wniosek o ustne przekazanie informacji, (ii) metoda, którą zweryfikowano tożsamość osoby, której dane dotyczą (w stosownych przypadkach – zob. pkt 20 powyżej) oraz (iii) fakt, że informacje zostały przekazane osobie, której dane dotyczą.

*Wolne od opłat*

22. Zgodnie z art. 12 ust. 5[27] administratorzy danych zasadniczo nie mogą pobierać od osób, których dane dotyczą, opłat za przekazywanie informacji udzielanych na podstawie art. 13 i 14 ani za komunikację i działania podejmowane na podstawie art. 15–22 (dotyczących praw osób, których dane dotyczą) i 34 (dotyczącego zawiadamiania osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych)[28]. Ten aspekt przejrzystości oznacza również, że nie wolno uzależniać przekazania informacji udzielanych zgodnie z wymogami przejrzystości od dokonania transakcji finansowej, np. zapłaty za usługi lub towary bądź ich zakupu[29].

[27] Zgodnie z tym artykułem „informacje podawane na mocy art. 13 i 14 oraz komunikacja i działania podejmowane na mocy art. 15–22 i 34 są wolne od opłat".

[28] Zgodnie z art. 12 ust. 5 administrator może jednak pobrać rozsądną opłatę, jeżeli np. żądanie osoby, której dane dotyczą, względem informacji udzielanych na podstawie art. 13 i 14 lub praw przewidzianych w art. 15–22 lub 34 jest ewidentnie nieuzasadnione lub nadmierne. (Oddzielnie administrator może – w związku z prawem dostępu przewidzianym w art. 15 ust. 3 – pobrać rozsądną opłatę, uwzględniając administracyjne koszty kolejnych kopii danych osobowych sporządzanych na wniosek osoby, której dane dotyczą).

[29] Na przykład, jeżeli dane osobowe osoby, której dane dotyczą, są zbierane w związku z zakupem, informacje, które należy podać na podstawie art. 13, powinny zostać przekazane przed dokonaniem płatności i w momencie zbierania informacji, a nie po zawarciu transakcji. Jeżeli jednak osobie, której dane dotyczą, oferowane są nieodpłatne usługi, wówczas informacje przewidziane w art. 13 również muszą być udzielone przed rejestracją, a nie po niej, ponieważ w art. 13 ust. 1 przewidziano wymóg podania informacji „podczas pozyskiwania danych osobowych".

## Informacje udzielane osobie, której dane dotyczą – art. 13 i 14

*Treść*

23. W RODO wymieniono kategorie informacji, których należy udzielić osobie, której dane dotyczą, w związku z przetwarzaniem danych osobowych tej osoby, bez względu na to, czy zostały zebrane od osoby, której dane dotyczą (art. 13), czy też pozyskane z innego źródła (art. 14). W tabeli w załączniku do niniejszych wytycznych podsumowano kategorie informacji, których należy udzielić na podstawie art. 13 i 14. W tabeli opisano również charakter, zakres i treść tych wymogów. Należy wyjaśnić, że GR29 reprezentuje stanowisko, iż status informacji udzielanych na podstawie ust. 1 i 2 odpowiednio w art. 13 oraz w art. 14 jest taki sam. Wszystkie informacje, o których mowa w tych ustępach, są równie ważne i muszą zostać udzielone osobie, której dane dotyczą.

*Odpowiednie środki*

24. Ważna jest nie tylko treść, ale również forma i sposób, w który informacje udzielane na podstawie art. 13 i 14 powinny być przekazane osobie, której dane dotyczą. Powiadomienie zawierające takie informacje zwane jest często powiadomieniem o ochronie danych, informacją o polityce prywatności, polityką ochrony prywatności, oświadczeniem o ochronie prywatności lub informacją o rzetelnym przetwarzaniu. W RODO nie określono formatu lub sposobu udzielania takich informacji osobie, której dane dotyczą, ale stwierdzono w nim wyraźnie, że administrator danych ma obowiązek podjąć „odpowiednie środki" w związku z udzielaniem wymaganych informacji do celów zapewnienia przejrzystości. Oznacza to, że wybierając właściwy sposób i format udzielania informacji, administrator danych powinien uwzględnić wszelkie okoliczności zbierania i przetwarzania danych. W szczególności należy ocenić odpowiednie środki pod kątem doświadczenia użytkownika produktu/usługi. Oznacza to uwzględnienie urządzenia, z którego korzysta użytkownik (w stosownych przypadkach), charakterystyki interfejsów użytkownika / komunikacji z administratorem danych („zestaw interakcji" użytkownika) oraz ograniczeń, które wynikają z tych czynników. Jak wskazano powyżej w pkt 17, GR29 zaleca, by korzystano z warstwowego internetowego oświadczenia o ochronie prywatności / warstwowej informacji o polityce prywatności, jeżeli administrator danych działa w internecie.

25. Aby ułatwić określenie najwłaściwszych sposobów udzielania informacji, zanim zostaną zastosowane w praktyce, administratorzy danych mogą sprawdzić różne sposoby w drodze testowania przez użytkownika (np. badania typu *hall test* lub inne standardowe testy czytelności lub przystępności), aby uzyskać informacje zwrotne od użytkownika na temat przystępności, zrozumienia i łatwości stosowania proponowanego środka. (Zob. również powyższe szczegółowe uwagi na temat innych mechanizmów przeprowadzania testów przez użytkownika w pkt 9). Udokumentowanie tego podejścia powinno ponadto pomóc administratorom danych w wywiązaniu się z ich obowiązków w zakresie rozliczalności, ponieważ będą mogli w ten sposób wykazać, dlaczego narzędzie/podejście wybrane do podania informacji jest najwłaściwszym w danych okolicznościach.

*Czas podawania informacji*

26. W art. 13 i 14 określono informacje, których należy udzielić osobie, której dane dotyczą, na początku cyklu przetwarzania[30]. Art. 13 ma zastosowanie do scenariusza, w którym dane zbiera się od osoby, której dane dotyczą. Obejmuje dane osobowe, które:

- osoba, której dane dotyczą, świadomie przekazuje administratorowi danych (np. wypełniając formularz internetowy); lub
- administrator danych pozyskuje od osoby, której dane dotyczą, w drodze obserwacji (np. przy zastosowaniu automatycznych rejestratorów danych lub oprogramowania rejestrującego dane, np. kamer, urządzeń sieciowych, śledzenia sieci Wi-Fi, RFID lub innych rodzajów sensorów).

Art. 14 ma zastosowanie do scenariusza, w którym danych nie pozyskano od osoby, której dotyczą. Obejmują one dane osobowe, które administrator danych pozyskał ze źródeł takich jak:

- zewnętrzni administratorzy danych;
- źródła dostępne publicznie;
- pośrednicy danych; lub
- inne osoby, których dane dotyczą.

27. Jeżeli chodzi o czas udzielania tych informacji, ich udzielenie w odpowiednim czasie stanowi ważny element wykonania obowiązku zapewnienia przejrzystości i obowiązku rzetelnego przetwarzania danych. Jeżeli zastosowanie ma art. 13, informacje przewidziane w art. 13 ust. 1 muszą być podawane „podczas pozyskiwania danych osobowych". W przypadku danych osobowych pozyskiwanych pośrednio na podstawie art. 14, terminy, w których należy udzielić wymaganych informacji osobie, której dane dotyczą, określono w art. 14 ust. 3 lit. a)–c):

- zgodnie z ogólnym wymogiem informacje należy przekazać w „rozsądnym terminie" po pozyskaniu danych osobowych, a najpóźniej w ciągu miesiąca, „mając na uwadze konkretne okoliczności przetwarzania danych osobowych" (art. 14 ust. 3 lit. a));

- ogólny termin jednego miesiąca, o którym mowa w art. 14 ust. 3 lit. a), może zostać skrócony na podstawie art. 14 ust. 3 lit. b)[31], jeżeli dane są wykorzystywane do komunikacji z osobą, której dane dotyczą. Wówczas informacji należy udzielić najpóźniej przy pierwszej komunikacji z osobą, której dane dotyczą. Jeżeli pierwsza komunikacja następuje przed upływem terminu jednego miesiąca po uzyskaniu danych osobowych, wówczas informacji należy udzielić

[30] Zgodnie z zasadami rzetelności i ograniczenia celu organizacja, która pozyskuje dane osobowe od osoby, której dane dotyczą, zawsze powinna określić cele przetwarzania danych w momencie ich zbierania. Jeżeli jednym z takich celów jest tworzenie implikowanych danych osobowych, osoba, której dane dotyczą, zawsze musi zostać poinformowana o zamierzonym celu tworzenia i dalszego przetwarzania takich implikowanych danych oraz kategorii przetwarzanych implikowanych danych w momencie zbierania danych lub przed dalszym przetwarzaniem do nowego celu zgodnie z art. 13 ust. 3 lub art. 14 ust. 4.

[31] Użycie sformułowania „jeżeli dane osobowe mają być stosowane do […]" w art. 14 ust. 3 lit. b) wskazuje na uszczegółowienie ogólnego stanowiska dotyczącego maksymalnego terminu, który ustalono w art. 14 ust. 3 lit. a), ale nie zastępuje tego stanowiska.

*najpóźniej* przy pierwszej komunikacji z osobą, której dane dotyczą, niezależnie od tego, że termin jednego miesiąca od chwili pozyskania danych nie upłynął. Jeżeli pierwsza komunikacja z osobą, której dane dotyczą, następuje po ponad jednym miesiącu od uzyskania danych osobowych, wówczas zastosowanie ma w dalszym ciągu art. 14 ust. 3 lit. a), tj. informacje udzielane na podstawie art. 14 muszą zostać przekazane osobie, której dane dotyczą, najpóźniej w ciągu jednego miesiąca od ich uzyskania;

- ogólny termin jednego miesiąca[32], o którym mowa w art. 14 ust. 3 lit. a), może zostać skrócony również na podstawie art. 14 ust. 3 lit. c), który ma zastosowanie, jeżeli planuje się ujawnić dane innemu odbiorcy (bez względu na to, czy jest on osobą trzecią)[33]. W takim przypadku informacji należy udzielić najpóźniej przy pierwszym ujawnieniu. Jeżeli wówczas pierwsze ujawnienie następuje przed upływem terminu jednego miesiąca, wówczas informacji należy udzielić *najpóźniej* przy pierwszym ujawnieniu, chociaż termin jednego miesiąca od chwili pozyskania danych nie upłynął. Podobnie do stanowiska, o którym mowa w art. 14 ust. 3 lit. b), jeżeli dane osobowe zostaną ujawnione później niż w ciągu jednego miesiąca od uzyskania danych osobowych, wówczas zastosowanie ma ponownie art. 14 ust. 3 lit. a), tj. informacje udzielane na podstawie art. 14 muszą zostać przekazane osobie, której dane dotyczą, najpóźniej w ciągu jednego miesiąca od ich pozyskania.

28. W związku z tym w każdym przypadku maksymalny termin, w którym należy udzielić informacji, o których mowa w art. 14, osobie, której dane dotyczą, wynosi jeden miesiąc. Zasady rzetelności i rozliczalności w ramach RODO wymagają jednak, aby podejmując decyzję o tym, w którym momencie udzielić informacji przewidzianych w art. 14, administratorzy danych zawsze brali pod uwagę rozsądne oczekiwania osób, których dane dotyczą, potencjalny wpływ przetwarzania na te osoby i ich zdolność do wykonywania praw w związku z tym przetwarzaniem. Zasada rozliczalności wymaga, aby administratorzy wykazywali logikę, na której opierają swoje decyzje, i uzasadniali, dlaczego informacje podano w konkretnym czasie. W praktyce spełnienie tych wymogów może być trudne, jeżeli informacji udziela się „w ostatniej chwili". W tym względzie w motywie 39 przewidziano m.in., 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". W motywie 60 odniesiono się również do wymogu, zgodnie z którym osoba, której dane dotyczą, musi być informowana o prowadzeniu operacji przetwarzania i o jej celach w kontekście zasad rzetelnego i przejrzystego przetwarzania. W świetle powyższego GR29 jest zdania, że w każdym przypadku, gdy jest to możliwe, administratorzy danych powinni – zgodnie z zasadą rzetelności – udzielać informacji osobom, których dane dotyczą, z dużym wyprzedzeniem w stosunku do określonych w prawie terminów. Dalsze uwagi na temat odpowiednich okresów między powiadomieniem osób, których dane dotyczą,

[32] Użycie sformułowania „jeżeli planuje się ujawnić dane osobowe innemu odbiorcy" w art. 14 ust. 3 lit. c) również wskazuje na uszczegółowienie ogólnego stanowiska dotyczącego maksymalnego terminu, który ustalono w art. 14 ust. 3 lit. a), ale nie zastępuje tego stanowiska.

[33] W art. 4 pkt 9 znajduje się definicja „odbiorcy", zgodnie z którą odbiorca, któremu ujawniane są dane osobowe, nie musi być stroną trzecią. W związku z tym odbiorcą może być administrator danych, współadministrator lub podmiot przetwarzający.

o operacjach przetwarzania a rzeczywistym przeprowadzeniem takich operacji przetwarzania zamieszczono w pkt 30–31 i 48.

*Zmiany w informacjach, o których mowa w art. 13 i 14*

29. Rozliczalność w zakresie przejrzystości ma zastosowanie nie tylko w chwili zbierania danych osobowych, ale przez cały czas przetwarzania, bez względu na przekazywane informacje lub komunikację. Ma to miejsce np. przy zmianie treści dotychczasowych oświadczeń o ochronie prywatności / informacji o polityce prywatności. Administrator powinien przestrzegać tych samych zasad, zarówno gdy przekazuje pierwsze oświadczenie o ochronie prywatności / informację o polityce prywatności, jak i gdy powiadamia o wszelkich istotnych lub dużych zmianach w tym oświadczeniu / tej informacji. Czynniki, które administratorzy powinni uwzględnić przy ocenie, czym jest istotna lub duża zmiana, obejmują wpływ na osoby, których dane dotyczą (w tym ich zdolność do wykonywania swoich praw), oraz na ile zmiana będzie niespodziewana lub zaskakująca dla osób, których dane dotyczą. Osoby, których dane dotyczą, zawsze powinny być informowane m.in. o następujących zmianach w oświadczeniu o ochronie prywatności / informacji o polityce prywatności: zmiana celu przetwarzania; zmiana tożsamości administratora; zmiana sposobu, w jaki osoby, których dane dotyczą, mogą wykonywać swoje prawa w związku z przetwarzaniem. Przykłady zmian w oświadczeniu o ochronie prywatności / informacji o polityce prywatności, które – zdaniem GR29 – nie są istotne ani duże, obejmują poprawę literówek lub błędów stylistycznych/gramatycznych. Ponieważ większość klientów lub użytkowników jedynie pobieżnie czyta komunikaty na temat zmian w oświadczeniach o ochronie prywatności / informacjach o polityce prywatności, administrator powinien zastosować wszelkie niezbędne środki, aby zapewnić komunikowanie tych zmian w taki sposób, aby większość odbiorców rzeczywiście je dostrzegła. Oznacza to np. że komunikat w sprawie zmian powinien być zawsze przekazywany za pośrednictwem odpowiedniego środka (np. pocztą elektroniczną, listem, w wyskakującym oknie na stronie internetowej lub w inny sposób, który rzeczywiście zwróci uwagę na zmiany) specjalnie poświęconego tym zmianom (a nie np. razem z treściami z zakresu marketingu bezpośredniego), przy czym komunikat musi również spełniać wymogi przewidziane w art. 12, tj. zostać sporządzony w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Zamieszczenie w oświadczeniu o ochronie prywatności / informacji o polityce prywatności zalecenia dla osoby, której dane dotyczą, aby regularnie sprawdzała oświadczenie o ochronie prywatności / informację o polityce prywatności pod kątem zmian lub aktualizacji, uznaje się nie tylko za niewystarczające, ale również za nierzetelne w kontekście art. 5 ust. 1 lit. a). Dalsze wskazówki dotyczące terminów powiadamiania o zmianach osób, których dane dotyczą, zostały zamieszczone poniżej w pkt 30–31.

*Terminy powiadamiania o zmianach w informacjach, o których mowa w art. 13 i 14*

30. W RODO nie poruszono kwestii wymogów czasowych (ani metod), które mają zastosowanie do powiadamiania o zmianach w informacjach, których wcześniej udzielono osobie, której dane dotyczą, na podstawie art. 13 lub 14 (z wyjątkiem zamierzonego dalszego celu przetwarzania – w takim przypadku informacji na temat takiego dalszego celu należy udzielić przed rozpoczęciem dalszego przetwarzania, co wynika z art. 13 ust. 3 i art. 14 ust. 4 – zob. pkt 45 poniżej). Jak jednak wspomniano powyżej

w kontekście terminów podawania informacji określonych w art. 14, administrator danych również w tym wypadku musi przestrzegać zasad rzetelności i rozliczalności w zakresie wszelkich rozsądnych oczekiwań osoby, której dane dotyczą, lub potencjalnego wpływu tych zmian na osobę, której dane dotyczą. Jeżeli zmiana w informacjach wskazuje na istotną zmianę charakteru przetwarzania (np. rozszerzenie kategorii odbiorców lub rozpoczęcie przekazywanie danych do państw trzecich) lub zmianę, która nie musi być istotna w kontekście operacji przetwarzania, ale może mieć znaczenie dla osoby, której dane dotyczą, i wpływać na nią, wówczas takie informacje należy udostępnić osobie, której dane dotyczą, z dużym wyprzedzeniem w stosunku do wejścia zmiany w życie, a metoda zastosowana do zawiadomienia o tych zmianach osoby, której dane dotyczą, powinna zapewniać jasność i skuteczność. Celem powyższego jest zapewnienie, by osoba, której dane dotyczą, nie „przegapiła" zmiany i by zapewnić jej rozsądny czas na (a) rozważenie charakteru i wpływu zmiany i (b) wykonanie swoich praw na mocy RODO w związku ze zmianą (np. wycofanie zgody lub wniesienie sprzeciwu wobec przetwarzania).

31. Administratorzy danych powinni ostrożnie rozważyć okoliczności i kontekst każdej sytuacji, w której konieczna jest aktualizacja informacji dotyczących przejrzystości, w tym potencjalny wpływ zmian na osobę, której dane dotyczą, i sposób wykorzystany do powiadomienia o zmianach, oraz powinni być w stanie wykazać, w jaki sposób odstęp czasowy między powiadomieniem o zmianach a wejściem zmian w życie spełnia zasadę rzetelności względem osoby, której dane dotyczą. Ponadto GR29 jest zdania, że powiadamiając o takich zmianach osoby, których dane dotyczą, administrator danych powinien również wyjaśnić – zgodnie z zasadą rzetelności – jaki będzie prawdopodobny wpływ tych zmian na osoby, których dane dotyczą. Spełnienie wymogów przejrzystości nie może jednak kamuflować sytuacji, w której zmiany w przetwarzaniu są tak istotne, że charakter przetwarzania zmienia się całkowicie względem stanu poprzedniego. GR29 podkreśla, że wszystkie pozostałe zasady określone w RODO, w tym te związane z niewłaściwym dalszym przetwarzaniem, mają w dalszym ciągu zastosowanie, bez względu na konieczność wypełnienia obowiązków zapewnienia przejrzystości.

32. Ponadto nawet jeżeli informacje dotyczące przejrzystości (np. zawarte w oświadczeniu o ochronie prywatności / informacji o polityce prywatności) nie zmienią się w istotnym stopniu, istnieje prawdopodobieństwo, że osoby, których dane dotyczą i które korzystały z danej usług przez dłuższy czas, nie będą pamiętać, jakich informacji im udzielono na początku na podstawie art. 13 lub 14. GR29 zaleca, by administratorzy ułatwili osobom, których dane dotyczą, dalszy łatwy dostęp do informacji, aby mogły one ponownie się zapoznać z zakresem przetwarzania danych. Zgodnie z zasadą rozliczalności administratorzy powinni również rozważyć, czy i w jakich odstępach czasu powinni przesyłać osobom, których dane dotyczą, przypomnienia o istnieniu oświadczenia o ochronie prywatności / informacji o polityce prywatności i o miejscu, w którym mogą je znaleźć.

*Tryb i format udzielania informacji*

33. Zarówno w art. 13, jak i w art. 14 przewidziano obowiązek, zgodnie z którym administrator danych „podaje jej [osobie, której dane dotyczą] wszystkie następujące informacje (…)". Słowo „podaje" ma tutaj kluczowe znaczenie. Oznacza ono, że

administrator danych musi czynnie podjąć działania w celu udzielenia osobie, której dane dotyczą, przedmiotowych informacji lub czynnie skierować ją do miejsca, w którym znajdują się te informacje (np. podając bezpośredni link, zachęcając do skorzystania z kodu QR itd.). Osoba, której dane dotyczą, nie powinna być zmuszona do czynnego szukania informacji, o których mowa we wspomnianych artykułach, wśród innych informacji, takich jak regulamin korzystania ze strony internetowej lub z aplikacji. Kwestię tę zilustrowano przykładem w pkt 11. Jak wskazano w pkt 17 powyżej, GR29 zaleca, by wszystkie informacje skierowane do osoby, której dane dotyczą, były dla niej również dostępne w jednym miejscu lub w ramach jednego dokumentu (np. elektronicznego na stronie internetowej lub papierowego), który powinien być łatwo dostępny na wypadek, gdyby osoba ta chciała zapoznać się z całością informacji.

34. W RODO istnieje pewien kontrast między, z jednej strony, wymogami przekazania osobom, których dane dotyczą, wyczerpujących informacji wymaganych na podstawie RODO, a z drugiej strony wymogami przekazania tych informacji w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie. Mając na uwadze fundamentalne zasady rozliczalności i rzetelności, administratorzy muszą samodzielnie przeanalizować charakter, okoliczności, zakres i kontekst prowadzonego przez nich przetwarzania danych osobowych oraz postanowić – w ramach wymogów prawnych ustanowionych w RODO i po uwzględnieniu zaleceń wskazanych w niniejszych wytycznych, w szczególności w pkt 36 poniżej – które z wymaganych informacji potraktować priorytetowo oraz jakie są właściwe poziomy szczegółowości i metody przekazywania informacji.

*Warstwowe podejście w otoczeniu cyfrowym i warstwowe oświadczenia o ochronie prywatności / warstwowe informacje o polityce prywatności*

35. W kontekście cyfrowym, biorąc pod uwagę ilość informacji, których należy udzielić osobie, której dane dotyczą, administratorzy danych mogą przyjąć warstwowe podejście, jeżeli chcą połączyć różne metody w celu zapewnienia przejrzystości. GR29 zaleca w szczególności, aby korzystano z warstwowych oświadczeń o ochronie prywatności / warstwowych informacji o polityce prywatności w celu odsyłania do różnych kategorii informacji, które należy podać osobie, której dane dotyczą, zamiast wyświetlać na ekranie wszystkie te informacje w formie ciągłego tekstu. Dzięki temu można uniknąć przeładowania informacyjnego. Warstwowe oświadczenia o ochronie prywatności / warstwowe informacje o polityce prywatności mogą pomóc zrównoważyć kwestie kompletności i zrozumienia, w szczególności dzięki umożliwieniu użytkownikom bezpośredniego przejścia do tej sekcji oświadczenia/informacji, którą chcą przeczytać. Należy podkreślić, że warstwowe oświadczenia o ochronie prywatności / warstwowe informacje o polityce prywatności nie są zwykłymi podstronami, które wymagają kilku kliknięć, aby dotrzeć do danej informacji. Struktura i wygląd pierwszej warstwy oświadczenia o ochronie prywatności / informacji o polityce prywatności powinny dawać osobie, której dane dotyczą, jasny obraz, jakie informacje są dostępne na temat przetwarzania jej danych osobowych, oraz gdzie i w jaki sposób może znaleźć te szczegółowe informacje w warstwach oświadczenia o ochronie prywatności / informacji o polityce prywatności. Ważne jest również, aby informacje zawarte w poszczególnych warstwach informacji były ze sobą spójne i by nie znajdowały się tam sprzeczne informacje.

36. Jeżeli chodzi o treści podawane w ramach pierwszego sposobu, z którego korzysta administrator w celu przekazania informacji osobom, których dane dotyczą, w ramach warstwowego podejścia (innymi słowy – głównego sposobu, w który administrator po raz pierwszy wchodzi w interakcję z osobą, której dane dotyczą) lub treści zawarte w pierwszej warstwie oświadczenia o ochronie prywatności / informacji o polityce prywatności, GR29 zaleca, by ta pierwsza warstwa lub pierwszy sposób obejmowały szczegółowe informacje na temat celów przetwarzania, tożsamości administratora i opisu praw osoby, której dane dotyczą. (Ponadto na te informacje należy bezpośrednio zwrócić uwagę osoby, której dane dotyczą, w momencie pozyskiwania danych osobowych, np. wyświetlać je w momencie, kiedy osoba, której dane dotyczą, wypełnia formularz online.) Znaczenie podawania tych informacji z góry jest szczególnie podkreślone w motywie 39[34]. Chociaż administratorzy muszą być w stanie wykazać rozliczalność co do tego, jakie dalsze informacje postanowili traktować priorytetowo, GR29 uważa, że – zgodnie z zasadą rzetelności – obok informacji wskazanych powyżej w niniejszym punkcie, pierwsza warstwa / pierwszy sposób powinien również zawierać informacje na temat przetwarzania, które ma największy wpływ na osobę, której dane dotyczą, oraz przetwarzania, które może zaskoczyć taką osobę. W związku z tym osoba, której dane dotyczą, powinna być w stanie zrozumieć na podstawie informacji zawartych w pierwszej warstwie / pierwszym sposobie, jakie konsekwencje pociągnie za sobą dla niej to przetwarzanie (zob. również powyżej pkt 10).

37. W kontekście cyfrowym poza zapewnieniem warstwowego internetowego oświadczenia o ochronie prywatności / warstwowej informacji o polityce prywatności administrator danych może również postanowić, że zastosuje *dodatkowe* narzędzia do celów zapewnienia przejrzystości (zob. dalsze przykłady przeanalizowane poniżej), które komunikują poszczególnym osobom, których dane dotyczą, informacje specjalnie dostosowane do ich sytuacji oraz do towarów/usług, z których korzystają. Należy jednak podkreślić, że chociaż GR29 zaleca stosowanie warstwowych internetowych oświadczeń o ochronie prywatności /warstwowych informacji o polityce prywatności, niniejsze zalecenie nie wyklucza możliwości opracowania i stosowania innych innowacyjnych metod zapewniających przestrzeganie wymogów w zakresie przejrzystości.

*Warstwowe podejście w otoczeniu innym niż cyfrowe*

38. Warstwowe podejście do udzielania informacji dotyczących przejrzystości osobom, których dane dotyczą, można zastosować również w kontekście innym niż internetowy/cyfrowy (np. w kontaktach osobistych lub w rozmowie telefonicznej), gdzie administratorzy danych mogą zastosować różne sposoby w celu ułatwienia podawania informacji. (Zob. również pkt 33–37 i 39–40 w odniesieniu do różnych sposobów podawania informacji.) Nie należy mylić tego pojęcia z odrębną kwestią warstwowych oświadczeń o ochronie prywatności / warstwowych informacji o polityce prywatności. Niezależnie od formatów stosowanych w takim warstwowym podejściu GR29 zaleca, by

[34] W odniesieniu do zasady przejrzystości motyw 39 stanowi, że „zasada ta dotyczy w szczególności informowania osób, których dane dotyczą, o tożsamości administratora i celach przetwarzania danych 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".

w pierwszej „warstwie” (innymi słowy – w ramach głównego sposobu, w który administrator po raz pierwszy wchodzi w interakcję z osobą, której dane dotyczą) przekazywano zasadniczo najważniejsze informacje (wskazane w pkt 36 powyżej), tj. szczegółowe informacje na temat celów przetwarzania, tożsamość administratora i wskazanie istniejących praw osoby, której dane dotyczą, a także informacje na temat najważniejszych skutków przetwarzania lub na temat przetwarzania, które może zaskoczyć osobę, której dane dotyczą. Na przykład, jeżeli pierwszy kontakt z osobą, której dane dotyczą, ma miejsce drogą telefoniczną, informacje te mogłyby zostać przekazane podczas rozmowy telefonicznej, a pozostałe informacje wymagane na podstawie art. 13 i 14 mogłyby zostać jej przekazane za pośrednictwem innych, dodatkowych środków, takich jak przesłanie kopii polityki ochrony prywatności w wiadomości e-mail lub przesłanie osobie, której dane dotyczą, linku do warstwowego internetowego oświadczenia o ochronie prywatności / warstwowej internetowej informacji o polityce prywatności administratora.

*Powiadomienia typu „push” i „pull”*

39. Innym możliwym sposobem dostarczania informacji dotyczących przejrzystości są powiadomienia typu „push” i „pull”. Powiadomienia typu „push” obejmują wysyłanie powiadomień zawierających informacje dotyczące przejrzystości typu „just-in-time”, natomiast powiadomienia typu „pull” ułatwiają dostęp do informacji za pomocą takich metod, jak zarządzanie pozwoleniem, pulpity nawigacyjne prywatności oraz samouczki „dowiedz się więcej”. Zapewniają one osobie, której dane dotyczą, przekazanie informacji o przejrzystości w sposób bardziej ukierunkowany na użytkownika.

- Pulpit nawigacyjny prywatności jest jednym punktem, z którego osoby, których dane dotyczą, mogą przeglądać informacje na temat ochrony prywatności i zarządzać swoimi preferencjami w zakresie prywatności, zezwalając na określone sposoby wykorzystania danych, które ich dotyczą, przez daną usługę albo uniemożliwiając takie wykorzystanie. Jest to szczególnie przydatne w przypadku korzystania przez osoby, których dane dotyczą, z tej samej usługi na różnych urządzeniach, ponieważ zapewnia im dostęp do swoich danych osobowych i kontrolę nad nimi bez względu na sposób korzystania z usługi. Umożliwienie osobom, których dane dotyczą, ręcznego dostosowania ustawień prywatności za pośrednictwem pulpitu nawigacyjnego prywatności może również ułatwić spersonalizowanie oświadczenia o ochronie prywatności / informacji o polityce prywatności poprzez uwzględnienie jedynie tych rodzajów przetwarzania, które mają miejsce w przypadku danej osoby. Pożądane jest włączenie pulpitu nawigacyjnego prywatności do istniejącej architektury usługi (np. wykorzystując ten sam wzór i tę samą markę, co w przypadku pozostałej części usługi), ponieważ zapewni to intuicyjność dostępu do pulpitu oraz korzystania z niego, a także może zachęcić użytkowników do zainteresowania się informacjami o prywatności na równi z innymi aspektami usługi. Może być to skuteczny sposób wykazania, że informacje na temat ochrony prywatności stanowią konieczną i integralną część usługi, a nie długie wykazy napisane żargonem prawnym.

- Powiadomienie typu „just-in-time" jest wykorzystywane w celu przekazania konkretnych informacji dotyczących prywatności na zasadzie *ad hoc* – w najodpowiedniejszym czasie dla osoby, której dane dotyczą. Metoda ta jest przydatna do przekazywania informacji na różnych etapach procesu pozyskiwania danych; pomaga podzielić przekazywane informacje na krótsze, łatwiejsze do zrozumienia części, dzięki czemu administratorzy danych mogą w mniejszym stopniu korzystać z oświadczenia o ochronie prywatności / informacji o polityce prywatności w formie jednego ciągłego dokumentu, który jest trudny do zrozumienia bez kontekstu. Na przykład, jeżeli osoba, której dane dotyczą, zakupi produkt przez internet, krótkie informacje wyjaśniające można podać w wyskakujących okienkach towarzyszących odpowiednim polom tekstu. Informacje podane obok pola zawierającego prośbę o numer telefonu osoby, której dane dotyczą, mogłyby na przykład zawierać wyjaśnienie, że dane te są zbierane wyłącznie do celów kontaktów w sprawie zakupu oraz że zostaną ujawnione wyłącznie do celów usługi doręczenia.

*Inne rodzaje „odpowiednich środków"*

40. Biorąc pod uwagę bardzo wysoki poziom dostępu do internetu w UE oraz fakt, że osoby, których dane dotyczą, mogą uzyskać dostęp do internetu w dowolnym momencie, z wielu miejsc i z wielu urządzeń, GR29 jest zdania – jak już stwierdzono powyżej – że „odpowiednim środkiem" służącym przekazaniu informacji dotyczących przejrzystości w przypadku administratorów danych, którzy działają w środowisku cyfrowym/online, jest elektroniczne oświadczenie o ochronie prywatności / elektroniczna informacja o polityce prywatności. Ze względu na okoliczności pozyskiwania i przetwarzania danych administrator może jednak stwierdzić konieczność dodatkowego (lub alternatywnego – jeżeli administrator danych nie działa w środowisku cyfrowym/online) stosowania innych sposobów oraz formatów przekazywania informacji. Inne możliwe sposoby przekazywania informacji osobie, której dane dotyczą, związane z następującymi różnymi środowiskami danych osobowych, mogą obejmować następujące sposoby właściwe w określonym, wskazanym poniżej środowisku. Jak zauważono powyżej, administratorzy mogą przyjąć podejście warstwowe, gdy decydują się na zastosowanie kombinacji takich metod, zapewniając jednocześnie, by najważniejsze informacje (zob. pkt 36 i 38) zawsze były przekazywane za pośrednictwem pierwszego sposobu wykorzystywanego do komunikacji z osobą, której dane dotyczą.

a. Forma papierowa np. w przypadku zawierania umów drogą pocztową: wyjaśnienia pisemne, ulotki, informacje w dokumentacji umownej, komiksy, infografiki lub schematy blokowe;
b. Łączność telefoniczna: wyjaśnienia ustne przez człowieka, aby umożliwić interakcję i udzielanie odpowiedzi na pytania, albo zautomatyzowane bądź nagrane wcześniej informacje umożliwiające wybór opcji odsłuchania bardziej szczegółowych informacji;
c. Technologie urządzeń inteligentnych bez ekranu / środowisko internetu rzeczy, takie jak analiza śledzenia Wi-Fi: znaki graficzne, kody QR, ostrzeżenia głosowe, informacje pisemne zawarte w papierowych instrukcjach konfiguracji, filmy wideo zawarte w cyfrowych instrukcjach konfiguracji, informacje pisemne na temat urządzenia inteligentnego, wiadomości wysłane SMS-em lub pocztą elektroniczną,

widoczne tablice zawierające informacje, oznakowanie informacyjne lub publiczne kampanie informacyjne;

d. Kontakty bezpośrednie, takie jak udział w sondażu opinii publicznej, osobista rejestracja w celu skorzystania z usługi: wyjaśnienia ustne lub pisemne przekazane w formie papierowej lub elektronicznej;

e. Środowisko „rzeczywiste", w którym prowadzone są nagrania z użyciem CCTV / bezzałogowych statków powietrznych: widoczne tablice zawierające informacje, oznakowanie informacyjne, publiczne kampanie informacyjne lub ogłoszenia w gazetach / mediach.

*Informacje dotyczące profilowania i zautomatyzowanego podejmowania decyzji*

41. Informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i art. 22 ust. 4, wraz z istotnymi informacjami o zasadach ich podejmowania, a także o znaczących i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą, stanowią część obowiązkowych informacji, które należy przekazać tej osobie zgodnie z art. 13 ust. 2 lit. f) i art. 14 ust. 2 lit. g). GR29 sporządziła wytyczne dotyczące zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania[35], do których należy się odwołać w celu uzyskania dalszych wskazówek na temat sposobu zapewnienia przejrzystości w określonych sytuacjach związanych z profilowaniem. Należy zauważyć, że oprócz szczególnych wymogów w zakresie przejrzystości mających zastosowanie do zautomatyzowanego podejmowania decyzji na podstawie art. 13 ust. 2 lit. f) oraz art. 14 ust. 2 lit. g) zawarte w tych wytycznych uwagi dotyczące znaczenia informowania osób, których dane dotyczą, o konsekwencjach przetwarzania ich danych osobowych, a także określona w nich ogólna zasada, zgodnie z którą nie można zaskakiwać osoby przetwarzaniem jej danych, mają również zastosowanie do profilowania w ujęciu ogólnym (a nie tylko profilowania, o którym mowa w art. 22[36]), jako rodzaju przetwarzania[37].

*Inne kwestie – ryzyko, zasady i zabezpieczenia*

42. Motyw 39 RODO odnosi się również do przekazywania określonych informacji, które nie są wyraźnie objęte zakresem stosowania art. 13 i art. 14 (zob. tekst motywu powyżej w pkt 28). Zawarte w tym motywie odniesienie do uświadamiania osobom, których dane dotyczą, ryzyka, zasad i zabezpieczeń w odniesieniu do przetwarzania danych osobowych jest związane z szeregiem innych kwestii. Obejmują one oceny skutków dla ochrony danych. Jak wskazano w wytycznych GR29 dotyczących ocen skutków dla ochrony danych[38], administratorzy danych mogą rozważyć publikację oceny skutków dla ochrony danych (lub jej części) w ramach zwiększania zaufania do operacji przetwarzania oraz

[35] Wytyczne w sprawie zautomatyzowanego podejmowania decyzji i profilowania do celów rozporządzenia 2016/679, GR 251.

[36] Zasada ta ma zastosowanie do procesu podejmowania decyzji polegającego wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, które wywołuje skutki prawne wobec osoby, której dane dotyczą, lub w podobny sposób istotnie na nią wpływa.

[37] Istotne znaczenie ma w tym kontekście motyw 60, który stanowi: „Ponadto należy poinformować osobę, której dane dotyczą, o fakcie profilowania oraz o konsekwencjach takiego profilowania".

[38] Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679, GR 248 rev.1

wykazania przejrzystości i rozliczalności, chociaż jej publikacja nie jest obowiązkowa. Ponadto przestrzeganie kodeksu postępowania (przewidzianego w art. 40) może mieć na celu wykazanie przejrzystości, ponieważ kodeksy postępowania mogą być sporządzane w celu doprecyzowania stosowania RODO między innymi w odniesieniu do: rzetelnego i przejrzystego przetwarzania; informowania opinii publicznej i osób, których dane dotyczą; informowania i ochrony dzieci.

43. Inną istotną kwestią związaną z przejrzystością jest uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych (zgodnie z wymogami określonymi w art. 25). Zgodnie z tymi zasadami administratorzy danych muszą od samego początku uwzględniać kwestie ochrony danych w swoich operacjach i systemach przetwarzania, a nie traktować ją jako formalność do dopełnienia w ostatniej chwili. Motyw 78 odnosi się do środków wykonawczych administratorów danych, które spełniają wymogi w zakresie ochrony danych w fazie projektowania oraz domyślnej ochrony danych, w tym środków polegających na zapewnieniu przejrzystości w odniesieniu do funkcji i przetwarzania danych osobowych.

44. Niezależnie od tego, zadania współadministratorów również wiążą się z uświadamianiem osobom, których dane dotyczą, ryzyka, zasad i zabezpieczeń. Zgodnie z art. 26 ust. 1 współadministratorzy w przejrzysty sposób określają 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. Zgodnie z art. 26 ust. 2 zasadnicza treść uzgodnień między administratorami danych jest udostępniana osobom, których dane dotyczą. Innymi słowy, osoba, której dane dotyczą, musi mieć całkowitą pewność, do którego administratora danych może się zwrócić, jeżeli zamierza wykonać prawo lub prawa przysługujące jej na podstawie RODO[39].

<u>Informacje związane z dalszym przetwarzaniem</u>

45. Zarówno art. 13, jak i art. 14 zawierają przepis[40] nakładający na administratora danych wymóg poinformowania osoby, której dane dotyczą, jeżeli planuje on dalej przetwarzać jej dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane/pozyskane. W takim przypadku „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 wprowadzają w życie zasadę określoną w art. 5 ust. 1 lit. b), zgodnie z którą dane osobowe są zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach, przy czym dalsze przetwarzanie w sposób *niezgodny* z tymi celami jest zabronione[41]. Część druga art. 5 ust. 1 lit. b) stanowi, że dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych

[39] Zgodnie z art. 26 ust. 3 niezależnie od dokonanych przez współadministratorów uzgodnień, o których mowa w art. 26 ust. 1, osoba, której dane dotyczą, może wykonywać przysługujące jej prawa wynikające z RODO wobec każdego ze współadministratorów.

[40] Art. 13 ust. 3 i art. 14 ust. 4 mają identyczne brzmienie, z wyjątkiem słowa „zebrane", którego użyto w art. 13 i który zastąpiono słowem „pozyskane" w art. 14.

[41] W odniesieniu do tej zasady zob. np. motywy 47, 50, 61, 156 i 158; art. 6 ust. 4 i art. 89.

lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami. W przypadku dalszego przetwarzania danych osobowych do celów *zgodnych* z pierwotnymi celami (art. 6 ust. 4 zawiera informacje dotyczące tej kwestii[42]) zastosowanie mają art. 13 ust. 3 i art. 14 ust. 4. Zawarty w powyższych artykułach wymóg informowania osób, których dane dotyczą, o dalszym przetwarzaniu propaguje określone w RODO stanowisko, zgodnie z którym w czasie i w kontekście, w którym zbierane są dane osobowe, osoba, której dane dotyczą, powinna mieć rozsądne przesłanki, by spodziewać się, że może nastąpić przetwarzanie danych w tym celu[43]. Innymi słowy, osoba, której dane dotyczą, nie powinna być zaskoczona celem przetwarzania jej danych osobowych.

46. Art. 13 ust. 3 i art. 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 interpretować jako pozostawiające administratorowi danych pewien stopień swobody wyboru co do zakresu i konkretnych kategorii informacji określonych w odpowiednim ust. 2 (tj., w zależności od przypadku, art. 13 ust. 2 albo art. 14 ust. 2), których należy udzielić osobie, której dane dotyczą. (W motywie 61 określono je mianem „innych niezbędnych informacji".) Zasadnicze stanowisko jest jednak takie, że osobie, której dane dotyczą, należy udzielić wszystkich tego rodzaju informacji określonych w tym ustępie, chyba że przynajmniej jedna kategoria informacji nie istnieje lub nie ma zastosowania.

47. GR29 zaleca, aby w celu zapewnienia przejrzystości, rzetelności i rozliczalności administratorzy rozważyli udostępnienie osobom, których dane dotyczą, w oświadczeniu o ochronie prywatności / informacji o polityce prywatności informacji o analizie zgodności przeprowadzanej zgodnie z art. 6 ust. 4[44], jeżeli nowy cel przetwarzania opiera się na podstawie prawnej innej niż zgoda lub prawo krajowe / unijne. (Innymi słowy, wyjaśnienie, w jaki sposób przetwarzanie w innym celu (w innych celach) jest zgodne z pierwotnym celem). Celem jest zapewnienie osobom, których dane dotyczą, możliwości rozważenia zgodności dalszego przetwarzania i udzielonych zabezpieczeń, a także podjęcia decyzji o ewentualnym wykonaniu przysługujących im praw, tj. m.in. prawa do ograniczenia przetwarzania lub prawa do wniesienia sprzeciwu wobec przetwarzania[45]. Jeżeli administratorzy postanowią nie włączać takich informacji do informacji o polityce prywatności / oświadczenia o ochronie prywatności, GR29 zaleca, by wyjaśnili osobom, których dane dotyczą, że mogą otrzymać te informacje na wniosek.

48. Z wykonywaniem przez osobę, której dane dotyczą, przysługujących jej praw wiąże się kwestia czasu. Jak podkreślono powyżej, przekazanie informacji w odpowiednim czasie jest kluczowym elementem wymogów dotyczących przejrzystości określonych w art. 13

---

[42] Art. 6 ust. 4 zawiera katalog otwarty czynników, które należy uwzględnić, aby ustalić, czy przetwarzanie w innym celu jest zgodne z celem, w którym dane osobowe zostały pierwotnie zebrane, tj.: związek między celami; kontekst, w którym zebrano dane osobowe; charakter danych osobowych (w szczególności czy przetwarzane są szczególne kategorie danych osobowych lub dane osobowe dotyczące naruszeń prawa i wyroków skazujących); ewentualne konsekwencje zamierzonego dalszego przetwarzania dla osób, których dane dotyczą; istnienie odpowiednich zabezpieczeń.

[43] Motywy 47 i 50.

[44] Mowa o tym również w motywie 50.

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

i 14 i jest nieodłącznie związane z koncepcją rzetelnego przetwarzania. Informacje dotyczące *dalszego przetwarzania* należy przekazać „przed takim dalszym przetwarzaniem". GR29 stoi na stanowisku, że należy zapewnić rozsądny okres pomiędzy powiadomieniem a rozpoczęciem przetwarzania, a nie rozpoczynać przetwarzanie bezzwłocznie po otrzymaniu powiadomienia przez osobę, której dane dotyczą. Przynosi to osobom, których dane dotyczą, praktyczne korzyści wynikające z zasady przejrzystości, dając im faktyczną możliwość rozważenia dalszego przetwarzania (i ewentualnego wykonania związanych z tym praw). Pojęcie „rozsądny termin" zależy od danej sytuacji. Zgodnie z zasadą rzetelności im bardziej inwazyjne (lub im mniej spodziewane) jest dalsze przetwarzanie, tym okres ten powinien być dłuższy. Zgodnie z zasadą rozliczalności administratorzy danych powinni być też w stanie wykazać, w jaki sposób okoliczności uzasadniają ustalenia dokonane przez nich w odniesieniu do czasu przekazania tych informacji oraz dlaczego taki termin jest rzetelny wobec osób, których dane dotyczą. (Zob. również uwagi dotyczące ustalania rozsądnych terminów powyżej w pkt 30–32.)

Narzędzia wizualizacyjne

49. Co istotne, zasada przejrzystości określona w RODO nie ogranicza się jedynie do komunikacji językowej (pisemnej czy ustnej). W RODO przewidziano w stosownych przypadkach narzędzia wizualizacyjne (w szczególności odniesienia, znaki graficzne, mechanizmy certyfikacji oraz znaki jakości i oznaczenia w dziedzinie ochrony danych). W motywie 58[46] wskazano, że dostępność informacji kierowanych do ogółu społeczeństwa lub osób, których dane dotyczą, ma szczególne znaczenie w środowisku online[47].

*Znaki graficzne*

50. W motywie 60 przewidziano przekazywanie informacji osobie, której dane dotyczą, „w połączeniu" ze standardowymi znakami graficznymi, umożliwiając tym samym warstwowe podejście. Wykorzystywanie znaków graficznych nie powinno jednak po prostu zastępować informacji koniecznych do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw ani nie należy traktować tego rodzaju znaków jako elementu zastępującego konieczność wykonywania przez administratora danych obowiązków nałożonych na niego na podstawie art. 13 i 14. W art. 12 ust. 7 przewidziano wykorzystywanie takich znaków graficznych, stwierdzając, 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".

[46] „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".

[47] W tym kontekście administratorzy powinni uwzględniać słabowidzące osoby, których dane dotyczą (np. cierpiące na daltonizm).

51. Ponieważ art. 12 ust. 7 stanowi, że „jeżeli znaki te są przedstawione elektronicznie, muszą się nadawać do odczytu maszynowego", sugeruje to, iż mogą wystąpić sytuacje, w których znaki graficzne nie są przedstawiane elektronicznie[48], na przykład znaki graficzne na dokumentach w formie papierowej, urządzeniach połączonych za pośrednictwem internetu lub opakowaniach takich urządzeń, powiadomieniach w miejscach publicznych dotyczących śledzenia Wi-Fi, kodach QR oraz powiadomieniach dotyczących CCTV.

52. Celem stosowania znaków graficznych jest najwyraźniej zwiększenie przejrzystości dla osób, których dane dotyczą, dzięki potencjalnemu ograniczeniu potrzeby przekazywania osobie, której dane dotyczą, ogromnych ilości informacji pisemnych. Użyteczność znaków graficznych w celu skutecznego przekazywania osobom, których dane dotyczą, informacji wymaganych zgodnie z art. 13 i 14 zależy jednak od standaryzacji symboli/rysunków, które mają być powszechnie wykorzystywane i uznawane w całej UE jako skrótowe przedstawienie tych informacji. W tym względzie w RODO nałożono odpowiedzialność za sporządzenie kodu znaków graficznych na Komisję, ale ostatecznie opinię na temat takich znaków graficznych może przedstawić Komisji, na wniosek Komisji albo z urzędu, Europejska Rada Ochrony Danych[49].GR29 przyznaje, że zgodnie z motywem 166 opracowanie kodu znaków graficznych powinno się opierać na podejściu opartym na dowodach, a zanim nastąpi jakakolwiek standaryzacja konieczne będzie przeprowadzenie, we współpracy z sektorem i ogółem społeczeństwa, szeroko zakrojonych badań dotyczących skuteczności znaków graficznych w tym kontekście.

*Mechanizmy certyfikacji, znaki jakości i oznaczenia*

53. Oprócz wykorzystywania standardowych znaków graficznych RODO (art. 42) odnosi się również do wykorzystywania mechanizmów certyfikacji oraz znaków jakości i oznaczeń w zakresie ochrony danych osobowych mających świadczyć o tym, że operacje przetwarzania prowadzone przez administratorów danych i podmioty przetwarzające są

[48] RODO nie zawiera definicji pojęcia „nadający się do odczytu maszynowego", jednak w motywie 21 dyrektywy 2013/37/UE17 zdefiniowano pojęcie „przeznaczony do odczytu komputerowego" jako:

„format pliku zorganizowany w sposób umożliwiający aplikacjom komputerowym łatwe identyfikowanie, rozpoznawanie i pozyskiwanie z niego określonych danych. 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".

[49] Art. 12 ust. 8 stanowi, że Komisji przysługuje prawo przyjmowania aktów delegowanych zgodnie z art. 92 w celu określenia informacji przedstawianych za pomocą znaków graficznych i informacji dotyczących ustanowienia standardowych znaków graficznych. W motywie 166 (dotyczącym aktów delegowanych Komisji w ujęciu ogólnym), który ma charakter pouczenia, stwierdzono, że w czasie prac przygotowawczych Komisja musi prowadzić stosowne konsultacje, w tym na szczeblu eksperckim. Jednak Europejska Rada Ochrony Danych ma również do odegrania istotną rolę konsultacyjną w odniesieniu do standaryzacji znaków graficznych, ponieważ art. 70 ust. 1 lit. r) stanowi, że Europejska Rada Ochrony Danych – z urzędu lub w stosownych przypadkach na wniosek Komisji – udziela Komisji opinii w sprawie znaków graficznych.

zgodne z RODO oraz mają na celu zwiększenie przejrzystości dla osób, których dane dotyczą[50]. GR29 wyda wytyczne dotyczące mechanizmów certyfikacji w stosownym czasie.

Wykonywanie uprawnień przysługujących osobom, których dane dotyczą

54. W świetle RODO wymóg przejrzystości oznacza dla administratorów danych potrójny obowiązek, jeżeli chodzi o prawa osób, których dane dotyczą, ponieważ są oni zobowiązani do[51]:

- udzielania osobom, których dane dotyczą, informacji dotyczących przysługujących im praw[52] (zgodnie z art. 13 ust. 2 lit. b) oraz art. 14 ust. 2 lit. c));
- przestrzegania zasady przejrzystości (tj. odnoszącej się do jakości komunikacji przewidzianej w art. 12 ust. 1) podczas komunikowania się z osobami, których dane dotyczą, w zakresie ich praw określonych w art. 15–22 i art. 34; oraz
- ułatwiania osobom, których dane dotyczą, wykonywania praw przysługujących im na mocy art. 15–22.

55. Określone w RODO wymogi dotyczące wykonywania tych praw oraz charakter wymaganych informacji mają na celu zapewnienie osobom, których dane dotyczą, *realnej możliwości* dochodzenia swoich praw i pociągnięcia administratorów danych do odpowiedzialności za przetwarzanie ich danych osobowych. W motywie 59 podkreślono, 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". Sposób, w jaki administrator danych zapewnia osobom, których dane dotyczą, możliwość wykonania przysługujących im praw, powinien być odpowiedni do kontekstu i charakteru stosunków oraz interakcji między administratorem a osobą, której dane dotyczą. W tym celu administrator danych może zdecydować się zapewnić inną metodę wykonania praw lub większą liczbę takich innych metod, aby uwzględnić szczególne sposoby interakcji osób, których dane dotyczą, z administratorami danych.

**Przykład**

Podmiot świadczący usługi zdrowotne udostępnia formularz elektroniczny na swojej stronie internetowej oraz formularze w formie papierowej w recepcjach przychodni, aby ułatwić składanie wniosków o udostępnienie danych osobowych zarówno online, jak i osobiście. Obok tych metod placówka zdrowotna przyjmuje wnioski o udostępnienie danych składane inną drogą (na przykład listownie lub e-mailem) oraz zapewnia dedykowany punkt kontaktowy (do którego można uzyskać dostęp drogą e-mailową lub telefonicznie), aby pomóc osobom, których dane

[50] Zob. odniesienie w motywie 100.

[51] Na podstawie sekcji RODO dotyczącej przejrzystości i trybu korzystania z praw przez osobę, której dane dotyczą (rozdział III sekcja 1 art. 12)

[52] Praw dostępu do danych, ich sprostowania lub usunięcia, ograniczenia przetwarzania, sprzeciwu wobec przetwarzania, przenoszenia danych.

dotyczą, w wykonywaniu przysługujących im praw.

## Wyjątki od obowiązku udzielenia informacji

*Wyjątki określone w art. 13*

56. Jedyny wyjątek od ciążących na administratorze danych obowiązków określonych w art. 13 – jeżeli zebrał on dane osobowe bezpośrednio od osoby, której dane dotyczą – występuje, „gdy – i w zakresie, w jakim – osoba, której dane dotyczą, dysponuje już tymi informacjami”[53]. Zgodnie z zasadą rozliczalności administratorzy danych muszą wykazać (i udokumentować), jakie informacje posiada już osoba, której dane dotyczą, w jaki sposób i kiedy je otrzymała oraz że od tego czasu nie nastąpiły żadne zmiany w tych informacjach, które spowodowałyby ich dezaktualizację. Ponadto zastosowanie w art. 13 ust. 4 wyrażenia „w zakresie, w jakim” wyjaśnia, że nawet jeżeli osobie, której dane dotyczą, przekazano już pewne kategorie informacji z wykazu informacji zawartego w art. 13, na administratorze danych wciąż spoczywa obowiązek uzupełnienia tych informacji w celu zapewnienia, by osoba, której dane dotyczą, posiadała kompletny zestaw informacji wymienionych w art. 13 ust. 1 i art. 13 ust. 2. Następujący przykład to najlepsza praktyka dotycząca preferowanej wykładni zawężającej wyjątku określonego w art. 13 ust. 4.

**Przykład**

Osoba fizyczna rejestruje się w celu korzystania z internetowej usługi poczty elektronicznej, otrzymując wszystkie informacje wymagane zgodnie z art. 13 ust. 1 i art. 13 ust. 2 w chwili rejestracji. Sześć miesięcy później osoba, której dane dotyczą, aktywuje połączoną funkcję wiadomości błyskawicznej za pośrednictwem dostawcy usług poczty elektronicznej i podaje w tym celu swój numer telefonu komórkowego. Usługodawca przekazuje osobie, której dane dotyczą, niektóre informacje określone w art. 13 ust. 1 i art. 13 ust. 2 dotyczące przetwarzania numeru telefonu (np. dotyczące celów i podstawy prawnej przetwarzania, odbiorców, okresu zatrzymywania), ale nie przekazuje innych informacji, które osoba ta posiada już od 6 miesięcy i które się nie zmieniły (np. tożsamości i danych kontaktowych administratora oraz inspektora ochrony danych, informacji dotyczących praw osoby, której dane dotyczą, oraz prawa do wniesienia skargi do właściwego organu nadzorczego). Zgodnie z najlepszą praktyką osoba, której dane dotyczą, powinna jednak ponownie otrzymać pełen zestaw informacji, ale powinna być również w stanie z łatwością stwierdzić, które z podanych informacji są nowe. Nowe przetwarzanie do celów usługi wiadomości błyskawicznej może wpłynąć na osobę, której dane dotyczą, w sposób skłaniający ją do wykonania przysługującego jej

[53] Art. 13 ust. 4.

prawa, o którym mogła zapomnieć z uwagi na fakt, że poinformowano ją o nim sześć miesięcy wcześniej. Ponowne udzielenie wszystkich informacji pozwala zapewnić, by osoba, której dane dotyczą, w dalszym ciągu była dobrze poinformowana, w jaki sposób wykorzystywane są jej dane i jak może korzystać ze swoich praw.

*Wyjątki określone w art. 14*

57. W art. 14 ustanowiono znacznie szerszy katalog wyjątków od ciążącego na administratorze danych obowiązku udzielenia informacji, jeżeli danych osobowych nie pozyskano od osoby, której dane dotyczą. Co do zasady należy dokonywać wykładni tych wyjątków oraz stosować je w sposób zawężający. Oprócz sytuacji, w której osoba, której dane dotyczą, posiada już przedmiotowe informacje (art. 14 ust. 5 lit. a)), w art. 14 ust. 5 dopuszczono również następujące wyjątki:

- udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku; w szczególności w przypadku przetwarzania do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych lub o ile obowiązek ten mógłby uniemożliwić lub poważnie utrudnić realizację celów takiego przetwarzania;
- administrator danych podlega określonemu w prawie krajowym lub prawie Unii wymogowi pozyskania lub ujawnienia danych osobowych, przy czym w prawie tym przewidziano odpowiednią ochronę uzasadnionych interesów osoby, której dane dotyczą; lub
- 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.

*Okazuje się niemożliwe, niewspółmiernie duży wysiłek oraz poważne utrudnienie realizacji celów*

58. W art. 14 ust. 5 lit. b) przewidziano 3 odrębne sytuacje, w których uchylony zostaje obowiązek udzielenia informacji określony w art. 14 ust. 1, art. 14 ust. 2 i art. 14 ust. 4:

(i) jeżeli okazuje się to niemożliwe (w szczególności do celów archiwalnych, do celów badań naukowych/historycznych lub do celów statystycznych);
(ii) jeżeli wymagałoby niewspółmiernie dużego wysiłku (w szczególności do celów archiwalnych, do celów badań naukowych/historycznych lub do celów statystycznych); lub
(iii) jeżeli udzielenie informacji wymaganych zgodnie z art. 14 ust. 1 mogłoby uniemożliwić lub poważnie utrudnić realizację celów takiego przetwarzania.

„Okazuje się niemożliwe”

59. Sytuacja, w której zgodnie z art. 14 ust. 5 lit. b) udzielenie informacji „okazuje się niemożliwe”, jest sytuacją zero-jedynkową, ponieważ dana sytuacja albo jest niemożliwa, albo jest możliwa; nie istnieją stopnie „niemożliwości”. Jeżeli administrator danych zamierza powołać się na to odstępstwo, musi wskazać czynniki, które faktycznie

*uniemożliwiają mu* udzielenie odnośnych informacji osobom, których dane dotyczą. Jeżeli po upływie określonego czasu czynniki, które spowodowały „niemożliwość", przestaną istnieć i administrator danych uzyska możliwość udzielenia informacji osobom, których dane dotyczą, powinien bezzwłocznie to uczynić. W praktyce istnieje bardzo niewiele sytuacji, w których administrator danych może wykazać faktyczną niemożliwość udzielenia informacji osobom, których dane dotyczą. Kwestię tę ilustruje następujący przykład.

**Przykład**

Osoba, której dane dotyczą, rejestruje się w celu korzystania z usługi subskrypcji online na zasadzie abonamentowej. Po rejestracji administrator danych zbiera od biura informacji kredytowej dane dotyczące wiarygodności kredytowej osoby, której dane dotyczą, aby podjąć decyzję, czy ma świadczyć usługę. Protokół administratora danych ma na celu poinformowanie osób, których dane dotyczą, o zebraniu danych dotyczących wiarygodności kredytowej w terminie trzech dni od dnia ich zebrania – zgodnie z art. 14 ust. 3 lit. a). Adres i numer telefonu osoby, której dane dotyczą, nie figurują jednak w rejestrach publicznych (osoba, której dane dotyczą, mieszka za granicą). Podczas rejestracji w celu korzystania z usługi osoba, której dane dotyczą, nie podała swojego adresu e-mail lub adres ten jest nieprawidłowy. Administrator stwierdza, że nie ma możliwości bezpośredniego skontaktowania się z osobą, której dane dotyczą. W tym przypadku administrator może jednak udzielić informacji o zbieraniu danych dotyczących kredytów na swojej stronie internetowej przed rejestracją. W tym przypadku udzielenie informacji zgodnie z art. 14 nie byłoby niemożliwe.

*Niemożność podania źródła danych*

60. W motywie 61 stwierdzono, że „jeżeli osobie, której dane dotyczą, nie można podać pochodzenia danych osobowych, ponieważ korzystano z różnych źródeł, informacje należy przedstawić w sposób ogólny". Uchylenie wymogu udzielenia osobom, których dane dotyczą, informacji dotyczących źródła ich danych osobowych ma zastosowanie wyłącznie wówczas, gdy nie jest to możliwe, ponieważ nie można przypisać różnych danych osobowych dotyczących tej samej osoby, której dane dotyczą, do konkretnego źródła. Przykładowo sam fakt, że baza danych obejmująca dane osobowe wielu osób została skompilowana przez administratora z wykorzystaniem więcej niż jednego źródła, nie wystarcza, by uchylić ten wymóg, jeżeli można (chociaż jest to czasochłonne lub uciążliwe) określić źródło, z którego pochodzą dane osobowe poszczególnych osób. Biorąc pod uwagę wymogi dotyczące uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych[54], systemy przetwarzania powinny być od początku wyposażone w mechanizmy przejrzystości, tak by wszystkie źródła danych osobowych otrzymywanych przez organizację można było monitorować, a także prześledzić ich historię aż do źródła na każdym etapie przetwarzania danych (zob. pkt 43 powyżej).

[54] Art. 25

„Niewspółmiernie duży wysiłek”

61. Zgodnie z art. 14 ust. 5 lit. b), podobnie jak w sytuacji, w której przetwarzanie „okazuje się niemożliwe”, może również mieć zastosowanie „niewspółmiernie duży wysiłek”, zwłaszcza w przypadku przetwarzania „do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem warunków i zabezpieczeń, o których mowa w art. 89 ust. 1”. W motywie 62 odniesiono się również do tych celów jako do przypadków, w których udzielenie informacji osobie, której dane dotyczą, wymagałoby niewspółmiernie dużego wysiłku, przy czym stwierdzono w nim, że uwzględnić przy tym należy liczbę osób, których dane dotyczą, okres przechowywania danych oraz wszelkie przyjęte odpowiednie zabezpieczenia. Biorąc pod uwagę nacisk, jaki położono w motywie 62 i w art. 14 ust. 5 lit. b) na cele archiwalne, cele badań naukowych i cele statystyczne w odniesieniu do stosowania tego odstępstwa, GR29 stoi na stanowisku, że wyjątek ten nie powinien być *rutynowo* stosowany przez administratorów danych, którzy nie przetwarzają danych osobowych do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych. GR29 podkreśla, że w przypadkach gdy są to zamierzone cele, należy wciąż spełnić warunki określone w art. 89 ust. 1 i udzielenie informacji musi wiązać się z niewspółmiernie dużym wysiłkiem.

62. Przy określaniu, co może stanowić niemożliwość albo niewspółmiernie duży wysiłek zgodnie z art. 14 ust. 5 lit. b), istotne jest, że nie istnieją porównywalne wyłączenia na podstawie art. 13 (gdy dane osobowe są zbierane od osoby, której dane dotyczą). Jedyną różnicą między sytuacją określoną w art. 13 a sytuacją określoną w art. 14 jest fakt, że w tym ostatnim przypadku dane osobowe nie są zbierane od osoby, której dane dotyczą. Wynika z tego zatem, że niemożliwość lub niewspółmiernie duży wysiłek wynikają co do zasady z okoliczności, które nie występują, jeżeli dane osobowe są zbierane od osoby, której dane dotyczą. Innymi słowy, niemożliwość lub niewspółmiernie duży wysiłek muszą bezpośrednio wynikać z faktu, że dane osobowe zebrano w inny sposób niż od osoby, której dane dotyczą.

**Przykład**

Duży szpital metropolitalny wymaga od wszystkich pacjentów z oddziału dziennego, przyjętych na dłuższy okres i zgłaszających się na wizytę wypełnienia formularza informacji o pacjencie, w którym należy podać dane dwóch osób bliskich (osób, których dane dotyczą). Biorąc pod uwagę bardzo dużą liczbę pacjentów korzystających codziennie z usług szpitala, niewspółmiernie dużego wysiłku ze strony szpitala wymagałoby udzielenie wszystkim osobom, które zostały wymienione jako „osoby bliskie" na formularzach wypełnianych każdego dnia przez pacjentów, informacji wymaganych zgodnie z art. 14.

63. Czynniki, o których mowa powyżej w motywie 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 zgodnie z art. 14.

**Przykład**

Naukowcy zajmujący się badaniami historycznymi, którzy chcą prześledzić pochodzenie na podstawie nazwisk, pośrednio uzyskują obszerny zbiór danych dotyczących 20 000 osób. Dane należące do zbioru zostały jednak zebrane 50 lat temu i nie były od tego czasu aktualizowane oraz nie zawierają żadnych danych kontaktowych. Biorąc pod uwagę wielkość bazy danych, a w szczególności okres przechowywania danych, podjęcie przez naukowców indywidualne próby odnalezienia osób, których dane dotyczą, w celu udzielenia im informacji określonych w art. 14 wymagałoby niewspółmiernie dużego wysiłku.

64. Jeżeli administrator danych ma zamiar powołać się na wyjątek określony w art. 14 ust. 5 lit. b) na tej podstawie, że udzielenie informacji wymagałoby niewspółmiernie dużego wysiłku, powinien przeprowadzić test równowagi, aby porównać wysiłek wkładany przez administratora danych w udzielenie informacji osobie, której dane dotyczą, z konsekwencjami i skutkami dla tej osoby w przypadku nieudzielenia tego rodzaju informacji. Administrator danych powinien udokumentować tę ocenę zgodnie ze spoczywającymi na nim obowiązkami w zakresie rozliczalności. W takim przypadku art. 14 ust. 5 lit. b) stanowi, że administrator musi wprowadzić odpowiednie środki, by chronić prawa i wolności oraz prawnie uzasadnione interesy osoby, której dane dotyczą. Zasada ta ma zastosowanie również wówczas, gdy administrator uzna, że udzielenie informacji jest niemożliwe lub mogłoby uniemożliwić lub poważnie utrudnić realizację celów przetwarzania. Jednym z odpowiednich środków – zgodnie z art. 14 ust. 5 lit. b) – jakie administrator musi zawsze podejmować, jest udostępnianie informacji publicznie. Administrator może udostępnić informacje publicznie na wiele sposobów, na przykład umieszczając informacje na swojej stronie internetowej lub aktywnie je ogłaszając w gazecie bądź na plakatach w swojej siedzibie. Inne odpowiednie środki – oprócz udostępniania informacji publicznie – będą zależały od okoliczności przetwarzania, lecz mogą obejmować: przeprowadzenie oceny skutków dla ochrony danych; zastosowanie technik pseudonimizacji danych; zminimalizowanie ilości zbieranych danych i okresu ich przechowywania; oraz wdrażanie środków technicznych i organizacyjnych w celu zapewnienia wysokiego poziomu bezpieczeństwa. Ponadto mogą zaistnieć sytuacje, w których administrator danych przetwarza dane osobowe, co nie wymaga identyfikacji osoby, której dane dotyczą (na przykład w przypadku danych pseudonimicznych). W takich przypadkach istotny może być również art. 11 ust. 1, ponieważ stanowi on, 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.

*Poważne utrudnienie realizacji celów*

65. Ostatnią sytuacją opisaną w art. 14 ust. 5 lit. b) jest sytuacja, w której udzielenie informacji osobie, której dane dotyczą, przez administratora danych zgodnie z art. 14 ust. 1 może uniemożliwić lub poważnie utrudnić realizację celów przetwarzania. Aby powołać się na ten wyjątek, administratorzy danych muszą wykazać, że samo udzielenie informacji określonych w art. 14 ust. 1 zniweczyłoby cele przetwarzania. W szczególności powołanie się na ten aspekt art. 14 ust. 5 lit. b) zakłada, że przetwarzanie danych jest zgodne ze wszystkimi zasadami określonymi w art. 5 oraz – co najważniejsze – że

w każdych okolicznościach przetwarzanie danych osobowych jest rzetelne i ma podstawę prawną.

**Przykład**

Bank A podlega określonemu w przepisach dotyczących przeciwdziałaniu praniu pieniędzy obowiązkowemu wymogowi zgłaszania do właściwego organu ścigania przestępstw finansowych podejrzanej działalności związanej z rachunkami prowadzonymi przez ten bank. Bank A otrzymuje od banku B (mającego siedzibę w innym państwie członkowskim) informację, że posiadacz rachunku zlecił mu dokonanie przelewu środków pieniężnych na inne konto prowadzone przez bank A, co wydaje się podejrzane. Bank A przekazuje te dane dotyczące posiadacza rachunku i podejrzanych działań właściwemu organowi ścigania przestępstw finansowych. Przedmiotowe przepisy dotyczące przeciwdziałaniu praniu pieniędzy stanowią, że przestępstwem jest ostrzeżenie posiadacza rachunku przez zgłaszający bank, że może on zostać objęty dochodzeniem regulacyjnym. W tej sytuacji zastosowanie ma art. 14 ust. 5 lit. b), ponieważ udzielenie osobie, której dane dotyczą (posiadaczowi rachunku w banku A) informacji określonych w art. 14 dotyczących przetwarzania danych osobowych posiadacza rachunku otrzymanych od banku B poważnie utrudniłoby realizację celów przepisów, w tym zapobiegania ostrzeżeniom. Wszystkim posiadaczom rachunku w banku A należy jednak przedstawić w momencie otwierania rachunku ogólne informacje, że ich dane osobowe mogą być przetwarzane do celów przeciwdziałania praniu pieniędzy.

*Pozyskiwanie lub ujawnianie jest wyraźnie uregulowane w prawie*

66. Art. 14 ust. 5 lit. c) umożliwia zniesienie wymogów udzielenia informacji określonych w art. 14 ust. 1, art. 14 ust. 2 i art. 14. ust.4, o ile pozyskiwanie lub ujawnianie danych osobowych „jest wyraźnie uregulowane prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator". Odstępstwo to jest zależne od odnośnego prawa przewidującego „odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą". Prawo takie musi bezpośrednio odnosić się do administratora danych, a przedmiotowe pozyskiwanie lub ujawnianie powinno być obowiązkowe dla administratora danych. W związku z tym administrator danych musi być w stanie wykazać, w jaki sposób przedmiotowe prawo odnosi się do niego i wymaga, aby pozyskał albo ujawnił odnośne dane osobowe. Chociaż to w prawie Unii lub państwa członkowskiego ma zostać sformułowane prawo w taki sposób, aby przewidywało „odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą", administrator danych powinien zapewnić (i być w stanie wykazać) zgodność pozyskania lub ujawnienia danych osobowych z tymi środkami. Ponadto administrator danych powinien wyraźnie poinformować osobę, której dane dotyczą, że pozyskuje lub ujawnia dane osobowe zgodnie z odnośnym prawem, o ile nie istnieje prawny zakaz uniemożliwiający administratorowi danych wykonanie tych czynności. Jest to zgodne z motywem 41 RODO, w którym stwierdzono, że taka podstawa prawna lub taki akt prawny powinny być jasne i precyzyjne, a ich zastosowanie przewidywalne dla osób im podlegających – jak wymaga tego orzecznictwo Trybunału Sprawiedliwości UE i Europejskiego Trybunału Praw Człowieka. Art. 14 ust. 5 lit. c) jednak nie będzie miał

zastosowania, w przypadku gdy administrator danych podlega obowiązkowi pozyskania danych *bezpośrednio od osoby, której dane dotyczą*, w którym to przypadku zastosowanie będzie miał art. 13. W takim przypadku jedynym odstępstwem na podstawie RODO zwalniającym administratora z obowiązku udzielenia osobie, której dane dotyczą, informacji na temat przetwarzania, będzie odstępstwo na podstawie art. 13 ust. 4 (tzn. gdy – i w zakresie, w jakim – osoba, której dane dotyczą, dysponuje już tymi informacjami). Zgodnie z art. 23 państwa członkowskie mogą jednak ustanowić na poziomie krajowym również akty prawne dotyczące dalszych szczególnych ograniczeń prawa do przejrzystości na mocy art. 12 i informacji na podstawie art. 13 i 14, o czym mowa poniżej w pkt 68.

**Przykład**

Na podstawie prawa krajowego organ podatkowy podlega obowiązkowemu wymogowi pozyskania od pracodawcy szczegółowych informacji na temat wynagrodzenia pracowników. Dane osobowe nie zostają pozyskane od osoby, której dane dotyczą, i w związku z tym organ podatkowy podlega wymogom określonym w art. 14. Ponieważ pozyskiwanie danych osobowych od pracodawcy przez organ podatkowy jest wyraźnie uregulowane prawem, w tym przypadku wymogi udzielenia informacji określone w art. 14 nie mają zastosowania do organu podatkowego.

*Poufność wynikająca z obowiązku zachowania tajemnicy*

67. Art. 14 ust. 5 lit. d) przewiduje odstępstwo od wymogu udzielenia informacji, któremu podlega administrator danych, w przypadku 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 zamierza powołać się na to odstępstwo, musi być w stanie wykazać, że właściwie je zidentyfikował i przedstawić, w jaki sposób zawodowy obowiązek zachowania tajemnicy bezpośrednio odnosi się do administratora danych, tak że nie wolno mu przekazać osobie, której dane dotyczą, wszystkich informacji określonych w art. 14 ust. 1, art. 14 ust. 2 i art. 14 ust. 4.

**Przykład**

Przedstawiciel zawodu medycznego (administrator danych) podlega zawodowemu obowiązkowi zachowania tajemnicy w odniesieniu do informacji medycznych dotyczących jego pacjenta. Pacjentka (w odniesieniu do której zawodowy obowiązek zachowania tajemnicy ma zastosowanie) dostarcza przedstawicielowi zawodu medycznego informacje dotyczące jej zdrowia związane z chorobą genetyczną, na którą cierpi również wielu jej krewnych. Pacjentka dostarcza również przedstawicielowi zawodu medycznego niektóre dane osobowe dotyczącego jej krewnych (osób, których dane dotyczą), którzy cierpią na tę samą chorobę. Przedstawiciel zawodu medycznego nie ma obowiązku udzielania krewnym informacji, o których mowa w art. 14, ponieważ zastosowanie ma odstępstwo określone w art. 14 ust. 5 lit. d). Jeśli przedstawiciel zawodu medycznego udzieliłby krewnym informacji, o których mowa w art. 14, naruszony zostałby obowiązek zachowania tajemnicy

zawodowej, który przedstawiciel zawodu medycznego ma wobec swojego pacjenta.

Ograniczenia praw osoby, której dane dotyczą

68. Art. 23 przewiduje, że państwa członkowskie (lub UE) mogą ustanowić akty prawne dotyczące dalszych ograniczeń zakresu praw osoby, której dane dotyczą, w odniesieniu do przejrzystości i praw podmiotowych osoby, której dane dotyczą[55], jeżeli takie akty prawne nie naruszają istoty podstawowych praw i wolności oraz stanowią niezbędny i proporcjonalny środek dla zabezpieczenia jednego lub większej liczby spośród dziesięciu celów określonych w art. 23 ust. 1 lit. a)–j). W przypadku gdy krajowe akty prawne ograniczają szczególne prawa osoby, której dane dotyczą, lub ogólne obowiązki zapewnienia przejrzystości, które w przeciwnym wypadku miałyby zastosowanie do administratora danych zgodnie z RODO, administrator danych powinien być w stanie wykazać, w jaki sposób przepis krajowy ma do niego zastosowanie. Jak określono w art. 23 ust. 2 lit. h), akt prawny musi zawierać przepis o prawie osób, których dane dotyczą, do uzyskania informacji o ograniczeniach ich praw, o ile poinformowanie ich o tym nie narusza celu ograniczenia. Spójnie z powyższym oraz zgodnie z zasadą rzetelności, administrator danych powinien również poinformować osoby, których dane dotyczą, że opierają się (lub będą się opierać w przypadku wykonywania określonego prawa osoby, której dane dotyczą) na takim *krajowym ograniczeniu prawnym* dotyczącym wykonywania prawa osoby, której dane dotyczą, lub obowiązku zapewnienia przejrzystości, o ile nie narusza to celu ograniczenia prawnego. Przejrzystość jako taka wymaga od administratora danych, aby z góry przedstawił osobie, której dane dotyczą, informacje na temat jej praw oraz ewentualnych zastrzeżeń dotyczących tych praw, na które to zastrzeżenia administrator może mieć zamiar się powoływać, tak aby osoba, której dane dotyczą, nie była zaskoczona rzekomym ograniczeniem określonego prawa, gdy w późniejszym terminie będzie próbowała wykonać je w stosunku do administratora. W odniesieniu do pseudonimizacji i minimalizacji danych, oraz w zakresie, w jakim administrator danych może powoływać się na art. 11 RODO, GR29 potwierdził już wcześniej w opinii nr 3/2017[56], że art. 11 RODO należy interpretować jako sposób egzekwowania rzeczywistej minimalizacji danych pozostający bez uszczerbku dla wykonywania przez osoby, których dane dotyczą, przysługujących im praw, oraz że należy umożliwić wykonywanie praw osoby, której dane dotyczą, przy pomocy dodatkowych informacji dostarczonych przez tę osobę.

69. Ponadto w art. 85 nakłada się na państwa członkowskie wymóg, aby przyjęły przepisy pozwalające pogodzić ochronę danych osobowych z prawem do wolności wypowiedzi i informacji. Wymaga to od państw członkowskich między innymi, aby przewidziały właściwe odstępstwa lub wyjątki od niektórych przepisów RODO (w tym wymogów przejrzystości na podstawie art. 12–14) dla przetwarzania do celów wypowiedzi dziennikarskiej, akademickiej, artystycznej lub literackiej, jeśli są one niezbędne, aby pogodzić oba prawa.

[55] Jak określono w art. 12–22 oraz art. 34 i art. 5, o ile jego przepisy odpowiadają prawom i obowiązkom przewidzianym w art. 12–22.

[56] Opinia nr 03/2017 dotycząca przetwarzania danych osobowych w ramach współpracujących inteligentnych systemów transportowych (C-ITS) – zob. pkt 4.2.

Przejrzystość oraz naruszenie ochrony danych

70. GR29 opracowała oddzielne wytyczne w sprawie naruszenia ochrony danych[57], jednak do celów niniejszych wytycznych obowiązki administratora danych w odniesieniu do zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych muszą w pełni uwzględniać wymogi przejrzystości określone w art. 12[58]. Zawiadomienie o naruszeniu ochrony danych musi spełniać te same wymogi, opisane szczegółowo powyżej (w szczególności dotyczące jasnego i prostego języka), które mają zastosowanie do wszelkiej innej komunikacji z osobą, której dane dotyczą, w odniesieniu do jej praw lub w związku z udzielaniem informacji na podstawie art. 13 i 14.

[57] Wytyczne w sprawie powiadomień o naruszeniu ochrony danych osobowych na mocy rozporządzenia 2016/679, GR 250.

[58] Jest to wyraźnie określone w art. 12 ust. 1, w którym mowa w szczególności o „wszelkiej komunikacji z osobą, której dane dotyczą, na mocy art. 15–22 i 34 w sprawie przetwarzania […]". (pogrubienie i podkreślenie dodano).

## Załącznik
## Informacje, które należy przekazać osobie, której dane dotyczą, na podstawie art. 13 lub art. 14

| Wymagany rodzaj informacji | Stosowny artykuł (jeśli dane osobowe zostały zebrane bezpośrednio od osoby, której dane dotyczą) | Stosowny artykuł (jeśli dane osobowe nie zostały pozyskane od osoby, której dane dotyczą) | Uwagi GR29 na temat wymogu udzielenia informacji |
|---|---|---|---|
| Tożsamość i dane kontaktowe administratora oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe jego przedstawiciela[59] | Art. 13 ust. 1 lit. a) | Art. 14 ust. 1 lit. a) | Informacje te powinny umożliwiać łatwą identyfikację administratora. Najlepiej byłoby również, gdyby umożliwiały różne formy komunikacji z administratorem danych (np. numer telefonu, adres e-mail, adres korespondencyjny itp.) |
| Gdy ma to zastosowanie – dane kontaktowe inspektora ochrony danych | Art. 13 ust. 1 lit. b) | Art. 14 ust. 1 lit. b) | Zob. Wytyczne GR29 dotyczące inspektorów ochrony danych[60]. |
| Cele i podstawa prawna przetwarzania | Art. 13 ust. 1 lit. c) | Art. 14 ust. 1 lit. c) | Oprócz określenia celów przetwarzania danych osobowych należy określić stosowną podstawę prawną, na której opiera się przetwarzanie na podstawie art. 6. W przypadku szczególnych kategorii danych osobowych należy określić stosowne przepisy art. 9 (w stosownych przypadkach także mające zastosowanie prawo Unii lub państwa |

[59] Jak określono w art. 4 pkt 17 RODO (i o czym mowa w motywie 80), „przedstawiciel" oznacza osobę fizyczną lub prawną mającą miejsce zamieszkania lub siedzibę w UE, która została wyznaczona na piśmie przez administratora lub podmiot przetwarzający na podstawie art. 27 i reprezentuje administratora lub podmiot przetwarzający w zakresie ich obowiązków wynikających z RODO. Obowiązek ten ma zastosowanie w przypadku, gdy zgodnie z art. 3 ust. 2 administrator lub podmiot przetwarzający nie posiada jednostek organizacyjnych w UE, ale przetwarza dane osobowe osób, których dane dotyczą, przebywających w UE, a przetwarzanie wiąże się z oferowaniem towarów lub usług osobom w UE, których dane dotyczą, lub monitorowaniem ich zachowania.

[60] Wytyczne dotyczące inspektorów ochrony danych, GR243 rev.01, ostatnio zmienione i przyjęte w dniu 5 kwietnia 2017 r.

| | | | |
|---|---|---|---|
| | | | członkowskiego, na mocy którego przetwarza się dane). W przypadku gdy na podstawie art. 10 przetwarza się dane osobowe dotyczące wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa na podstawie art. 6 ust. 1, w stosownych przypadkach należy określić stosowne prawo Unii lub państwa członkowskiego, na mocy którego dokonuje się przetwarzania. |
| Jeżeli podstawę prawną przetwarzania stanowią uzasadnione interesy (art. 6 ust. 1 lit. f)) – prawnie uzasadnione interesy realizowane przez administratora danych lub przez stronę trzecią | Art. 13 ust. 1 lit. d) | Art. 14 ust. 2 lit. b) | Odnośny szczególny interes należy określić wobec osoby, której dane dotyczą. W ramach najlepszej praktyki administrator może również przedstawić osobie, której dane dotyczą, informacje uzyskane w wyniku *testu równowagi,* który należy przeprowadzić, aby można było oprzeć się na art. 6 ust. 1 lit. f) jako podstawie prawnej przetwarzania, zanim jakiekolwiek dane osobowe osoby, której dane dotyczą, zostaną zebrane. Aby nie przytłoczyć odbiorcy informacjami, można je włączyć do warstwowego oświadczenia o ochronie prywatności / warstwowej informacji o polityce prywatności (zob. pkt 35). W każdym przypadku stanowisko GR29 jest takie, że z informacji udzielonych osobie, której dane dotyczą, powinno jasno wynikać, iż informacje dotyczące testu równowagi mogą uzyskać na żądanie. Jest to istotne dla skutecznej przejrzystości w przypadku gdy osoby, których |

| | | | |
|---|---|---|---|
| | | | dane dotyczą, mają wątpliwości, czy test równowagi przeprowadzono rzetelnie lub chcą złożyć skargę do organu nadzorczego. |
| Kategorie odnośnych danych osobowych | Nie jest wymagane | Art. 14 ust. 1 lit. d) | Informacje te są wymagane w ramach scenariusza dotyczącego art. 14, ponieważ dane osobowe nie zostały pozyskane od osoby, której dane dotyczą i która w związku z tym nie wie, jakie kategorie jej danych osobowych pozyskał administrator danych. |
| Informacje o odbiorcach[61] danych osobowych (lub o kategoriach odbiorców) | Art. 13 ust. 1 lit. e) | Art. 14 ust. 1 lit. e) | Termin „odbiorca" określono w art. 4 pkt 9 jako „osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, **niezależnie od tego, czy jest stroną trzecią**" [pogrubienie dodano] Odbiorca jako taki nie musi być stroną trzecią. W związku z tym termin „odbiorca" obejmuje innych administratorów danych, współadministratorów i podmioty przetwarzające, którym przekazano lub ujawniono dane, a informacje na temat tych odbiorców należy przedstawić dodatkowo do informacji na temat odbiorców będących stronami trzecimi.<br>Należy podać informacje o faktycznych odbiorcach (wymienionych z nazwiska lub nazwy) danych osobowych lub o kategoriach odbiorców. Zgodnie z zasadą rzetelności administratorzy muszą przedstawić informacje na temat odbiorców, którzy mają największe znaczenie dla |

[61] Określonych w art. 4 pkt 9 RODO i o których mowa w motywie 31

| | | | |
|---|---|---|---|
| | | | osoby, której dane dotyczą. W praktyce zazwyczaj będzie to odbiorca wymieniony z nazwiska lub nazwy, tak aby osoby, których dane dotyczą, wiedziały dokładnie, kto jest w posiadaniu ich danych osobowych. Jeśli administrator zamierza przedstawić kategorie odbiorców, informacje powinny być w jak największym stopniu szczegółowe, tzn. należy wskazać rodzaj odbiorcy (np. poprzez odniesienie do działalności, którą prowadzi), branżę, sektor, podsektor oraz lokalizację odbiorcy. |
| Szczegóły przekazań do państw trzecich, fakt ich przekazania oraz szczegóły dotyczące stosownych zabezpieczeń[62] (w tym stwierdzenia lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony[63]) oraz możliwości uzyskania kopii danych lub informacje o miejscu udostępnienia danych. | Art. 13 ust. 1 lit. f) | Art. 14 ust. 1 lit. f) | Należy określić stosowny artykuł RODO zezwalający na przekazanie oraz odpowiedni mechanizm (np. decyzja stwierdzająca odpowiedni stopień ochrony na podstawie art. 45 / wiążące reguły korporacyjne na mocy art. 47 / standardowe klauzule ochrony danych na podstawie art. 46 ust. 2 / wyjątki i zabezpieczenia na podstawie art. 49 itd.). Należy również poinformować, gdzie i w jaki sposób można uzyskać dostęp do stosownego dokumentu lub sam dokument, np. podając link do zastosowanego mechanizmu. Zgodnie z zasadą rzetelności podane informacje na temat przekazań do państw trzecich powinny być w jak największym stopniu znaczące dla osób, których dane dotyczą, zazwyczaj będzie to oznaczać, że wymieniono nazwę państwa trzeciego. |
| Okres przechowywania (a | Art. 13 ust. 2 | Art. 14 | Jest to powiązane z wymogiem |

[62] Określone w art. 46 ust. 2 i art. 46 ust. 3

[63] Zgodnie z art. 45

| | | | |
|---|---|---|---|
| gdy nie jest to możliwe, kryteria ustalania tego okresu) | lit. a) | ust. 2 lit. a) | dotyczącym minimalizacji danych określonym w art. 5 ust. 1 lit. c) oraz wymogiem w zakresie ograniczenia przechowywania, o którym mowa w art. 5 ust. 1 lit. e).<br>Okres przechowywania (lub kryteria jego ustalania) może być podyktowany takimi czynnikami, jak wymogi ustawowe lub wytyczne branżowe, jednak informacja o nim powinna być sformułowana w taki sposób, aby osoba, której dane dotyczą, miała możliwość ocenienia – na podstawie własnej sytuacji – ile będzie trwał okres zatrzymywania w przypadku określonych danych/celów. Ogólne stwierdzenie przez administratora danych, że dane osobowe będą przechowywane tak długo, jak jest to niezbędne do prawnie uzasadnionych celów przetwarzania, jest niewystarczające.<br>W stosownych przypadkach należy ustalić różne okresy przechowywania dla różnych kategorii danych osobowych lub różnych celów przetwarzania, w tym w stosownych przypadkach, okresy archiwizacji. |
| Prawa osoby, której dane dotyczą, do:<br><br>• dostępu;<br>• sprostowania;<br>• usunięcia;<br>• ograniczenia przetwarzania;<br>• sprzeciwu wobec przetwarzania oraz<br>• przenoszenia. | Art. 13 ust. 2 lit. b) | Art. 14 ust. 2 lit. c) | Informacje te powinny być dostosowane do scenariusza przetwarzania oraz zawierać podsumowanie tego, co jest objęte tym prawem, oraz sposobu, w jaki osoba, której dane dotyczą, może podjąć kroki, aby wykonać to prawo, oraz wszelkich ograniczeń tego prawa (zob. pkt 68 powyżej).<br>W szczególności osoba, której |

| | | | |
|---|---|---|---|
| | | | dane dotyczą, musi zostać wyraźnie poinformowana o prawie sprzeciwu wobec przetwarzania najpóźniej przy okazji pierwszego kontaktu z taką osobą oraz należy przedstawić jej to prawo jasno i odrębnie od wszelkich innych informacji[64].<br>W odniesieniu do prawa do przenoszenia zob. Wytyczne GR29 dotyczące prawa do przenoszenia danych[65]. |
| Jeżeli przetwarzanie odbywa się na podstawie zgody (lub wyraźnej zgody), prawo do cofnięcia zgody w dowolnym momencie | Art. 13 ust. 2 lit. c) | Art. 14 ust. 2 lit. d) | Informacja ta powinna obejmować sposób, w jaki można wycofać zgodę, biorąc pod uwagę wymóg, że wycofanie zgody przez osobę, której dane dotyczą, musi być równie łatwe jak jej wyrażenie[66]. |
| Informacje o prawie wniesienia skargi do organu nadzorczego | Art. 13 ust. 2 lit. d) | Art. 14 ust. 2 lit. e) | Informacja ta powinna zawierać wyjaśnienie, że zgodnie z art. 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 o tym, czy istnieje wymóg prawny lub umowny dotyczący przedstawienia informacji, czy przedstawienie informacji jest warunkiem zawarcia umowy lub czy istnieje obowiązek przedstawienia informacji oraz jakie są ewentualne konsekwencje | Art. 13 ust. 2 lit. e) | Nie jest wymagane | Na przykład w kontekście zatrudnienia przedstawienie niektórych informacji obecnemu lub potencjalnemu pracodawcy może stanowić warunek zawarcia umowy.<br>Internetowe formularze powinny wyraźnie określać, które pola są „wymagane”, a które nie, oraz jakie będą |

[64] Art. 21 ust. 4 oraz motyw 70 (który ma zastosowanie do marketingu bezpośredniego)

[65] Wytyczne dotyczące prawa do przenoszenia danych, GR242 rev.01, ostatnio zmienione i przyjęte w dniu 5 kwietnia 2017 r.

[66] Art. 7 ust. 3

| | | | |
|---|---|---|---|
| ich nieprzedstawienia. | | | konsekwencje niewypełnienia wymaganych pól. |
| Źródło pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródła publicznie dostępnego. | Nie jest wymagane | Art. 14 ust. 2 lit. f) | Należy przedstawić konkretne źródło danych, chyba że jest to niemożliwe – zob. dalsze wskazówki w pkt 60. Jeśli nazwa konkretnego źródła nie została wymieniona, przedstawione informacje powinny obejmować: charakter źródła (tzn. źródło publiczne/prywatne) oraz rodzaj organizacji/branży/sektora. |
| Informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, oraz – w stosownych przypadkach – istotne informacje o zasadach ich podejmowania oraz o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą. | Art. 13 ust. 2 lit. f) | Art. 14 ust. 2 lit. g) | Zob. Wytyczne GR29 w sprawie zautomatyzowanego podejmowania decyzji i profilowania[67]. |

[67] Wytyczne w sprawie zautomatyzowanego podejmowania decyzji i profilowania do celów rozporządzenia 2016/679, GR 251.