

Bruksela, 11 czerwca 2015 r.  
(OR. en)

9565/15

---

Międzyinstytucjonalny numer  
referencyjny:  
2012/0011 (COD)

---

**DATAPROTECT 97**  
**JAI 420**  
**MI 369**  
**DIGIT 49**  
**DAPIX 94**  
**FREMP 133**  
**COMIX 259**  
**CODEC 823**

#### **NOTA**

|                 |                                                                                                                                                                                                                                                                             |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Od:             | Prezydencja                                                                                                                                                                                                                                                                 |
| Do:             | Rada                                                                                                                                                                                                                                                                        |
| Nr poprz. dok.: | 9398/15                                                                                                                                                                                                                                                                     |
| Dotyczy:        | Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (ogólne rozporządzenie o ochronie danych)<br>Przygotowanie podejścia ogólnego |

#### Wprowadzenie

W dniu 25 stycznia 2012 r. Komisja przyjęła wniosek w sprawie ogólnego rozporządzenia o ochronie danych (5853/12). Nowe rozporządzenie miałoby zastąpić dyrektywę 95/46/WE. Jego dwojakim celem jest zwiększyć ochronę praw osób fizycznych, których dane osobowe są przetwarzane, oraz poszerzyć możliwości biznesowe, ułatwiając swobodny przepływ danych osobowych na jednolitym rynku cyfrowym.

Równolegle z wnioskiem w sprawie ogólnego rozporządzenia o ochronie danych Komisja przyjęła komunikat polityczny wskazujący przyświecające jej cele (5852/12) oraz dyrektywę w sprawie przetwarzania danych do celów egzekwowania prawa (5833/12). Nowa dyrektywa miałaby zastąpić ramową decyzję o ochronie danych z 2008 r.

Parlament Europejski przyjął stanowisko w pierwszym czytaniu w sprawie rozporządzenia i dyrektywy o ochronie danych w dniu 12 marca 2014 r.

#### Tekst kompromisowy

W zbliżeniu poglądów Rady na cały wniosek w sprawie ogólnego rozporządzenia o ochronie danych pomogło kilka częściowych podejść ogólnych. Tekst rozporządzenia, który prezydencja przedkłada do zatwierdzenia jako całościowe podejście, znajduje się w załączniku. Wszelkie zmiany wprowadzone do pierwotnego wniosku Komisji zaznaczono podkreśleniem, wszelkie skreślenia – nawiasami, a przeniesienia – *kursywą*. Uwagi delegacji co do rozporządzania, które nie zawierało wtedy jednak nowych propozycji prezydencji co do motywów 118 i 134, znajdują się w dokumencie z wynikami posiedzenia Komitetu Stałych Przedstawicieli z dnia 9 czerwca 2015 r. (9788/15).

W świetle posiedzenia Komitetu Stałych Przedstawicieli z dnia 9 czerwca 2015 r. prezydencja wprowadziła dwie zmiany.

#### *Prawo do odszkodowania i odpowiedzialność prawna – art. 77 i motyw 118*

Prezydencja sugeruje, by zmienić motyw 118, po to by doprecyzować, że horyzontalnym celem art. 77 i motywu 118 jest zapewnić podmiotowi danych pełne i skuteczne odszkodowanie za poniesioną szkodę. Zważywszy że systemy prawne państw członkowskich różnią się odnośnie do rozstrzygania odpowiedzialności prawnej, podmiot danych może otrzymać takie odszkodowanie od administratora albo podmiotu przetwarzającego pociągniętych do odpowiedzialności za całość szkody lub – w państwach członkowskich, których system prawny pozwala łączyć postępowania – odszkodowaniem można obarczyć więcej niż jednego administratora lub podmiot przetwarzający.

Aby zapewnić administratorom i podmiotom przetwarzającym, których obecne przetwarzanie danych osobowych opiera się na dyrektywie 95/46/WE, dostateczną pewność prawa, prezydencja proponuje doprecyzować zakres zastosowania rozporządzenia w motywie 134.

### Wnioski

Aby prezydencja mogła rozpocząć negocjacje z przedstawicielami Parlamentu Europejskiego, Rada jest proszona o zatwierdzenie – jako podejścia ogólnego – tekstu ogólnego rozporządzenia o ochronie danych w wersji z załącznika.

---

Wniosek

**ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY**

**w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych  
i w sprawie swobodnego przepływu takich danych (ogólne rozporządzenie o ochronie  
danych)**

(Tekst mający znaczenie dla EOG)

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 16 ust. 2 (...),

uwzględniając wniosek Komisji Europejskiej,

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,

uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego,

po zasięgnięciu opinii Europejskiego Inspektora Ochrony Danych,

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą,

a także mając na uwadze, co następuje:

- 1) Ochrona osób fizycznych w związku z przetwarzaniem danych osobowych jest jednym z praw podstawowych. Artykuł 8 ust. 1 Karty praw podstawowych Unii Europejskiej oraz art. 16 ust. 1 Traktatu stanowią, że każda osoba ma prawo do ochrony danych osobowych jej dotyczących.
- 2) (...) Zasady i przepisy dotyczące ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych powinny – niezależnie od obywatelstwa czy miejsca zamieszkania takich osób – respektować ich podstawowe prawa i wolności, zwłaszcza prawo do ochrony danych osobowych. To zaś powinno przyczyniać się do tworzenia obszaru wolności, bezpieczeństwa i sprawiedliwości oraz unii gospodarczej, do postępu społeczno-gospodarczego, do wzmacniania i konwergencji gospodarek na rynku wewnętrznym, a także do dobrostanu ludzi.
- 3) Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych miała na celu zharmonizować ochronę podstawowych praw i wolności osób fizycznych w związku z czynnościami przetwarzania oraz zagwarantować swobodny przepływ danych osobowych między państwami członkowskimi.
- 3a) Prawo do ochrony danych osobowych nie jest prawem bezwzględnym: należy je postrzegać w kontekście jego funkcji społecznej i wyważyć względem innych praw podstawowych w myśl zasady proporcjonalności. Niniejsze rozporządzenie respektuje wszelkie prawa podstawowe i zachowuje zasady uznane w Karcie praw podstawowych Unii Europejskiej – zapisane w traktatach – zwłaszcza prawo do poszanowania życia prywatnego i rodzinnego, domu oraz komunikowania się, prawo do ochrony danych osobowych, wolność myśli, sumienia i religii, wolność wypowiedzi i informacji, wolność prowadzenia działalności gospodarczej, prawo do skutecznego środka ochrony prawnej i dostępu do bezstronnego sądu oraz prawo do różnorodności kulturowej, religijnej i językowej.

- 4) Integracja społeczno-gospodarcza wynikająca z funkcjonowania rynku wewnętrznego doprowadziła do znacznego zwiększenia ruchu transgranicznego. Wzrosła wymiana danych między (...) podmiotami publicznymi i prywatnymi, w tym między osobami fizycznymi i przedsiębiorstwami w Unii. Organy krajowe państw członkowskich coraz częściej są wzywane prawem Unii do tego, by w celu wykonania swoich obowiązków lub w celu realizacji zadań w imieniu organu innego państwa członkowskiego współpracowały ze sobą i wymieniały się danymi osobowymi.
- 5) Szybki rozwój technologiczny i globalizacja przyniosły nowe wyzwania w dziedzinie ochrony danych osobowych. Skala wymiany i zbierania danych niezwykle wzrosła. Dzięki technologii zarówno przedsiębiorstwa prywatne, jak i organy publiczne mogą na niespotykaną dotąd skalę wykorzystywać dane osobowe w swojej działalności. Osoby fizyczne coraz częściej udostępniają informacje osobowe publicznie i globalnie. Technologia zmieniła gospodarkę i życie społeczne, i powinna nadal ułatwiać swobodny przepływ danych w Unii oraz ich przekazywanie do państw trzecich i organizacji międzynarodowych, równocześnie zaś powinna zapewniać wysoki poziom ochrony danych osobowych.
- 6) Przemiany te wymagają (...) stabilnych, spójniejszych ram ochrony danych w Unii oraz zdecydowanego egzekwowania ich przepisów, gdyż ważna jest budowa zaufania, które pozwoli na rozwój gospodarki cyfrowej na rynku wewnętrznym. Osoby fizyczne powinny mieć kontrolę nad własnymi danymi osobowymi, a osoby fizyczne, podmioty gospodarcze i organy publiczne powinny zyskać większe poczucie pewności prawa i jego praktycznych zastosowań.
- 6a) Jeżeli niniejsze rozporządzenie dopuszcza doprecyzowanie lub zaostrzenie jego przepisów przez prawo państw członkowskich, państwa członkowskie mogą – jeżeli jest to niezbędne, by krajowe przepisy były spójne i zrozumiałe dla osób, do których mają zastosowanie – włączyć elementy niniejszego rozporządzenia do prawa krajowego.

- 7) Cele i zasady dyrektywy 95/46/WE pozostają aktualne, jednak wdrażając ochronę danych w Unii, nie uniknięto fragmentaryzacji, niepewności prawnej oraz upowszechnienia się poglądu, że ochrona osób fizycznych jest znacznie zagrożona, w szczególności w związku z działaniami w internecie. Różnice w poziomie ochrony praw i wolności osób fizycznych w państwach członkowskich – w szczególności prawa do ochrony danych osobowych – w związku z przetwarzaniem danych osobowych mogą utrudniać swobodny przepływ danych osobowych w Unii. Mogą zatem stanowić przeszkodę w prowadzeniu działalności gospodarczej na szczeblu Unii, zakłócać konkurencję oraz utrudniać organom wykonywanie obowiązków nałożonych na nie prawem Unii. Różnice w poziomie ochrony wynikają z różnic we wdrażaniu i stosowaniu dyrektywy 95/46/WE.
- 8) Aby zapewnić wysoki i spójny poziom ochrony osób fizycznych oraz usunąć przeszkody w przepływie danych osobowych w Unii, należy zadbać o równorzędny we wszystkich państwach członkowskich poziom ochrony praw i wolności osób fizycznych w związku z przetwarzaniem takich danych. Należy zapewnić spójne i jednolite stosowanie w całej Unii przepisów o ochronie podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych. Jeżeli chodzi o przetwarzanie danych osobowych w celu wypełnienia obowiązku prawnego, w celu wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi, państwa członkowskie powinny móc zachować lub wprowadzić krajowe przepisy doprecyzowujące zastosowanie przepisów niniejszego rozporządzenia. Obok ogólnego, horyzontalnego prawa o ochronie danych wdrażającego dyrektywę 95/46/WE państwa członkowskie mają uregulowania sektorowe w kilku dziedzinach wymagających przepisów bardziej szczegółowych. Także niniejsze rozporządzenie daje państwom członkowskim pole do doprecyzowania jego przepisów. W ramach tego pola manewru uregulowania sektorowe, które państwa członkowskie wprowadziły przy wdrażaniu dyrektywy 95/46/WE, powinny móc zostać zachowane.

- 9) Aby ochrona danych osobowych w Unii była skuteczna, należy wzmocnić i doprecyzować prawa podmiotów danych oraz obowiązki podmiotów przetwarzających dane osobowe i kierujących przetwarzaniem, ale też zapewnić równorzędne uprawnienia do monitorowania i egzekwowania przepisów o ochronie danych osobowych oraz równorzędne sankcje wobec podmiotów naruszających te przepisy w państwach członkowskich.
- 10) Artykuł 16 ust. 2 Traktatu powierza Parlamentowi Europejskiemu i Radzie określenie zasad ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz zasad swobodnego przepływu takich danych.
- 11) Aby zapewnić spójny poziom ochrony osób fizycznych w Unii oraz zapobiegać różnicom hamującym swobodny przepływ danych na rynku wewnętrznym, należy przyjąć rozporządzenie, które zagwarantuje podmiotom gospodarczym – w tym mikroprzedsiębiorstwom oraz małym i średnim przedsiębiorstwom – pewność prawa i przejrzystość, a osobom fizycznym we wszystkich państwach członkowskich ten sam poziom prawnie egzekwowalnych praw oraz obowiązków i zadań administratorów i podmiotów przetwarzających (...), które pozwoli spójnie monitorować przetwarzanie danych osobowych, a także zapewni równoważne sankcje we wszystkich państwach członkowskich oraz skuteczną współpracę organów nadzorczych z różnych państw członkowskich. Aby rynek wewnętrzny mógł właściwie funkcjonować, swobodny przepływ danych osobowych w Unii nie powinien być ograniczany ani zakazany z powodów odnoszących się do ochrony osób fizycznych w związku z przetwarzaniem danych osobowych. (...)
- Z uwagi na szczególną sytuację mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw niniejsze rozporządzenie przewiduje szereg odstępstw. Ponadto zachęca się instytucje i organy Unii, państwa członkowskie oraz ich organy nadzorcze, by stosując niniejsze rozporządzenie, uwzględniały szczególne potrzeby mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw. Pojęcie mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw powinno się opierać na zaleceniu Komisji 2003/361/WE z dnia 6 maja 2003 r. dotyczącym definicji mikroprzedsiębiorstwa oraz małego i średniego przedsiębiorstwa.



- 12) Niniejsze rozporządzenie zapewnia ochronę osobom fizycznym – niezależnie od ich obywatelstwa czy miejsca zamieszkania – w związku z przetwarzaniem danych osobowych. Jeżeli chodzi o przetwarzanie danych dotyczących osób prawnych, w szczególności przedsiębiorstw będących osobami prawnymi (w tym danych o firmie i formie prawnej oraz danych kontaktowych osoby prawnej), niniejsze rozporządzenie nie powinno być stosowane do dochodzenia ochrony przez takie osoby. (...).
- 13) Ochrona osób fizycznych powinna być technologicznie neutralna i niezależna od stosowanych technik; w przeciwnym razie groziłoby poważne ryzyko obchodzenia prawa. Ochrona osób fizycznych powinna mieć zastosowanie do zautomatyzowanego przetwarzania danych osobowych oraz do przetwarzania ręcznego, jeżeli dane znajdują się lub mają się znaleźć w zbiorze danych. Zbiory lub zestawy zbiorów oraz ich strony tytułowe, które nie są uporządkowane według konkretnych kryteriów, nie powinny wchodzić w zakres niniejszego rozporządzenia.
- 14) Niniejsze rozporządzenie nie odnosi się do kwestii ochrony podstawowych praw i wolności ani swobodnego przepływu danych w związku z działalnością nieobjętą zakresem prawa Unii, taką jak działalność dotycząca bezpieczeństwa narodowego, (...) ani nie obejmuje przetwarzania danych osobowych przez państwa członkowskie podczas prowadzenia działalności związanej ze wspólną polityką zagraniczną i bezpieczeństwa Unii.
- 14a) Do przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne Unii ma zastosowanie rozporządzenie (WE) nr 45/2001. Rozporządzenie (WE) nr 45/2001 oraz inne unijne akty prawne mające zastosowanie do takiego przetwarzania danych osobowych należy dostosować do zasad i przepisów niniejszego rozporządzenia.
- 15) Niniejsze rozporządzenie nie powinno mieć zastosowania do przetwarzania danych osobowych przez osobę fizyczną w ramach działalności osobistej lub domowej, czyli bez związku z działalnością zawodową lub handlową. Działalność osobista i domowa to między innymi podtrzymywanie więzi społecznych oraz działalność internetowa podejmowana w ramach takiej działalności osobistej i domowej. Niniejsze rozporządzenie powinno jednak (...) mieć zastosowanie do administratorów lub podmiotów przetwarzających, którzy udostępniają środki przetwarzania danych osobowych na potrzeby takiej działalności osobistej lub domowej.

- 16) Ochrona osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, ich wykrywania lub ścigania, wykonywania sankcji karnych lub do ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom, a także swobodny przepływ takich danych podlegają na szczeblu Unii szczegółowemu aktowi prawnemu.

Niniejsze rozporządzenie nie powinno więc mieć zastosowania do czynności przetwarzania w tych celach. Jeżeli jednak dane przetwarzane przez organy publiczne na mocy niniejszego rozporządzenia są wykorzystywane do zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, ich wykrywania lub ścigania lub do wykonywania sankcji karnych, dane te powinny podlegać bardziej szczegółowemu aktowi prawnemu na szczeblu Unii (dyrektywie XX/YYYY). Państwa członkowskie mogą powierzyć właściwym organom w rozumieniu dyrektywy (XX/YYYY) inne zadania, które niekoniecznie służą zapobieganiu przestępstwom, prowadzeniu dochodzeń w ich sprawie, ich wykrywaniu lub ściganiu, wykonywaniu sankcji karnych lub ochronie przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganiu takim zagrożeniom, tak by przetwarzanie danych osobowych do tych innych celów, o ile mieści się w zakresie prawa Unii, wchodziło w zakres niniejszego rozporządzenia.

Jeżeli chodzi o przetwarzanie danych osobowych przez te właściwe organy do celów wchodzących w zakres ogólnego rozporządzenia o ochronie danych, państwa członkowskie mogą zachować lub wprowadzić bardziej szczegółowe przepisy dostosowujące stosowanie przepisów ogólnego rozporządzenia o ochronie danych. Takie przepisy mogą precyzyjniej określać szczegółowe wymogi przetwarzania danych przez te właściwe organy do tych innych celów, z uwzględnieniem konstytucyjnych, organizacyjnych i administracyjnych struktur danego państwa członkowskiego.

Jeżeli przetwarzanie danych osobowych przez (...) podmioty prywatne wchodzi w zakres niniejszego rozporządzenia, niniejsze rozporządzenie powinno pod konkretnymi warunkami dawać państwom członkowskim możliwość prawnego ograniczenia niektórych obowiązków i praw, o ile takie ograniczenie stanowi w demokratycznym społeczeństwie niezbędny i proporcjonalny środek chroniący konkretne, ważne interesy, w tym bezpieczeństwo publiczne oraz zapobieganie przestępstwom, prowadzenie dochodzeń w ich sprawie, ich wykrywanie lub ściganie. Jest to istotne na przykład w przeciwdziałaniu praniu pieniędzy lub w działalności laboratoriów kryminalistycznych.

- 16a) Niniejsze rozporządzenie ma zastosowanie również do działalności sądów i innych organów wymiaru sprawiedliwości, niemniej prawo Unii lub prawo państwa członkowskiego może doprecyzować operacje i procedury przetwarzania danych osobowych przez sądy i inne organy wymiaru sprawiedliwości. Właściwość organów nadzorczych nie powinna dotyczyć przetwarzania danych osobowych przez sądy w ramach sprawowania wymiaru sprawiedliwości – tak by chronić niezawisłość wymiaru sprawiedliwości w wykonywaniu zadań sądowych, w tym podejmowaniu decyzji. Nadzór na takimi operacjami przetwarzania danych można powierzyć specjalnym organom w systemie wymiaru sprawiedliwości państwa członkowskiego, organy te powinny zaś w szczególności kontrolować przestrzeganie przepisów niniejszego rozporządzenia, propagować w wymiarze sprawiedliwości wiedzę o jego obowiązkach wynikających z niniejszego rozporządzenia oraz rozpatrywać skargi związane z takim przetwarzaniem.
- 17) Dyrektywa 2000/31/WE nie ma zastosowania do kwestii związanych z usługami społeczeństwa informacyjnego objętych niniejszym rozporządzeniem. Dyrektywa ta ma przyczyniać się do właściwego funkcjonowania rynku wewnętrznego przez zapewnienie swobodnego przepływu usług społeczeństwa informacyjnego między państwami członkowskimi. Niniejsze rozporządzenie nie powinno wpłynąć na jej stosowanie. Niniejsze rozporządzenie powinno więc pozostawać bez uszczerbku dla stosowania dyrektywy 2000/31/WE, w szczególności dla zasad odpowiedzialności usługodawców będących pośrednikami, o których to zasadach mowa w art. 12–15 tej dyrektywy.
- 18) (...)
- 19) Każde przetwarzanie danych osobowych w kontekście działalności prowadzonej przez siedzibę administratora lub podmiotu przetwarzającego w Unii powinno się odbywać zgodnie z niniejszym rozporządzeniem, niezależnie od tego, czy samo przetwarzanie ma miejsce w Unii czy poza nią. Pojęcie „siedziba” zakłada skuteczne i faktycznie prowadzenie działalności poprzez stabilne struktury. Forma prawna takich struktur, niezależnie od tego, czy chodzi o oddział czy spółkę zależną o osobowości prawnej, nie jest w tym względzie czynnikiem decydującym.

- 20) Aby osoby fizyczne nie zostały pozbawione ochrony, która przysługuje im na mocy niniejszego rozporządzenia, przetwarzanie przez administratora niemającego siedziby w Unii danych osobowych podmiotów, które mają miejsce zamieszkania w Unii, powinno podlegać niniejszemu rozporządzeniu, jeżeli czynności przetwarzania wiążą się z oferowaniem takim podmiotom towarów lub usług w Unii, niezależnie od tego, czy pociąga to za sobą płatność. Aby stwierdzić, czy administrator oferuje towary lub usługi takim podmiotom danych w Unii, należy ustalić, czy jest oczywiste, że planuje on prowadzić interesy z podmiotami danych mającymi miejsce zamieszkania w co najmniej jednym państwie członkowskim Unii. O ile do ustalenia takiego zamiaru nie wystarczy sama dostępność w Unii strony internetowej administratora lub pośrednika lub adresu poczty elektronicznej i innych danych kontaktowych ani posługiwanie się językiem powszechnie stosowanym w państwie trzecim, w którym siedzibę ma administrator, o tyle potwierdzeniem oczywistości faktu, że administrator planuje oferować towary lub usługi podmiotom danych w Unii, mogą być czynniki takie, jak posługiwanie się językiem lub walutą powszechnie stosowanymi w co najmniej jednym państwie członkowskim oraz możliwość zamówienia towarów i usług w tym języku lub wzmianka o klientach lub użytkownikach mających miejsce zamieszkania w Unii.
- 21) Przetwarzanie danych osobowych podmiotów danych mających miejsce zamieszkania w Unii przez administratora niemającego siedziby w Unii powinno podlegać niniejszemu rozporządzeniu także wtedy, gdy wiąże się z monitorowaniem ich zachowania w Unii Europejskiej. Aby stwierdzić, czy czynność przetwarzania można uznać za „monitorowanie zachowania” podmiotów danych, należy ustalić, czy osoby fizyczne są obserwowane w internecie za pomocą technik przetwarzania danych polegających na profilowaniu osoby fizycznej, w szczególności w celu podjęcia decyzji jej dotyczącej lub przeanalizowania lub prognozowania jej osobistych preferencji, zachowań i postaw.
- 22) Niniejsze rozporządzenie powinno mieć zastosowanie do administratora niemającego siedziby w Unii także tam, gdzie na mocy prawa międzynarodowego publicznego stosuje się prawo krajowe państwa członkowskiego, na przykład na terenie misji dyplomatycznej lub placówki konsularnej państwa członkowskiego.

23) Zasady ochrony danych powinny mieć zastosowanie do wszelkich informacji o zidentyfikowanych lub możliwych do zidentyfikowania osobach fizycznych. Dane, w tym dane spseudonimizowane, które przy użyciu dodatkowych informacji można przypisać osobie fizycznej, należy uznać za informacje o możliwej do zidentyfikowania osobie fizycznej. Aby stwierdzić, czy dana osoba jest możliwa do zidentyfikowania, należy wziąć pod uwagę wszelkie racjonalnie prawdopodobne sposoby, którymi mogą się posłużyć administrator lub ktokolwiek inny w celu jej bezpośredniego lub pośredniego zidentyfikowania. Aby stwierdzić, czy dany sposób może z racjonalnym prawdopodobieństwem posłużyć do zidentyfikowania danej osoby, należy wziąć pod uwagę wszelkie obiektywne czynniki, takie jak koszt i czas potrzebne do jej zidentyfikowania, oraz uwzględnić zarówno technologie dostępną w momencie przetwarzania danych, jak i postęp techniczny. Zasady ochrony danych nie powinny więc mieć zastosowania do informacji anonimowych, tzn. informacji, które nie wiążą się ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną, ani do danych zanonimizowanych w taki sposób, że podmiotu danych w ogóle nie można zidentyfikować lub już nie można zidentyfikować. Niniejsze rozporządzenie nie dotyczy więc przetwarzania takich anonimowych informacji, w tym przetwarzania do celów statystycznych i naukowych.

23aa) Zasady ochrony danych nie powinny mieć zastosowania do osób zmarłych. Prawo krajowe państw członkowskich może przewidywać przepisy o przetwarzaniu danych osób zmarłych.

23a) Pseudonimizacja danych osobowych może ograniczyć zagrożenia wobec odnośnych podmiotów danych oraz pomóc administratorom i podmiotom przetwarzającym wywiązać się z obowiązku ochrony danych. Bezpośrednie wprowadzenie pojęcia „pseudonimizacja” w artykułach niniejszego rozporządzenia nie służy zatem wykluczeniu innych środków ochrony danych.

23b) (...)

- 23c) Aby zachęcić do stosowania pseudonimizacji podczas przetwarzania danych osobowych, należy umożliwić stosowanie u tego samego administratora środków pseudonimizacyjnych niewykluczających ogólnej analizy, o ile administrator ten przedsięwziął środki techniczne i organizacyjne niezbędne do wdrożenia przepisów niniejszego rozporządzenia, uwzględniając odnośne przetwarzanie danych i dbając, by dodatkowe informacje pozwalające przypisać dane osobowe konkretnemu podmiotowi danych były przechowywane osobno. Termin „administrator przetwarzający dane” powinien oznaczać także uprawnione osoby u tego administratora. W takim przypadku jednak administrator powinien dopilnować, by w metadanych nie znalazły się informacje o osobie(-bach) fizycznej(-nych) dokonującej(-cych) pseudonimizacji.
- 24) Osobom fizycznym, które korzystają z usług internetowych, mogą zostać przypisane identyfikatory internetowe, takie jak adresy IP czy identyfikatory plików cookie, generowane przez ich urządzenia, aplikacje, narzędzia i protokoły. Może to skutkować zostawianiem śladów, które w połączeniu z unikatowymi identyfikatorami i innymi informacjami uzyskiwanymi przez serwery mogą być wykorzystywane do tworzenia profili tych osób i do identyfikacji tych osób. Numerów identyfikacyjnych, danych o lokalizacji, identyfikatorów internetowych ani innych szczególnych czynników (...) nie należy samych w sobie uznawać za dane osobowe, jeżeli nie identyfikują one osoby fizycznej lub nie umożliwiają jej zidentyfikowania.
- 25) Zgoda powinna być udzielona jednoznacznie, w odpowiedni sposób umożliwiający podmiotowi danych dobrowolne, konkretne i świadome okazanie woli, bądź w formie pisemnego (w tym elektronicznego) lub ustnego oświadczenia, bądź jeśli wymagają tego szczególne okoliczności – wszelkiego innego klarownego działania podmiotu danych potwierdzającego jego przyzwolenie na przetwarzanie danych osobowych go dotyczących. Może to polegać na zaznaczeniu okienka wyboru podczas przeglądania strony internetowej lub też na innym oświadczeniu bądź zachowaniu, które w danym kontekście klarownie wskazuje, że podmiot danych zaakceptował proponowane przetwarzanie jego danych osobowych. Milczenie lub niepodjęcie działania nie powinny zatem oznaczać zgody. Jeżeli jest to technicznie możliwe i efektywne, podmiot danych może udzielić zgody na przetwarzanie, stosując odpowiednie ustawienie przeglądarki lub innej aplikacji. W takim przypadku wystarczy, by podmiot danych otrzymał informację niezbędną do dobrowolnego udzielenia konkretnej i świadomej zgody przy pierwszym korzystaniu z usługi. (...). Zgoda powinna dotyczyć wszystkich czynności przetwarzania dokonywanych w tym samym celu lub w tych samych celach. Jeżeli przetwarzanie służy wielorakim celom, potrzebna jest jednoznaczna zgoda na wszystkie te cele. Jeżeli podmiot danych ma udzielić zgody w odpowiedzi na elektroniczne zapytanie, zapytanie takie musi być jasne, zwięzłe i nie zakłócać niepotrzebnie korzystania z usługi, której dotyczy.

- 25a) Dane genetyczne należy zdefiniować jako dane osobowe o odziedziczonych lub nabytych cechach genetycznych osoby fizycznej, wynikające z analizy próbki biologicznej danej osoby, w szczególności z analizy chromosomów, kwasu dezoksyrybonukleinowego (DNA) lub kwasu rybonukleinowego (RNA) lub z analizy wszelkich innych elementów umożliwiających pozyskanie równoważnych informacji.
- 25aa) Niekiedy w momencie zbierania danych nie da się w pełni zidentyfikować celu przetwarzania danych, jeżeli chodzi o cel naukowy. Dlatego podmioty danych mogą udzielić zgody na niektóre obszary badań naukowych, o ile badania te trzymają się uznanych norm etycznych w zakresie badań naukowych. Podmioty danych powinny móc udzielić zgody tylko na niektóre obszary badań lub elementy projektów badawczych, o ile umożliwia to zamierzony cel i o ile nie powoduje to nieproporcjonalnego wysiłku z punktu widzenia ochrony.
- 26) Do danych osobowych dotyczących zdrowia należy zaliczyć (...) dane o stanie zdrowia podmiotu danych ujawniające informacje o przeszłym, obecnym lub przyszłym zdrowiu fizycznym lub psychicznym podmiotu danych, w tym informacje o zarejestrowaniu danej osoby fizycznej celem świadczenia usług opieki zdrowotnej (...), numer, symbol lub oznaczenie przypisane danej osobie w celu jednoznacznego zidentyfikowania jej do celów zdrowotnych, (...) informacje pochodzące z laboratoryjnych lub lekarskich badań części ciała lub płynów ustrojowych, w tym danych genetycznych i próbek biologicznych, (...) lub wszelkie informacje na przykład o chorobie, niepełnosprawności, ryzyku choroby, historii medycznej, leczeniu klinicznym lub aktualnym stanie fizjologicznym lub biomedycznym podmiotu danych, nienależnie od ich źródła, którym może być na przykład lekarz lub inny pracownik służby zdrowia, szpital, urządzenie medyczne lub badanie diagnostyczne *in vitro*.

- 27) Główną siedzibą administratora w Unii powinno być miejsce, w którym znajduje się jego centralna administracja w Unii, o ile decyzje co do celów i sposobów przetwarzania danych osobowych nie zapadają w innej siedzibie administratora w Unii. Wtedy bowiem za główną siedzibę należy uznać to drugie miejsce. Główną siedzibę administratora w Unii należy ustalić na podstawie obiektywnych kryteriów; powinna ona oznaczać skuteczne i faktycznie zarządzanie za pośrednictwem stabilnych struktur polegające na podejmowaniu najważniejszych decyzji co do celów (...) i sposobów przetwarzania. Kryterium to nie powinno zależeć od faktu, czy przetwarzanie danych osobowych rzeczywiście odbywa się w tej lokalizacji; obecność i wykorzystywanie środków technicznych i technologii do przetwarzania danych osobowych lub do czynności przetwarzania nie przesądzają same w sobie o takiej głównej siedzibie, nie są więc kryteriami wyznaczającymi główną siedzibę. Główną siedzibą podmiotu przetwarzającego powinno być miejsce, w którym znajduje się jego centralna administracja w Unii, a jeżeli nie ma on centralnej administracji w Unii – miejsce, w którym odbywają się główne czynności przetwarzania w Unii. Jeżeli sprawa dotyczy zarówno administratora, jak i podmiotu przetwarzającego, właściwym głównym organem nadzorczym powinien pozostać organ nadzorczy państwa członkowskiego, w którym administrator ma główną siedzibę, ale organ nadzorczy podmiotu przetwarzającego powinien być uznawany za zainteresowany organ nadzorczy i powinien uczestniczyć w procedurze współpracy przewidzianej w niniejszym rozporządzeniu. Organy nadzorcze państwa członkowskiego lub państw członkowskich, w których podmiot przetwarzający ma jedną siedzibę lub większą ich liczbę, nie powinny być w żadnym razie uznawane za zainteresowane organy nadzorcze, jeżeli projekt decyzji dotyczy wyłącznie administratora.
- Jeżeli przetwarzania dokonuje grupa przedsiębiorstw, za jej główną siedzibę należy uznać główną siedzibę przedsiębiorstwa sprawującego kontrolę, chyba że cel i sposoby przetwarzania określa inne przedsiębiorstwo.



- 28) Grupa przedsiębiorstw powinna obejmować przedsiębiorstwo sprawujące kontrolę oraz przedsiębiorstwa kontrolowane, przy czym przedsiębiorstwo sprawujące kontrolę powinno być przedsiębiorstwem, które może wywierać dominujący wpływ na pozostałe przedsiębiorstwa ze względu na przykład na strukturę właścicielską, udział finansowy lub przepisy regulujące jego działalność, lub też uprawnienia do nakazywania wdrożenia przepisów o ochronie danych osobowych. Za grupę przedsiębiorstw można uznać jednostkę złożoną z przedsiębiorstwa centralnego i przedsiębiorstw zależnych, w których przedsiębiorstwo centralne kontroluje przetwarzanie danych osobowych.
- 29) Szczególnej ochrony pod względem danych osobowych wymagają dzieci (...), gdyż mogą one być mniej świadome zagrożeń, konsekwencji, gwarancji i praw przysługujących im w związku z przetwarzaniem danych osobowych. (...). Chodzi tu w szczególności o korzystanie z danych osobowych dzieci do celów marketingowych lub do tworzenia profili osobowych lub profili użytkownika oraz o zbieranie danych dzieci, gdy korzystają one z usług skierowanych bezpośrednio do nich.
- 30) Wszelkie przetwarzanie danych osobowych powinno być zgodne z prawem i rzetelne. (...). Dla osób fizycznych powinno być przejrzyste, czy dotyczące ich dane osobowe są zbierane, wykorzystywane, przeglądane lub w inny sposób przetwarzane oraz w jakim stopniu dane te są lub będą przetwarzane. Zasada przejrzystości wymaga, by wszelkie informacje i wszelkie komunikaty związane z przetwarzaniem tych danych były łatwo dostępne i zrozumiałe oraz sformułowane jasnym i prostym językiem. Dotyczy to zwłaszcza informowania podmiotów danych o tożsamości administratora i celach przetwarzania oraz innych informacji mających zapewnić rzetelność i przejrzystość przetwarzania w stosunku do osób zainteresowanych, a także prawa zainteresowanych osób do uzyskania potwierdzenia i informacji o przetwarzanych danych ich dotyczących. Osobom fizycznym należy uświadomić zagrożenia, zasady, gwarancje i prawa związane z przetwarzaniem danych osobowych oraz sposoby korzystania z praw przysługujących im w związku z tym przetwarzaniem. Wyraźne, uzasadnione i określone w momencie zbierania danych powinny być w szczególności konkretne cele ich przetwarzania. Dane powinny być ilościowo i treściowo odpowiednie (...) do celów, w których są przetwarzane; wymaga to w szczególności dopilnowania, by zebrane dane nie były nadmierne i by okres ich przechowywania był ograniczony do ścisłego minimum. (...). Dane osobowe powinny być przetwarzane tylko wtedy, gdy celu przetwarzania nie można racjonalnie osiągnąć innymi sposobami. Aby zapobiec przechowywaniu danych przez okres dłuższy, niż jest to niezbędne, administrator powinien ustalić termin ich usuwania lub okresowego przeglądu.

Należy podjąć wszelkie racjonalne działania gwarantujące poprawienie lub usunięcie danych osobowych, które są nieścisle. Dane osobowe powinny być przetwarzane w sposób zapewniający im odpowiednie bezpieczeństwo i odpowiednią poufność, w tym ochronę przed nieuprawnionym dostępem do nich samych i do sprzętu służącego ich przetwarzaniu oraz przed nieuprawnionym korzystaniem z tych danych i z tego sprzętu.

- 31) Aby przetwarzanie danych było zgodne z prawem, powinno się odbywać na podstawie zgody osoby zainteresowanej lub na innej uzasadnionej podstawie prawnej przewidzianej prawem: albo w niniejszym rozporządzeniu, albo w innym prawie Unii lub prawie państwa członkowskiego, o których mowa w niniejszym rozporządzeniu, w tym musi się ono odbywać z poszanowaniem obowiązku prawnego, któremu podlega administrator, lub z poszanowaniem umowy, której stroną jest podmiot danych, lub w celu podjęcia działań na wniosek podmiotu danych przed zawarciem umowy.
- 31a) Ilekcroć w niniejszym rozporządzeniu jest mowa o podstawie prawnej lub środku ustawodawczym, niekoniecznie wymaga to aktu ustawodawczego przyjętego przez parlament – bez uszczerbku dla wymogów wynikających z porządku konstytucyjnego danego państwa członkowskiego – jednak taka podstawa prawna lub taki środek ustawodawczy powinny być jasne i precyzyjne, a ich zastosowanie przewidywalne dla osób im podlegających – jak wymaga tego orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej i Europejskiego Trybunału Praw Człowieka.
- 32) Jeśli przetwarzanie odbywa się na podstawie zgody podmiotu danych, administrator powinien być w stanie wykazać, że podmiot danych udzielił zgody na operację przetwarzania. Zwłaszcza w przypadku pisemnego oświadczenia składanego w innej sprawie powinny istnieć gwarancje, tak by podmiot danych był świadomy udzielenia zgody oraz jej zakresu. Oświadczenie o udzieleniu zgody przygotowane przez administratora powinno mieć zrozumiałą i łatwo dostępną formę, być sformułowane jasnym i prostym językiem, a jego treść nie powinna odbiegać charakterem od ogólnego kontekstu. Aby udzielenie zgody było świadome, podmiot danych powinien znać przynajmniej tożsamość administratora oraz zamierzone cele przetwarzania danych osobowych; udzielenia zgody nie należy uznawać za dobrowolne, jeżeli podmiot danych nie ma rzeczywistego i wolnego wyboru oraz nie może odmówić ani wycofać zgody bez poniesienia szkody.
- 33) (...)

- 34) Aby istniała gwarancja dobrowolności, zgoda nie powinna stanowić prawomocnej podstawy prawnej przetwarzania danych osobowych w szczególnej sytuacji, w której istnieje wyraźny brak równowagi między podmiotem danych a administratorem i ze względu na tę nierównowagę jest mało prawdopodobne, by zgody udzielono dobrowolnie we wszystkich okolicznościach tej konkretnej sytuacji. Zgody nie uważa się za dobrowolną, jeżeli nie można jej udzielić z osobna na różne operacje przetwarzania danych – mimo że w danym przypadku byłoby to stosowne – lub gdy od zgody uzależnione jest wykonanie umowy, choć do jej wykonania nie jest ona niezbędna, a podmiot danych nie może w racjonalny sposób bez zgody uzyskać równoważnych usług z innego źródła.
- 35) Przetwarzanie powinno być zgodne z prawem, jeżeli jest ono niezbędne w kontekście umowy lub zamiaru zawarcia umowy.
- 35a) Niniejsze rozporządzenie zawiera ogólne przepisy o ochronie danych oraz przewiduje, że w przypadkach szczególnych państwa członkowskie są uprawnione do ustanawiania także krajowych przepisów o ochronie danych. Rozporządzenie nie wyklucza więc możliwości istnienia prawa państw członkowskich określającego okoliczności konkretnych sytuacji związanych z przetwarzaniem danych, w tym dokładniejszego określania warunków, które decydują o zgodności przetwarzania z prawem. Prawo krajowe może też przewidywać szczegółowe warunki przetwarzania dla konkretnych sektorów oraz dla przetwarzania szczególnych kategorii danych.
- 36) Jeżeli przetwarzanie odbywa się w celu wypełnienia obowiązku prawnego, któremu podlega administrator, lub jeżeli jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej, podstawę (...) przetwarzania powinno stanowić prawo Unii lub prawo krajowe państwa członkowskiego. (...). Prawo Unii lub prawo krajowe powinno określać także cel przetwarzania. Ponadto (...) podstawa ta może doprecyzowywać ogólne warunki rozporządzenia regulujące zgodność przetwarzania z prawem, określać sposoby wskazywania administratora, rodzaj danych podlegających przetwarzaniu, zainteresowane podmioty danych, podmioty, którym można ujawniać dane, celowość, okres przechowywania oraz inne środki zapewniające zgodność z prawem i rzetelność przetwarzania.

Prawo Unii lub prawo krajowe powinny określać także, czy administratorem wykonującym zadanie realizowane w interesie publicznym lub w ramach sprawowania władzy publicznej powinien być organ publiczny czy inna osoba fizyczna lub prawna podlegająca prawu publicznemu lub prawu prywatnemu, np. stowarzyszenie zawodowe, jeżeli uzasadnia to interes publiczny, w tym cele zdrowotne, takie jak zdrowie publiczne, ochrona socjalna oraz zarządzanie usługami opieki zdrowotnej.

- 37) Przetwarzanie danych osobowych należy uznać za zgodne z prawem również wtedy, gdy jest niezbędne do ochrony interesu, który ma istotne znaczenie dla życia podmiotu danych lub innej osoby. (...). Niektóre rodzaje przetwarzania danych mogą służyć zarówno ważnemu interesowi publicznemu, jak i żywotnym interesom podmiotu danych, np. gdy przetwarzanie jest niezbędne do celów humanitarnych, w tym monitorowania epidemii i jej rozprzestrzeniania się lub w nadzwyczajnych sytuacjach humanitarnych, zwłaszcza w przypadku klęsk żywiołowych.
- 38) Podstawę prawną przetwarzania mogą stanowić uzasadnione interesy administratora, w tym administratora, któremu dane mogą zostać ujawnione, lub strony trzeciej, pod warunkiem że charakteru nadrzędnego nie mają interesy lub podstawowe prawa i wolności podmiotu danych. Uzasadniony interes może istnieć na przykład wtedy, gdy zachodzi istotny i odpowiedni związek między podmiotem danych a administratorem, np. gdy podmiot danych jest klientem administratora lub świadczy wobec niego usługi. (...) Aby stwierdzić istnienie uzasadnionego interesu, należałoby w każdym razie przeprowadzić dokładną ocenę, w tym ocenę tego, czy w czasie i w kontekście, w którym zbierane są dane, podmiot danych ma prawo się spodziewać, że może nastąpić przetwarzanie danych w tym celu. Podczas takiej oceny należy w szczególności wziąć pod uwagę fakt, czy podmiotem danych nie jest dziecko, zważywszy że dzieci wymagają szczególnej ochrony. Podmiot danych powinien mieć prawo sprzeciwić się przetwarzaniu ze względu na swoją indywidualną sytuację i w sposób wolny od opłat. Aby zapewnić przejrzystość, administrator powinien być zobowiązany wyraźnie poinformować podmiot danych o realizowanych przez siebie uzasadnionych interesach oraz o prawie do sprzeciwu, a także powinien być zobowiązany interesy te udokumentować. (...)

38a) Administratorzy, którzy są częścią grupy przedsiębiorstw lub instytucji zależnej od podmiotu centralnego, mogą mieć uzasadniony interes w przekazywaniu danych osobowych w ramach grupy przedsiębiorstw do wewnętrznych celów administracyjnych, co dotyczy też przetwarzania danych osobowych klientów lub pracowników. Pozostaje to bez wpływu na (...) ogólne zasady przekazywania danych osobowych w ramach grupy przedsiębiorstw przedsiębiorstwu mieszczącemu się w państwie trzecim.

39) Przetwarzanie danych w zakresie bezwzględnie niezbędnym do zapewnienia bezpieczeństwa sieci i informacji – tj. zapewnienia odporności sieci lub systemu informacyjnego na danym poziomie poufności na przypadkowe zdarzenia albo niezgodne z prawem lub nieprzyjemne działania naruszające dostępność, autentyczność, integralność i poufność przechowywanych lub przesyłanych danych – oraz bezpieczeństwa związanych z nimi usług oferowanych lub udostępnianych poprzez te sieci i systemy przez organy publiczne, zespoły reagowania na zagrożenia komputerowe (CERT), zespoły reagowania na komputerowe incydenty naruszające bezpieczeństwo (CSIRT), dostawców sieci i usług łączności elektronicznej oraz dostawców technologii i usług w zakresie bezpieczeństwa jest uzasadnionym interesem *zainteresowanego* administratora. Może to obejmować na przykład zapobieganie nieuprawnionemu dostępowi do sieci łączności elektronicznej i rozprowadzaniu złośliwych kodów, przerywanie ataków typu „odmowa usługi”, a także przeciwdziałanie uszkodzeniu systemów komputerowych i systemów łączności elektronicznej. Uzasadnionym interesem zainteresowanego administratora jest również przetwarzanie danych osobowych ściśle niezbędnych do zapobiegania oszustwom. Za działanie wykonywane w uzasadnionym interesie można uznać przetwarzanie danych osobowych do celów marketingu bezpośredniego.

- 40) Przetwarzanie danych osobowych do celów innych niż cele, w których dane zostały pierwotnie zebrane, powinno być dozwolone wyłącznie wtedy, gdy jest zgodne z celami, w których dane zostały pierwotnie zebrane. W takim przypadku nie jest wymagana osobna podstawa prawna inna niż podstawa prawna, która umożliwiła zebranie danych. (...) Jeżeli przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi, prawo Unii lub prawo państwa członkowskiego mogą określać i precyzować zadania i cele, w których dalsze przetwarzanie powinno być uznawane za zgodne z prawem. Za operacje przetwarzania zgodne z prawem i z pierwotnymi celami należy uznać dalsze przetwarzanie do celów archiwizacyjnych w interesie publicznym lub do celów (...) statystycznych, naukowych lub historycznych (...), lub do celów przyszłego rozstrzygnięcia sporów. Podstawa prawna zbierania i przetwarzania danych osobowych przewidziana prawem Unii lub prawem państwa członkowskiego może być również podstawą prawną dalszego przetwarzania do innych celów, jeżeli cele te są zgodne z wyznaczonym zadaniem, a administratorowi przysługuje prawo zbierania danych do tych innych celów.

Aby ustalić, czy cel dalszego przetwarzania danych jest zgodny z celem, w którym dane zostały pierwotnie zebrane, administrator – po spełnieniu wszystkich wymogów warunkujących zgodność pierwotnego przetwarzania z prawem – powinien uwzględnić między innymi wszelkie powiązania pomiędzy tymi celami a celami zamierzonego dalszego przetwarzania, kontekst, w którym dane zostały zebrane (w tym racjonalne oczekiwania podmiotów danych co do dalszego wykorzystania danych), charakter danych osobowych, konsekwencje zamierzonego dalszego przetwarzania dla podmiotów danych oraz istnienie odpowiednich gwarancji zarówno podczas pierwotnej, jak i zamierzonej operacji przetwarzania. Jeśli taki zamierzony inny cel nie jest zgodny z celem pierwotnym, w którym dane zostały zebrane, administrator powinien uzyskać zgodę podmiotu danych na realizację tego innego celu lub powinien oprzeć przetwarzanie na innej uzasadnionej podstawie zapewniającej zgodność przetwarzania z prawem, w szczególności jeżeli jest przewidziana prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator. (...).

W każdym przypadku należy zapewnić stosowanie zasad przewidzianych w niniejszym rozporządzeniu, w szczególności stosowanie zasady informowania podmiotu danych o tych innych celach oraz o jego prawach, w tym prawie do sprzeciwu. (...) Wskazanie przez administratora ewentualnych działań przestępczych czy zagrożeń dla bezpieczeństwa publicznego oraz przekazanie odnośnych danych właściwym organom należy uznać za zrealizowanie przez administratora uzasadnionego interesu. Jednak takie przekazanie w uzasadnionym interesie administratora lub dalsze przetwarzanie danych osobowych powinno być zabronione, jeżeli jest niezgodne z prawnym, służbowym lub innym wiążącym obowiązkiem dochowania tajemnicy.

- 41) Dane osobowe, które z racji swego charakteru są szczególnie newralgiczne (...) w związku z podstawowymi prawami i wolnościami, zasługują na szczególną ochronę, gdyż kontekst ich przetwarzania może powodować duże zagrożenia dla podstawowych praw i wolności. Do danych takich powinny zaliczać się także dane osobowe ujawniające pochodzenie rasowe lub etniczne, przy czym użycie w niniejszym rozporządzeniu terminu „pochodzenie rasowe” nie oznacza, że Unia Europejska akceptuje teorie sugerujące istnienie osobnych ras ludzkich. Takich danych nie należy przetwarzać, chyba że niniejsze rozporządzenie dopuszcza ich przetwarzanie w szczególnych przypadkach; przy czym należy uwzględnić, że prawo państw członkowskich może ustanowić przepisy szczegółowe o ochronie danych dostosowujące zastosowanie przepisów niniejszego rozporządzenia, by można było wypełnić obowiązki prawne lub wykonać zadanie realizowane w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. Oprócz wymogów szczegółowych mających zastosowanie do takiego przetwarzania, zastosowanie powinny mieć zasady ogólne i inne przepisy niniejszego rozporządzenia, zwłaszcza jeżeli chodzi o warunki zgodności przetwarzania z prawem. Należy wyraźnie przewidzieć odstępstwa od ogólnego zakazu przetwarzania takich danych osobowych szczególnych kategorii, m.in. w razie wyrażnej zgody podmiotu danych lub ze względu na szczególne potrzeby, zwłaszcza gdy przetwarzanie danych odbywa się w ramach uzasadnionych działań niektórych stowarzyszeń lub fundacji, których celem jest umożliwienie korzystania z podstawowych wolności.

Dane osobowe szczególnych kategorii można przetwarzać także wtedy, gdy zostały w sposób ewidentny podane do wiadomości publicznej lub dobrowolnie na wniosek podmiotu danych przekazane administratorowi w konkretnym celu określonym przez podmiot danych, o ile przetwarzanie odbywa się w interesie podmiotu danych.

Prawo państwa członkowskiego i prawo Unii mogą przewidywać, że w niektórych przypadkach wyraźna zgoda podmiotu danych nie może uchylić ogólnego zakazu przetwarzania danych szczególnych kategorii.

- 42) Na odstępstwa od zakazu przetwarzania newralgicznych kategorii danych należy także zezwolić – o ile przewiduje to prawo Unii lub prawo państwa członkowskiego i podlega to odpowiednim gwarancjom chroniącym dane osobowe i inne prawa podstawowe – jeżeli uzasadnia to (...) interes publiczny, zwłaszcza przetwarzanie danych w dziedzinie prawa pracy, prawa zabezpieczenia społecznego i ochrony socjalnej, w tym emerytur, oraz do celów bezpieczeństwa, monitorowania i ostrzegania zdrowotnego, zapobieganie chorobom zakaźnym i innych poważnym zagrożeniom zdrowotnym lub ich kontrola lub zapewnianie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej i usług zdrowotnych oraz produktów leczniczych lub wyrobów medycznych, lub ocena polityki publicznej w dziedzinie zdrowia, także przez tworzenie wskaźników jakości i działań.

Może to służyć celom zdrowotnym, w tym zdrowiu publicznemu oraz zarządzaniu usługami opieki zdrowotnej, zwłaszcza zapewnianiu jakości i ekonomicznej zasadności procedur stosowanych do rozstrzygania roszczeń w sprawie świadczeń i usług w ramach systemu ubezpieczeń zdrowotnych, lub celom archiwizacyjnym w interesie publicznym, lub celom (...) historycznym, statystycznym i naukowym.

Należy także przewidzieć odstępstwo pozwalające przetwarzać takie dane, jeżeli jest to niezbędne do ustalenia, realizacji lub obrony roszczeń prawnych, niezależnie od rodzaju postępowania – sądowego, administracyjnego czy innego pozasądowego.



- 42a) Dane osobowe szczególnych kategorii zasługujące na większą ochronę mogą być przetwarzane do celów zdrowotnych wyłącznie wtedy, gdy jest to niezbędne do realizacji tych celów z korzyścią dla osób fizycznych i ogółu społeczeństwa, zwłaszcza w kontekście zarządzania usługami i systemami opieki zdrowotnej i socjalnej, w tym przetwarzania takich danych przez organy zarządcze i centralne krajowe organy ds. zdrowia do celów kontroli jakości, pozyskiwania informacji zarządczych oraz ogólnego krajowego i lokalnego nadzoru nad systemem opieki zdrowotnej i socjalnej oraz zapewniania ciągłości opieki zdrowotnej lub socjalnej oraz transgranicznej opieki zdrowotnej lub do celów bezpieczeństwa, monitorowania i ostrzegania zdrowotnego lub do celów archiwizacyjnych w interesie publicznym, historycznych, statystycznych lub naukowych, a także na potrzeby analiz prowadzonych w interesie publicznym w dziedzinie zdrowia publicznego. Niniejsze rozporządzenie powinno zatem przewidywać zharmonizowane warunki przetwarzania szczególnych kategorii danych osobowych dotyczących zdrowia, ze względu na szczególne potrzeby, zwłaszcza gdy dane te są przetwarzane w określonych celach zdrowotnych przez osoby podlegające prawnemu obowiązkowi dochowania tajemnicy służbowej (...). Prawo Unii lub prawo państwa członkowskiego powinny przewidywać konkretne, odpowiednie środki chroniące prawa podstawowe i dane osobowe osób fizycznych. (...).
- 42b) Niezbędne ze względu na przesłanki interesu publicznego w dziedzinie zdrowia publicznego może być przetwarzanie danych osobowych specjalnych kategorii (...) bez zgody podmiotu danych. Przetwarzanie to podlega konkretnym, odpowiednim środkom chroniącym prawa i wolności osób fizycznych. W tym kontekście „zdrowie publiczne” należy interpretować zgodnie z definicją z rozporządzenia (WE) nr 1338/2008 Parlamentu Europejskiego i Rady z dnia 16 grudnia 2008 r. w sprawie statystyk Wspólnoty w zakresie zdrowia publicznego oraz zdrowia i bezpieczeństwa w pracy, czyli jako wszystkie elementy związane ze zdrowiem, mianowicie stan zdrowia, w tym zachorowalność i niepełnosprawność, czynniki warunkujące stan zdrowia, potrzeby w zakresie opieki zdrowotnej, zasoby opieki zdrowotnej, oferowane usługi opieki zdrowotnej i powszechny dostęp do nich, wydatki na opiekę zdrowotną i sposób jej finansowania oraz przyczyny zgonów. Przetwarzanie danych osobowych dotyczących zdrowia ze względu na przesłanki interesu publicznego nie powinno skutkować przetwarzaniem danych osobowych do innych celów przez strony trzecie, takie jak pracodawcy, zakłady ubezpieczeń i banki.

- 43) W interesie publicznym obywateli odbywa się ponadto przetwarzanie danych osobowych przez organy publiczne do celów – określonych w prawie konstytucyjnym lub prawie międzynarodowym publicznym – oficjalnie uznanych stowarzyszeń religijnych.
- 44) Jeżeli w trakcie działań wyborczych funkcjonowanie systemu demokratycznego w państwie członkowskim wymaga zbierania przez partie polityczne danych o opiniach politycznych obywateli, można zezwolić na przetwarzanie tych danych ze względu na przesłanki interesu publicznego pod warunkiem ustanowienia odpowiednich gwarancji.
- 45) Jeżeli dane przetwarzane przez administratora nie pozwalają mu zidentyfikować osoby fizycznej (...), nie powinien on mieć obowiązku uzyskania dodatkowych informacji w celu zidentyfikowania podmiotu danych wyłącznie po to, by zastosować się do przepisów niniejszego rozporządzenia. (...). Administrator nie powinien jednak odmawiać przyjęcia dodatkowych informacji, których dostarcza podmiot danych w celu skorzystania ze swoich praw.
- 46) Zasada przejrzystości wymaga, by wszelkie informacje kierowane do ogółu społeczeństwa lub podmiotu danych były łatwo dostępne i zrozumiałe, by były formułowane jasnym i prostym językiem, a dodatkowo – w stosownym przypadku – wizualizowane. Informacje te mogą być także zapewniane w formie elektronicznej, na przykład za pomocą strony internetowej, gdy są kierowane do ogółu społeczeństwa. Dotyczy to w szczególności sytuacji takich jak reklama w internecie, gdy duża liczba podmiotów i złożoność technologiczna działań sprawiają, że podmiotowi danych trudno jest dowiedzieć się i zrozumieć, czy dotyczące go dane osobowe są zbierane, przez kogo oraz w jakim celu. 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 go bez trudu zrozumieć.

- 47) Należy przewidzieć sposoby ułatwiające podmiotowi danych korzystanie z praw przysługujących mu na mocy niniejszego rozporządzenia, w tym mechanizmy składania wniosków, (...) w szczególności wniosków o dostęp do danych, ich poprawienie i usunięcie, oraz mechanizmy korzystania z prawa do sprzeciwu. Administrator powinien więc zapewnić także możliwość składania wniosków drogą elektroniczną, zwłaszcza gdy dane osobowe są przetwarzane drogą elektroniczną. Administrator powinien być zobowiązany udzielić odpowiedzi na wnioski podmiotów danych bez zbędnej zwłoki – najpóźniej w stałym terminie jednego miesiąca, a jeżeli nie zamierza zastosować się do wniosku podmiotu danych – podać tego przyczyny.

Jeżeli jednak wnioski są ewidentnie nieuzasadnione lub nadmierne – tak jak wtedy, gdy podmiot danych nieracjonalnie i ustawicznie żąda informacji lub gdy nadużywa prawa do informacji, np. podając fałszywe lub mylne dane przy występowaniu z wnioskiem, administrator może odmówić podjęcia działań względem wniosku.

- 48) Zasady rzetelnego i przejrzystego przetwarzania wymagają, by podmiot danych był informowany (...) o prowadzeniu operacji przetwarzania i o jej celach (...). Administrator powinien podać podmiotowi danych wszelkie inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania. Ponadto należy poinformować podmiot danych o fakcie profilowania oraz o konsekwencjach takiego profilowania. Jeżeli zbiera się dane od podmiotu danych, należy go też poinformować, czy ma on obowiązek je podać, oraz o konsekwencjach ich niepodania.
- 49) Informacje o przetwarzaniu danych osobowych dotyczących podmiotu danych należy mu przekazać w momencie zbierania danych, a jeżeli danych nie zbiera się od podmiotu danych – w rozsądnym terminie, zależnie od okoliczności sprawy. Jeżeli dane można zasadnie ujawnić innemu odbiorcy, należy poinformować o tym podmiot danych w momencie pierwszorazowego ujawnienia danych temu odbiorcy. Jeżeli administrator planuje przetwarzać dane w celu innym niż cel, w których dane zostały zebrane, powinien on przed takim dalszym przetwarzaniem poinformować podmiot danych o tym innym celu oraz dostarczyć mu innych niezbędnych informacji. Jeżeli podmiotowi danych nie można podać pochodzenia danych, ponieważ korzystano z różnych źródeł, odnośne informacje należy przedstawić w sposób ogólny.

- 50) Nałożenie tego obowiązku nie jest jednak konieczne, jeżeli podmiot danych dysponuje już tymi informacjami lub jeżeli rejestracja lub ujawnienie danych są wyraźnie przewidziane prawem, lub jeżeli poinformowanie podmiotu danych okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku. Ten ostatni wariant dotyczy zwłaszcza sytuacji, w której dane są przetwarzane do celów archiwizacyjnych w interesie publicznym oraz do celów (...) historycznych, statystycznych lub naukowych; w takim przypadku można wziąć pod uwagę liczbę podmiotów danych, wiek danych oraz wszelkie przyjęte odpowiednie gwarancje.
- 51) Każda osoba fizyczna powinna mieć prawo dostępu do zebranych danych jej dotyczących oraz móc łatwo korzystać z tego prawa w rozsądnych odstępach czasu, by mieć świadomość przetwarzania danych i móc zweryfikować jego zgodność z prawem. *Odnosi się to m.in. do prawa dostępu osób fizycznych do danych osobowych dotyczących ich zdrowia, na przykład do danych w dokumentacji medycznej zawierającej takie informacje, jak diagnoza, wyniki badań, oceny dokonywane przez lekarzy prowadzących, stosowane terapie czy przeprowadzone zabiegi.* Dlatego też każdy podmiot danych powinien mieć prawo do wiedzy i informacji, w szczególności w jakich celach dane są przetwarzane, w miarę możliwości przez jaki okres, jacy odbiorcy otrzymują dane, jakie są założenia ewentualnego automatycznego przetwarzania danych oraz jakie mogą być konsekwencje takiego przetwarzania, przynajmniej w przypadku profilowania. Prawo to nie powinno negatywnie wpływać na prawa i wolności innych osób, w tym tajemnice handlowe lub własność intelektualną, w szczególności na prawa autorskie chroniące oprogramowanie. Względy te nie powinny jednak powodować odmowy udzielenia podmiotowi danych jakichkolwiek informacji. Jeżeli administrator przetwarza duże ilości informacji o podmiocie danych, może przed podaniem informacji zażądać, by podmiot danych sprecyzował, których informacji lub których czynności przetwarzania dotyczy wniosek.
- 52) Administrator powinien skorzystać z wszelkich racjonalnych środków w celu zweryfikowania tożsamości podmiotu danych, który zwraca się z wnioskiem o dostęp, w szczególności w kontekście usług internetowych i identyfikatorów internetowych. (...) Weryfikacja tożsamości powinna obejmować cyfrową identyfikację podmiotu danych, np. poprzez mechanizm uwierzytelniania, taki jak te same dane uwierzytelniające, których podmiot danych używa, by zalogować się do usług internetowych oferowanych przez administratora. Administrator nie powinien zatrzymywać danych osobowych wyłącznie po to, by móc odpowiadać na potencjalne wnioski.

- 53) Każda osoba fizyczna powinna mieć prawo do poprawienia danych osobowych jej dotyczących oraz prawo do „bycia zapomnianym”, jeżeli zatrzymywanie takich danych nie jest zgodne z niniejszym rozporządzeniem lub z prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator. Podmioty danych powinny w szczególności mieć prawo do tego, by ich dane osobowe zostały usunięte i przestały być przetwarzane, jeżeli dane te nie są już niezbędne do celów, w których były zebrane lub w inny sposób przetwarzane, jeżeli podmioty danych cofnęły zgodę na przetwarzanie lub jeżeli wnoszą sprzeciw wobec przetwarzania danych osobowych ich dotyczących, lub jeżeli przetwarzanie ich danych osobowych nie jest z innego powodu zgodne z niniejszym rozporządzeniem. Prawo to ma szczególne znaczenie wtedy, gdy podmiot danych wyraził zgodę jako dziecko, gdy nie był w pełni świadomy zagrożeń związanych z przetwarzaniem, a w późniejszym czasie chce usunąć takie dane osobowe, zwłaszcza z internetu. Podmiot danych powinien móc skorzystać z tego prawa, mimo że już nie jest dzieckiem. Niemniej dalsze zatrzymywanie danych powinno być uznane za zgodne z prawem, jeżeli jest niezbędne do *korzystania z prawa wolności wypowiedzi i informacji, do wywiązania się z obowiązku prawnego, do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi, ze względu na przesłanki interesu publicznego w dziedzinie zdrowia publicznego, do celów archiwizacyjnych w interesie publicznym, do celów (...) historycznych, statystycznych i naukowych lub do ustalenia, realizacji lub obrony roszczeń prawnych*.
- 54) Aby wzmocnić prawo do „bycia zapomnianym” w internecie, należy także w taki sposób rozszerzyć prawo do usunięcia danych, by administrator, który upublicznił te dane, miał obowiązek poinformować administratorów, którzy przetwarzają takie dane, (...) żeby usunęli wszelkie łącza do tych danych, kopie tych danych lub ich replikacje.

Aby zapewnić przekazanie wyżej określonych informacji, administrator powinien poczynić (...) racjonalne kroki – z uwzględnieniem dostępnych technologii i dostępnych mu środków – w tym przedsięwziąć środki techniczne w odniesieniu do danych, za których publikację odpowiada. (...).

54a) Wśród metod pozwalających ograniczyć przetwarzanie danych osobowych mogą się znaleźć między innymi: czasowe przeniesienie wybranych danych do innego systemu przetwarzania lub uniemożliwienie użytkownikom dostępu do wybranych danych, lub czasowe usunięcie opublikowanych danych ze strony internetowej. W zautomatyzowanych zbiorach danych przetwarzanie danych osobowych należy zasadniczo ograniczyć środkami technicznymi, a fakt ograniczenia przetwarzania danych osobowych – zaznaczyć w systemie tak, by było jasne, że przetwarzanie tych danych jest ograniczone.

55) Aby zyskać jeszcze większą kontrolę nad własnymi danymi (...) w kontekście zautomatyzowanego przetwarzania danych osobowych, podmiot danych powinien także móc otrzymywać dotyczące go dane osobowe, których dostarczył administratorowi, w ustrukturyzowanym, powszechnie używanym i maszynowo czytelnym formacie oraz przenosić je do innego administratora.

Prawo to powinno mieć zastosowanie wtedy, gdy podmiot danych dostarczył danych osobowych na podstawie własnej zgody lub w związku z wykonaniem umowy. Nie powinno mieć zastosowania, jeżeli przetwarzanie opiera się na podstawie prawnej innej niż zgoda lub umowa. Z prawa tego – z uwagi na jego charakter – nie powinno się korzystać w stosunku do administratorów przetwarzających dane w ramach wykonywania obowiązków publicznych. Dlatego nie powinno ono mieć zastosowania w szczególności wtedy, gdy przetwarzanie danych osobowych jest niezbędne do wywiązania się z obowiązku prawnego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

Przysługujące podmiotowi danych prawo do przenoszenia danych osobowych nie nakłada na administratorów obowiązku prowadzenia lub wprowadzenia kompatybilnych technicznie systemów przetwarzania danych.

Jeżeli określony zestaw danych osobowych odnosi się do więcej niż jednego podmiotu danych, prawo do przenoszenia danych nie powinno powodować uszczerbku dla wymogu, by przetwarzanie danych osobowych dotyczących innego podmiotu danych było zgodne z prawem w świetle niniejszego rozporządzenia. Prawo to powinno pozostawać bez uszczerbku także dla prawa podmiotu danych do spowodowania, by dane osobowe zostały usunięte, oraz bez uszczerbku dla ograniczeń tego prawa określonych w niniejszym rozporządzeniu i nie powinno w szczególności skutkować usunięciem danych osobowych dotyczących podmiotu danych, których podmiot ten dostarczył do wykonania umowy, o ile i w takim zakresie, w jakim dane te są niezbędne do wykonania tej umowy. (...)

- 56) Nawet jeżeli dane osobowe mogą być przetwarzane zgodnie z prawem (...), gdyż przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi lub ze względu na (...) uzasadnione interesy administratora lub strony trzeciej, każdemu podmiotowi danych powinno przysługiwać prawo sprzeciwu wobec przetwarzania danych dotyczących jego indywidualnej sytuacji. Za wykazanie, że ewidentne uzasadnione interesy administratora mogą mieć charakter nadrzędny wobec interesów lub podstawowych praw i wolności podmiotu danych, powinien odpowiadać administrator.
- 57) Jeżeli dane osobowe są przetwarzane do celów marketingu bezpośredniego, podmiot danych powinien mieć prawo do tego, by w sposób prosty, skuteczny i wolny od opłat wnieść sprzeciw wobec takiego przetwarzania, pierwotnego lub dalszego.

- 58) Podmiot danych powinien mieć prawo do tego, by nie podlegać decyzji oceniającej jego czynniki osobowe (...), która opiera się wyłącznie na przetwarzaniu automatycznym, wywołuje wobec tego podmiotu skutki prawne lub znacznie na niego wpływa, jak np. automatyczne odrzucenie elektronicznego wniosku kredytowego czy elektroniczne metody rekrutacji bez interwencji ludzkiej. Do takiego przetwarzania zalicza się też „profilowanie” – które polega na jakimkolwiek zautomatyzowanym przetwarzaniu danych osobowych pozwalającym ocenić czynniki osobowe osoby fizycznej, a w szczególności analizować lub prognozować aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się – o ile wywołuje skutki prawne względem tej osoby lub znacznie na nią wpływa. Niemniej podejmowanie decyzji na podstawie takiego przetwarzania, w tym profilowania, powinno być dozwolone, gdy jest dopuszczone prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator, w tym do monitorowania i do prewencji oszustw i uchylania się od podatków oraz do zapewniania bezpieczeństwa i niezawodności usług świadczonych przez administratora, lub gdy jest niezbędne do zawarcia lub wykonania umowy między podmiotem danych a administratorem, lub gdy podmiot danych udzielił wyraźnej zgody. Przetwarzanie takie powinno zawsze podlegać odpowiednim gwarancjom, w tym konkretnemu informowaniu podmiotu danych i prawu do uzyskania interwencji ludzkiej, prawu do wyrażenia własnego stanowiska, prawu do uzyskania wyjaśnienia co do decyzji wynikłej z takiej oceny oraz prawu do zakwestionowania takiej decyzji. Aby zapewnić rzetelność i przejrzystość przetwarzania wobec podmiotu danych, mając na uwadze konkretne okoliczności i kontekst przetwarzania danych osobowych, administrator powinien stosować odpowiednie matematyczne lub statystyczne procedury profilowania, wdrożyć środki techniczne i organizacyjne gwarantujące w szczególności korektę czynników nieścisłości danych i maksymalne zmniejszenie ryzyka błędów, zabezpieczyć dane osobowe w sposób uwzględniający potencjalne zagrożenia dla interesów i praw podmiotu danych oraz zapobiegający m.in. skutkom w postaci dyskryminacji osób fizycznych z uwagi na pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania, przynależność do związków zawodowych, stan genetyczny lub zdrowotny, orientację seksualną lub skutkujący środkami mającymi taki efekt. Automatyczne podejmowanie decyzji i profilowanie oparte na danych osobowych specjalnych kategoriach powinny być dozwolone wyłącznie pod konkretnymi warunkami.



- 58a) Profilowanie jako takie podlega przepisom (ogólnym) niniejszego rozporządzenia, które obwarowują przetwarzanie danych osobowych (podstawy prawne przetwarzania, zasady ochrony danych itp.) konkretnymi gwarancjami (np. obowiązkiem przeprowadzenia w niektórych przypadkach oceny skutków lub przepisami o udzieleniu danej osobie określonych informacji). Możliwość wydawania wskazówek w tym kontekście powinna mieć Europejska Rada Ochrony Danych.
- 59) Prawem Unii lub prawem państwa członkowskiego można nałożyć ograniczenia na konkretne zasady oraz na prawo do informacji, dostępu, poprawiania i usuwania lub prawo do przenoszenia danych, prawo do sprzeciwu, środki oparte na profilowaniu, zawiadamianie podmiotu danych o naruszeniu ochrony danych osobowych oraz pewne powiązane obowiązki administratorów, o ile jest to niezbędne i proporcjonalne w społeczeństwie demokratycznym, by zagwarantować bezpieczeństwo publiczne, w tym ochronę życia ludzkiego – zwłaszcza w ramach reakcji na klęski żywiołowe lub katastrofy spowodowane przez człowieka – zapobieganie przestępstwom lub naruszeniom zasad etyki w zawodach regulowanych, prowadzenie dochodzeń w ich sprawie i ich ściganie, ochronę innych publicznych interesów Unii lub państwa członkowskiego, w szczególności ważnego interesu gospodarczego lub finansowego Unii lub państwa członkowskiego, prowadzenie rejestrów publicznych z uwagi na przesłanki ogólnego interesu publicznego, dalsze przetwarzanie zarchiwizowanych danych osobowych w celu dostarczenia konkretnych informacji o postawie politycznej w ramach dawnych systemów państw totalitarnych lub ochronę podmiotu danych lub praw i wolności innych osób, w tym cele w dziedzinie ochrony socjalnej, zdrowia publicznego i cele humanitarne, takie jak wykonanie zadania przynależnego Międzynarodowemu Ruchowi Czerwonego Krzyża i Czerwonego Półksiężycu (...). Ograniczenia te powinny być zgodne z wymogami Karty praw podstawowych Unii Europejskiej oraz Europejskiej konwencji o ochronie praw człowieka i podstawowych wolności.
- 59a) Żaden z przepisów niniejszego rozporządzenia nie powinien stanowić odstępstwa od (...) przewidzianego prawem międzynarodowym przywileju nieujawniania poufnych informacji Międzynarodowego Komitetu Czerwonego Krzyża, który należy stosować w postępowaniu sądowym i administracyjnym. (...)

- 60) Należy obciążyć administratora odpowiedzialnością, w tym odpowiedzialnością prawną, za przetwarzanie danych osobowych przez niego samego lub w jego imieniu. W szczególności administrator powinien (...) mieć obowiązek wdrożyć odpowiednie środki oraz być w stanie wykazać zgodność czynności przetwarzania z niniejszym rozporządzeniem (...). Środki te powinny uwzględniać charakter, zakres, kontekst i cele przetwarzania oraz zagrożenie dla praw i wolności osób fizycznych.
- 60a) Zagrożenia takie, o różnym prawdopodobieństwie i różnej powadze, mogą wynikać z przetwarzania danych mogącego prowadzić do szkód fizycznych, materialnych lub moralnych, w szczególności: jeżeli przetwarzanie może poskutkować dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych chronionych tajemnicą służbową, niedozwolonym cofnięciem pseudonimizacji lub wszelką inną znaczną szkodą gospodarczą lub społeczną; lub jeżeli podmioty danych mogą zostać pozbawione przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi; jeżeli przetwarzane są dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania światopoglądowe, lub przynależność do związków zawodowych oraz jeżeli przetwarzane są dane genetyczne lub dane dotyczące zdrowia lub seksualności, lub dane o wyrokach skazujących i przestępstwach lub o odnośnych środkach zabezpieczających; jeżeli oceniane są czynniki osobowe, w szczególności analizowane i prognozowane aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się – w celu tworzenia lub wykorzystywania profili osobistych; jeżeli przetwarzane są dane osobowe osób wymagających szczególnej troski, zwłaszcza dzieci; jeżeli przetwarzanie dotyczy dużej ilości danych osobowych i wpływa na dużą liczbę podmiotów danych (...).
- 60b) *Prawdopodobieństwo i powagę zagrożenia należy określić, odwołując się do charakteru, zakresu, kontekstu i celów przetwarzania danych. Zagrożenie należy oszacować na podstawie obiektywnej oceny, w ramach której stwierdza się, czy operacje przetwarzania danych niosą duże zagrożenie. Duże zagrożenie jest szczególnym zagrożeniem naruszenia praw i wolności osób fizycznych (...).*

- 60c) Administrator lub podmiot przetwarzający może otrzymać wskazówki co do tego, jak wdrożyć odpowiednie środki oraz wykazać przestrzeganie rozporządzenia – zwłaszcza jeżeli chodzi o identyfikowanie zagrożenia związanego z przetwarzaniem, o jego ocenę pod kątem źródła, charakteru, prawdopodobieństwa i powagi oraz o sprawdzone rozwiązania pozwalające zminimalizować to zagrożenie – w szczególności w formie zatwierdzonych kodeksów postępowania, zatwierdzonej certyfikacji, wytycznych Europejskiej Rady Ochrony Danych lub poprzez sugestie inspektora ochrony danych. Europejska Rada Ochrony Danych może wydawać wytyczne także w sprawie operacji przetwarzania, których nie uznaje się za mogące nieść duże zagrożenie dla praw i wolności osób fizycznych, i wskazywać, jakie środki mogą wystarczyć w takich przypadkach dla zaradzenia takiemu zagrożeniu. (...)
- 61) Ochrona praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych wymaga wdrożenia odpowiednich środków technicznych i organizacyjnych, by zapewnić spełnienie wymogów rozporządzenia. Aby móc wykazać przestrzeganie niniejszego rozporządzenia, administrator powinien przyjąć wewnętrzne strategie i wdrożyć odpowiednie środki zgodne w szczególności z zasadą uwzględniania ochrony danych w fazie projektowania oraz z zasadą domyślnej ochrony danych. Takie środki mogą polegać m.in. na minimalizacji przetwarzania danych osobowych, (...) jak najszybszej pseudonimizacji danych osobowych, przejrzystości co do funkcji i przetwarzania danych osobowych, umożliwieniu podmiotowi danych monitorowania przetwarzania danych, umożliwieniu administratorowi tworzenia i doskonalenia zabezpieczeń. Jeżeli opracowywane, projektowane, wybierane i użytkowane są aplikacje, usługi i produkty, które opierają się na przetwarzaniu danych osobowych albo przetwarzają dane osobowe w celu realizacji swojego zadania, należy zachęcać wytwórców tych produktów, usług i aplikacji, by podczas opracowywania i projektowania takich produktów, usług i aplikacji wzięli pod uwagę prawo do ochrony danych osobowych i z należyтым uwzględnieniem nowoczesnych rozwiązań zapewnili administratorom i podmiotom przetwarzającym możliwość wywiązania się ze spoczywających na nich obowiązków ochrony danych.
- 62) Ochrona praw i wolności podmiotów danych oraz odpowiedzialność, w tym odpowiedzialność prawna, administratorów i podmiotów przetwarzających – także w odniesieniu do monitorowania ze strony organów nadzorczych i do środków przez nie stosowanych – wymagają dokonania w ramach niniejszego rozporządzenia jasnego podziału obowiązków, w tym na wypadek gdyby administrator określał cele (...) i sposoby przetwarzania wspólnie z innymi administratorami lub gdyby operacji przetwarzania dokonywano w imieniu administratora.

63) Jeżeli administrator niemający siedziby w Unii przetwarza dane osobowe podmiotów danych mających miejsce zamieszkania w Unii, a jego czynności przetwarzania wiążą się z oferowaniem towarów lub usług tym podmiotom lub z monitorowaniem ich zachowania w Unii, (...) powinien on wyznaczyć przedstawiciela, chyba że (...) przetwarzanie, którego dokonuje, ma charakter okazjonalny i jest mało prawdopodobne, by przez swój charakter, zakres, kontekst i cele niosło zagrożenie dla praw i wolności podmiotów danych, lub administrator jest organem lub podmiotem publicznym (...). Przedstawiciel powinien działać w imieniu administratora i może być adresatem ewentualnych działań organu nadzorczego. Administrator powinien wyznaczyć przedstawiciela w wyraźny sposób za pomocą pisemnego upoważnienia do podejmowania działań w jego imieniu w odniesieniu do obowiązków administratora wynikających z niniejszego rozporządzenia. Wyznaczenie przedstawiciela nie wpływa na odpowiedzialność, w tym odpowiedzialność prawną, administratora wynikającą z niniejszego rozporządzenia. Przedstawiciel powinien wykonywać swoje zadania zgodnie z upoważnieniem otrzymanym od administratora, w tym współpracować z właściwymi organami nadzorczymi odnośnie do działań służących przestrzeganiu niniejszego rozporządzenia. W razie jego nieprzestrzegania przez administratora wyznaczony przedstawiciel powinien podlegać działaniom egzekucyjnym.

63a) Aby zapewnić przestrzeganie wymogów niniejszego rozporządzenia w przypadku przetwarzania, którego w imieniu administratora ma dokonać podmiot przetwarzający, administrator powinien, powierzając podmiotowi przetwarzającemu czynności przetwarzania, korzystać z usług wyłącznie podmiotów przetwarzających, które dają wystarczające gwarancje – zwłaszcza jeżeli chodzi o wiedzę fachową, wiarygodność i zasoby – wdrożenia środków technicznych i organizacyjnych odpowiadających wymogom niniejszego rozporządzenia, w tym wymogom bezpieczeństwa przetwarzania. (...) Stosowanie przez podmiot przetwarzający zatwierdzonego kodeksu postępowania lub zatwierdzonego mechanizmu certyfikacji może posłużyć za element wykazujący wywiązywanie się z obowiązków administratora. Przetwarzanie przez podmiot przetwarzający powinno być regulowane umową lub innym aktem prawnym, które podlegają prawu Unii lub prawu państwa członkowskiego, wiążą podmiot przetwarzający z administratorem, określają przedmiot i czas trwania przetwarzania, charakter i cele przetwarzania, rodzaj danych osobowych i kategorie podmiotów danych oraz które uwzględniają konkretne zadania i obowiązki podmiotu przetwarzającego w kontekście planowanego przetwarzania oraz zagrożenie dla praw i wolności podmiotu danych.

Administrator i podmiot przetwarzający mogą postanowić skorzystać z umowy indywidualnej lub ze standardowych klauzul umownych, które zostały przyjęte bezpośrednio przez Komisję albo które zostały przyjęte przez organ nadzorczy zgodnie z mechanizmem spójności, a następnie przyjęte przez Komisję, albo które są elementem certyfikacji udzielonej w ramach mechanizmu certyfikacji. Po zakończeniu przetwarzania w imieniu administratora podmiot przetwarzający powinien zwrócić lub usunąć dane osobowe, chyba że prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający, nakładają obowiązek przechowywania danych.

64) (...)

65) Aby wykazać przestrzeganie niniejszego rozporządzenia, administrator lub podmiot przetwarzający powinni prowadzić rejestry ze wszystkimi kategoriami czynności przetwarzania, za które są odpowiedzialni. Każdy administrator i każdy podmiot przetwarzający powinni być zobowiązani współpracować z organem nadzorczym oraz udostępniać mu te rejestry na żądanie, tak by mogły posłużyć do monitorowania tych operacji przetwarzania.

- 66) W celu zachowania bezpieczeństwa i zapobieżenia przetwarzaniu niezgodnemu z niniejszym rozporządzeniem administrator lub podmiot przetwarzający powinni oszacować (...) zagrożenia właściwe dla przetwarzania oraz wdrożyć środki minimalizujące to zagrożenie. Środki te powinny zapewnić odpowiedni poziom bezpieczeństwa, w tym poufność – z uwzględnieniem dostępnej technologii oraz kosztów wdrożenia (...) – w stosunku do zagrożenia i charakteru danych osobowych podlegających ochronie. (...). Oceniając zagrożenie dla bezpieczeństwa danych, należy wziąć pod uwagę zagrożenia cechujące przetwarzanie danych – takie jak przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych przenoszonych, przechowywanych lub w inny sposób przetwarzanych – i mogące w szczególności prowadzić do szkód fizycznych, materialnych lub moralnych.
- 66a) Aby bardziej zadbać o przestrzeganie niniejszego rozporządzenia, gdy operacje przetwarzania mogą nieść duże zagrożenie dla praw i wolności osób fizycznych, należy zobowiązać administratora do dokonania oceny skutków pod kątem ochrony danych w celu oszacowania w szczególności źródła, charakteru, specyfiki i powagi tego zagrożenia. Wyniki oceny należy uwzględnić przy określaniu odpowiednich środków, które należy zastosować, by wykazać, że przetwarzanie danych osobowych odbywa się zgodnie z niniejszym rozporządzeniem. Jeżeli ocena skutków pod kątem ochrony danych wykaże, że operacje przetwarzania niosą duże zagrożenie, którego administrator nie może zminimalizować odpowiednimi środkami z punktu widzenia dostępnej technologii i kosztów wdrożenia, przed przetwarzaniem należy skonsultować się z organem nadzorczym.

- 67) Przy braku odpowiedniej i szybkiej reakcji naruszenie ochrony danych osobowych może przysporzyć osobom fizycznym szkód fizycznych, materialnych lub moralnych, takich jak utrata kontroli nad własnymi danymi osobowymi lub ograniczenie (...) praw, dyskryminacja, kradzież tożsamości lub oszustwo dotyczące tożsamości, strata finansowa, niedozwolone cofnięcie pseudonimizacji, naruszenie dobrego imienia, naruszenie poufności danych chronionych tajemnicą służbową lub wszelkie inne szkody gospodarcze lub społeczne. (...). Dlatego tuż po stwierdzeniu naruszenia ochrony danych osobowych, które może przysporzyć (...) szkód fizycznych, materialnych lub moralnych, administrator powinien bez zbędnej zwłoki – jeżeli to wykonalne, w ciągu 72 godzin – zgłosić naruszenie organowi nadzorczemu. Jeśli nie jest to możliwe w ciągu 72 godzin, zgłoszeniu powinno towarzyszyć wyjaśnienie przyczyn opóźnienia. Osoby, na których prawa i wolności naruszenie takie mogłoby poważnie wpłynąć, powinny zostać bez zbędnej zwłoki zawiadomione, tak by mogły podjąć niezbędne środki ostrożności. (...). Zawiadomienie powinno zawierać opis charakteru naruszenia ochrony danych osobowych oraz zalecenia dla danej osoby fizycznej co do minimalizacji potencjalnych niekorzystnych skutków. Zawiadomienia należy przekazywać podmiotom danych tak szybko, jak jest to racjonalnie możliwe, w ścisłej współpracy z organem nadzorczym oraz z poszanowaniem wskazówek przekazanych przez ten organ lub inne właściwe organy (np. organy ścigania). Na przykład (...) aby zminimalizować bezpośrednie ryzyko szkody, należałoby zawiadomić podmiot danych szybko, natomiast aby wdrożyć odpowiednie środki przeciwko takim samym lub podobnym naruszeniom ochrony danych, można poświęcić na działania więcej czasu.
- 68) (...) Należy się upewnić, czy wdrożono wszelkie odpowiednie techniczne środki ochrony i wszelkie odpowiednie środki organizacyjne, by od razu stwierdzić naruszenie ochrony danych osobowych i szybko poinformować organ nadzorczy i podmiot danych (...). To, czy zawiadomienia dokonano bez zbędnej zwłoki, należy ustalić z uwzględnieniem zwłaszcza charakteru i powagi naruszenia ochrony danych osobowych, jego konsekwencji oraz niekorzystnych skutków dla podmiotu danych. Takie zawiadomienie może skutkować interwencją organu nadzorczego, zgodnie z jego zadaniami i uprawnieniami określonymi w niniejszym rozporządzeniu.

- 68a) Zawiadomienie podmiotu danych o naruszeniu ochrony danych osobowych nie powinno być wymagane, jeżeli administrator wdrożył odpowiednie techniczne środki ochrony i środki te zostały zastosowane do danych, których ochronę naruszono. Takimi technicznymi środkami ochrony powinny być między innymi środki uniemożliwiające odczyt danych osobie nieupoważnionej do dostępu do nich, zwłaszcza szyfrowanie danych osobowych (...).
- 69) Przy określaniu szczegółowych przepisów o formie i procedurach mających zastosowanie do zawiadamiania o naruszeniu ochrony danych osobowych należy wziąć pod uwagę okoliczności naruszenia, w tym fakt, czy dane osobowe były zabezpieczone odpowiednimi technicznymi środkami ochrony skutecznie ograniczającymi prawdopodobieństwo oszustwa dotyczącego tożsamości lub innych form nadużycia. W przepisach tych i procedurach należy ponadto uwzględnić uzasadnione interesy organów ścigania, jeżeli przedwczesne ujawnienie mogłoby niepotrzebnie utrudnić badanie okoliczności naruszenia.
- 70) Dyrektywa 95/46/WE przewidywała ogólny obowiązek zawiadamiania organów nadzorczych o przetwarzaniu danych osobowych. Obowiązek ten powoduje jednak obciążenia administracyjne i finansowe i nie zawsze przyczyniał się do poprawy ochrony danych osobowych. Dlatego należy znieść te powszechne, ogólne obowiązki zawiadamiania i zastąpić je skutecznymi procedurami i mechanizmami koncentrującymi się w zamian na tych rodzajach operacji przetwarzania, które ze względu na swój charakter, zakres, *kontekst* i cele mogą nieść duże zagrożenie dla praw i wolności osób fizycznych (...). Takimi rodzajami operacji przetwarzania mogą być te, które w szczególności wiążą się z użyciem nowych technologii lub są nowe i administrator nie dokonał wcześniej oceny ich skutków pod kątem ochrony danych, lub stały się niezbędne z uwagi na upływ czasu od pierwotnego przetwarzania.



- 70a) W takim przypadku przed przetwarzaniem administrator (...) powinien dokonać oceny skutków pod kątem ochrony danych – po to by ocenić konkretne prawdopodobieństwo i konkretną powagę tego dużego zagrożenia, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz źródła zagrożenia – ocena ta zaś powinna w szczególności obejmować planowane środki, gwarancje i mechanizmy mające minimalizować to zagrożenie, zapewniać ochronę danych osobowych oraz wykazać przestrzeganie niniejszego rozporządzenia.
- 71) Powinno to mieć zastosowanie w szczególności do (...) operacji przetwarzania o dużej skali – które służą przetwarzaniu znacznej ilości danych osobowych na szczeblu regionalnym, krajowym lub ponadnarodowym i które mogą wpłynąć na dużą liczbę podmiotów danych oraz które mogą nieść duże zagrożenie, na przykład (ze względu na swoją newralgiczność) gdy zgodnie ze stanem wiedzy technicznej stosowana jest na dużą skalę nowa technologia – oraz do innych operacji przetwarzania niosących (...) duże zagrożenie dla praw i wolności podmiotów danych, w szczególności gdy operacje te utrudniają podmiotom danych korzystanie z przysługujących im praw. Oceny skutków pod kątem ochrony danych należy także dokonywać w przypadkach, w których dane przetwarza się w celu podjęcia decyzji wobec konkretnej osoby fizycznej po dokonaniu systematycznej, kompleksowej oceny czynników osobowych osób fizycznych na podstawie profilowania tych danych lub po przetworzeniu danych osobowych szczególnych kategorii, danych biometrycznych lub danych o wyrokach skazujących za przestępstwa, o przestępstwach lub o odnośnych środkach zabezpieczających. Ocena skutków pod kątem ochrony danych jest również niezbędna w przypadku monitorowania na dużą skalę miejsc publicznie dostępnych – zwłaszcza za pomocą urządzeń optyczno-elektronicznych – lub wszelkich innych operacji, względem których właściwy organ nadzorczy uznaje, że przetwarzanie może nieść duże zagrożenie dla praw i wolności podmiotów danych, w szczególności dlatego, że operacje te uniemożliwiają podmiotom danych korzystanie z prawa, usługi lub umowy lub mają systematyczny charakter i dużą skalę. Przetwarzanie (...) danych osobowych – niezależnie od ilości czy charakteru tych danych – nie powinno być uznawane za przetwarzanie o dużej skali, jeżeli przetwarzanie tych danych jest chronione tajemnicą służbową, (...) tak jak przetwarzanie danych osobowych pacjentów lub klientów przez pojedynczego lekarza, pracownika służby zdrowia, szpital lub adwokata. W tych przypadkach ocena skutków pod kątem ochrony danych nie powinna być obowiązkowa.

- 72) W niektórych okolicznościach rozsądnie i korzystnie byłoby nie ograniczać oceny skutków pod kątem ochrony danych do pojedynczego projektu, na przykład wtedy gdy organy lub podmioty publiczne zamierzają ustanowić wspólną aplikację lub platformę przetwarzania lub gdy kilku administratorów planuje wprowadzić wspólną aplikację lub środowisko przetwarzania obejmujące sektor lub segment gospodarki lub szeroko rozpowszechnioną działalność horyzontalną.
- 73) Oceny skutków pod kątem ochrony danych może dokonać organ lub podmiot publiczny, o ile oceny takiej nie dokonano już przy okazji przyjmowania prawa krajowego, na którym opiera się wykonywanie zadań przez ten organ lub podmiot publiczny i które reguluje konkretną operację przetwarzania lub konkretny zestaw operacji.
- 74) Jeżeli ocena skutków pod kątem ochrony danych wykaże, że mimo planowanych gwarancji, środków bezpieczeństwa oraz mechanizmów minimalizujących zagrożenie przetwarzanie niosłoby duże zagrożenie dla praw i wolności osób fizycznych (...), a administrator jest zdania, że zagrożenia tego nie da się zminimalizować środkami racjonalnymi z punktu widzenia dostępnych technologii i kosztów wdrożenia, wtedy przed rozpoczęciem czynności przetwarzania należy skonsultować się z organem nadzorczym. Takie duże zagrożenie (...) mogą nieść pewne rodzaje przetwarzania danych oraz pewien zakres i pewna częstotliwość przetwarzania, które mogą skutkować także (...) szkodą lub (...) ingerencją w prawa i wolności podmiotu danych. Na wniosek o konsultację organ nadzorczy powinien odpowiedzieć w określonym terminie. Jednak brak reakcji ze strony organu nadzorczego w tym terminie nie powinien wykluczać interwencji tego organu zgodnie z jego zadaniami i uprawnieniami ustanowionymi w niniejszym rozporządzeniu, w tym uprawnieniami do zakazania operacji przetwarzania. W ramach konsultacji można przedłożyć organowi nadzorczemu wyniki oceny skutków pod kątem ochrony danych dokonanej w odniesieniu do danego przetwarzania zgodnie z art. 33, a w szczególności środki planowane w celu zminimalizowania zagrożenia dla praw i wolności osób fizycznych.
- 74a) W razie potrzeby i na wniosek podmiot przetwarzający powinien pomagać administratorowi w zapewnieniu przestrzegania obowiązków wynikających z dokonania oceny skutków pod kątem ochrony danych oraz z uprzednich konsultacji z organem nadzorczym.

- 74b) Konsultacji z organem nadzorczym należy dokonać również w trakcie przygotowywania środka ustawodawczego lub regulacyjnego przewidującego przetwarzanie danych osobowych, (...) po to by zapewnić zgodność zamierzonego przetwarzania z niniejszym rozporządzeniem, a w szczególności zminimalizować ewentualne zagrożenie dla podmiotu danych.
- 75) Jeżeli przetwarzanie odbywa się w sektorze publicznym lub jeżeli w sektorze prywatnym przetwarzanie jest prowadzone przez dużą firmę, lub jeżeli główna działalność firmy, niezależnie od jej wielkości, obejmuje operacje przetwarzania wymagające regularnego i systematycznego monitorowania, administratora lub podmiot przetwarzający może wspomagać w monitorowaniu wewnętrznego przestrzegania niniejszego rozporządzenia osoba dysponująca wiedzą fachową na temat prawa i praktyk w dziedzinie ochrony danych. Tacy inspektorzy ochrony danych – którzy mogą być pracownikami administratora – powinni być w stanie wykonywać swoje obowiązki i zadania w sposób niezależny.
- 76) Należy zachęcać stowarzyszenia lub inne organy reprezentujące administratorów lub podmioty przetwarzające różnych kategorii do sporządzania kodeksów postępowania, w granicach niniejszego rozporządzenia, by ułatwiać skuteczne stosowanie niniejszego rozporządzenia, z uwzględnieniem szczególnych cech przetwarzania prowadzonego w niektórych sektorach i szczególnych potrzeb mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw. W takich kodeksach można w szczególności dopasować obowiązki administratorów i podmiotów przetwarzających do zagrożenia, jakie przetwarzanie może nieść dla praw i wolności osób fizycznych.
- 76a) Sporządzając kodeks postępowania bądź zmieniając go lub poszerzając, stowarzyszenia i inne organy reprezentujące administratorów lub podmioty przetwarzające różnych kategorii powinny konsultować się z odpowiednimi zainteresowanymi stronami, w tym jeżeli jest to wykonalne, z podmiotami danych, oraz mieć na względzie uwagi i opinie otrzymane w ramach takich konsultacji.
- 77) Aby zwiększyć przejrzystość i przestrzeganie niniejszego rozporządzenia, należy zachęcać do ustanowienia mechanizmów certyfikacji oraz do wprowadzenia pieczęci i oznaczeń w dziedzinie ochrony danych, pozwalając w ten sposób podmiotom danych szybko ocenić poziom ochrony danych, której podlegają stosowne produkty i usługi.

- 78) Transgraniczny przepływ danych osobowych do państw spoza Unii i do organizacji międzynarodowych oraz z takich państw i z takich organizacji jest niezbędnym warunkiem rozwoju handlu międzynarodowego i współpracy międzynarodowej. Wzrost tego przepływu spowodował nowe wyzwania i problemy w dziedzinie ochrony danych osobowych. Przekazując dane osobowe z Unii administratorom, podmiotom przetwarzającym lub innym odbiorcom w państwach trzecich lub organizacjom międzynarodowym, nie należy jednak obniżać poziomu ochrony osób fizycznych gwarantowanego w Unii niniejszym rozporządzeniem; powinno to dotyczyć także wtórnego przekazywania danych osobowych: z państwa trzeciego lub organizacji międzynarodowej administratorowi, podmiotowi przetwarzającemu w tym samym lub kolejnym państwie trzecim lub tej samej lub kolejnej organizacji międzynarodowej. W każdym przypadku przekazywanie danych do państw trzecich i organizacji międzynarodowych może się odbywać wyłącznie w pełnej zgodzie z niniejszym rozporządzeniem. Przekazywanie może mieć miejsce wyłącznie wtedy, gdy administrator lub podmiot przetwarzający przestrzegają warunków ustanowionych w rozdziale V – z zastrzeżeniem pozostałych przepisów niniejszego rozporządzenia.
- 79) Niniejsze rozporządzenie pozostaje bez uszczerbku dla umów międzynarodowych między Unią a państwami trzecimi regulujących przekazywanie danych osobowych, w tym zawierających odpowiednie gwarancje dla podmiotów danych. Państwa członkowskie mogą zawierać umowy międzynarodowe przewidujące m.in. przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych, o ile umowy takie nie wpływają na niniejsze rozporządzenie ani na inne przepisy prawa UE i o ile zawierają gwarancje chroniące prawa podmiotów danych.

- 80) Komisja może (...) stwierdzić ze skutkiem dla całej Unii, że niektóre państwa trzecie – lub też terytorium lub określony sektor, taki jak sektor prywatny czy konkretny sektor lub konkretne sektory gospodarcze w państwie trzecim – bądź organizacja międzynarodowa oferują odpowiedni poziom ochrony danych, i tym samym zagwarantować pewność i jednolitość prawną w całej Unii, jeżeli chodzi o państwa trzecie lub organizacje międzynarodowe uznawane za zapewniające taki poziom ochrony. W takich przypadkach przekazywanie danych osobowych do tych państw może się odbywać bez potrzeby uzyskania specjalnego zezwolenia.
- 81) Zgodnie z podstawowymi wartościami, na których opiera się Unia, w szczególności z ochroną praw człowieka, w swojej ocenie państwa trzeciego lub terytorium, lub określonego sektora w państwie trzecim Komisja powinna wziąć pod uwagę sposób, w jaki dane państwo trzecie przestrzega praworządności, dostępu do wymiaru sprawiedliwości oraz międzynarodowych norm i standardów ochrony praw człowieka, jego prawo ogólne i sektorowe, w tym ustawodawstwo dotyczące bezpieczeństwa publicznego, obrony, bezpieczeństwa narodowego i porządku publicznego, a także prawo karne. Stwierdzając, czy poziom ochrony na terytorium lub w określonym sektorze w państwie trzecim jest odpowiedni, należy wziąć pod uwagę jasne i obiektywne kryteria, takie jak konkretne czynności przetwarzania, zakres mających zastosowanie standardów prawnych i ustawodawstwo obowiązujące w danym państwie trzecim. Państwo trzecie powinno oferować gwarancje zapewniające odpowiedni poziom ochrony w szczególności wtedy, gdy dane są przetwarzane w jednym konkretnym sektorze lub większej ich liczbie. W szczególności państwo trzecie powinno zapewnić skuteczny nadzór nad ochroną danych oraz powinno przewidzieć mechanizmy współpracy z europejskimi organami ochrony danych, a podmioty danych powinny uzyskać skuteczne i egzekwowalne prawa oraz skuteczne administracyjne i sądowe środki zaskarżenia.

- 81a) Poza międzynarodowymi zobowiązaniami, które zaciągnęły państwo trzecie lub organizacja międzynarodowa, Komisja powinna brać pod uwagę także obowiązki wynikające z udziału państwa trzeciego lub organizacji międzynarodowej w systemach wielostronnych lub regionalnych, zwłaszcza w odniesieniu do ochrony danych osobowych, a także realizację takich obowiązków. W szczególności należy wziąć pod uwagę przystąpienie państwa trzeciego do konwencji Rady Europy z dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych. Oceniając poziom ochrony w państwach trzecich lub organizacjach międzynarodowych, Komisja powinna konsultować się z Europejską Radą Ochrony Danych.
- 81b) Komisja powinna monitorować obowiązywanie decyzji o poziomie ochrony w państwie trzecim – lub na terytorium, lub w określonym sektorze w państwie trzecim – bądź w organizacji międzynarodowej, w tym decyzji przyjętych na podstawie art. 25 ust. 6 lub art. 26 ust. 4 dyrektywy 95/46/WE. Komisja powinna w rozsądnym terminie ocenić obowiązywanie decyzji drugiego typu i przekazać wszelkie istotne wnioski komitetowi w rozumieniu rozporządzenia (UE) nr 182/2011 ustanowionemu na mocy niniejszego rozporządzenia.
- 82) Komisja może (...) uznać, że państwo trzecie – lub też terytorium, lub określony sektor w państwie trzecim – bądź organizacja międzynarodowa (...) przestały zapewniać odpowiedni poziom ochrony danych. W związku z tym przekazywanie danych osobowych do tego państwa trzeciego lub tej organizacji międzynarodowej powinno zostać zakazane, chyba że spełnione są wymogi art. 42–44. W takim przypadku należy przewidzieć konsultacje między Komisją a takimi państwami trzecimi lub organizacjami międzynarodowymi. Komisja powinna na czas poinformować to państwo trzecie lub tę organizację międzynarodową o powodach oraz podjąć z nimi konsultacje w celu zaradzenia sytuacji.

- 83) W razie braku stwierdzenia odpowiedniego poziomu ochrony danych administrator lub podmiot przetwarzający powinni zastosować środki rekompensujące brak ochrony danych w państwie trzecim, oferując podmiotowi danych odpowiednie gwarancje. Takie odpowiednie gwarancje mogą polegać na skorzystaniu z wiążących reguł korporacyjnych, standardowych klauzul ochrony danych przyjętych przez Komisję, standardowych klauzul ochrony danych przyjętych przez organ nadzorczy, doraźnych klauzul umownych dozwolonych przez organ nadzorczy lub też z innych właściwych i proporcjonalnych środków uzasadnionych w świetle wszystkich okoliczności związanych z operacją przekazania danych lub zestawem takich operacji, o ile zezwoli na to organ nadzorczy. Gwarancje te powinny zapewniać przestrzeganie wymogów ochrony danych oraz praw podmiotów danych, w tym prawa do skutecznych administracyjnych lub sądowych środków dochodzenia roszczeń. Powinny one dotyczyć w szczególności przestrzegania ogólnych zasad związanych z przetwarzaniem danych osobowych, dostępności egzekwowalnych praw podmiotu danych i skutecznych środków ochrony prawnej oraz zasad uwzględniania ochrony danych w fazie projektowania i domyślnej ochrony danych. Również organy lub podmioty publiczne mogą przekazywać dane organom lub podmiotom publicznym w państwach trzecich lub organizacjom międzynarodowym o analogicznych obowiązkach lub funkcjach, w tym na podstawie przepisów, które zostaną umieszczone w porozumieniach administracyjnych, takich jak protokół ustaleń. Jeżeli gwarancje znajdują się w porozumieniach administracyjnych niewiążących prawnie, należy uzyskać zezwolenie właściwego organu nadzorczego.

- 84) Możliwość korzystania przez administratora lub podmiot przetwarzający ze standardowych klauzul ochrony danych przyjętych przez Komisję lub organ nadzorczy nie powinna stanowić przeszkody we włączaniu przez nich standardowych klauzul ochrony danych do szerszej umowy, w tym do umowy między podmiotem przetwarzającym a innym podmiotem przetwarzającym, ani w dodawaniu innych klauzul lub dodatkowych gwarancji, pod warunkiem że nie są one bezpośrednio lub pośrednio sprzeczne ze standardowymi klauzulami umownymi przyjętymi przez Komisję lub organ nadzorczy ani nie naruszają podstawowych praw lub wolności podmiotów danych.
- 85) Grupa korporacyjna lub grupa firm prowadzących wspólną działalność gospodarczą powinny móc korzystać z zatwierdzonych wiążących reguł korporacyjnych przy międzynarodowym przekazywaniu danych z Unii do organizacji w tej samej korporacyjnej grupie przedsiębiorstw lub w grupie firm, o ile w skład takich reguł korporacyjnych wchodzi podstawowe zasady i egzekwowalne prawa zapewniające odpowiednie gwarancje na potrzeby przekazywania danych osobowych lub określonych kategorii przekazanych danych osobowych.
- 86) Należy przewidzieć możliwość przekazywania danych w niektórych okolicznościach, jeżeli podmiot danych udzielił na to wyraźnej zgody, jeżeli przekazanie jest okazjonalne w związku z umową lub roszczeniem prawnym – niezależnie od rodzaju postępowania: sądowego, administracyjnego lub jakiegokolwiek innego postępowania pozasądowego, w tym postępowania przed organami regulacyjnymi. Należy także przewidzieć możliwość przekazywania danych, jeżeli wymaga tego ważny interes publiczny ustanowiony prawem Unii lub prawem państwa członkowskiego lub jeżeli przekazanie następuje z rejestru utworzonego na mocy prawa i przeznaczonego do wglądu dla ogółu obywateli lub osób mających uzasadniony interes. W drugim z tych przypadków przekazanie nie powinno obejmować całości danych lub całych kategorii danych z rejestru, a jeżeli rejestr jest przeznaczony do wglądu dla osób mających uzasadniony interes, przekazanie danych powinno nastąpić wyłącznie wtedy, gdy osoby te o to wystąpią lub gdy osoby te mają być odbiorcami.



- 87) Przepisy te powinny mieć w szczególności zastosowanie do przekazywania danych wymaganego i niezbędnego ze względu na ważne przesłanki interesu publicznego, na przykład do międzynarodowej wymiany danych (...) między organami ds. konkurencji, organami podatkowymi lub celnymi, organami nadzoru finansowego, służbami odpowiedzialnymi za sprawy ubezpieczeń społecznych lub za zdrowie publiczne, na przykład w przypadku ustalania kontaktów zakaźnych w razie chorób zakaźnych lub w celu zmniejszenia lub wyeliminowania dopingu w sporcie (...). Przekazywanie danych osobowych należy uznać za zgodne z prawem również wtedy, gdy jest niezbędne w celu ochrony interesu, który ma istotne znaczenie dla żywotnych interesów podmiotu danych lub innej osoby, w tym integralności fizycznej lub życia, a podmiot danych nie jest w stanie udzielić zgody. W razie braku stwierdzenia odpowiedniego poziomu ochrony prawo Unii lub prawo państwa członkowskiego mogą ze względu na ważne przesłanki interesu publicznego wyraźnie nakładać ograniczenia na przekazywanie konkretnych kategorii danych do państwa trzeciego lub organizacji międzynarodowej. Państwa członkowskie powinny powiadomić Komisję o takich przepisach. Każde przekazanie danych osobowych podmiotu danych, który jest fizycznie lub prawnie niezdolny do udzielenia zgody, do międzynarodowych organizacji humanitarnych, takich jak krajowe stowarzyszenia Czerwonego Krzyża (...) czy Międzynarodowy Komitet Czerwonego Krzyża, aby wykonane zostało zadanie przynależne – na mocy konwencji genewskich – Międzynarodowemu Ruchowi Czerwonego Krzyża i Czerwonego Półksiężyca lub rzetelnie zastosowane zostało międzynarodowe prawo humanitarne obowiązujące w czasie konfliktów zbrojnych, można uznać za niezbędne ze względu na ważną przesłankę interesu publicznego lub za leżące w żywotnym interesie podmiotu danych.

- 88) Przekazanie, którego nie można uznać za mające duży zakres ani częste, może także być możliwe ze względu na uzasadnione interesy realizowane przez administratora lub podmiot przetwarzający, przy założeniu że charakter nadrzędnego wobec tych interesów nie mają interesy lub prawa i wolności podmiotu danych i że administrator lub podmiot przetwarzający ocenili wszelkie okoliczności związane z przekazaniem danych. Administrator lub podmiot przetwarzający powinni zwrócić szczególną uwagę na charakter danych, cel i czas trwania proponowanej operacji przetwarzania lub proponowanych operacji przetwarzania oraz na sytuację w państwie pochodzenia, państwie trzecim i państwie ostatecznego przeznaczenia, a także na przywoływane odpowiednie gwarancje poszanowania praw podstawowych i podstawowych wolności osób fizycznych w związku z przetwarzaniem ich danych osobowych. W przypadku przetwarzania do celów historycznych, statystycznych i naukowych należy wziąć pod uwagę uzasadnione oczekiwania społeczne co do wzrostu wiedzy. Aby ocenić, czy przekazywanie ma duży zakres lub jest częste, należy uwzględnić ilość danych osobowych i liczbę podmiotów danych oraz okazjonalność bądź regularność przekazywania.

- 89) W każdym przypadku jeżeli Komisja nie podjęła decyzji stwierdzającej odpowiedni poziom ochrony danych w państwie trzecim, administrator lub podmiot przetwarzający powinni skorzystać z rozwiązań, które dają podmiotom danych gwarancję, że po przekazaniu danych nadal będą im przysługiwać podstawowe prawa i gwarancje w związku z przetwarzaniem ich danych w Unii.
- 90) Niektóre państwa trzecie przyjmują ustawy, rozporządzenia i inne instrumenty prawne mające bezpośrednio regulować czynności przetwarzania podejmowane przez osoby fizyczne i prawne podlegające jurysdykcji państw członkowskich. Pozaterytorialne stosowanie tych ustaw, rozporządzeń i innych instrumentów prawnych może naruszać prawo międzynarodowe i uniemożliwiać zapewnienie osobom fizycznym ochrony gwarantowanej w niniejszym rozporządzeniu przez Unię. Przekazywanie danych powinno być dopuszczalne wyłącznie wtedy, gdy spełnione są warunki przekazywania do państw trzecich ustanowione w niniejszym rozporządzeniu. Tak może być m.in. wtedy, gdy ujawnienie jest niezbędne ze względu na ważny interes publiczny uznany prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator. (...)
- 91) Transgraniczne przekazywanie danych osobowych poza Unię może spowodować wzrost ryzyka, że osoby fizyczne nie będą mogły skorzystać z praw do ochrony danych osobowych, w szczególności w celu ochrony przed niezgodnym z prawem wykorzystaniem lub ujawnieniem tych informacji. Jednocześnie organy nadzorcze mogą uznać, że nie są w stanie rozpatrzyć skargi lub przeprowadzić dochodzenia w sprawie działalności, która ma miejsce poza granicami ich państwa. Ich staraniom na rzecz współpracy w kontekście transgranicznym mogą także przeszkodzić niewystarczające uprawnienia prewencyjne lub zaradcze, niespójne systemy prawne oraz przeszkody praktyczne, takie jak ograniczone środki. Należy więc promować ściślejszą współpracę między organami nadzorującymi ochronę danych, by pomóc im wymieniać informacje i prowadzić dochodzenia z ich międzynarodowymi odpowiednikami. Aby stworzyć mechanizmy współpracy międzynarodowej, ułatwiające i przewidujące wzajemną międzynarodową pomoc w egzekwowaniu ustawodawstwa z zakresu ochrony danych osobowych, Komisja i organy nadzorcze powinny w ramach działań związanych z wykonywaniem swoich uprawnień wymieniać się informacjami i współpracować z właściwymi organami państw trzecich na zasadzie wzajemności i zgodnie z przepisami niniejszego rozporządzenia, w tym przepisami rozdziału V.

- 92) Zasadniczym elementem ochrony osób fizycznych w związku z przetwarzaniem danych osobowych jest utworzenie w państwach członkowskich organów nadzorczych, uprawnionych do wykonywania zadań i korzystania z uprawnień w sposób całkowicie niezależny. Aby odzwierciedlić swoją strukturę konstytucyjną, organizacyjną i administracyjną, państwa członkowskie mogą utworzyć więcej niż jeden organ nadzorczy.
- 92a) Niezależność organów nadzorczych nie powinna oznaczać, że organy te nie mogą podlegać mechanizmom kontroli lub monitorowania pod kątem wydatków. Nie oznacza ona też, że organy nadzorcze nie mogą podlegać kontroli sądowej.
- 93) Jeżeli państwo członkowskie utworzy kilka organów nadzorczych, powinno ustanowić prawem mechanizmy zapewniające skuteczny udział tych organów w stosowaniu mechanizmu spójności. Takie państwo członkowskie powinno w szczególności wyznaczyć organ nadzorczy, który pełnił funkcję pojedynczego punktu kontaktowego do celów skutecznego udziału tych organów w stosowaniu mechanizmu, po to by zapewnić sprawną i płynną współpracę z innymi organami nadzorczymi, Europejską Radą Ochrony Danych oraz Komisją.
- 94) Każdy organ nadzorczy powinien zostać wyposażony w (...) zasoby finansowe i kadrowe, pomieszczenia i infrastrukturę niezbędne do skutecznego wykonywania zadań, w tym zadań związanych z wzajemną pomocą i współpracą z innymi organami nadzorczymi z całej Unii. Każdy organ nadzorczy powinien dysponować osobnym budżetem rocznym, który może być częścią ogólnego budżetu krajowego lub państwowego.
- 95) Ogólne warunki bycia członkiem organu nadzorczego powinny zostać określone w prawie każdego państwa członkowskiego i powinny w szczególności przewidywać, że członków tego organu mianują parlament, rząd lub głowa państwa członkowskiego lub niezależny organ, któremu prawo państwa członkowskiego powierzyło zadanie mianowania drogą przejrzystej procedury. Aby zapewnić niezależność organu nadzorczego, jego członek lub członkowie powinni powstrzymać się od wszelkich czynności niezgodnych z obowiązkami i w trakcie swojej kadencji nie powinni podejmować żadnej funkcji – zarobkowej ani niezarobkowej – stojącej w sprzeczności z tymi obowiązkami. (...).

- 95a) Każdy organ nadzorczy powinien mieć właściwość na terytorium własnego państwa członkowskiego do korzystania z uprawnień i wykonywania zadań powierzonych mu w myśl niniejszego rozporządzenia. Powinno to dotyczyć zwłaszcza przetwarzania w ramach działalności siedziby administratora lub podmiotu przetwarzającego na terytorium tego państwa członkowskiego, przetwarzania danych osobowych przez organy publiczne lub podmioty prywatne działające w interesie publicznym, przetwarzania mającego wpływ na podmioty danych na tym terytorium lub przetwarzania dokonywanego przez administratora lub podmiot przetwarzający niemających siedziby w Unii Europejskiej, jeżeli zwracają się oni do podmiotów danych mających miejsce zamieszkania na tym terytorium. Powinno to dotyczyć m.in. rozpatrywania skarg wnoszonych przez podmioty danych, prowadzenia dochodzeń w sprawie stosowania rozporządzenia, uświadamiania zagrożeń, zasad, gwarancji i praw związanych z przetwarzaniem danych osobowych.
- 96) Organy nadzorcze powinny monitorować stosowanie przepisów niniejszego rozporządzenia oraz przyczyniać się do jego spójnego stosowania w całej Unii, po to by chronić osoby fizyczne w związku z przetwarzaniem ich danych osobowych oraz ułatwiać swobodny przepływ danych osobowych na rynku wewnętrznym. W tym celu niniejsze rozporządzenie powinno zobowiązywać i uprawniać organy nadzorcze do współpracy ze sobą nawzajem i z Komisją bez konieczności zawierania przez państwa członkowskie porozumień o wzajemnej pomocy lub współpracy.

- 97) Jeżeli przetwarzanie danych osobowych odbywa się w ramach działalności siedziby administratora lub podmiotu przetwarzającego w Unii, a administrator lub podmiot przetwarzający mają siedzibę w więcej niż jednym państwie członkowskim lub jeżeli przetwarzanie, które odbywa się w ramach działalności pojedynczej siedziby administratora lub podmiotu przetwarzającego w Unii, znacznie wpływa lub może znacznie wpłynąć na podmioty danych w więcej niż jednym państwie członkowskim, organem głównym powinien być organ nadzorczy głównej siedziby administratora lub podmiotu przetwarzającego lub pojedynczej siedziby administratora lub podmiotu przetwarzającego. Powinien on współpracować z innymi organami, które są tym zainteresowane z uwagi na to, że administrator lub podmiot przetwarzający mają siedzibę na terytorium ich państwa członkowskiego, że odnotowuje się znaczny wpływ na podmioty danych mające miejsce zamieszkania na tym terytorium lub że wniesiono do tych organów skargę. Także wtedy, gdy skargę wniósł podmiot danych niemający miejsca zamieszkania w tym państwie członkowskim, organ nadzorczy, do którego wniesiono skargę, powinien być uznawany za zainteresowany organ nadzorczy. W ramach zadania, którym jest opracowywanie wytycznych co do stosowania niniejszego rozporządzenia, Europejska Rada Ochrony Danych może opracować wytyczne zwłaszcza w sprawie kryteriów, które należy uwzględnić, by stwierdzić, czy dane przetwarzanie znacznie wpływa na podmioty danych w więcej niż jednym państwie członkowskim, oraz w sprawie tego, czym jest istotny i zasadny sprzeciw.
- 97a) Główny organ nadzorczy powinien być właściwy do przyjmowania wiążących decyzji co do środków wdrażających uprawnienia powierzone mu zgodnie z przepisami niniejszego rozporządzenia. Organ nadzorczy sprawujący funkcję organu głównego powinien ściśle angażować w proces decyzyjny zainteresowane organy nadzorcze i powinien go z nimi koordynować. Jeżeli na mocy decyzji skarga podmiotu danych ma zostać w całości lub w części odrzucona, decyzję tę powinien przyjmować organ nadzorczy, do którego wniesiono skargę.

97b) Decyzja powinna być uzgadniana wspólnie przez główny organ nadzorczy i zainteresowane organy nadzorcze, powinna być skierowana do głównej lub pojedynczej siedziby administratora lub podmiotu przetwarzającego i powinna być wiążąca dla administratora i podmiotu przetwarzającego. Administrator lub podmiot przetwarzający powinni przedsięwziąć wszelkie niezbędne środki, by zastosować się do niniejszego rozporządzenia i wdrożyć decyzję notyfikowaną przez główny organ nadzorczy głównej siedzibie administratora lub podmiotu przetwarzającego w odniesieniu do czynności przetwarzania w Unii.

97c) Każdy organ nadzorczy (...) niepełniący funkcji głównego organu nadzorczego powinien być właściwy (...) w sprawach lokalnych, gdy administrator lub podmiot przetwarzający mają siedzibę w więcej niż jednym państwie członkowskim, ale przedmiot danego przetwarzania dotyczy wyłącznie przetwarzania prowadzonego w pojedynczym państwie członkowskim i wyłącznie podmiotów danych w tym pojedynczym państwie członkowskim, np. gdy chodzi o przetwarzanie danych pracowników w szczegółowym kontekście zatrudnienia w państwie członkowskim. W takim przypadku organ nadzorczy powinien niezwłocznie poinformować o sprawie główny organ nadzorczy. Po otrzymaniu informacji główny organ nadzorczy powinien postanowić, czy zajmie się daną sprawą w ramach mechanizmu kompleksowej obsługi, czy też powinien się nią zająć na szczeblu lokalnym organ nadzorczy, który o niej poinformował. Podejmując decyzję, czy zająć się sprawą, główny organ nadzorczy powinien uwzględnić, czy w państwie członkowskim, którego organ nadzorczy przekazał mu informacje, znajduje się siedziba administratora lub podmiotu przetwarzającego – po to by zapewnić skuteczne wykonanie decyzji względem administratora lub podmiotu przetwarzającego. Jeżeli główny organ nadzorczy postanowi zająć się daną sprawą, organ nadzorczy, który przekazał mu informacje, powinien mieć możliwość przedłożyć projekt decyzji, którą główny organ nadzorczy powinien w jak największym stopniu uwzględnić, przygotowując projekt swojej decyzji w ramach mechanizmu kompleksowej obsługi.

98) Przepisy dotyczące głównego organu nadzorczego i mechanizmu kompleksowej obsługi nie powinny mieć zastosowania, gdy przetwarzania dokonują organy publiczne lub podmioty prywatne działające w interesie publicznym. W takich przypadkach jedynym organem nadzorczym właściwym do korzystania z uprawnień przyznanych zgodnie z niniejszym rozporządzeniem powinien być organ nadzorczy państwa członkowskiego, w którym organ publiczny lub podmiot prywatny mają siedzibę.

99) (...)

100) Aby zapewnić spójne monitorowanie i egzekwowanie niniejszego rozporządzenia w całej Unii, organy nadzorcze powinny mieć w każdym państwie członkowskim te same zadania i faktyczne uprawnienia, w tym uprawnienia dochodzeniowe, korekcyjne, sankcyjne oraz uprawnienia autoryzacyjne i doradcze, w szczególności w przypadku skarg osób fizycznych, i – bez uszczerbku dla uprawnień organów prokuratorskich na mocy prawa krajowego – uprawnienia do zgłaszania naruszeń niniejszego rozporządzenia organom wymiaru sprawiedliwości i/lub do udziału w postępowaniu sądowym. Wśród tych uprawnień powinno być także uprawnienie do tego, by zakazać przetwarzania, w sprawie którego z organem się skonsultowano. Państwa członkowskie mogą wskazać także inne zadania związane z ochroną danych osobowych na mocy niniejszego rozporządzenia. Z uprawnień organów nadzorczych (...) należy korzystać zgodnie z odpowiednimi gwarancjami proceduralnymi przewidzianymi w prawie Unii i prawie krajowym, bezstronnie, sprawiedliwie i w racjonalnym terminie. W szczególności każdy środek powinien być odpowiedni, niezbędny i proporcjonalny, aby zapewnić przestrzeganie niniejszego rozporządzenia – z uwzględnieniem okoliczności danej sprawy, z poszanowaniem prawa do wysłuchania danej osoby przed zastosowaniem indywidualnego środka, który miałby niekorzystnie na nią wpłynąć, i bez nadmiernych kosztów i niedogodności dla danej osoby. Z uprawnień dochodzeniowych, jeżeli chodzi o dostęp do pomieszczeń, należy korzystać zgodnie ze szczegółowymi wymogami krajowego prawa procesowego, takimi jak wymóg uzyskania uprzedniego zezwolenia sądu.

Każdy prawnie wiążący środek organu nadzorczego powinien być sporządzony na piśmie, mieć jasny i jednoznaczny charakter, wskazywać organ nadzorczy, który wydał środek, i datę wydania środka, nosić podpis szefa lub członka organu nadzorczego przez niego upoważnionego, podawać powody zastosowania środka oraz informować o prawie do skutecznego środka ochrony prawnej. Nie powinno to wykluczać dodatkowych wymogów na mocy krajowego prawa procesowego. Przyjęcie takiej prawnie wiążącej decyzji oznacza, że może ona być przedmiotem kontroli sądowej w państwie członkowskim organu nadzorczego, który ją przyjął.

101) (...).



101a) Jeżeli organ nadzorczy, do którego wniesiono skargę, nie jest głównym organem nadzorczym, główny organ nadzorczy powinien ściśle współpracować z organem nadzorczym, do którego wniesiono skargę, zgodnie z przepisami o współpracy i spójności ustanowionymi w niniejszym rozporządzeniu. W takim przypadku główny organ nadzorczy powinien, stosując środki mające wywołać skutki prawne, w tym nakładając grzywny administracyjne, w jak największym stopniu brać pod uwagę opinię organu nadzorczego, do którego wniesiono skargę, ten zaś powinien pozostać właściwy do przeprowadzenia dochodzenia na terytorium własnego państwa członkowskiego w kontakcie z właściwym organem nadzorczym.

101b) Organ nadzorczy, do którego wniesiono skargę lub który wykrył lub w inny sposób dowiedział się o sytuacjach mogących skutkować ewentualnymi naruszeniami niniejszego rozporządzenia, powinien dążyć do rozwiązania polubownego, a jeżeli okaże się to niemożliwe, skorzystać z pełni uprawnień, które mu przysługują, jeżeli funkcję głównego organu nadzorczego wobec czynności przetwarzania prowadzonych przez administratora lub podmiot przetwarzający powinien pełnić inny organ nadzorczy, ale konkretny przedmiot skargi lub ewentualnego naruszenia dotyczy wyłącznie czynności przetwarzania prowadzonych przez administratora lub podmiot przetwarzający w państwie członkowskim, w którym wniesiono skargę lub wykryto ewentualne naruszenie, a sprawa nie wpływa znacznie lub najprawdopodobniej nie wpłynie znacznie na podmioty danych w innych państwach członkowskich. Powinno to dotyczyć także konkretnego przetwarzania prowadzonego na terytorium państwa członkowskiego organu nadzorczego lub odnośnie do podmiotów danych na terytorium tego państwa członkowskiego lub przetwarzania prowadzonego w ramach oferowania towarów lub usług konkretnie podmiotom danych na terytorium państwa członkowskiego organu nadzorczego lub podlegającego ocenie z uwagi na stosowne obowiązki prawne wynikające z prawa krajowego.

102) Na uświadamiające działania organów nadzorczych skierowane do opinii publicznej powinny się składać m.in. konkretne środki adresowane do administratorów i podmiotów przetwarzających, w tym do mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw, a także do osób fizycznych, zwłaszcza w ramach edukacji.

- 103) Organy nadzorcze powinny wspierać się wzajemnie w wykonywaniu swoich zadań oraz świadczyć sobie wzajemną pomoc, by zapewnić spójne stosowanie i egzekwowanie niniejszego rozporządzenia na rynku wewnętrznym. Jeżeli organ nadzorczy występujący z wnioskiem o wzajemną pomoc przyjmie – w razie braku odpowiedzi organu nadzorczego będącego adresatem wniosku w terminie jednego miesiąca od otrzymania wniosku – tymczasowy środek, taki tymczasowy środek powinien być należycie uzasadniony i mieć wyłącznie przejściowy charakter.
- 104) Każdy organ nadzorczy powinien mieć prawo uczestniczyć we wspólnych operacjach organów nadzorczych. Organ nadzorczy będący adresatem takiego wniosku powinien mieć obowiązek udzielić odpowiedzi w określonym terminie.
- 105) Aby zapewnić spójne stosowanie niniejszego rozporządzenia w całej Unii, należy ustanowić mechanizm spójności na potrzeby współpracy między organami nadzorczymi (...). Mechanizm ten powinien mieć w szczególności zastosowanie wtedy, gdy organ nadzorczy zamierza przyjąć środek mający wywoływać skutki prawne w odniesieniu do operacji przetwarzania, które znacznie wpływają na istotną liczbę podmiotów danych w kilku państwach członkowskich (...). Powinien mieć zastosowanie także wtedy, gdy *zainteresowany* organ nadzorczy lub Komisja występują z wnioskiem o rozwiązanie danej kwestii w ramach mechanizmu spójności. Mechanizm ten powinien pozostawać bez uszczerbku dla środków, które Komisja może przedsięwziąć w ramach korzystania z uprawnień przysługujących jej na mocy traktatów.
- 106) W ramach stosowania mechanizmu spójności Europejska Rada Ochrony Danych powinna w określonym terminie wydawać opinie, jeżeli tak postanowią większością głosów jej członkowie (...) lub jeżeli zwrócą się do niej z takim wnioskiem *zainteresowany* organ nadzorczy lub Komisja. Europejska Rada Ochrony Danych powinna być także umocowana do przyjmowania prawnie wiążących decyzji w razie sporów między organami nadzorczymi. W tym celu powinna wydawać, zasadniczo większością dwóch trzecich głosów swoich członków, prawnie wiążące decyzje w jasno określonych przypadkach, gdy wśród organów nadzorczych panują sprzeczne opinie – zwłaszcza w ramach mechanizmu współpracy między głównym organem nadzorczym a zainteresowanymi organami nadzorczymi – co do meritum sprawy, w szczególności tego, czy doszło do naruszenia niniejszego rozporządzenia.
- 107) (...)

- 108) Może wystąpić pilna potrzeba podjęcia działań w celu ochrony praw i wolności podmiotów danych, w szczególności gdy istnieje ryzyko, że wyegzekwowanie prawa przysługującego podmiotowi danych może być znacznie utrudnione. Dlatego organ nadzorczy, stosując mechanizm spójności, powinien móc przyjmować środki tymczasowe o określonym czasie obowiązywania.
- 109) Jeżeli zastosowanie mechanizmu jest obowiązkowe, od jego zastosowania powinna zależeć zgodność z prawem środka, który stosuje organ nadzorczy i który ma wywołać skutki prawne. W innych przypadkach o znaczeniu transgranicznym należy stosować mechanizm współpracy między głównym organem nadzorczym a zainteresowanymi organami nadzorczymi oraz można świadczyć wzajemną pomoc i prowadzić wspólne operacje między zainteresowanymi organami nadzorczymi na zasadzie dwustronnej lub wielostronnej bez uruchamiania mechanizmu spójności.
- 110) Aby propagować spójne stosowanie niniejszego rozporządzenia, należy utworzyć – jako niezależny organ Unii – Europejską Radę Ochrony Danych. Rada ta, by móc zrealizować swoje cele, powinna mieć osobowość prawną. Europejską Radę Ochrony Danych powinien reprezentować jej przewodniczący. Powinna ona zastąpić Grupę Roboczą ds. Ochrony Osób Fizycznych w zakresie Przetwarzania Danych Osobowych, powołaną na mocy dyrektywy 95/46/WE. W jej skład powinni wejść szefowie organów nadzorczych wszystkich państw członkowskich lub ich przedstawiciele (...). W jej działaniach powinni uczestniczyć Komisja i Europejski Inspektor Ochrony Danych, ale bez prawa głosu. Europejska Rada Ochrony Danych powinna przyczyniać się do spójnego stosowania niniejszego rozporządzenia w całej Unii, m.in. poprzez doradzanie Komisji – w szczególności w sprawie poziomu ochrony w państwach trzecich lub organizacjach międzynarodowych – i propagowanie współpracy organów nadzorczych w całej Unii. Wypełniając swoje zadania, Europejska Rada Ochrony Danych powinna działać w sposób niezależny.

- 110a) Europejską Radę Ochrony Danych powinien wspierać sekretariat, którego obsługę powinien zapewnić Europejski Inspektor Ochrony Danych. Personel sekretariatu Europejskiego Inspektora Ochrony Danych uczestniczący w wykonywaniu zadań, które niniejsze rozporządzenie powierza Europejskiej Radzie Ochrony Danych, powinien wykonywać swoje zadania wyłącznie pod kierunkiem przewodniczącego Europejskiej Rady Ochrony Danych i jemu podlegać. Organizacyjny rozdział personelu powinien dotyczyć wszystkich służb niezbędnych do niezależnego funkcjonowania Europejskiej Rady Ochrony Danych.
- 111) Każdy podmiot danych powinien mieć prawo wnieść skargę do organu nadzorczego, w szczególności w państwie członkowskim, w którym ma miejsce zwykłego pobytu, a jeżeli uzna, że jego prawa wynikające z niniejszego rozporządzenia są naruszane, lub jeżeli organ nadzorczy nie reaguje na skargę, częściowo lub w całości ją odrzuca lub oddala, lub nie podejmuje działań, choć jest to niezbędne do ochrony praw tego podmiotu – powinien mieć prawo do skutecznego środka ochrony prawnej, zgodnie z art. 47 karty praw podstawowych. Dochodzenie na podstawie skargi powinno być prowadzone – z zastrzeżeniem kontroli sądowej – w zakresie odpowiadającym konkretnej sprawie. Organ nadzorczy powinien w racjonalnym terminie poinformować podmiot danych o postępach i wynikach rozpatrywania skargi. Jeżeli dana sprawa wymaga dalszego dochodzenia lub koordynacji działań z innym organem nadzorczym, podmiot danych powinien zostać o tym uprzednio poinformowany. Aby ułatwić wnoszenie skarg, każdy organ nadzorczy powinien przedsięwziąć takie środki, jak udostępnienie formularza skargi, który można wypełnić także elektronicznie, przy czym nie należy wykluczać innych sposobów komunikacji.
- 112) Jeżeli podmiot danych uzna, że naruszane są jego prawa wynikające z niniejszego rozporządzenia, powinien mieć prawo zlecić wniesienie skargi w swoim imieniu do organu nadzorczego lub skorzystanie z prawa do sądowego środka ochrony prawnej w swoim imieniu organowi, organizacji lub stowarzyszeniu, które stawiają sobie za cel ochronę praw i interesów podmiotów danych w związku z ochroną ich danych i które zostały ustanowione zgodnie z prawem państwa członkowskiego. Państwa członkowskie mogą przewidzieć, że taki organ, taka organizacja lub takie stowarzyszenie powinny mieć prawo wnieść w tym państwie członkowskim skargę niezależnie od zlecenia otrzymanego od podmiotu danych lub powinny mieć prawo do skutecznego sądowego środka ochrony prawnej, jeżeli mają powody, by uznać, że (...) w wyniku przetwarzania danych osobowych niezgodnie z niniejszym rozporządzeniem naruszone zostały prawa podmiotu danych. Takiemu organowi, takiej organizacji lub takiemu stowarzyszeniu nie można umożliwiać ubiegania się o odszkodowanie w imieniu podmiotu danych.

113) Każda osoba fizyczna lub prawna ma prawo wnieść do Trybunału Sprawiedliwości Unii Europejskiej („Trybunał”) skargę o unieważnienie decyzji Europejskiej Rady Ochrony Danych na warunkach przewidzianych w art. 263 TFUE. Zainteresowane organy nadzorcze, które chcą takie decyzje zaskarżyć – jako adresaci takich decyzji – muszą wnieść pozew w terminie dwóch miesięcy od momentu, w którym decyzje te im notyfikowano, zgodnie z art. 263 TFUE. Jeżeli decyzje Europejskiej Rady Ochrony Danych bezpośrednio i indywidualnie dotyczą administratora, podmiotu przetwarzającego lub skarżącego, ten ostatni może wnieść skargę o unieważnienie tych decyzji; powinien to zrobić w terminie dwóch miesięcy od ich publikacji na internetowej stronie Europejskiej Rady Ochrony Danych, zgodnie z art. 263 TFUE. Bez uszczerbku dla tego prawa, które wynika z art. 263 TFUE, każda osoba fizyczna lub prawna powinna mieć prawo skorzystać przed właściwym sądem krajowym ze skutecznego środka ochrony prawnej względem decyzji organu nadzorczego wywołującej wobec niej skutki prawne. Taka decyzja może dotyczyć zwłaszcza korzystania przez organ nadzorczy z uprawnień dochodzeniowych, korekcyjnych i autoryzacyjnych lub oddalania lub odrzucania skarg. Prawo to nie dotyczy jednak innych niewiążących prawnie środków organów nadzorczych, takich jak wydawane przez nie opinie czy porady. Pozew przeciwko organowi nadzorcemu należy wnieść do sądu państwa członkowskiego, w którym organ nadzorczy ma siedzibę, a postępowanie powinno się toczyć zgodnie z krajowym prawem procesowym tego państwa członkowskiego. Sądom tym powinna przypadać pełna właściwość, w tym właściwość do analizy wszystkich faktycznych i prawnych kwestii mających zastosowanie do rozpatrywanego przez nie sporu. Jeżeli organ nadzorczy odrzuci lub oddali skargę, skarżący może wnieść pozew do sądu tego samego państwa członkowskiego. W kontekście środków ochrony prawnej dotyczących stosowania niniejszego rozporządzenia sądy krajowe uznające, że decyzja w tej kwestii jest niezbędna do wydania wyroku, mogą, a w przypadku przewidzianym w art. 267 TFUE – muszą, zwrócić się do Trybunału Sprawiedliwości o orzeczenie w trybie prejudycjalnym w sprawie wykładni prawa Unii, w tym niniejszego rozporządzenia.

Ponadto jeżeli decyzja organu nadzorczego wdrażająca decyzję Europejskiej Rady Ochrony Danych zostanie zaskarżona przed sądem krajowym, a przedmiotem będzie ważność decyzji Europejskiej Rady Ochrony Danych, sąd krajowy nie jest uprawniony do stwierdzenia nieważności decyzji Europejskiej Rady Ochrony Danych, ale jeżeli uważa tę decyzję za nieważną, musi przekazać sprawę jej ważności Trybunałowi Sprawiedliwości zgodnie z art. 267 TFUE, którego wykładni Trybunał Sprawiedliwości dokonał w sprawie *Foto-frost*<sup>1</sup>. Sąd krajowy nie może jednak przekazać Trybunałowi sprawy ważności decyzji Europejskiej Rady Ochrony Danych na wniosek osoby fizycznej lub prawnej, która miała możliwość wnieść skargę o unieważnienie tej decyzji, zwłaszcza gdy decyzja ta bezpośrednio i indywidualnie jej dotyczyła, ale nie zrobiła tego w terminie przewidzianym w art. 263 TFUE.

113a) Jeżeli sąd, przed którym toczy się postępowanie przeciwko decyzji organu nadzorczego, ma powody przypuszczać, że w sądzie właściwym innego państwa członkowskiego wszczęto postępowanie w sprawie tego samego przetwarzania – np. odnośnie do tego samego przedmiotu w związku z przetwarzaniem prowadzonym przez tego samego administratora lub przez ten sam podmiot przetwarzający lub odnośnie do tej samej przyczyny – powinien skontaktować się z tym sądem, aby potwierdzić fakt takiego powiązanego postępowania. Jeżeli przed sądem w innym państwie członkowskim toczy się powiązane postępowanie, każdy sąd inny niż sąd, przed którym jako pierwszym wszczęto postępowanie, może zawiesić postępowanie lub może – na wniosek jednej ze stron – stwierdzić brak swojej jurysdykcji na rzecz sądu, przed którym jako pierwszym wszczęto postępowanie, jeżeli ten ma jurysdykcję w danej sprawie, a jego prawo zezwala na połączenie takich powiązanych postępowań. Postępowania uznaje się za powiązane, jeżeli związek między nimi jest tak ścisły, że celowe jest ich łączne rozpatrzenie i rozstrzygnięcie, tak by uniknąć ryzyka zapadnięcia sprzecznych orzeczeń w odrębnych postępowaniach.

114) (...)

115) (...)

---

<sup>1</sup> Sprawa C-314/85.

116) W przypadku postępowania przeciwko administratorowi lub podmiotowi przetwarzającemu powód powinien mieć możliwość wybrania sądu, do którego chce wnieść pozew: do sądu w państwie członkowskim, w którym mają siedzibę administrator lub podmiot przetwarzający, lub do sądu, w którym podmiot danych ma miejsce zamieszkania, chyba że administrator jest organem publicznym działającym w ramach wykonywania swoich uprawnień publicznych.

117) (...).

118) Za szkodę, którą dana osoba poniosła wskutek przetwarzania niezgodnego z niniejszym rozporządzeniem, powinno przysługiwać odszkodowanie od administratora lub podmiotu przetwarzającego; ci jednak powinni zostać zwolnieni z odpowiedzialności prawnej, jeżeli udowodnią, że szkoda w żadnym razie nie powstała z ich winy (...). Pojęcie szkody należy interpretować szeroko, w świetle orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej, w sposób w pełni zgodny z celami niniejszego rozporządzenia. Pozostaje to bez uszczerbku dla wszelkich roszczeń z tytułu szkód wynikających z naruszenia innych przepisów prawa Unii lub prawa państwa członkowskiego. (...)

Jeżeli mowa jest o przetwarzaniu niezgodnym z niniejszym rozporządzeniem, dotyczy to także przetwarzania, które jest niezgodne z aktami delegowanymi i wykonawczymi przyjętymi w myśl niniejszego rozporządzenia oraz z prawem krajowym doprecyzującym niniejsze rozporządzenie.

Podmiot danych powinien uzyskać pełne i skuteczne odszkodowanie na poniesioną szkodę. Jeżeli administratorzy lub podmioty przetwarzające uczestniczą w tym samym przetwarzaniu, każdy administrator lub podmiot przetwarzający powinien odpowiadać prawnie za całość szkody. Jeżeli jednak zostaną włączeni do jednego postępowania sądowego zgodnie z prawem krajowym, odszkodowaniem można obarczyć każdego z administratorów i każdy z podmiotów przetwarzających stosownie do ich winy za szkodę wynikłą z przetwarzania, o ile podmiotowi danych zapewnione zostanie pełne i skuteczne odszkodowanie za poniesioną szkodę. Każdy administrator lub podmiot przetwarzający, który (...) wypłacił pełne odszkodowanie, może następnie wszcząć postępowanie regresowe wobec innych administratorów lub podmiotów przetwarzających uczestniczących w tym samym przetwarzaniu.

118a) Jeżeli niniejsze rozporządzenie przewiduje szczegółowe przepisy o jurysdykcji – w szczególności odnośnie do postępowań w zakresie sądowych środków ochrony prawnej, w tym odszkodowania, przeciwko administratorowi lub podmiotowi przetwarzającemu – uszczerbku dla stosowania takich szczegółowych przepisów nie powinny powodować ogólne przepisy o jurysdykcji, takie jak rozporządzenie (UE) nr 1215/2012.

- 118b) Aby egzekwowanie przepisów niniejszego rozporządzenia było skuteczniejsze, można za jego naruszenie – oprócz lub zamiast odpowiednich środków nakładanych przez organ nadzorczy na mocy niniejszego rozporządzenia – nakładać kary i grzywny administracyjne. Jeżeli naruszenie jest niewielkie lub jeżeli grożąca grzywna stanowiłaby dla osoby fizycznej nieproporcjonalne obciążenie, zamiast nakładać grzywnę można udzielić upomnienia. Powinno się jednak zwrócić należytą uwagę na charakter, wagę oraz czas trwania naruszenia, na to, czy naruszenie nie było umyślne, na działania podjęte dla zminimalizowania szkody, na stopień odpowiedzialności lub wszelkie odnośne wcześniejsze naruszenia, na sposób, w jaki organ nadzorczy dowiedział się o naruszeniu, na przestrzeganie środków nałożonych na administratora lub podmiot przetwarzający, na stosowanie kodeksów postępowania oraz wszelkie inne czynniki obciążające lub łagodzące. Nakładanie kar i grzywien administracyjnych powinno podlegać odpowiednim gwarancjom proceduralnym zgodnym z ogólnymi zasadami prawa Unii i z Kartą praw podstawowych, w tym skutecznej ochronie prawnej i sprawiedliwości proceduralnej. Jeżeli prawo krajowe państwa członkowskiego nie przewiduje grzywien administracyjnych, takie państwo członkowskie może nie przewidywać grzywien administracyjnych za naruszenie niniejszego rozporządzenia, o ile naruszenia takie podlegają już sankcjom karnym w ramach prawa krajowego, a te są skuteczne, proporcjonalne i odstraszające, uwzględnivszy poziom grzywien administracyjnych przewidzianych w niniejszym rozporządzeniu.
- 119) Państwa członkowskie mogą ustanowić przepisy o sankcjach karnych za naruszenie niniejszego rozporządzenia, w tym za naruszenie krajowych przepisów przyjętych na jego mocy i w jego granicach. Sankcje te mogą również dopuszczać pozbawienie zysków wynikających z naruszenia niniejszego rozporządzenia. Jednak nałożenie sankcji karnych za naruszenie takich krajowych przepisów oraz nałożenie sankcji administracyjnych nie powinno prowadzić do złamania zasady *ne bis in idem*, zgodnie z wykładnią Trybunału Sprawiedliwości.



- 120) W celu wzmocnienia i zharmonizowania kar administracyjnych za naruszenie niniejszego rozporządzenia każdy organ nadzorczy powinien być uprawniony do nakładania grzywien administracyjnych. W niniejszym rozporządzeniu należy wymienić czyny zabronione, wskazać górną granicę i kryteria ustalania odnośnych grzywien administracyjnych, które właściwy organ nadzorczy powinien określać oddzielnie dla każdego przypadku z uwzględnieniem wszystkich stosownych okoliczności danej sytuacji, z należyтым uwzględnieniem w szczególności charakteru, wagi, czasu trwania naruszenia i jego konsekwencji, a także środków podjętych w celu zastosowania się do obowiązków wynikających z niniejszego rozporządzenia oraz w celu zapobieżenia konsekwencjom naruszenia lub w celu zminimalizowania tych konsekwencji. Jeżeli grzywna jest nakładana na podmiot niebędący przedsiębiorstwem handlowym, organ nadzorczy, ustalając właściwy poziom grzywny, powinien wziąć pod uwagę ogólny poziom dochodów w danym państwie członkowskim. Aby propagować spójne stosowanie grzywien administracyjnych, można także użyć mechanizmu spójności. Państwa członkowskie powinny określić, czy i w jakim zakresie grzywnom administracyjnym powinny podlegać organy publiczne. Nałożenie grzywny administracyjnej lub wydanie ostrzeżenia nie wpływa na stosowanie innych uprawnień organów nadzorczych ani innych sankcji na mocy niniejszego rozporządzenia.
- 120a) W sytuacjach, w których niniejsze rozporządzenie nie harmonizuje kar administracyjnych, lub w razie potrzeby w innych przypadkach, np. w przypadku poważnego naruszenia niniejszego rozporządzenia, państwa członkowskie powinny wdrożyć system przewidujący skuteczne, proporcjonalne i odstraszające kary. Charakter takich kar (karny lub administracyjny) powinno określać prawo krajowe.

121) Prawo państw członkowskich powinno godzić przepisy regulujące wolność wypowiedzi i informacji, w tym wypowiedzi dziennikarskiej, akademickiej, artystycznej lub literackiej, z prawem do ochrony danych osobowych na mocy niniejszego rozporządzenia. Przetwarzanie danych osobowych do celów dziennikarskich lub do celów wypowiedzi akademickiej, artystycznej lub literackiej powinno podlegać odstępstwom lub wyjątkom od niektórych przepisów niniejszego rozporządzenia, jeżeli jest to niezbędne, by pogodzić prawo do ochrony danych osobowych z prawem do wolności wypowiedzi i informacji, zagwarantowanymi w art. 11 Karty praw podstawowych Unii Europejskiej. Powinno mieć to zastosowanie w szczególności do przetwarzania danych osobowych w dziedzinie audiowizualnej oraz w archiwach i bibliotekach prasowych. Państwa członkowskie powinny więc przyjąć środki ustawodawcze ustanawiające wyjątki i odstępstwa niezbędne do zapewnienia równowagi między tymi prawami podstawowymi. Państwa członkowskie powinny przyjąć takie wyjątki i odstępstwa w odniesieniu do zasad ogólnych, praw przysługujących podmiotowi danych, administratora i podmiotu przetwarzającego, przekazywania danych do państw trzecich lub organizacji międzynarodowych, niezależnych organów nadzorczych, współpracy i spójności. Jeżeli wyjątki i odstępstwa różnią się zależnie od państwa członkowskiego, zastosowanie powinno mieć prawo krajowe państwa członkowskiego, któremu podlega administrator. Aby uwzględnić, jak ważne dla każdego demokratycznego społeczeństwa jest prawo do wolności wypowiedzi, pojęcia dotyczące tej wolności, takie jak dziennikarstwo, należy interpretować szeroko. (...)

121a) Niniejsze rozporządzenie pozwala uwzględnić przy stosowaniu jego przepisów zasadę publicznego dostępu do dokumentów urzędowych. Publiczny dostęp do dokumentów urzędowych można uznać za interes publiczny. Organ publiczny lub podmiot publiczny powinny móc publicznie ujawniać dane osobowe z dokumentów przez siebie przechowywanych, jeżeli takie ujawnienie jest przewidziane prawem Unii lub prawem państwa członkowskiego, któremu organ ten lub podmiot podlegają. Prawa takie powinny godzić publiczny dostęp do dokumentów urzędowych i ponowne wykorzystywanie informacji sektora publicznego z prawem do ochrony danych osobowych, i dlatego mogą przewidywać niezbędne odstępstwa od przepisów niniejszego rozporządzenia. Wzmianka o organach i podmiotach publicznych powinna w tym kontekście dotyczyć wszystkich organów lub innych podmiotów objętych prawem państwa członkowskiego o publicznym dostępie do dokumentów. Dyrektywa 2003/98/WE Parlamentu Europejskiego i Rady z dnia 17 listopada 2003 r. w sprawie ponownego wykorzystywania informacji sektora publicznego nie narusza ani w żaden sposób nie wpływa na poziom ochrony osób fizycznych w związku z przetwarzaniem danych osobowych wynikający z przepisów prawa Unii i prawa krajowego, a zwłaszcza nie zmienia obowiązków i praw przewidzianych w niniejszym rozporządzeniu. Dyrektywa ta nie powinna mieć zastosowania w szczególności do dokumentów, do których – na mocy systemów dostępu – dostęp jest wykluczony lub ograniczony z powodu ochrony danych osobowych, ani do fragmentów dokumentów dostępnych na mocy tych systemów, ale zawierających dane osobowe, których ponowne wykorzystanie zostało określone w prawie jako niezgodne z prawem o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych.

122) (...).

123) (...).

124) W prawie krajowym lub układach zbiorowych (w tym umowach zakładowych) mogą być przewidziane przepisy szczegółowe o przetwarzaniu danych osobowych pracowników w kontekście zatrudnienia, w szczególności do celów procedury rekrutacyjnej, wykonania umowy o pracę, w tym wykonania obowiązków określonych prawem lub umowami zbiorowymi, zarządzania, planowania i organizacji pracy, równości i różnorodności w miejscu pracy, bezpieczeństwa i higieny pracy oraz do celów indywidualnego lub zbiorowego wykonywania praw i korzystania ze świadczeń związanych z zatrudnieniem, a także do celów zakończenia stosunku pracy.

125) Przetwarzanie danych osobowych do celów historycznych, statystycznych lub (...) naukowych oraz do celów archiwizacyjnych w interesie publicznym (...) powinno być zgodne nie tylko z ogólnymi zasadami i szczegółowymi przepisami niniejszego rozporządzenia – zwłaszcza jeżeli chodzi o warunki zgodności z prawem – lecz także powinno respektować inne odnośne przepisy, takie jak przepisy o próbach klinicznych. Dalsze przetwarzanie danych osobowych do celów historycznych, statystycznych i naukowych oraz do celów archiwizacyjnych w interesie publicznym (...) nie powinno być uznawane za niezgodne z celami, w których dane te zostały pierwotnie zebrane, i może trwać przez okres dłuższy niż okres niezbędny do pierwotnego celu (...). Państwa członkowskie powinny móc przewidzieć – na konkretnych warunkach i z zastrzeżeniem istnienia odpowiednich gwarancji dla podmiotów danych – szczegóły i odstępstwa dotyczące wymogu informacji oraz dotyczące prawa do dostępu, poprawiania, usuwania, prawa do „bycia zapomnianym”, ograniczeń przetwarzania i prawa do przenoszenia danych oraz prawa do sprzeciwu, gdy dane osobowe są przetwarzane do celów historycznych, statystycznych lub naukowych i do celów archiwizacyjnych (...). Przedmiotowe warunki i gwarancje mogą skutkować szczegółowymi procedurami korzystania z tych praw przez podmioty danych – jeżeli jest to właściwe w świetle celów, którym służy konkretne przetwarzanie – oraz środkami technicznymi i organizacyjnymi mającymi ograniczyć przetwarzanie danych osobowych w myśl zasady proporcjonalności i zasady konieczności.

125a) (...).

125aa) Łącząc ze sobą informacje z rejestrów, naukowcy mogą uzyskać nową, wartościową wiedzę np. o częstych chorobach, takich jak choroba układu krążenia, rak czy depresja. Korzystając z rejestrów, można pogłębić wyniki badań naukowych, gdyż będą się one opierać na większej próbie. W naukach społecznych badania oparte na rejestrach pozwalają naukowcom uzyskać kluczową wiedzę o długoterminowych skutkach wielu czynników społecznych, np. bezrobocia czy edukacji, i łączyć te informacje z innymi czynnikami bytowymi. Wyniki badań uzyskane na podstawie rejestrów dostarczają solidnej, dobrej jakościowo wiedzy, która może posłużyć do opracowywania i realizowania polityki opartej na wiedzy, podnieść jakość życia wielu osób, a także zwiększyć skuteczność usług społecznych itp.

Dla ułatwienia badań naukowych dopuszcza się przetwarzanie danych osobowych w celach naukowych z zastrzeżeniem odpowiednich warunków i gwarancji przewidzianych w prawie państwa członkowskiego lub w prawie Unii. Zatem nie dla każdego dalszego przetwarzania do celów naukowych powinna być konieczna zgoda podmiotu danych.

125b) W rezolucji z dnia 6 maja 2003 r. o archiwach w państwach członkowskich Rada zwróciła uwagę na znaczenie archiwów dla zrozumienia historii i kultury Europy oraz na fakt, że dobrze zachowane i dostępne archiwa przyczyniają się do funkcjonowania naszych społeczeństw w sposób demokratyczny<sup>2</sup>. Jeżeli dane osobowe są przetwarzane do celów archiwizacyjnych, niniejsze rozporządzenie powinno mieć zastosowanie także do takiego przetwarzania; należy jednak pamiętać, że niniejsze rozporządzenie nie powinno mieć zastosowania do osób zmarłych.

Organy lub podmioty publiczne lub podmioty prywatne posiadające rejestry będące przedmiotem interesu publicznego powinny być służbami, które – zgodnie z prawem Unii lub prawem państwa członkowskiego – mają prawny obowiązek nabywania, ochrony, oszacowywania, systematyzowania, opisywania, przekazywania, promowania, rozpowszechniania i udostępniania rejestrów o długotrwałej wartości dla ogólnego interesu publicznego. Państwa członkowskie powinny także mieć prawo przewidzieć, że dane osobowe mogą być dalej przetwarzane do celów archiwizacyjnych, na przykład z myślą o dostarczeniu konkretnych informacji o postawie politycznej w ramach dawnych systemów państw totalitarnych.

---

<sup>2</sup> Dz.U. C 113 z 13.5.2003, s. 2.

We właściwym stosowaniu niniejszego rozporządzenia, w tym gdy dane osobowe są przetwarzane do celów archiwizacyjnych w interesie publicznym, pomóc mogą kodeksy postępowania, doprecyzowujące odpowiednie gwarancje dla praw i wolności podmiotu danych. Takie kodeksy powinny zostać opracowane przez oficjalne archiwa państw członkowskich lub Europejski Zespół ds. Archiwów. Jeżeli chodzi o międzynarodowe przekazywanie danych osobowych zawartych w archiwach, musi się ono odbywać bez uszczerbku dla stosowania europejskich i krajowych przepisów o obiegu dóbr kultury i dóbr narodowych.

126) Jeżeli dane osobowe są przetwarzane do celów naukowych, niniejsze rozporządzenie powinno mieć zastosowanie także do takiego przetwarzania. Do celów niniejszego rozporządzenia przetwarzanie danych osobowych do celów naukowych powinno obejmować badania podstawowe, badania stosowane, badania finansowane ze środków prywatnych oraz powinno uwzględniać cel Unii określony w art. 179 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej, którym jest utworzenie europejskiej przestrzeni badawczej. Cele naukowe powinny obejmować także badania prowadzone w interesie publicznym w dziedzinie zdrowia publicznego. Aby uwzględniona została specyfika przetwarzania danych osobowych do celów naukowych, zastosowanie powinny mieć specjalne warunki, zwłaszcza w odniesieniu do publikacji lub innego ujawniania danych osobowych w kontekście celów naukowych. Jeżeli wynik badań naukowych, w szczególności w kontekście zdrowotnym, uzasadnia dalsze środki w interesie podmiotu danych, do środków tych powinny mieć zastosowanie przepisy ogólne niniejszego rozporządzenia.

126a) Jeżeli dane osobowe są przetwarzane do celów historycznych, niniejsze rozporządzenie powinno mieć zastosowanie także do takiego przetwarzania. Powinno to dotyczyć m.in. badań historycznych i badań do celów genealogicznych; należy jednak pamiętać, że niniejsze rozporządzenie nie powinno mieć zastosowania do osób zmarłych.

126b) Do celów wyrażenia zgody na udział w badaniach naukowych podczas prób klinicznych (...) zastosowanie powinny mieć odnośne przepisy rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 536/2014.

126c) Jeżeli dane osobowe są przetwarzane do celów statystycznych, niniejsze rozporządzenie powinno mieć zastosowanie do takiego przetwarzania. Prawo Unii lub prawo państwa członkowskiego powinny – w granicach niniejszego rozporządzenia – określać treść statystyczną, kontrolę dostępu, warunki przetwarzania danych osobowych do celów statystycznych oraz odpowiednie środki mające chronić prawa i wolności podmiotu danych oraz gwarantować poufność statystyczną.

126d) Należy chronić informacje poufne, które organy statystyczne Unii i państw członkowskich zbierają do celów opracowywania oficjalnych statystyk europejskich i krajowych. Statystyki europejskie należy projektować, tworzyć i rozpowszechniać zgodnie z zasadami statystycznymi przewidzianymi w art. 338 ust. 2 Traktatu o funkcjonowaniu Unii Europejskiej, przy czym statystyki krajowe powinny być także zgodne z prawem krajowym. Dalsze szczegółowe informacje o statystycznej poufności statystyki europejskiej zawiera rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 223/2009 z dnia 11 marca 2009 r. w sprawie statystyki europejskiej oraz uchylające rozporządzenie Parlamentu Europejskiego i Rady (WE, Euratom) nr 1101/2008 w sprawie przekazywania do Urzędu Statystycznego Wspólnot Europejskich danych statystycznych objętych zasadą poufności, rozporządzenie Rady (WE) nr 322/97 w sprawie statystyk Wspólnoty oraz decyzję Rady 89/382/EWG, Euratom w sprawie ustanowienia Komitetu ds. Programów Statystycznych Wspólnot Europejskich<sup>3</sup>.

127) Jeżeli chodzi o uprawnienia organów nadzorczych do uzyskania od administratora lub podmiotu przetwarzającego dostępu do danych osobowych oraz do pomieszczeń, państwa członkowskie mogą przyjąć prawem, w granicach niniejszego rozporządzenia, przepisy szczegółowe mające chronić obowiązek dochowania tajemnicy służbowej lub innej równoważnej tajemnicy, o ile jest to niezbędne, by pogodzić prawo do ochrony danych osobowych z obowiązkiem dochowania tajemnicy służbowej. Pozostaje to bez uszczerbku dla istniejących obowiązków państw członkowskich w zakresie stosowania tajemnicy służbowej na mocy prawa Unii.

128) Niniejsze rozporządzenie respektuje status przyznany kościołom oraz stowarzyszeniom lub wspólnotom religijnym na mocy prawa konstytucyjnego obowiązującego w państwach członkowskich i nie narusza tego statusu – jak uznano w art. 17 Traktatu o funkcjonowaniu Unii Europejskiej. (...).

---

<sup>3</sup> Dz.U. L 87 z 31.3.2009, s. 164–173.

- 129) Aby spełnić cele niniejszego rozporządzenia, mianowicie chronić podstawowe prawa i wolności osób fizycznych, w szczególności prawo do ochrony danych osobowych, oraz zagwarantować swobodny przepływ danych osobowych w Unii, należy przekazać Komisji uprawnienia do przyjmowania aktów zgodnie z art. 290 Traktatu o funkcjonowaniu Unii Europejskiej. Akty delegowane powinny zostać przyjęte w szczególności w odniesieniu do (...); kryteriów i wymogów mechanizmów certyfikacji; (...); (...). Szczególnie ważne jest, aby w czasie swoich prac przygotowawczych Komisja prowadziła odpowiednie konsultacje, w tym na szczeblu eksperckim. W trakcie przygotowywania i opracowywania aktów delegowanych Komisja powinna zapewnić jednoczesne, terminowe i odpowiednie przekazywanie stosownych dokumentów Parlamentowi Europejskiemu i Radzie.
- 130) Aby zapewnić jednolite warunki wdrażania niniejszego rozporządzenia, należy powierzyć Komisji uprawnienia wykonawcze w odniesieniu do: (...); standardowych klauzul umownych między administratorami a podmiotami przetwarzającymi oraz między podmiotami przetwarzającymi; kodeksów postępowania; (...) technicznych standardów i mechanizmów certyfikacji; odpowiedniego poziomu ochrony zapewnianego przez państwo trzecie, terytorium lub sektor przetwarzania w tym państwie trzecim bądź organizację międzynarodową; przyjmowania standardowych klauzul ochrony danych; formatów i procedur wymiany informacji między administratorami, podmiotami przetwarzającymi i organami nadzorczymi na potrzeby wiążących reguł korporacyjnych; (...) wzajemnej pomocy; (...); uzgodnień w sprawie wymiany informacji drogą elektroniczną między organami nadzorczymi oraz między organami nadzorczymi a Europejską Radą Ochrony Danych. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 182/2011 z dnia 16 lutego 2011 r. ustanawiającym przepisy i zasady ogólne dotyczące trybu kontroli przez państwa członkowskie wykonywania uprawnień wykonawczych przez Komisję. W tym kontekście Komisja powinna rozważyć wprowadzenie szczególnych środków dla mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw.



- 131) Procedurę sprawdzającą należy stosować do przyjmowania aktów wykonawczych w odniesieniu do: standardowych klauzul umownych między administratorami a podmiotami przetwarzającymi oraz między podmiotami przetwarzającymi; kodeksów postępowania; (...) technicznych standardów i mechanizmów certyfikacji; odpowiedniego poziomu ochrony zapewnianego przez państwo trzecie, terytorium lub sektor przetwarzania w tym państwie trzecim bądź organizację międzynarodową; przyjmowania standardowych klauzul ochrony danych; formatów i procedur wymiany informacji drogą elektroniczną między administratorami, podmiotami przetwarzającymi i organami nadzorczymi na potrzeby wiążących reguł korporacyjnych; wzajemnej pomocy; (...); uzgodnień w sprawie wymiany informacji drogą elektroniczną między organami nadzorczymi oraz między organami nadzorczymi a Europejską Radą Ochrony Danych, o ile akty te mają zakres ogólny.
- 132) Komisja powinna przyjmować akty wykonawcze o natychmiastowym zastosowaniu, jeżeli jest to szczególnie pilne w należycie uzasadnionych przypadkach dotyczących państwa trzeciego, terytorium lub sektora przetwarzania w tym państwie trzecim bądź organizacji międzynarodowej, które nie zapewniają odpowiedniego poziomu ochrony (...).
- 133) Ponieważ celów niniejszego rozporządzenia, mianowicie zapewnienia równoważnego poziomu ochrony osób fizycznych i swobodnego przepływu danych w całej Unii, nie mogą w wystarczającym stopniu osiągnąć państwa członkowskie, natomiast z uwagi na zakres i skutki proponowanego działania możliwe jest lepsze ich osiągnięcie na szczeblu unijnym, Unia może przyjąć środki zgodnie z zasadą pomocniczości, o której mowa w art. 5 Traktatu o Unii Europejskiej. Zgodnie z zasadą proporcjonalności określoną w tym samym artykule niniejsze rozporządzenie nie wykracza poza zakres niezbędny do osiągnięcia tego celu.

- 134) Niniejszym rozporządzeniem należy uchylić dyrektywę 95/46/WE. Przetwarzanie, które w dniu wejścia w życie niniejszego rozporządzenia już się toczy, powinno w terminie dwóch lat od wejścia w życie niniejszego rozporządzenia zostać dostosowane do jego przepisów. Jeżeli jednak takie przetwarzanie jest zgodne z dyrektywą 95/46/WE, wymogi niniejszego rozporządzenia dotyczące dokonywania oceny skutków pod kątem ochrony danych oraz uprzednich konsultacji z organem nadzorczym nie powinny mieć zastosowania do operacji przetwarzania, które przed wejściem w życie niniejszego rozporządzenia już się toczyły, gdyż wymogów tych z uwagi na ich charakter należy dopełnić przed przetwarzaniem. Jeżeli takie przetwarzanie jest zgodne z dyrektywą 95/46/WE, podmiot danych nie musi też ponownie udzielać zgody, aby administrator mógł kontynuować przetwarzanie po terminie zastosowania niniejszego rozporządzenia.

Decyzje przyjęte przez Komisję oraz zezwolenia wydane przez organy nadzorcze na podstawie dyrektywy 95/46/WE pozostają w mocy do czasu ich zmiany, zastąpienia lub uchylenia.

- 135) Niniejsze rozporządzenie powinno mieć zastosowanie do wszystkich tych kwestii dotyczących ochrony podstawowych praw i wolności w związku z przetwarzaniem danych osobowych, które nie podlegają szczególnym obowiązkom mającym ten sam cel określonym w dyrektywie 2002/58/WE, w tym obowiązkom nałożonym na administratora oraz prawom osób fizycznych. Aby doprecyzować związek między niniejszym rozporządzeniem a dyrektywą 2002/58/WE, dyrektywę tę należy odpowiednio zmienić. Gdy niniejsze rozporządzenie zostanie przyjęte, dyrektywa 2002/58/WE powinna zostać poddana przeglądowi, w szczególności w celu zapewnienia jej spójności z niniejszym rozporządzeniem (...).

136) (...)

137) (...)

138) (...).

139) (...)

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

## **ROZDZIAŁ I**

### **PRZEPISY OGÓLNE**

#### *Artykuł 1*

##### ***Przedmiot i cele***

1. W niniejszym rozporządzeniu ustanowione zostają przepisy dotyczące ochrony osób fizycznych w związku z przetwarzaniem danych osobowych oraz przepisy dotyczące swobodnego przepływu danych osobowych.
2. Niniejsze rozporządzenie chroni podstawowe prawa i wolności osób fizycznych, w szczególności ich prawo do ochrony danych osobowych.
- 2a. Państwa członkowskie mogą zachować lub wprowadzić bardziej szczegółowe przepisy, aby dostosować stosowanie przepisów niniejszego rozporządzenia do przetwarzania danych osobowych służącego wypełnieniu obowiązku prawnego lub wykonaniu zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi lub służącego innym szczególnym sytuacjom związanym z przetwarzaniem, o których mowa w art. 6 ust. 1 lit. c) i e), poprzez dokładniejsze określenie szczegółowych wymogów przetwarzania i innych środków w celu zapewnienia zgodności przetwarzania z prawem i jego rzetelności, także w innych szczególnych sytuacjach związanych z przetwarzaniem przewidzianych w rozdziale IX.
3. Nie ogranicza się ani nie zakazuje swobodnego przepływu danych osobowych w Unii z powodów odnoszących się do ochrony osób fizycznych w związku z przetwarzaniem danych osobowych.

#### *Artykuł 2*

##### ***Zakres materialny***

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

2. Niniejsze rozporządzenie nie ma zastosowania do przetwarzania danych osobowych:
- a) w ramach działalności nieobjętej zakresem prawa Unii (...);
  - b) przez instytucje, organy i jednostki organizacyjne Unii;
  - c) przez państwa członkowskie w ramach wykonywania działań wchodzących w zakres tytułu V rozdział 2 Traktatu o Unii Europejskiej;
  - d) przez osobę fizyczną (...) w ramach (...) działalności (...) osobistej lub domowej;
  - e) przez właściwe organy (...) do zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, ich wykrywania lub ścigania, wykonywania sankcji karnych lub ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom.
3. (...).

### *Artykuł 3*

#### ***Zakres terytorialny***

1. Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych w kontekście działalności prowadzonej przez siedzibę administratora lub podmiotu przetwarzającego w Unii.
2. Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych podmiotów danych mających miejsce zamieszkania w Unii przez administratora niemającego siedziby w Unii, jeżeli czynności przetwarzania wiążą się z:
- a) oferowaniem towarów lub usług takim podmiotom danych w Unii – niezależnie od tego, czy wymaga się od tych podmiotów płatności; lub
  - b) monitorowaniem ich zachowania, o ile do zachowania tego dochodzi w Unii Europejskiej.
3. Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych przez administratora niemającego siedziby w Unii, ale mającego siedzibę w miejscu, w którym na mocy prawa międzynarodowego publicznego ma zastosowanie prawo krajowe państwa członkowskiego.

## Artykuł 4

### Definicje

Do celów niniejszego rozporządzenia:

- (1) „dane osobowe” oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („podmiocie danych”); osoba możliwa do zidentyfikowania to osoba, którą można bezpośrednio lub pośrednio zidentyfikować (...), w szczególności na podstawie identyfikatora, takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub co najmniej jeden znak szczególny związany z jej tożsamością fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną.
- (2a) (...)
- (3) „przetwarzanie” oznacza każdą operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub nie, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przekazanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie (...), ograniczanie, usuwanie lub niszczenie;
- (3a) „ograniczenie przetwarzania” oznacza odcinanie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
- (3b) „pseudonimizacja” oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnemu podmiotowi danych bez użycia dodatkowych informacji, o ile takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie (...).
- (4) „zbiór danych” oznacza każdy uporządkowany zestaw danych osobowych, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

- (5) „administrator” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę organizacyjną lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele (...) i sposoby przetwarzania danych osobowych; jeżeli cele (...) i sposoby przetwarzania są ustalane prawem Unii lub prawem państwa członkowskiego, to również prawem Unii lub prawem państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;
- (6) „podmiot przetwarzający” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę organizacyjną lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
- (7) „odbiorca” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę organizacyjną lub inny podmiot (...), któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią; niemniej za odbiorców nie uznaje się organów, które mogą otrzymywać dane w ramach konkretnego dochodzenia;
- (8) „zgoda podmiotu danych” oznacza dobrowolne, konkretne i świadome (...) okazanie woli, którym podmiot danych w formie oświadczenia lub wyraźnego działania potwierdzającego przyzwala na przetwarzanie dotyczących go danych osobowych;
- (9) „naruszenie ochrony danych osobowych” oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przenoszonych, przechowywanych lub w inny sposób przetwarzanych;
- (10) „dane genetyczne” oznaczają wszelkie dane osobowe o odziedziczonych lub nabytych cechach genetycznych osoby fizycznej, (...) które skutkują niepowtarzalnymi informacjami o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy jej próbki biologicznej;
- (11) „dane biometryczne” oznaczają wszelkie dane osobowe, które wynikają z konkretnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;

- (12) „dane dotyczące zdrowia” oznaczają dane o zdrowiu fizycznym lub psychicznym osoby fizycznej, ujawniające informacje o stanie jej zdrowia;
- (12a) „profilowanie” oznacza każdą formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu tych danych do oceny czynników osobowych osoby fizycznej, w szczególności do analizy i prognozy aspektów dotyczących efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się;
- (12b) (...)
- (13) „główna siedziba” oznacza
- jeżeli chodzi o administratora mającego siedzibę w więcej niż jednym państwie członkowskim – miejsce, w którym znajduje się jego centralna administracja w Unii, a jeżeli decyzje co do celów (...) i sposobów przetwarzania danych osobowych zapadają w innej siedzibie tego administratora w Unii i siedziba ta ma prawo nakazać wykonanie takich decyzji, to za główną siedzibę uznaje się siedzibę, w której zapadły takie decyzje.
  - jeżeli chodzi o podmiot przetwarzający mający siedzibę w więcej niż jednym państwie członkowskim – miejsce, w którym znajduje się jego centralna administracja w Unii, a jeżeli podmiot przetwarzający nie ma centralnej administracji w Unii – siedziba podmiotu przetwarzającego w Unii, w której odbywają się główne czynności przetwarzania w ramach działalności siedziby podmiotu przetwarzającego, w zakresie w jakim podmiot przetwarzający podlega szczegółowym obowiązkom na mocy niniejszego rozporządzenia;
- (14) „przedstawiciel” oznacza każdą osobę fizyczną lub prawną mającą miejsce zamieszkania lub siedzibę w Unii, (...) która wyznaczona na piśmie przez administratora na mocy art. 25 reprezentuje administratora w odniesieniu do jego obowiązków wynikających z niniejszego rozporządzenia (...);
- (15) „firma” oznacza każdą osobę fizyczną lub prawną prowadzącą działalność gospodarczą, niezależne od formy prawnej, (...) w tym (...) partnerstwo lub stowarzyszenie prowadzące regularną działalność gospodarczą;

- (16) „grupa przedsiębiorstw” oznacza przedsiębiorstwo sprawujące kontrolę oraz przedsiębiorstwa przez nie kontrolowane;
- (17) „wiązące reguły korporacyjne” oznaczają strategie ochrony danych osobowych stosowane przez administratora lub podmiot przetwarzający, którzy mają siedzibę na terytorium państwa członkowskiego Unii, przy przekazaniu lub przekazywaniu danych osobowych administratorowi lub podmiotowi przetwarzającemu w co najmniej jednym państwie trzecim w ramach grupy przedsiębiorstw lub grupy firm prowadzących wspólną działalność gospodarczą;
- (18) (...)
- (19) „organ nadzorczy” oznacza niezależny organ publiczny ustanowiony przez państwo członkowskie na mocy art. 46;
- (19a) „zainteresowany organ nadzorczy” oznacza
- organ nadzorczy, którego dotyczy przetwarzanie, ponieważ:
    - a) administrator lub podmiot przetwarzający mają siedzibę na terytorium państwa członkowskiego tego organu;
    - b) przetwarzanie znacznie wpływa lub może znacznie wpłynąć na podmioty danych mające miejsce zamieszkania w tym państwie członkowskim; lub
    - c) wniesiono do niego odnośną skargę.
- (19b) „transnarodowe przetwarzanie danych osobowych” oznacza albo:
- (a) przetwarzanie, które odbywa się w ramach działalności siedzib w więcej niż jednym państwie członkowskim administratora lub podmiotu przetwarzającego w Unii, a administrator lub podmiot przetwarzający mają siedzibę w więcej niż jednym państwie członkowskim; albo
  - (b) przetwarzanie, które odbywa się w ramach działalności pojedynczej siedziby administratora lub podmiotu przetwarzającego w Unii, ale które znacznie wpływa lub może znacznie wpłynąć na podmioty danych w więcej niż jednym państwie członkowskim.



- (19c) „istotny i zasadny sprzeciw” oznacza:  
sprzeciw co tego, czy doszło do naruszenia niniejszego rozporządzenia lub – zależnie  
od przypadku – czy planowane działanie wobec administratora lub podmiotu  
przetwarzającego jest zgodne z niniejszym rozporządzeniem. Sprzeciw musi jasno  
wskazywać wagę zagrożeń wynikających z projektu decyzji dla podstawowych praw  
i wolności podmiotów danych, a w stosownym przypadku dla swobodnego  
przepływu danych osobowych.
- (20) „usługa społeczeństwa informacyjnego” oznacza każdą usługę w rozumieniu art. 1  
ust. 2 dyrektywy 98/34/WE Parlamentu Europejskiego i Rady z dnia 22 czerwca  
1998 r. ustanawiającej procedurę udzielania informacji w zakresie norm i przepisów  
technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego.
- (21) „organizacja międzynarodowa” oznacza organizację i organy jej podlegające będące  
podmiotami prawa międzynarodowego publicznego lub inny organ powołany  
porozumieniem między co najmniej dwoma państwami lub na podstawie takiego  
porozumienia;

## ROZDZIAŁ II

### ZASADY

#### *Artykuł 5*

#### *Zasady przetwarzania danych osobowych*

1. Dane osobowe muszą być:

- a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla podmiotu danych;
- b) zbierane w konkretnych, wyraźnych i uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie danych osobowych do celów archiwizacyjnych w interesie publicznym lub do celów naukowych, statystycznych lub historycznych nie jest uznawane w myśl z art. 83 za niezgodne z pierwotnymi celami;
- c) ilościowo i treściowo odpowiednie oraz nienadmierne w stosunku do celów, w których są przetwarzane (...);
- d) ściśle i w razie potrzeby uaktualniane; należy podjąć wszelkie racjonalne działania, aby dane osobowe, które są nieściśle w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub poprawione;
- e) przechowywane w formie umożliwiającej identyfikację podmiotów danych przez okres nie dłuższy, niż jest to niezbędne do celów, w których są przetwarzane (...); dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane do celów archiwizacyjnych w interesie publicznym lub do celów naukowych, statystycznych lub historycznych na mocy art. 83, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności podmiotów danych;
- ee) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych.
- f) (...)

2. Za przestrzeganie przepisów ust. 1 odpowiada administrator.

#### *Artykuł 6*

#### ***Zgodność przetwarzania z prawem***

1. Przetwarzanie danych osobowych jest zgodne z prawem wyłącznie wtedy, gdy – i w takim zakresie, w jakim – zachodzi co najmniej jeden z poniższych warunków:
  - a) podmiot danych udzielił jednoznacznej zgody na przetwarzanie swoich danych osobowych w jednym lub większej liczbie konkretnych celów;
  - b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest podmiot danych, lub do podjęcia działań na wniosek podmiotu danych przed zawarciem umowy;
  - c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
  - d) przetwarzanie jest niezbędne do ochrony żywotnych interesów podmiotu danych lub innej osoby;
  - e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
  - f) przetwarzanie jest niezbędne do celów wynikających z uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności podmiotu danych wymagające ochrony danych osobowych, w szczególności gdy podmiotem danych jest dziecko. (...).
2. Przetwarzanie danych osobowych niezbędne do celów archiwizacyjnych w interesie publicznym lub do celów historycznych, statystycznych lub naukowych jest zgodne z prawem, z zastrzeżeniem warunków i gwarancji, o których mowa w art. 83.

3. Podstawa przetwarzania, o którym mowa w ust. 1 lit. c) i e), musi być ustalona zgodnie z:

- a) prawem Unii; lub
- b) krajowym prawem państwa członkowskiego, któremu podlega administrator.

W podstawie prawnej określony zostaje cel przetwarzania lub jeżeli chodzi o przetwarzanie, o którym mowa w ust. 1 lit. e) – jest ono niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. Podstawa prawna może zawierać przepisy szczegółowe dostosowujące zastosowanie przepisów niniejszego rozporządzenia, m.in. ogólne warunki zgodności z prawem przetwarzania danych przez administratora, rodzaj danych podlegających przetwarzaniu, zainteresowane podmioty danych, podmioty, którym można ujawnić dane, cele, w których można je ujawnić, celowość, okresy przechowywania oraz operacje i procedury przetwarzania, w tym środki zapewniające zgodność z prawem i rzetelność przetwarzania, w tym w innych szczególnych sytuacjach związanych z przetwarzaniem, o których mowa w rozdziale IX.

3a. Aby ustalić, czy cel dalszego przetwarzania (...) jest zgodny z celem, w którym pierwotnie zebrano dane, administrator bierze pod uwagę – o ile podmiot danych nie udzielił zgody – między innymi:

- a) wszelkie związki między celami, w których zebrano dane, a celami zamierzonego dalszego przetwarzania;
- b) kontekst, w którym zebrano dane;
- c) charakter danych osobowych, zwłaszcza czy przetwarzane są dane szczególnych kategorii zgodnie z art. 9;
- d) ewentualne konsekwencje zamierzonego dalszego przetwarzania dla podmiotów danych;
- e) istnienie odpowiednich gwarancji.

4. Gdy cel dalszego przetwarzania jest niezgodny z celem, w którym dane osobowe zostały zebrane przez tego samego administratora, dalsze przetwarzanie musi się opierać na co najmniej jednej z podstaw prawnych, o których mowa w ust. 1 lit. a)–e). Dalsze przetwarzanie przez tego samego administratora w celach niezgodnych z celami pierwotnymi dokonywane z powodu uzasadnionych interesów tego administratora lub strony trzeciej jest zgodne z prawem, jeżeli interesy te mają charakter nadrzędny wobec interesów podmiotu danych.
5. (...)

#### *Artykuł 7*

#### **Warunki udzielenia zgody**

1. Jeżeli zastosowanie ma art. 6 ust. 1 lit. a), administrator musi być w stanie wykazać, że podmiot danych udzielił jednoznacznej zgody.
- 1a. Jeżeli zastosowanie ma art. 9 ust. 2 lit. a), administrator musi być w stanie wykazać, że podmiot danych udzielił wyraźnej zgody.
2. Jeżeli podmiot danych ma udzielić zgody w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od (...) pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.
3. Podmiot danych ma prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Podmiot danych jest o tym informowany, zanim udzieli zgody.
4. (...)

## Artykuł 8

### **Warunki mające zastosowanie do zgody dziecka w związku z usługami społeczeństwa informacyjnego**

1. Jeżeli zastosowanie ma art. 6 ust. 1 lit. a), w przypadku usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku przetwarzanie danych osobowych dziecka (...) jest zgodne z prawem wyłącznie wtedy, gdy – i w takim zakresie, w jakim – zgody udzieliła lub zaaprobowwała ją osoba sprawująca odpowiedzialność rodzicielską nad dzieckiem lub udzieliło jej dziecko w okolicznościach, w których prawo Unii lub prawo państwa członkowskiego uznają ją za ważną.
- 1a. W takich przypadkach administrator, uwzględniając dostępną technologię, podejmuje racjonalne starania, by zweryfikować, czy osoba sprawująca odpowiedzialność rodzicielską nad dzieckiem udzieliła zgody lub ją zaaprobowwała.
2. Ustęp 1 nie wpływa na ogólne przepisy prawa umów państw członkowskich, takie jak przepisy o ważności, zawieraniu lub skutkach umowy wobec dziecka.
3. (...)
4. (...).

## Artykuł 9

### ***Przetwarzanie danych osobowych szczególnych kategorii***

1. Zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych lub danych dotyczących zdrowia lub seksualności (...).
2. Ustęp 1 nie ma zastosowania, jeżeli zachodzi jeden z poniższych warunków (...)
  - a) podmiot danych udzielił wyraźnej zgody na przetwarzanie tych danych osobowych (...), chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż podmiot danych nie może uchylić zakazu, o którym mowa w ust. 1; lub

- b) przetwarzanie jest niezbędne do wypełnienia obowiązków i skorzystania ze szczególnych praw przez administratora lub podmiot danych w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub umową zbiorową na mocy prawa państwa członkowskiego przewidującymi odpowiednie gwarancje; lub
- c) przetwarzanie jest niezbędne do ochrony żywotnych interesów podmiotu danych lub innej osoby, a podmiot danych jest fizycznie lub prawnie niezdolny do udzielenia zgody; lub
- d) przetwarzania dokonuje się w ramach uzasadnionej działalności prowadzonej z zachowaniem odpowiednich gwarancji przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane nie są ujawniane na zewnątrz bez zgody podmiotów danych; lub
- e) przetwarzanie dotyczy danych osobowych, które podmiot danych w sposób ewidentny podał do wiadomości publicznej (...); lub
- f) przetwarzanie jest niezbędne do ustalenia, realizacji lub obrony roszczeń prawnych lub gdy sądy działają w ramach sprawowania wymiaru sprawiedliwości; lub
- g) przetwarzanie jest niezbędne (...) ze względu na przesłanki interesu publicznego, na podstawie prawa Unii lub prawa państwa członkowskiego przewidujących odpowiednie, konkretne środki ochrony uzasadnionych interesów podmiotu danych; lub
- h) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub socjalnej lub leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub socjalnej na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową ze specjalistą w dziedzinie opieki zdrowotnej i z zastrzeżeniem warunków i gwarancji, o których mowa w ust. 4; lub
- ha) (...);

hb) przetwarzanie jest niezbędne ze względu na przesłanki interesu publicznego w dziedzinie zdrowia publicznego, taki jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności podmiotów danych; lub

i) przetwarzanie jest niezbędne do celów archiwizacyjnych w interesie publicznym lub do celów historycznych, statystycznych lub (...) naukowych i podlega warunkom i gwarancjom ustanowionym w prawie Unii lub prawie państwa członkowskiego, w tym warunkom i gwarancjom, o których mowa w art. 83;

j) (...)

3. (...)

4. *Dane osobowe, o których mowa w ust. 1, mogą – na podstawie prawa Unii lub prawa państwa członkowskiego – być przetwarzane do celów, o których mowa w ust. 2 lit. h) (...), jeżeli są przetwarzane przez – lub na odpowiedzialność – (...) pracownika podlegającego obowiązkowi dochowania tajemnicy służbowej na mocy prawa Unii lub prawa państwa członkowskiego, lub przepisów ustanowionych przez właściwe organy krajowe lub przez inną osobę również podlegającą obowiązkowi dochowania tajemnicy służbowej na mocy prawa Unii lub prawa państwa członkowskiego, lub przepisów ustanowionych przez właściwe organy krajowe.*

4a. (...).

5. Państwa członkowskie mogą zachować lub wprowadzić bardziej szczegółowe przepisy odnośnie do danych genetycznych lub danych dotyczących zdrowia. Oznacza to m.in. możliwość wprowadzenia przez państwa członkowskie (...) dalszych warunków przetwarzania tych danych.



### Artykuł 9a

#### **Przetwarzanie danych o wyrokach skazujących za przestępstwa i o przestępstwach**

Przetwarzania danych o wyrokach skazujących za przestępstwa oraz o przestępstwach lub o odnośnych środkach zabezpieczających na podstawie art. 6 ust. 1 wolno dokonywać wyłącznie pod nadzorem oficjalnego organu (...) lub jeżeli przetwarzanie jest (...) dozwolone prawem Unii lub prawem państwa członkowskiego przewidującymi odpowiednie gwarancje praw i wolności podmiotów danych. Kompletny rejestr wyroków skazujących za przestępstwa wolno prowadzić wyłącznie pod nadzorem oficjalnego organu.

### Artykuł 10

#### **Przetwarzanie niewymagające identyfikacji**

1. Jeżeli cele, w których administrator przetwarza dane osobowe, nie wymagają lub już nie wymagają zidentyfikowania przez niego podmiotu danych, administrator nie ma obowiązku zachowania lub uzyskania (...) dodatkowych informacji ani dokonania dodatkowego przetwarzania w celu zidentyfikowania podmiotu danych wyłącznie po to, by zastosować się do (...) niniejszego rozporządzenia (...)
2. Jeżeli w takim przypadku administrator nie jest w stanie zidentyfikować podmiotu danych, zastosowania nie mają art. 15, 16, 17, 17a, 17b ani 18, chyba że podmiot danych w celu skorzystania z praw przysługujących mu na mocy tych artykułów dostarczy dodatkowych informacji pozwalających go zidentyfikować.

**ROZDZIAŁ III**  
**PRAWA PODMIOTU DANYCH**

**SEKCJA 1**  
**PRZEJRZYSTOŚĆ ORAZ TRYB KORZYSTANIA Z PRAW**

*Artykuł 11*

***Przejrzyste informowanie i przejrzysta komunikacja***

1. (...)
2. (...)

## Artykuł 12

### **Przejrzyste informowanie i przejrzysta komunikacja oraz tryb korzystania z praw przez podmiot danych**

1. Administrator przedsięwzię odpowiednio środki, aby w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem udzielić podmiotowi danych wszelkich informacji, o których mowa w art. 14 i 14a, oraz prowadzić z nim wszelką komunikację na mocy art. 15–19 i 32 w sprawie przetwarzania danych osobowych. Informacji udziela się na piśmie lub innymi sposobami, a w stosownym przypadku – elektronicznie. Jeżeli podmiot danych składa wniosek w formie elektronicznej, informacje można zasadniczo przekazywać w formie elektronicznej, chyba że podmiot danych zażąda innej formy. Jeżeli podmiot danych tego zażąda, informacji można udzielić ustnie, o ile potwierdzi się tożsamość podmiotu danych.
- 1a. Administrator ułatwia podmiotowi danych korzystanie z praw przysługujących mu na mocy art. 15–19. W przypadkach, o których mowa w art. 10 ust. 2, administrator nie odmawia podjęcia działań na wniosek podmiotu danych, który chce skorzystać z praw przysługujących mu na mocy art. 15–19, chyba że wykaze, iż nie jest w stanie zidentyfikować podmiotu danych.
2. Administrator bez zbędnej zwłoki – najpóźniej w terminie jednego miesiąca od otrzymania wniosku – udziela podmiotowi danych (...) informacji o działaniach podjętych względem wniosku w myśl art. 15 i 16–19 (...). W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter wniosku oraz liczbę wniosków. Jeżeli zastosowanie ma termin przedłużony, w terminie jednego miesiąca od otrzymania wniosku informuje się podmiot danych o przyczynach opóźnienia.

3. Jeżeli administrator nie podejmuje działań względem wniosku podmiotu danych, to bez zbędnej zwłoki – najpóźniej w terminie jednego miesiąca od otrzymania wniosku – informuje podmiot danych o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego (...).
4. Informacje podawane na mocy art. 14 i 14a (...) oraz wszelka komunikacja na mocy art. 16–19 i 32 są wolne od opłat. Jeżeli wnioski podmiotu danych są ewidentnie nieuzasadnione lub nadmierne, zwłaszcza ze względu na swój ustawiczny charakter, administrator (...) może odmówić podjęcia działań względem wniosku. W takim przypadku obowiązek wykazania, że wniosek ma ewidentnie nieuzasadniony lub nadmierny charakter, spoczywa na administratorze.
- 4a. Bez uszczerbku dla art. 10, jeżeli administrator ma uzasadnione wątpliwości co do tożsamości osoby składającej wniosek, o którym mowa w art. 15–19, może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości podmiotu danych.
5. (...)
6. (...)

*Artykuł 13*  
***Prawa odbiorców***

(...)

## SEKCJA 2

### INFORMACJE I DOSTĘP DO DANYCH

#### *Artykuł 14*

#### **Informacje podawane w przypadku zbierania danych od podmiotu danych**

1. Jeżeli dane osobowe o podmiocie danych są zbierane od podmiotu danych, administrator podczas pozyskiwania danych osobowych (...) podaje podmiotowi danych następujące informacje:
  - a) swoją tożsamość i dane kontaktowe oraz tożsamość i dane kontaktowe swojego przedstawiciela, jeżeli istnieje; administrator podaje też dane kontaktowe inspektora ochrony danych, jeżeli istnieje;
  - b) cele przetwarzania, do których mają posłużyć dane osobowe (...), oraz podstawę prawną przetwarzania.
- 1a. Poza informacjami, o których mowa w ust. 1, administrator podczas pozyskiwania danych osobowych podaje podmiotowi danych inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania (...) i uwzględnia przy tym konkretne okoliczności i konkretny kontekst przetwarzania danych osobowych:
  - a) (...);
  - b) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) – uzasadnione interesy realizowane przez administratora lub przez stronę trzecią;
  - c) informacje o odbiorcy danych osobowych lub kategoriach tych odbiorców;
  - d) w stosownym przypadku swój zamiar przekazania danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej;

- e) informacje o prawie do tego, by zwrócić się do administratora z wnioskiem o dostęp do danych osobowych, ich poprawienie lub usunięcie, lub też ograniczenie przetwarzania danych osobowych dotyczących podmiotu danych oraz by wnieść sprzeciw wobec przetwarzania takich danych osobowych (...), a także o prawie do przenoszenia danych;
  - ea) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
  - f) informacje o prawie wniesienia skargi do organu nadzorczego (...);
  - g) informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym albo warunkiem przystąpienia do umowy oraz czy podmiot danych jest zobowiązany do ich podania i jakie są ewentualne konsekwencje niepodania danych;
  - h) *informacje o tym, że prowadzi się automatyczne podejmowanie decyzji, w tym profilowanie, o którym mowa w art. 20 ust. 1 i 3, oraz informacje o (...) trybie jego działania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla podmiotu danych.*
- 1b. Jeżeli administrator planuje dalej przetwarzać dane (...) w celu innym niż cel, w którym dane zostały zebrane, informuje on przed takim dalszym przetwarzaniem podmiot danych o tym innym celu oraz dostarcza mu wszelkich innych stosownych informacji, o których mowa w ust. 1a.
2. (...)
3. (...)
4. (...)

5. Ustępy 1, 1a i 1b nie mają zastosowania wtedy, gdy – i w takim zakresie, w jakim – podmiot danych dysponuje już tymi informacjami.
6. (...)
7. (...)
8. (...)

Artykuł 14a

**Informacje podawane w przypadku pozyskania danych w sposób inny niż od podmiotu danych**

1. Jeżeli danych osobowych nie pozyskano od podmiotu danych, administrator podaje podmiotowi danych następujące informacje:
  - a) swoją tożsamość i dane kontaktowe oraz tożsamość i dane kontaktowe swojego przedstawiciela, jeżeli istnieje; administrator podaje też dane kontaktowe inspektora ochrony danych, jeżeli istnieje;
  - b) cele przetwarzania, do których mają posłużyć dane osobowe (...), oraz podstawę prawną przetwarzania.
2. Poza informacjami, o których mowa w ust. 1, administrator podaje podmiotowi danych inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania wobec podmiotu danych, i uwzględnia przy tym konkretne okoliczności i konkretny kontekst przetwarzania danych osobowych (...):
  - a) kategorie odnośnych danych osobowych;
  - b) (...)

- c) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) – uzasadnione interesy realizowane przez administratora lub przez stronę trzecią;
- d) informacje o odbiorcach danych osobowych lub kategoriach tych odbiorców;
- da) w stosownym przypadku swój zamiar przekazania danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej;
- e) informacje o prawie do tego, by zwrócić się do administratora z wnioskiem o dostęp do danych osobowych, ich poprawienie lub usunięcie, lub też ograniczenie przetwarzania danych osobowych dotyczących podmiotu danych oraz by wnieść sprzeciw wobec przetwarzania takich danych osobowych, a także o prawie do przenoszenia danych (...);
- ea) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
- f) informacje o prawie wniesienia skargi do organu nadzorczego (...);
- g) źródło pochodzenia danych osobowych, chyba że pochodzą one ze źródeł publicznie dostępnych;
- h) *informacje o tym, że prowadzi się automatyczne podejmowanie decyzji, w tym profilowanie, o którym mowa w art. 20 ust. 1 i 3, oraz informacje o (...) trybie jego działania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla podmiotu danych.*

3. Informacje, o których mowa w ust. 1 i 2, administrator podaje:

- a) w racjonalnym terminie po pozyskaniu danych – najpóźniej w ciągu miesiąca – mając na uwadze konkretne okoliczności przetwarzania danych, lub



- b) jeżeli planuje się ujawnić dane innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu.
- 3a    Jeżeli administrator planuje dalej przetwarzać dane (...) w celu innym niż cel, w którym dane zostały pozyskane, informuje on przed takim dalszym przetwarzaniem podmiot danych o tym innym celu oraz dostarcza mu wszelkich innych stosownych informacji, o których mowa w ust. 2.
4.    Ustępy 1–3a nie mają zastosowania wtedy, gdy – i w takim zakresie, w jakim:
- a)    podmiot danych dysponuje już tymi informacjami; lub
  - b)    udzielenie takich informacji (...) okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku; w takim przypadku administrator przedsięwzię odpowiednie środki, by chronić prawa, wolności i uzasadnione interesy podmiotu danych; lub
  - c)    pozyskiwanie lub ujawnianie jest wyraźnie nakazane prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator, przewidującymi odpowiednie środki chroniące uzasadnione interesy podmiotu danych; lub
  - d)    (...);
  - e)    dane muszą pozostać poufne zgodnie prawem Unii lub prawem państwa członkowskiego (...).
5.    (...)
6.    (...)

*Artykuł 15*  
***Prawo dostępu przysługujące podmiotowi danych***

1. Podmiot danych ma prawo w sposób wolny od opłat, w racjonalnych odstępach czasu uzyskiwać od administratora (...) potwierdzenie, czy przetwarzane są dane osobowe go dotyczące, a jeżeli takie dane są przetwarzane – dostęp do nich i następujące informacje:
  - a) cele przetwarzania;
  - b) (...)
  - c) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
  - d) w miarę możliwości – planowany okres przechowywania danych osobowych;
  - e) informacje o prawie do tego, by zwrócić się do administratora o poprawienie, usunięcie, lub ograniczenie przetwarzania danych osobowych dotyczących podmiotu danych lub by wnieść sprzeciw wobec przetwarzania takich danych osobowych;
  - f) informacje o prawie wniesienia skargi do organu nadzorczego (...);
  - g) jeżeli dane osobowe nie zostały zebrane od podmiotu danych – wszelkie dostępne informacje o ich źródle;
  - h) w przypadku decyzji opartych na automatycznym przetwarzaniu, w tym na profilowaniu, o którym mowa w art. 20 ust. 1 i 3 – informacje o trybie jego działania oraz o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania.
- 1a. Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, podmiot danych ma prawo zostać poinformowany o odpowiednich gwarancjach, o których mowa w art. 42, związanych z przekazaniem.

- 1b. Na wniosek i bez nadmiernych opłat administrator dostarcza podmiotowi danych kopię danych osobowych podlegających przetwarzaniu.
2. (...)
- 2a. Prawo do uzyskania kopii, o której mowa w ust. 1b (...), nie ma zastosowania, jeżeli nie można jej dostarczyć bez ujawnienia danych osobowych innych podmiotów danych lub poufnych danych administratora. Ponadto prawo to nie ma zastosowania, jeżeli ujawnienie danych osobowych naruszyłoby prawa własności intelektualnej związane z przetwarzaniem tych danych.
3. (...)
4. (...)

## SEKCJA 3

### POPRAWIANIE I USUWANIE

#### *Artykuł 16*

#### ***Prawo do poprawienia danych***

1. (...) Podmiot danych ma prawo spowodować, by administrator bez zbędnej zwłoki poprawił dane osobowe go dotyczące, jeżeli są one nieścisłe. Z uwzględnieniem celów, w których przetworzono dane, podmiot danych ma prawo spowodować, by niekompletne dane osobowe zostały uzupełnione, w tym poprzez przedstawienie dodatkowego (...) oświadczenia.
2. (...)

#### *Artykuł 17*

#### ***Prawo do usunięcia danych i do „bycia zapomnianym”***

1. (...) Administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe – zwłaszcza dane osobowe zebrane, gdy ich podmiot był dzieckiem – a podmiot danych ma prawo spowodować, by administrator bez zbędnej zwłoki usunął dane osobowe go dotyczące, jeżeli zachodzi jedna z następujących okoliczności:
  - a) dane nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetworzone;
  - b) podmiot danych cofnął zgodę, na której opiera się przetwarzanie zgodnie z art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a), i (...) nie ma innej podstawy prawnej do przetwarzania danych;
  - c) podmiot danych wnosi sprzeciw na mocy art. 19 ust. 1 wobec przetwarzania danych osobowych i nie istnieją żadne nadrzędne uzasadnione podstawy do przetwarzania lub podmiot danych wnosi sprzeciw na mocy art. 19 ust. 2 wobec przetwarzania danych osobowych;

- d) dane zostały przetworzone niezgodnie z prawem;
  - e) dane muszą zostać usunięte w celu wywiązania się z obowiązku prawnego, któremu podlega administrator;
- 1a. Podmiot danych ma również prawo spowodować, by administrator bez zbędnej zwłoki usunął dane osobowe go dotyczące, jeżeli dane zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1.
- (...).
2. (...).
- 2a. *Jeżeli administrator (...) upublicznił dane osobowe, a na mocy ust. 1 ma obowiązek te dane usunąć, to – biorąc pod uwagę dostępną technologię i koszt realizacji – (...) przedsięwzięcie racjonalne kroki, w tym środki techniczne, (...) by poinformować administratorów przetwarzających te dane, że podmiot danych wystąpił o to, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych lub ich replikację.*
3. Ustępy 1, 1a i 2a nie mają zastosowania, w zakresie w jakim (...) przetwarzanie danych osobowych jest niezbędne:
- a. do skorzystania z prawa wolności wypowiedzi i informacji;
  - b. do wywiązania się z prawnego obowiązku wymagającego przetwarzania danych osobowych na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
  - c. ze względu na przesłanki interesu publicznego w dziedzinie zdrowia publicznego zgodnie z art. 9 ust. 2 lit. h) i hb) oraz art. 9 ust. 4;
  - d. do celów archiwizacyjnych w interesie publicznym lub do celów naukowych, statystycznych i historycznych (...) zgodnie z art. 83;

- e. (...)
  - f. (...)
  - g. do ustalenia, realizacji lub obrony roszczeń prawnych.
4. (...)
5. (...)

#### Artykuł 17a

#### **Prawo do ograniczenia przetwarzania**

1. Podmiot danych ma prawo spowodować, by administrator ograniczył przetwarzanie danych osobowych, jeżeli:
  - a) podmiot danych kwestionuje ścisłość danych – na okres pozwalający administratorowi sprawdzić ścisłość danych;
  - b) administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne podmiotowi danych do ustalenia, realizacji lub obrony roszczeń prawnych; lub
  - c) podmiot danych wniósł sprzeciw na mocy art. 19 ust. 1 wobec przetwarzania – do czasu stwierdzenia, czy uzasadnione podstawy po stronie administratora są nadrzędne wobec uzasadnionych podstaw podmiotu danych.
2. (...)
3. Jeżeli na mocy ust. 1 przetwarzanie danych osobowych zostało ograniczone, dane takie można przetwarzać, z wyjątkiem przechowywania, wyłącznie za zgodą podmiotu danych lub w celu ustalenia, realizacji lub obrony roszczeń prawnych lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub ze względu na ważne przesłanki interesu publicznego.

4. Przed uchyleniem ograniczenia przetwarzania administrator informuje o tym podmiot danych, który spowodował to ograniczenie na mocy ust. 1 (...).
5. (...)
- 5a. (...)

#### *Artykuł 17b*

#### **Obowiązek powiadomienia o poprawieniu danych, ich usunięciu lub ograniczeniu przetwarzania**

Administrator komunikuje poprawienie, usunięcie lub ograniczenie przetwarzania, których dokonał zgodnie z art. 16, art. 17 ust. 1 i art. 17a, każdemu odbiorcy, któremu ujawniono dane (...), chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.

#### *Artykuł 18*

#### ***Prawo do przenoszenia danych***

1. (...)
2. Podmiot danych ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym i maszynowo czytelnym formacie dane osobowe go dotyczące, których dostarczył administratorowi, oraz ma prawo przekazać te dane innemu administratorowi bez przeszkód ze strony administratora, któremu danych tych dostarczono, jeżeli:
  - a) przetwarzanie odbywa się na podstawie zgody w myśl art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) lub na podstawie umowy w myśl art. 6 ust. 1 lit. b); oraz
  - b) przetwarzanie odbywa się w sposób zautomatyzowany.

- 2a. Korzystanie z tego prawa pozostaje bez uszczerbku dla art. 17. Prawo, o którym mowa w ust. 2, nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.
- 2aa. Prawo, o którym mowa w ust. 2, nie ma zastosowania, jeżeli ujawnienie danych osobowych naruszyłoby prawa własności intelektualnej związane z przetwarzaniem tych danych.
3. (...)
4. (...).



## SEKCJA 4

### **PRAWO DO SPRZECIWU I AUTOMATYCZNE ZINDYWIDUALIZOWANE PODEJMOWANIE DECYZJI (...)**

#### *Artykuł 19*

#### ***Prawo do sprzeciwu***

1. Podmiot danych ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jego indywidualną sytuacją – wobec przetwarzania dotyczących go danych osobowych opartego na art. 6 ust. 1 lit. (...) e) lub f) lub art. 6 ust. 4 zdanie pierwsze w związku z art. 6 ust. 1 lit. e) lub art. 6 ust. 4 zdanie drugie.

Administratorowi nie wolno już przetwarzać tych danych osobowych (...), chyba że wykaże on istnienie ewidentnych uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, (...) praw i wolności podmiotu danych, lub do ustalenia, realizacji lub obrony roszczeń prawnych.

- 1a. (...)
2. Jeżeli dane osobowe są przetwarzane do celów marketingu bezpośredniego, podmiot danych ma prawo (...) w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących go danych osobowych do celów takiego marketingu. Najpóźniej przy okazji pierwszej komunikacji z podmiotem danych informuje się go wyrażnie o tym prawie oraz przedstawia się je jasno, odrębnie od wszelkich innych informacji.
- 2a. Jeżeli podmiot danych wniesie sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, danych osobowych nie wolno już przetwarzać do takich celów.
- 2aa. Jeżeli dane osobowe są przetwarzane do celów historycznych, statystycznych lub naukowych, podmiot danych ma prawo wnieść sprzeciw – z przyczyn związanych z jego indywidualną sytuacją – wobec przetwarzania danych osobowych go dotyczących, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.
3. (...)
4. (...)

*Artykuł 20*

**Automatyczne zindywidualizowane podejmowanie decyzji**

1. Podmiot danych ma prawo do tego, by nie podlegać decyzji (...), która opiera się wyłącznie na automatycznym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tego podmiotu skutki prawne lub istotnie na niego wpływa.
- 1a. Ustęp 1 nie ma zastosowania, jeżeli dana decyzja: (...)
  - a) jest niezbędna do zawarcia lub wykonania umowy między podmiotem danych a administratorem (...); lub
  - b) jest (...) dozwolona prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator i które przewiduje właściwe środki ochrony praw, wolności i uzasadnionych interesów podmiotu danych; lub
  - c) opiera się na wyraźnej zgodzie podmiotu danych (...).
- 1b. W przypadkach, o których mowa w ust. 1a lit. a) i c), administrator wdraża właściwe środki ochrony praw, wolności i uzasadnionych interesów podmiotu danych, a co najmniej prawa do uzyskania interwencji ludzkiej ze strony administratora, do wyrażenia własnego stanowiska i do zakwestionowania danej decyzji.
2. (...)
3. Decyzje, o których mowa w ust. 1a, nie mogą (...) opierać się na danych osobowych szczególnych kategorii, o których mowa w art. 9 ust. 1, chyba że zastosowanie ma art. 9 ust. 2 lit. a) lub g) i istnieją właściwe środki ochrony praw, wolności i uzasadnionych interesów podmiotu danych.
4. (...)
5. (...)

## SEKCJA 5 OGRANICZENIA

### *Artykuł 21*

#### ***Ograniczenia***

1. Prawo Unii lub prawo państwa członkowskiego, któremu podlegają administrator danych lub podmiot przetwarzający, może środkiem ustawodawczym ograniczyć zakres obowiązków i praw przewidzianych w (...) art. 12–20 i w art. 32, a także w art. 5 – o ile jego przepisy odpowiadają prawom i obowiązkom przewidzianym w art. 12–20 – jeżeli ograniczenie takie jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym, służącym:
  - aa) bezpieczeństwu narodowemu;
  - ab) obronie;
  - a) bezpieczeństwu publicznemu;
  - b) zapobieganiu przestępstwom, prowadzeniu dochodzeń w ich sprawie, ich wykrywaniu lub ściganiu lub wykonywaniu sankcji karnych, lub ochronie przez zagrożeniami dla bezpieczeństwa publicznego i zapobieganiu takim zagrożeniom;
  - c) innym ważnym celom leżącym w ogólnym interesie publicznym Unii lub państwa członkowskiego, w szczególności ważnemu interesowi gospodarczemu lub finansowemu Unii lub państwa członkowskiego, w tym kwestiom pieniężnym, budżetowym i podatkowym, zdrowiu publicznemu i zabezpieczeniu społecznemu oraz ochronie stabilności i integralności rynku;
  - ca) ochronie niezależności sądów i postępowania sądowego;
  - d) zapobieganiu naruszeniom zasad etyki w zawodach regulowanych, prowadzeniu dochodzeń w tej sprawie, ich wykrywaniu oraz ściganiu;

- e) funkcjom kontrolnym, inspekcyjnym lub regulacyjnym związanym, nawet sporadycznie, ze sprawowaniem władzy publicznej w przypadkach, o których mowa w lit. aa), ab), a), b), c) i d);
- f) ochronie podmiotu danych lub praw i wolności innych osób;
- g) egzekucji roszczeń cywilnoprawnych.

2. Środek ustawodawczy, o którym mowa w ust. 1, zawiera szczegółowe przepisy przynajmniej – w stosownym przypadku – o celach przetwarzania lub kategorii przetwarzania, kategoriach danych osobowych, zakresie wprowadzanych ograniczeń, określeniu administratora lub kategorii administratorów, okresach przechowywania oraz mających zastosowanie gwarancjach z uwzględnieniem charakteru, zakresu i celów przetwarzania lub kategorii przetwarzania oraz zagrożeń dla praw i wolności podmiotów danych.

## ROZDZIAŁ IV

### ADMINISTRATOR I PODMIOT PRZETWARZAJĄCY

#### SEKCJA 1

#### OBOWIĄZKI OGÓLNE

##### *Artykuł 22*

##### *Obowiązki administratora*

1. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz prawdopodobieństwo i powagę zagrożenia dla praw i wolności osób fizycznych, administrator (...) wdraża odpowiednie środki i jest w stanie wykazać, że przetwarzanie danych osobowych odbywa się zgodnie z niniejszym rozporządzeniem.
2. (...)
- 2a. Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, wśród środków, o których mowa w ust. 1, znajduje się realizacja przez administratora odpowiednich strategii ochrony danych.
- 2b. Wywiązywanie się z obowiązków administratora można wykazać między innymi poprzez stosowanie zatwierdzonych kodeksów postępowania na mocy art. 38 lub zatwierzonego mechanizmu certyfikacji na mocy art. 39.
3. (...)
4. (...)

***Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych***

1. (...) Mając na uwadze dostępną technologię i koszt wdrażania oraz uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz prawdopodobieństwo i powagę zagrożenia dla praw i wolności osób fizycznych wynikającego z przetwarzania, administratorzy wdrażają (...) środki techniczne i organizacyjne odpowiednie do wykonywanej czynności przetwarzania i do jej celów – np. minimalizację i pseudonimizację danych – w taki sposób, by przetwarzanie było zgodne z wymogami niniejszego rozporządzenia oraz chroniło prawa (...) podmiotów danych.
2. Administrator wdraża odpowiednie środki, aby domyślnie (...) przetwarzane były wyłącznie te dane osobowe, (...) które są niezbędne w stosunku do każdego konkretnego celu przetwarzania; dotyczy to ilości (...) zbieranych danych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. Jeżeli celem przetwarzania nie jest podanie informacji do wiadomości publicznej, mechanizmy te mają gwarantować, że domyślnie dane osobowe nie będą udostępniane bez ludzkiej interwencji nieokreślonej liczbie osób.
- 2a. Wywiązywanie się z obowiązków, o których mowa w ust. 1 i 2, można wykazać między innymi poprzez zatwierdzony mechanizm certyfikacji na mocy art. 39.
3. (...)
4. (...)

## Artykuł 24

### **Współadministratorzy**

1. Jeżeli dwaj administratorzy lub większa ich liczba wspólnie ustalają cele i sposoby przetwarzania danych osobowych, są oni współadministratorami. W drodze wspólnych uzgodnień w przejrzysty sposób określają oni podział zadań w zakresie wypełniania obowiązków wynikających z niniejszego rozporządzenia, w szczególności odnośnie do (...) korzystania przez podmiot danych z przysługujących mu praw, oraz podział obowiązków w zakresie podawania informacji, o których mowa w art. 14 i 14a, chyba że – i w takim zakresie, w jakim – przypadające im obowiązki określa prawo Unii lub prawo państwa członkowskiego, któremu administratorzy ci podlegają. W uzgodnieniach należy wskazać, który ze współadministratorów pełni funkcję pojedynczego punktu kontaktowego wobec podmiotów danych chcących skorzystać ze swoich praw.
2. Niezależnie od uzgodnień, o których mowa w ust. 1, podmiot danych może korzystać z przysługujących mu praw wynikających z niniejszego rozporządzenia wobec każdego z (...) administratorów i przeciwko każdemu z nich.
3. W uzgodnieniach należycie odzwierciedla się faktyczną rolę każdego ze współadministratorów i jego relacje z podmiotami danych, a zasadnicza treść uzgodnień jest udostępniana podmiotowi danych. Ustęp 2 nie ma zastosowania, jeżeli podmiot danych został w przejrzysty i jednoznaczny sposób poinformowany, który ze współadministratorów ponosi odpowiedzialność, chyba że takie uzgodnienie – inne niż określone prawem Unii lub prawem państwa członkowskiego – jest niesprawiedliwe względem jego praw (...).

## Artykuł 25

### **Przedstawiciele administratorów niemających siedziby w Unii**

1. Jeżeli zastosowanie ma art. 3 ust. 2, administrator na piśmie wyznacza swojego przedstawiciela w Unii.

2. Obowiązek ten nie ma zastosowania w przypadku:
- (a) (...); lub
  - (b) przetwarzania, które ma charakter sporadyczny i jest mało prawdopodobne, by ze względu na swój charakter, kontekst, zakres i cele niosło (...)  
zagrożenie dla praw i wolności osób fizycznych (...); lub
  - (c) organu lub podmiotu publicznego;
  - (d) (...)
3. Przedstawiciel ma siedzibę w jednym z państw członkowskich będących miejscem zamieszkania podmiotów danych, których dane osobowe są przetwarzane w związku z oferowaniem im towarów lub usług lub których zachowanie jest monitorowane.
- 3a. Przedstawiciel zostaje upoważniony przez administratora, by do celów zapewnienia przestrzegania niniejszego rozporządzenia mogły się do niego zwracać – oprócz lub zamiast do administratora – w szczególności organy nadzorcze i podmioty danych we wszystkich sprawach związanych z przetwarzaniem danych osobowych.
4. Wyznaczenie przedstawiciela przez administratora pozostaje bez uszczerbku dla postępowań sądowych, które mogą zostać wszczęte przeciwko administratorowi.

#### *Artykuł 26*

##### ***Podmiot przetwarzający***

1. (...). Administrator korzysta z usług wyłącznie takich podmiotów przetwarzających, które dają wystarczające gwarancje wdrożenia odpowiednich środków (...) technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom niniejszego rozporządzenia (...).
- 1a. Podmiot przetwarzający nie zatrudnia innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody administratora. W tym drugim przypadku podmiot przetwarzający powinien zawsze informować administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian.



1b. (...).

2. Przetwarzanie przez podmiot przetwarzający jest regulowane umową lub aktem prawnym, które podlegają prawu Unii lub prawu państwa członkowskiego, wiąże podmiot przetwarzający z administratorem, określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie podmiotów danych, prawa administratora (...) i stanowią w szczególności, że podmiot przetwarzający:
- a) przetwarza dane osobowe wyłącznie na polecenie administratora (...), chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający; w takim przypadku przed przetworzeniem danych podmiot przetwarzający informuje administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny;
  - b) (...)
  - c) przedsięwzię wszelkie (...) środki wymagane na mocy art. 30;
  - d) respektuje warunki zatrudnienia innego podmiotu przetwarzającego (...), takie jak wymóg szczegółowej uprzedniej zgody administratora;
  - e) (...) biorąc pod uwagę charakter przetwarzania, pomaga administratorowi odpowiadać na wnioski o możliwość skorzystania przez podmioty danych z praw ustanowionych w rozdziale III;
  - f) (...) pomaga administratorowi wywiązać się z obowiązków określonych w art. 30–34;
  - g) po zakończeniu świadczenia usługi przetwarzania danych określonej w umowie lub innym akcie prawnym zwraca lub usuwa – zależnie od decyzji administratora – dane osobowe, chyba że prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający, nakładają obowiązek przechowywania tych danych;
  - h) udostępnia administratorowi (...) wszelkie informacje niezbędne do wykazania wywiązywania się z obowiązków ustanowionych w niniejszym artykule oraz umożliwia administratorowi przeprowadzanie audytów i przyczynia się do nich.

Podmiot przetwarzający niezwłocznie informuje administratora, jeżeli jego zdaniem któreś z poleceń stanowi naruszenie niniejszego rozporządzenia lub przepisów Unii lub państw członkowskich o ochronie danych.

- 2a. Jeżeli do wykonania w imieniu administratora konkretnych czynności przetwarzania podmiot przetwarzający zatrudnia (...) inny podmiot przetwarzający, na ten inny podmiot przetwarzający nałożone zostają – na mocy umowy lub innego aktu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego – te same obowiązki ochrony danych jak w umowie lub innym akcie prawnym między administratorem a podmiotem przetwarzającym, o których to obowiązkach mowa w ust. 2, w szczególności obowiązek dania wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom niniejszego rozporządzenia. Jeżeli ten inny podmiot przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec administratora za wypełnienie obowiązków tego innego podmiotu przetwarzającego spoczywa na pierwotnym podmiocie przetwarzającym.
- 2aa. Wystarczające gwarancje, o których mowa w ust. 1 i 2a, podmiot przetwarzający może wykazać między innymi poprzez stosowanie zatwierdzonego kodeksu postępowania na mocy art. 38 lub zatwierdzonego mechanizmu certyfikacji na mocy art. 39.
- 2ab. Bez uszczerbku dla umów indywidualnych między administratorem a podmiotem przetwarzającym, umowa lub inny akt prawny, o których mowa w ust. 2 i 2a, mogą się opierać w całości lub w części na standardowych klauzulach umownych, o których mowa w ust. 2b i 2c, lub na standardowych klauzulach umownych, które są elementem certyfikacji udzielonej administratorowi lub podmiotowi przetwarzającemu na mocy art. 39 i 39a.
- 2b. Komisja może ustanowić standardowe klauzule umowne na potrzeby spraw, o których mowa w ust. 2 i 2a, zgodnie z procedurą sprawdzającą, o której mowa w art. 87 ust. 2.
- 2c. Organ nadzorczy może przyjąć standardowe klauzule umowne na potrzeby spraw, o których mowa w ust. 2 i 2a, zgodnie z mechanizmem spójności, o którym mowa w art. 57.

3. Umowa lub inny akt prawny, o których mowa w art. 2 i 2a, mają formę pisemną, w tym formę elektroniczną.
4. (...)
5. (...)

#### *Artykuł 27*

#### ***Przetwarzanie z upoważnienia administratora i podmiotu przetwarzającego***

(...)

#### *Artykuł 28*

#### ***Rejestrowanie kategorii czynności przetwarzania danych osobowych***

1. Każdy administrator (...) oraz – jeżeli istnieje, przedstawiciel administratora – prowadzi rejestr wszystkich podlegających mu kategorii czynności przetwarzania danych osobowych. W rejestrze tym znajdują się (...) następujące informacje:
  - a) imię i nazwisko/nazwa oraz dane kontaktowe administratora oraz wszelkich współadministratorów (...), a także jeżeli istnieją – przedstawiciela administratora oraz inspektora ochrony danych;
  - b) (...)
  - c) cele przetwarzania, w tym uzasadnione interesy, jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f);
  - d) opis kategorii podmiotów danych oraz kategorii danych osobowych ich dotyczących;
  - e) (...) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności odbiorców w państwach trzecich;

- f) w odpowiednim przypadku kategorie przekazanych danych osobowych do państwa trzeciego lub organizacji międzynarodowej (...);
  - g) w miarę możliwości planowane terminy usunięcia poszczególnych kategorii danych.
  - h) w miarę możliwości ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 30 ust. 1.
- 2a. Każdy podmiot przetwarzający prowadzi rejestr wszystkich kategorii czynności przetwarzania danych osobowych dokonywanych w imieniu administratora; znajdują się w nim:
- a) imię i nazwisko/nazwa oraz dane kontaktowe podmiotu przetwarzającego lub podmiotów przetwarzających oraz każdego administratora, w imieniu którego działa podmiot przetwarzający, a jeżeli istnieje – przedstawiciela administratora;
  - b) imię i nazwisko/nazwa oraz dane kontaktowe inspektora ochrony danych – jeżeli istnieje;
  - c) kategorie przetwarzanych danych dokonywanych w imieniu każdego z administratorów;
  - d) w odpowiednim przypadku kategorie przekazanych danych osobowych do państwa trzeciego lub organizacji międzynarodowej;
  - e) w miarę możliwości ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 30 ust. 1.
- 3a. Rejestry, o których mowa w ust. 1 i 2a, mają formę pisemną, w tym formę elektroniczną lub inną formę niemożliwą do odczytu, którą można przekształcić w formę możliwą do odczytu.
3. Na wniosek administrator i podmiot przetwarzający oraz – jeżeli istnieje, przedstawiciel administratora – udostępniają rejestr organowi nadzorczemu (...).
4. Obowiązki, o których mowa w ust. 1 i 2a, nie mają zastosowania do:
- a) (...);

- b) firmy lub organu zatrudniającego mniej niż 250 osób, chyba że przetwarzanie, którego dokonują, może ze względu na swój charakter, zakres, kontekst i cele nieść duże zagrożenie dla praw i wolności podmiotu danych, takie jak dyskryminacja, kradzież tożsamości lub oszustwo dotyczące tożsamości, niedozwolone cofnięcie pseudonimizacji, strata finansowa, naruszenie dobrego imienia, naruszenie poufności danych chronionych tajemnicą służbową lub wszelka inna szkoda gospodarcza lub społeczna dla podmiotów danych.
5. (...)
6. (...)

*Artykuł 29*

***Współpraca z organem nadzorczym***

(...)

## SEKCJA 2

### BEZPIECZEŃSTWO DANYCH

#### *Artykuł 30*

#### ***Bezpieczeństwo przetwarzania***

1. Mając na uwadze dostępną technologię i koszt wdrażania oraz uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz prawdopodobieństwo i powagę zagrożenia dla praw i wolności osób fizycznych, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, np. (...) pseudonimizację danych osobowych, aby zapewnić poziom bezpieczeństwa odpowiadający temu zagrożeniu.
  - 1a. Oceniając, czy poziom bezpieczeństwa jest odpowiedni, uwzględnia się zwłaszcza zagrożenia, które niesie przetwarzanie danych (...), w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przenoszonych, przechowywanych lub w inny sposób przetwarzanych.
2. (...)
  - 2a. Wywiązywanie się z obowiązków, o których mowa w ust. 1, można wykazać między innymi poprzez stosowanie zatwierdzonych kodeksów postępowania na mocy art. 38 lub zatwierdzonego mechanizmu certyfikacji na mocy art. 39.
  - 2b. Administrator oraz podmiot przetwarzający podejmują działania, by zagwarantować, że każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego, która ma dostęp do danych osobowych, będzie je przetwarzać wyłącznie na polecenie administratora, chyba że wymaga tego od niej prawo Unii lub prawo państwa członkowskiego.
3. (...)
4. (...)

**Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu**

1. Jeżeli dojdzie do naruszenia ochrony danych osobowych mogącego nieść duże zagrożenie dla praw i wolności osób fizycznych, takie jak dyskryminacja, kradzież tożsamości lub oszustwo dotyczące tożsamości, strata finansowa, niedozwolone cofnięcie pseudonimizacji, naruszenie dobrego imienia, naruszenie poufności danych chronionych tajemnicą służbową lub wszelka inna znaczna szkoda gospodarcza lub społeczna, administrator bez zbędnej zwłoki – jeżeli to wykonalne, nie później niż w ciągu 72 godzin po stwierdzeniu naruszenia – zgłasza naruszenie ochrony danych osobowych organowi nadzorczemu właściwemu zgodnie z art. 51. Zgłoszeniu skierowanemu do organu nadzorczego później niż w ciągu 72 godzin towarzyszy umotywowane wyjaśnienie.
- 1a. Zgłoszenie, o którym mowa w ust. 1, nie jest wymagane, jeżeli na mocy art. 32 ust. 3 lit. a) i b) nie jest wymagane zawiadomienie podmiotu danych.
2. (...) Podmiot przetwarzający bez zbędnej zwłoki po stwierdzeniu naruszenia ochrony danych osobowych zgłasza je administratorowi.
3. Zgłoszenie, o którym mowa w ust. 1, musi co najmniej:
  - a) opisywać charakter naruszenia ochrony danych osobowych, w tym jeżeli to możliwe i stosowne, wskazywać przybliżone kategorie i przybliżoną liczbę zainteresowanych podmiotów danych oraz kategorie i przybliżoną liczbę rekordów danych, których dotyczy naruszenie;
  - b) zawierać imię i nazwisko/nazwę oraz dane kontaktowe inspektora ochrony danych lub innego punktu kontaktowego, od którego można uzyskać więcej informacji;
  - c) (...)
  - d) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych stwierdzone przez administratora;

- e) opisywać środki przedsięwzięte lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych; oraz
  - f) w stosownym przypadku wskazywać środki mające zminimalizować ewentualne negatywne skutki naruszenia ochrony danych osobowych.
- 3a. Jeżeli – i w takim zakresie, w jakim – informacji, o których mowa w ust. 3 lit. d), e) i f), nie można przedstawić w tym samym czasie co informacji, o których mowa w ust. 3 lit. a) i b), administrator przedstawia te informacje bez dalszej zbędnej zwłoki.
4. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, o których mowa w ust. 1 i 2, w tym okoliczności naruszenia, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorcemu zweryfikować przestrzeganie niniejszego artykułu. (...).
5. (...)
6. (...)

### *Artykuł 32*

#### ***Zawiadamianie podmiotu danych o naruszeniu ochrony danych osobowych***

1. Jeżeli naruszenie ochrony danych osobowych może nieść duże zagrożenie dla praw i wolności osób fizycznych, takie jak dyskryminacja, kradzież tożsamości lub oszustwo dotyczące tożsamości, strata finansowa, naruszenie dobrego imienia, niedozwolone cofnięcie pseudonimizacji, naruszenie poufności danych chronionych tajemnicą służbową lub wszelka inna znaczna szkoda gospodarcza lub społeczna, administrator (...) bez zbędnej zwłoki zawiadamia podmiot danych o naruszeniu ochrony danych osobowych.
2. Zawiadomienie, o którym mowa w ust. 1, opisuje charakter naruszenia ochrony danych osobowych i zawiera przynajmniej informacje i zalecenia, o których mowa w art. 31 ust. 3 lit. b), e) i f).



3. Zawiadomienie, o którym mowa w ust. 1, (...) nie jest wymagane, jeżeli:
- a. administrator (...) wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych, których dotyczy naruszenie, zwłaszcza środki takie jak szyfrowanie, uniemożliwiające odczyt każdemu, kto nie ma prawa dostępu do nich; lub
  - b. administrator przedsięwziął następnie środki eliminujące prawdopodobieństwo dużego zagrożenia dla praw i wolności podmiotów danych, o którym mowa w ust. 1; lub
  - c. wymagałoby ono niewspółmiernie dużego wysiłku, w szczególności ze względu na liczbę odnośnych spraw. W takim przypadku wydany zostaje komunikat publiczny lub przedsięwzięty zostaje podobny środek, za pomocą którego podmioty danych zostają poinformowane w równie skuteczny sposób; lub
  - d. negatywnie wpłynęłoby na ważny interes publiczny.
4. (...)
5. (...)
6. (...)

# SEKCJA 3

## OCENA SKUTKÓW POD KĄTEM OCHRONY DANYCH I UPRZEDNIE KONSULTACJE

### *Artykuł 33*

#### *Ocena skutków pod kątem ochrony danych*

1. Jeżeli dany rodzaj przetwarzania – zwłaszcza z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele może nieść duże zagrożenie dla praw i wolności osób fizycznych, takie jak dyskryminacja, kradzież tożsamości lub oszustwo dotyczące tożsamości, strata finansowa, naruszenie dobrego imienia, niedozwolone cofnięcie pseudonimizacji, naruszenie poufności danych chronionych tajemnicą służbową lub wszelka inna znaczna szkoda gospodarcza lub społeczna, administrator (...) przed przetworzeniem dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. (...).
- 1a. Dokonując oceny pod kątem ochrony danych, administrator zasięga porady inspektora ochrony danych, jeżeli został on wyznaczony.
2. Ocena skutków pod kątem ochrony danych, o której mowa w ust. 1, jest wymagana w szczególności w następujących przypadkach:
  - a) systematyczna, kompleksowa ocena (...) osobowych czynników (...) osób fizycznych (...), która opiera się na profilowaniu i jest podstawą decyzji wywołujących skutki prawne wobec podmiotów danych lub poważnie wpływających na podmioty danych;
  - b) przetwarzanie danych osobowych szczególnych kategorii na mocy art. 9 ust. 1 (...), danych biometrycznych lub danych o wyrokach skazujących za przestępstwa i o przestępstwach lub o odnośnych środkach zabezpieczających – jeżeli dane te są przetwarzane na dużą skalę w celu podjęcia (...) decyzji wobec konkretnych osób fizycznych;

- c) monitorowanie *na dużą skalę* miejsc dostępnych publicznie, zwłaszcza za pomocą urządzeń optyczno-elektronicznych (...);
  - d) (...);
  - e) (...).
- 2a. Organ nadzorczy ustanawia i podaje do wiadomości publicznej wykaz rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków pod kątem ochrony danych na mocy ust. 1. Organ nadzorczy przekazuje te wykazy Europejskiej Radzie Ochrony Danych.
- 2b. Organ nadzorczy może także ustanowić i podać do wiadomości publicznej wykaz rodzajów operacji przetwarzania niepodlegających wymogowi dokonania oceny pod kątem ochrony danych. Organ nadzorczy przekazuje te wykazy Europejskiej Radzie Ochrony Danych.
- 2c. Jeżeli wykazy, o których mowa w ust. 2a i 2b, obejmują czynności przetwarzania związane z oferowaniem towarów lub usług podmiotom danych lub z monitorowaniem ich zachowania w kilku państwach członkowskich lub mogące znacznie wpłynąć na swobodny przepływ danych osobowych w Unii, przed przyjęciem takich wykazów właściwy organ nadzorczy stosuje mechanizm spójności, o którym mowa w art. 57.
3. Ocena zawiera co najmniej ogólny opis planowanych operacji przetwarzania, szacunek zagrożenia, o którym mowa w ust. 1, środki planowane w celu zaradzenia temu zagrożeniu, w tych gwarancje oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie niniejszego rozporządzenia, z uwzględnieniem praw i uzasadnionych interesów podmiotów danych i innych zainteresowanych osób.

- 3a. Oceniając – w szczególności do celów oceny skutków pod kątem ochrony danych – zgodność z prawem oraz skutki operacji przetwarzania wykonywanych przez administratora lub podmiot przetwarzający, uwzględnia się przestrzeganie przez takiego administratora lub taki podmiot przetwarzający zatwierdzonych kodeksów postępowania, o których mowa w art. 38.
4. *Administrator zasięga opinii podmiotów danych lub ich przedstawicieli w sprawie zamierzonego przetwarzania, bez uszczerbku dla ochrony interesów handlowych lub publicznych lub bezpieczeństwa operacji przetwarzania (...).*
5. Ustępy 1–3 nie mają zastosowania, jeżeli (...) przetwarzanie na mocy art. 6 ust. 1 lit. c) lub e) ma podstawę prawną w prawie Unii lub w prawie państwa członkowskiego, któremu podlega administrator, i prawo takie reguluje daną operację przetwarzania lub dany zestaw operacji, chyba że państwa członkowskie uznają za niezbędne, by przed podjęciem czynności przetwarzania dokonać takiej oceny.
6. (...)
7. (...)

#### *Artykuł 34*

#### ***Uprzednie (...) konsultacje***

1. (...)
2. Jeżeli ocena skutków pod kątem ochrony danych, o której mowa w art. 33, wskaże, że przetwarzanie niosłoby duże zagrożenie, gdyby administrator nie przedsięwziął środków w celu zminimalizowania tego zagrożenia, to przed przetworzeniem danych osobowych administrator (...) konsultuje się z organem nadzorczym.

3. Jeżeli organ nadzorczy jest zdania, że zamierzone przetwarzanie, o którym mowa w ust. 2, nie byłoby zgodne z niniejszym rozporządzeniem – w szczególności jeżeli administrator niedostatecznie zidentyfikował lub zminimalizował zagrożenie – to najpóźniej sześć tygodni po wpłynięciu wniosku o konsultację udziela administratorowi porady na piśmie i może skorzystać z dowolnego ze swoich uprawnień, o których mowa w art. 53 (...). Okres ten można przedłużyć o kolejnych sześć tygodni ze względu na złożony charakter zamierzonego przetwarzania. Jeżeli zastosowanie ma okres przedłużony, administrator lub podmiot przetwarzający są informowani w terminie jednego miesiąca od wpłynięcia wniosku o przyczynach tego opóźnienia.
4. (...)
5. (...)
6. Konsultując się z organem nadzorczym na mocy ust. 2, administrator przedstawia mu:
- a) w stosownym przypadku obowiązki administratora, współadministratorów oraz podmiotów przetwarzających uczestniczących w przetwarzaniu, w szczególności w przypadku przetwarzania w ramach grupy przedsiębiorstw;
  - b) cele i sposoby zamierzonego przetwarzania;
  - c) środki i gwarancje mające chronić prawa i wolności podmiotów danych zgodnie z niniejszym rozporządzeniem;
  - d) w stosownym przypadku dane kontaktowe inspektora ochrony danych;
  - e) ocenę skutków pod kątem ochrony danych, o której mowa w art. 33; oraz
  - f) wszelkie (...) inne informacje, których żąda organ nadzorczy (...).

7. Państwa członkowskie konsultują się z organem nadzorczym, przygotowując projekt środka ustawodawczego przyjmowanego przez parlament narodowy lub środka regulacyjnego opartego na takim środku ustawodawczym, jeżeli projekt przewiduje przetwarzanie danych osobowych (...).
- 7a. Niezależnie od ust. 2 prawo państw członkowskich może wymagać, by administratorzy konsultowali się z organem nadzorczym i uzyskiwali jego uprzednie zezwolenie odnośnie do przetwarzania danych osobowych przez administratora do celów wykonania zadania realizowanego przez administratora w interesie publicznym, w tym przetwarzania takich danych w związku z ochroną socjalną i zdrowiem publicznym.
8. (...)
9. (...)

## SEKCJA 4

### INSPEKTOR OCHRONY DANYCH

#### *Artykuł 35*

#### ***Wyznaczenie inspektora ochrony danych***

1. Administrator lub podmiot przetwarzający mogą wyznaczyć, a jeżeli wymaga tego prawo Unii lub prawo państwa członkowskiego – wyznaczają inspektora ochrony danych (...).
2. Grupa przedsiębiorstw może wyznaczyć jednego inspektora ochrony danych.
3. Jeżeli administrator lub podmiot przetwarzający są organem lub podmiotem publicznym, dla kilku takich organów lub podmiotów można wyznaczyć – z uwzględnieniem ich struktury organizacyjnej i wielkości – jednego inspektora ochrony danych.
4. (...).
5. (...) Inspektor ochrony danych jest wyznaczany na podstawie kwalifikacji zawodowych oraz w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 37, a zwłaszcza brak konfliktu interesów. (...).
6. (...)
7. (...). Poza poważnymi powodami przewidzianymi w prawie danego państwa członkowskiego uzasadniającymi odwołanie pracownika lub urzędnika służby cywilnej inspektor ochrony danych może podczas swojej kadencji zostać odwołany wyłącznie wtedy, gdy przestanie spełniać warunki niezbędne do wypełnienia zadań powierzonych mu na mocy art. 37.
8. Inspektor ochrony danych może być członkiem personelu administratora lub podmiotu przetwarzającego lub wykonywać zadania na podstawie umowy o świadczenie usług.
9. Administrator lub podmiot przetwarzający publikują dane kontaktowe inspektora ochrony danych i zawiadamiają o nich organ nadzorczy (...).

10. Podmioty danych moga kontaktować się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych oraz z korzystaniem z praw przysługujących im na mocy niniejszego rozporządzenia.
11. (...)

#### *Artykuł 36*

##### ***Status inspektora ochrony danych***

1. Administrator lub podmiot przetwarzający dopilnowują, by inspektor ochrony danych był właściwie i terminowo angażowany we wszystkie sprawy dotyczące ochrony danych osobowych.
2. Administrator lub podmiot przetwarzający wspierają inspektora ochrony danych w wypełnianiu przez niego zadań, o których mowa w art. 37, zapewniając mu (...) zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania.
3. Administrator lub podmiot przetwarzający dopilnowują, by inspektor ochrony danych mógł wypełniać swoje zadania w sposób niezależny i nie otrzymywał żadnych instrukcji co do wykonywania tych zadań. Nie jest on penalizowany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań. Inspektor ochrony danych bezpośrednio podlega najwyższemu kierownictwu administratora lub podmiotu przetwarzającego.
4. Inspektor ochrony danych może wypełniać inne zadania i obowiązki. Administrator lub podmiot przetwarzający dopilnowują, by takie zadania i obowiązki nie powodowały konfliktu interesów.

#### *Artykuł 37*

##### ***Zadania inspektora ochrony danych***

1. (...) Inspektor ochrony danych (...) ma następujące zadania:
  - a) informowanie administratora lub podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie (...);



- b) monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz strategii administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym przydział obowiązków, działania uwrażliwiające, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz odnośne kontrole;
- c) (...)
- d) (...)
- e) (...)
- f) udzielanie porad na żądanie co do oceny skutków pod kątem ochrony danych oraz monitorowanie jej wykonania na mocy art. 33;
- g) monitorowanie odpowiedzi na wnioski organu nadzorczego oraz – w ramach kompetencji inspektora ochrony danych – współpraca z organem nadzorczym na żądanie tego organu lub z inicjatywy inspektora ochrony danych;
- h) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych osobowych, w tym z uprzednimi konsultacjami, o których mowa w art. 34, oraz w stosownym przypadku udzielanie konsultacji we wszelkich innych sprawach.

2. (...)

2a. Inspektor ochrony danych wypełnia swoje zadania z należytym uwzględnieniem zagrożenia związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

## SEKCJA 5

### KODEKSY POSTĘPOWANIA I CERTYFIKACJA

#### *Artykuł 38*

#### ***Kodeksy postępowania***

1. Państwa członkowskie, organy nadzorcze, Europejska Rada Ochrony Danych oraz Komisja zachęcają do sporządzania kodeksów postępowania mających pomóc we właściwym stosowaniu niniejszego rozporządzenia – z uwzględnieniem szczególnych cech różnych sektorów przetwarzających dane oraz szczególnych potrzeb mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw.
- 1a. Stowarzyszenia i inne organy reprezentujące administratorów lub podmioty przetwarzające różnych kategorii mogą przygotowywać, zmieniać lub poszerzać kodeksy postępowania, aby doprecyzować zastosowanie przepisów niniejszego rozporządzenia, np. co do:
  - a) rzetelnego i przejrzystego przetwarzania danych;
  - aa) uzasadnionych interesów realizowanych przez administratorów w konkretnych kontekstach;
  - b) zbierania danych;
  - bb) pseudonimizacji danych osobowych;
  - c) informowania opinii publicznej i podmiotów danych;
  - d) korzystania przez podmioty danych z przysługujących im praw;
  - e) informowania i ochrony dzieci oraz sposobu pozyskiwania zgody rodzica i opiekuna;
  - ee) środków i procedur, o których mowa w art. 22 i 23, oraz środków zapewniających bezpieczeństwo przetwarzania, o których mowa w art. 30;

ef) zgłaszania organowi nadzorcemu naruszenia ochrony danych osobowych oraz zawiadamiania o nim podmiotów danych;

f) (...).

- 1ab. Poza administratorami lub podmiotami przetwarzającymi, którzy podlegają niniejszemu rozporządzeniu, kodeksów postępowania zatwierdzonych na mocy ust. 2 mogą przestrzegać także administratorzy lub podmioty przetwarzające, którzy zgodnie z art. 3 nie podlegają niniejszemu rozporządzeniu, w celu zapewnienia odpowiednich gwarancji w ramach przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych na warunkach określonych w art. 42 ust. 2 lit. d). Tacy administratorzy lub takie podmioty przetwarzające podejmują wiążące i egzekwowalne zobowiązanie – za pomocą instrumentów umownych lub w inny sposób – do stosowania tych odpowiednich gwarancji, w tym w odniesieniu do praw podmiotów danych.
- 1b. Kodeks postępowania przewiduje mechanizmy pozwalające podmiotowi, o którym mowa w art. 38a ust. 1, prowadzić obowiązkowe monitorowanie przestrzegania przepisów kodeksu przez administratorów lub podmioty przetwarzające, którzy podjęli się jego stosowania, bez uszczerbku dla zadań i uprawnień organu nadzorczego właściwego na mocy art. 51 lub 51a.
2. Stowarzyszenia i inne organy, o których mowa w ust. 1a, chcące przygotować kodeks postępowania lub zmienić lub poszerzyć kodeks już obowiązujący przedkładają jego projekt organowi nadzorcemu właściwemu na mocy art. 51. Organ nadzorczy wydaje opinię o zgodności projektu, zmienionego kodeksu lub poszerzonego kodeksu z niniejszym rozporządzeniem i zatwierdza taki projekt, zmieniony kodeks lub poszerzony kodeks, jeżeli uzna, że stanowią one wystarczające gwarancje.
- 2a. Jeżeli opinia, o której mowa w ust. 2, potwierdza, że kodeks postępowania, zmieniony kodeks postępowania lub poszerzony kodeks postępowania są zgodne z niniejszym rozporządzeniem i jeżeli kodeks ten zostaje zatwierdzony i nie dotyczy czynności przetwarzania prowadzonych w kilku państwach członkowskich, organ nadzorczy rejestruje ten kodeks i publikuje szczegółowe informacje o nim.

- 2b. Jeżeli projekt kodeksu postępowania dotyczy czynności przetwarzania prowadzonych w kilku państwach członkowskich, organ nadzorczy właściwy na mocy art. 51 przed zatwierdzeniem przedkłada go zgodnie z procedurą, o której mowa w art. 57, Europejskiej Radzie Ochrony Danych, która wydaje opinię o zgodności projektu, zmienionego kodeksu lub poszerzonego kodeksu z niniejszym rozporządzeniem lub w sytuacji określonej w ust. 1ab opinię o tym, czy stanowią one odpowiednie gwarancje.
3. Jeżeli opinia, o której mowa w ust. 2b, potwierdza, że kodeks postępowania, zmieniony kodeks postępowania lub poszerzony kodeks postępowania są zgodne z niniejszym rozporządzeniem lub w sytuacji określonej w ust. 1ab stanowią odpowiednie gwarancje, Europejska Rada Ochrony Danych przedkłada tę opinię Komisji.
4. Komisja może przyjmować akty wykonawcze w celu stwierdzenia, że zatwierdzone kodeksy postępowania oraz zmiany lub poszerzenia już obowiązujących zatwierdzonych kodeksów przedłożone jej na mocy ust. 3 mają ogólną moc obowiązującą w Unii. Te akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 87 ust. 2.
5. Komisja zapewnia odpowiednie propagowanie zatwierdzonych kodeksów, których ogólną moc obowiązującą stwierdziła zgodnie z ust. 4.
- 5a. Europejska Rada Ochrony Danych gromadzi w rejestrze wszystkie zatwierdzone kodeksy postępowania i zmiany do nich i udostępnia je opinii publicznej za pomocą odpowiednich środków, np. za pomocą europejskiego portalu e-Sprawiedliwość.

#### *Artykuł 38a*

#### **Monitorowanie zatwierdzonych kodeksów postępowania**

1. Bez uszczerbku dla zadań i uprawnień właściwego organu nadzorczego wynikających z art. 52 i 53 monitorowaniem przestrzegania kodeksu postępowania na mocy art. 38 ust. 1b może się zajmować podmiot, który dysponuje odpowiednim poziomem wiedzy fachowej w dziedzinie będącej przedmiotem kodeksu i został akredytowany w tym celu przez właściwy organ nadzorczy.

2. Podmiot, o którym mowa w ust. 1, może zostać akredytowany w tym celu, jeżeli:
- (a) w sposób satysfakcjonujący wykazał właściwemu organowi nadzorczemu swoją niezależność i wiedzę fachową w dziedzinie będącej przedmiotem kodeksu;
  - (b) dysponuje procedurami, które pozwalają mu ocenić zdolność konkretnych administratorów i podmiotów przetwarzających do stosowania kodeksu, monitorować przestrzeganie przez nich jego przepisów oraz okresowo weryfikować jego funkcjonowanie;
  - (c) dysponuje procedurami i strukturami, które pozwalają rozpatrywać skargi na naruszenie kodeksu przez administratora lub podmiot przetwarzający lub na sposób wdrożenia lub wdrażania kodeksu przez administratora lub podmiot przetwarzający oraz które pozwalają zapewnić przejrzystość tych procedur i struktur wobec podmiotów danych i opinii publicznej;
  - (d) w sposób satysfakcjonujący wykaże właściwemu organowi nadzorczemu, że jego zadania i obowiązki nie powodują konfliktu interesów.
3. Właściwy organ nadzorczy przedkłada proponowane kryteria akredytacji podmiotu, o którym mowa w ust. 1, Europejskiej Radzie Ochrony Danych zgodnie z mechanizmem spójności, o którym mowa w art. 57.
4. Bez uszczerbku dla przepisów rozdziału VIII podmiot, o którym mowa w ust. 1, może – z zastrzeżeniem odpowiednich gwarancji – podjąć odpowiednie działania w przypadku naruszenia kodeksu przez administratora lub podmiot przetwarzający, w tym zawiesić lub wykluczyć administratora lub podmiot przetwarzający spośród stosujących kodeks. O działaniach tych i powodach ich podjęcia informuje on właściwy organ nadzorczy.
5. Właściwy organ nadzorczy cofa akredytację podmiotu, o którym mowa w ust. 1, jeżeli podmiot ten nie spełnia lub przestał spełniać warunki akredytacji lub jeżeli działania przez niego podejmowane nie są zgodne z niniejszym rozporządzeniem.
6. Niniejszy artykuł nie ma zastosowania do przetwarzania danych osobowych przez organy i podmioty publiczne.

**Certyfikacja**

1. Państwa członkowskie, Europejska Rada Ochrony Danych oraz Komisja zachęcają – w szczególności na szczeblu Unii – do ustanawiania mechanizmów certyfikacji w dziedzinie ochrony danych osobowych oraz pieczęci i oznaczeń mających świadczyć o zgodności z niniejszym rozporządzeniem operacji przetwarzania prowadzonych przez administratorów i podmioty przetwarzające. Uwzględnia się szczególne potrzeby mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw.
- 1a. Mechanizmy certyfikacji oraz pieczęcie i oznaczenia w dziedzinie ochrony danych zatwierdzone na mocy ust. 2a i przestrzegane przez administratorów lub podmioty przetwarzające, którzy podlegają niniejszemu rozporządzeniu, mogą być ustanowione także do wykazania odpowiednich gwarancji przez administratorów lub podmioty przetwarzające, którzy zgodnie z art. 3 nie podlegają niniejszemu rozporządzeniu, w ramach przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych na warunkach określonych w art. 42 ust. 2 lit. e). Tacy administratorzy lub takie podmioty przetwarzające podejmują wiążące i egzekwowalne zobowiązanie – za pomocą instrumentów umownych lub w inny sposób – do stosowania tych odpowiednich gwarancji, w tym w odniesieniu do praw podmiotów danych.
2. Certyfikacja przewidziana w niniejszym artykule nie ogranicza spoczywającego na administratorze lub podmiocie przetwarzającym obowiązku przestrzegania niniejszego rozporządzenia i pozostaje bez uszczerbku dla zadań i uprawnień organu nadzorczego właściwego na mocy art. 51 lub 51a.
- 2a. Certyfikacji przewidzianej w niniejszym artykule dokonują podmioty certyfikujące, o których mowa w art. 39a, lub w stosownym przypadku dokonuje jej właściwy organ nadzorczy – na podstawie kryteriów zatwierdzonych przez właściwy organ nadzorczy lub w przypadku art. 57 przez Europejską Radę Ochrony Danych.
3. Administrator lub podmiot przetwarzający, którzy poddają swoje przetwarzanie mechanizmowi certyfikacji, udzielają podmiotowi certyfikującemu, o którym mowa w art. 39a, lub w stosownym przypadku właściwemu organowi nadzorczemu wszelkich informacji i wszelkiego dostępu do swoich czynności przetwarzania, które są niezbędne do przeprowadzenia procedury certyfikacji.

4. Certyfikacji udziela się administratorowi lub podmiotowi przetwarzającemu na maksymalny okres 3 lat; certyfikację można przedłużyć na tych samych warunkach, o ile nadal spełnione są stosowne wymogi. Organy certyfikujące, o których mowa w art. 39a, lub w stosownym przypadku właściwy organ nadzorczy cofają certyfikację, jeżeli jej wymogi nie są spełnione lub przestały być spełniane.
5. Europejska Rada Ochrony Danych gromadzi w rejestrze wszystkie mechanizmy certyfikacji i pieczęcie w dziedzinie ochrony danych i udostępnia je opinii publicznej za pomocą odpowiednich środków, np. za pomocą europejskiego portalu e-Sprawiedliwość.

*Artykuł 39a*

**Podmiot certyfikujący i procedura certyfikacji**

1. Bez uszczerbku dla zadań i uprawnień właściwego organu nadzorczego wynikających z art. 52 i 53 certyfikacji i jej przedłużenia dokonuje podmiot certyfikujący, który dysponuje odpowiednim poziomem wiedzy fachowej w dziedzinie ochrony danych. Każde państwo członkowskie określa, czy te podmioty certyfikujące są akredytowane przez:
- (a) organ nadzorczy właściwy na mocy art. 51 lub 51a; czy
  - (b) krajową jednostkę akredytującą określoną zgodnie z rozporządzeniem (WE) 765/2008 Parlamentu Europejskiego i Rady z dnia 9 lipca 2008 r. ustanawiającym wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu – w poszanowaniu EN-ISO/IEC 17065/2012 – oraz zgodnie z dodatkowymi wymogami ustanowionymi przez organ nadzorczy właściwy na mocy art. 51 lub 51a.
2. Podmiot certyfikujący, o którym mowa w ust. 1, może zostać akredytowany w tym celu wyłącznie wtedy, gdy:
- (a) w sposób satysfakcjonujący wykazał właściwemu organowi nadzorczemu swoją niezależność i wiedzę fachową w dziedzinie podlegającej certyfikacji;

- aa) podjął się respektowania kryteriów, o których mowa w art. 39 ust. 2a i które zostały zatwierdzone przez organ nadzorczy właściwy na mocy art. 51 lub 51a lub – w przypadku art. 57 – przez Europejską Radę Ochrony Danych;
  - b) dysponuje procedurami wydawania, okresowego weryfikowania i cofania pieczęci i oznaczeń w dziedzinie ochrony danych;
  - c) dysponuje procedurami i strukturami, które pozwalają rozpatrywać skargi na naruszenie certyfikacji przez administratora lub podmiot przetwarzający lub na sposób wdrożenia lub wdrażania certyfikacji przez administratora lub podmiot przetwarzający oraz które zapewniają przejrzystość tych procedur i struktur wobec podmiotów danych i opinii publicznej;
  - d) w sposób satysfakcjonujący wykaże właściwemu organowi nadzorcemu, że jego zadania i obowiązki nie powodują konfliktu interesów.
3. Akredytacja podmiotów certyfikujących, o których mowa w ust. 1, odbywa się na podstawie kryteriów zatwierdzonych przez organ nadzorczy właściwy na mocy art. 51 lub 51a lub – w przypadku art. 57 – przez Europejską Radę Ochrony Danych. W przypadku akredytacji na mocy ust. 1 lit. b) wymogi te są uzupełnieniem wymogów przewidzianych w rozporządzeniu 765/2008 oraz przepisów technicznych określających metody i procedury podmiotów certyfikujących.
4. Podmiot certyfikujący, o którym mowa w ust. 1, ma obowiązek przed udzieleniem lub cofnięciem certyfikacji dokonać właściwej oceny, bez uszczerbku dla spoczywającego na administratorze lub podmiocie przetwarzającym obowiązku przestrzegania niniejszego rozporządzenia. Akredytacji udziela się na maksymalny okres pięciu lat; można ją przedłużyć na tych samych warunkach, o ile podmiot spełnia wymogi.
5. Podmiot certyfikujący, o którym mowa w ust. 1, przedstawia właściwemu organowi nadzorcemu powody udzielenia lub cofnięcia żądanej certyfikacji.



6. Organ nadzorczy w łatwo dostępny sposób podaje do wiadomości publicznej wymogi, o których mowa w ust. 3, oraz kryteria, o których mowa w art. 39 ust. 2a. Organy nadzorcze przekazują je także Europejskiej Radzie Ochrony Danych. Europejska Rada Ochrony Danych gromadzi w rejestrze wszystkie mechanizmy certyfikacji i pieczęcie w dziedzinie ochrony danych i udostępnia je opinii publicznej za pomocą odpowiednich środków, np. za pomocą europejskiego portalu e-Sprawiedliwość.
- 6a. Bez uszczerbku dla przepisów rozdziału VIII właściwy organ nadzorczy lub krajowa jednostka akredytująca cofają akredytację udzieloną przez siebie podmiotowi certyfikującemu, o którym mowa w ust. 1, jeżeli podmiot ten nie spełnia lub przestał spełniać warunki akredytacji lub jeżeli działania przez niego podejmowane nie są zgodne z niniejszym rozporządzeniem.
7. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 86 w celu doprecyzowania kryteriów i wymogów, które należy uwzględnić w przypadku mechanizmów certyfikacji w dziedzinie ochrony danych, o których mowa w ust. 1 (...).
- 7a. Kryteria i wymogi, o których mowa w ust. 7, opiniuje dla Komisji Europejska Rada Ochrony Danych.
8. Komisja może ustanowić techniczne standardy mechanizmów certyfikacji oraz pieczęci i oznaczeń w dziedzinie ochrony danych, a także sposoby propagowania i uznawania mechanizmów certyfikacji oraz pieczęci i oznaczeń w dziedzinie ochrony danych. Te akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 87 ust. 2.

## ROZDZIAŁ V

### PRZEKAZYWANIE DANYCH OSOBOWYCH DO PAŃSTW TRZECICH LUB ORGANIZACJI MIĘDZYNARODOWYCH

#### *Artykuł 40*

#### ***Ogólna zasada przekazywania***

(...)

#### *Artykuł 41*

#### ***Przekazywanie na podstawie decyzji stwierdzającej odpowiedni poziom ochrony***

1. Przekazanie danych osobowych do (...) państwa trzeciego lub organizacji międzynarodowej może nastąpić wtedy, gdy Komisja stwierdzi, że to państwo trzecie, terytorium, określony sektor lub określone sektory w tym państwie trzecim lub dana organizacja międzynarodowa zapewniają odpowiedni poziom ochrony. Takie przekazanie nie wymaga specjalnego zezwolenia.
  
2. Oceniając, czy poziom ochrony jest odpowiedni, Komisja uwzględnia w szczególności następujące elementy:
  - a) praworządność, poszanowanie praw człowieka i podstawowych wolności, stosowne ustawodawstwo (...) – zarówno ogólne, jak i sektorowe – przepisy o ochronie danych i środki bezpieczeństwa, w tym zasady wtórnego przekazywania danych osobowych do kolejnego państwa trzeciego lub innej organizacji międzynarodowej, których przestrzega się w tym państwie trzecim lub w organizacji międzynarodowej, a także istnienie skutecznych i egzekwowalnych praw podmiotów danych oraz prawa podmiotów danych, których dane osobowe są przekazywane, do skutecznych administracyjnych i sądowych środków dochodzenia roszczeń (...);

- b) istnienie i skuteczne działanie co najmniej jednego niezależnego organu nadzorczego w państwie trzecim lub w stosunku do organizacji międzynarodowej, mającego obowiązek zapewniać i egzekwować przestrzeganie przepisów o ochronie danych – w tym odpowiednio uprawnionego do nakładania sankcji – pomagać i doradzać podmiotom danych w korzystaniu z przysługujących im praw, a także współpracować z organami nadzorczymi Unii i państw członkowskich;
  - c) międzynarodowe zobowiązania zaciągnięte przez dane państwo trzecie lub daną organizację międzynarodową lub inne (...) obowiązki wynikające z ich udziału w systemach wielostronnych lub regionalnych, w szczególności w dziedzinie ochrony danych osobowych.
- 2a. Europejska Rada Ochrony Danych wydaje opinie z przeznaczeniem dla Komisji na potrzeby oceny, czy poziom ochrony w państwie trzecim lub organizacji międzynarodowej jest odpowiedni, w tym na potrzeby oceny, czy państwo trzecie lub terytorium, lub organizacja międzynarodowa, lub określony sektor nie przestały zapewniać odpowiedniego poziomu ochrony.
3. Po dokonaniu oceny, czy poziom ochrony jest odpowiedni, Komisja może przyjąć decyzję stwierdzającą, że państwo trzecie lub terytorium, lub określony sektor, lub określone sektory w tym państwie trzecim, lub organizacja międzynarodowa zapewniają odpowiedni poziom ochrony w rozumieniu ust. 2. (...). W akcie wykonawczym zostaje określony terytorialny i sektorowy zakres jego zastosowania, a w stosownym przypadku wskazany (niezależny) organ nadzorczy (organy nadzorcze), o którym mowa w ust. 2 lit. b). Akt wykonawczy zostaje przyjęty zgodnie z procedurą sprawdzającą, o której mowa w art. 87 ust. 2.
- 3a. *Decyzje przyjęte przez Komisję na mocy art. 25 ust. 6 (...) dyrektywy 95/46/WE pozostają w mocy do czasu ich zmiany, zastąpienia lub uchylecia [...] decyzją Komisji przyjętą zgodnie z ust. 3 lub 5.*

4. (...)
- 4a. Komisja monitoruje obowiązywanie decyzji przyjętych na mocy ust. 3 oraz decyzji przyjętych na podstawie art. 25 ust. 6 lub art. 26 ust. 4 dyrektywy 95/46/WE.
5. Komisja może przyjąć decyzję stwierdzającą, że państwo trzecie, terytorium lub określony sektor w tym państwie trzecim, lub organizacja międzynarodowa przestały zapewniać odpowiedni poziom ochrony w rozumieniu ust. 2, a w razie potrzeby może taką decyzję uchylić, zmienić lub zawiesić bez mocy wstecznej. Akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 87 ust. 2, lub w przypadkach wyjątkowo pilnych (...) zgodnie z procedurą, o której mowa w art. 87 ust. 3. (...)
- 5a. Komisja podejmuje konsultacje z państwem trzecim lub organizacją międzynarodową w celu zaradzenia sytuacji będącej przyczyną decyzji przyjętej na mocy ust. 5.
6. Decyzja przyjęta na mocy ust. 5 pozostaje bez uszczerbku dla przekazywania danych osobowych do danego państwa trzeciego, terytorium lub określonego sektora w tym państwie trzecim lub do danej organizacji międzynarodowej na mocy art. 42–44. (...)
7. Komisja publikuje w *Dzienniku Urzędowym Unii Europejskiej* wykaz tych państw trzecich, terytoriów i określonych sektorów w państwie trzecim oraz tych organizacji międzynarodowych, co do których przyjęto decyzje na mocy ust. 3, 3a i 5.
8. (...)

***Przekazywanie na podstawie odpowiednich gwarancji***

1. W razie braku decyzji na mocy art. 41 ust. 3 administrator lub podmiot przetwarzający mogą przekazać dane osobowe (...) do państwa trzeciego lub organizacji międzynarodowej wyłącznie wtedy, gdy administrator lub podmiot przetwarzający powołają się na odpowiednie gwarancje, obejmujące także przekazanie wtórne (...).
2. Odpowiednie gwarancje, o których mowa w ust. 1, można zapewnić – (...) bez konieczności uzyskania specjalnego zezwolenia ze strony organu nadzorczego – za pomocą:
  - oa) prawnie wiążącego i egzekwowalnego instrumentu między organami lub podmiotami publicznymi; lub
  - a) wiążących reguł korporacyjnych, o których mowa w art. 43; lub
  - b) standardowych klauzul ochrony danych przyjętych przez Komisję (...) zgodnie z procedurą sprawdzającą, o której mowa w art. 87 ust. 2; lub
  - c) standardowych klauzul ochrony danych przyjętych przez organ nadzorczy (...) oraz przyjętych przez Komisję zgodnie z procedurą sprawdzającą, o której mowa w art. 87 ust. 2;
  - d) zatwierdzonego kodeksu postępowania opartego na art. 38 wraz z wiążącymi i egzekwowalnymi zobowiązaniami administratora lub podmiotu przetwarzającego (...) w państwie trzecim do stosowania odpowiednich gwarancji, w tym w odniesieniu do praw podmiotów danych; lub
  - e) zatwierdzonego mechanizmu certyfikacji opartego na art. 39 wraz z wiążącymi i egzekwowalnymi zobowiązaniami administratora lub podmiotu przetwarzającego (...) w państwie trzecim do stosowania odpowiednich gwarancji, w tym w odniesieniu do praw podmiotów danych.

- 2a. Z zastrzeżeniem zezwolenia ze strony właściwego organu nadzorczego odpowiednie gwarancje, o których mowa w ust. 1, można także zapewnić w szczególności za pomocą:
- a) klauzul umownych między administratorem lub podmiotem przetwarzającym a administratorem, podmiotem przetwarzającym lub odbiorcą danych (...) w państwie trzecim lub organizacji międzynarodowej; lub
  - b) (...)
  - c) (...)
  - d) przepisów, które zostaną zamieszczone w porozumieniach administracyjnych między organami lub podmiotami publicznymi (...).
3. (...)
4. (...)
5. (...)
- 5a. W przypadkach, o których mowa w art. 57 ust. 2 lit. ca), d), e) i f), organ nadzorczy stosuje mechanizm spójności.
- 5b. *Zezwolenia wydane przez państwo członkowskie lub organ nadzorczy na podstawie art. 26 ust. 2 dyrektywy 95/46/WE zachowują ważność do czasu ich zmiany, zastąpienia lub uchylenia przez ten organ. Decyzje przyjęte przez Komisję na mocy art. 26 ust. 4 dyrektywy 95/46/WE pozostają w mocy do czasu ich zmiany, zastąpienia lub uchylenia [...] decyzją Komisji przyjętą zgodnie z ust. 2 [...].*

#### *Artykuł 43*

#### ***Wiążące reguły korporacyjne***

1. Właściwy organ nadzorczy zatwierdza wiążące reguły korporacyjne zgodnie z mechanizmem spójności przewidzianym w art. 57, pod warunkiem że:
- a) są one prawnie wiążące oraz mają zastosowanie do każdego z zainteresowanych członków grupy przedsiębiorstw lub grupy firm prowadzących wspólną działalność gospodarczą i są przez każdego z nich egzekwowane;

- b) wyraźnie przyznają podmiotom danych egzekwowalne prawa w związku z przetwarzaniem ich danych osobowych;
- c) spełniają wymogi ustanowione w ust. 2.

2. W wiążących regułach korporacyjnych, o których mowa w ust. 1, określone zostają co najmniej:

- a) struktura i dane kontaktowe odnośnej grupy i każdego z jej członków;
- b) przekazania lub kategorie przekazanych danych, w tym rodzaje danych osobowych, rodzaj przetwarzania i jego cele, typy odnośnych podmiotów danych oraz nazwa danego państwa trzeciego lub danych państw trzecich;
- c) ich prawnie wiążący charakter, w wymiarze wewnętrznym i zewnętrznym;
- d) zastosowanie ogólnych zasad ochrony danych, w szczególności zasady celowości (...), jakości danych, podstawa prawna przetwarzania, przetwarzanie danych osobowych szczególnych kategorii, środki zapewniające bezpieczeństwo danych, wymogi w zakresie wtórnego przekazywania podmiotom (...) niezwiązanym wiążącymi regułami korporacyjnymi;
- e) prawa podmiotów danych w związku z przetwarzaniem ich danych osobowych oraz sposoby korzystania z tych praw, w tym z prawa do niepodlegania (...) decyzjom opartym wyłącznie na zautomatyzowanym przetwarzaniu – w tym profilowaniu – zgodnie z art. 20, prawa do wnoszenia skarg do właściwego organu nadzorczego i właściwych sądów państw członkowskich zgodnie z art. 75 oraz prawa do środka dochodzenia roszczeń, a w stosownym przypadku – odszkodowania za naruszenie wiążących reguł korporacyjnych;
- f) przyjęcie przez administratora lub podmiot przetwarzający mających siedzibę na terytorium państwa członkowskiego odpowiedzialności prawnej za naruszenie wiążących reguł korporacyjnych przez odnośnego członka niemającego siedziby w Unii; administrator lub podmiot przetwarzający mogą być zwolnieni z tej odpowiedzialności prawnej – w całości lub w części – wyłącznie wtedy, gdy udowodnią, że członek ten nie ponosi odpowiedzialności za wydarzenie, które doprowadziło do powstania szkody;
- g) sposób podawania podmiotom danych – zgodnie z art. 14 i 14a – informacji o wiążących regułach korporacyjnych, w szczególności o przepisach, o których mowa w lit. d), e) i f) niniejszego ustępu;

- h) zadania wszelkich inspektorów ochrony danych wyznaczonych zgodnie z art. 35 lub wszelkich innych osób lub podmiotów odpowiedzialnych za monitorowanie (...) przestrzegania wiążących reguł korporacyjnych w ramach grupy oraz monitorowanie szkoleń i rozpatrywania skarg;
- hh) procedury dotyczące skarg;
- i) stosowane w grupie (...) mechanizmy zapewniające weryfikację przestrzegania wiążących reguł korporacyjnych. Wśród takich mechanizmów są audyty w zakresie ochrony danych oraz metody zapewniania działań korekcyjnych mających chronić prawa podmiotów danych. Wyniki takiej weryfikacji powinny być przekazywane osobie lub podmiotowi, o których mowa w lit. h), oraz zarządowi przedsiębiorstwa sprawującego kontrolę lub zarządowi grupy firm i powinny być dostępne na żądanie dla właściwego organu nadzorczego;
- j) mechanizmy zgłaszania i rejestrowania zmian w regułach i zgłaszania tych zmian organowi nadzorcemu;
- k) mechanizm współpracy z organem nadzorczym zapewniający przestrzeganie reguł przez wszystkich członków grupy (...), w szczególności poprzez udostępnianie organowi nadzorcemu wyników weryfikacji środków, o której mowa w lit. i) niniejszego ustępu;
- l) mechanizm zgłaszania właściwemu organowi nadzorcemu wszelkich wymogów prawnych, którym podlega członek grupy w państwie trzecim i które mogą mieć znaczny niekorzystny wpływ na gwarancje przewidziane w wiążących regułach korporacyjnych; oraz
- m) właściwe szkolenia z zakresu ochrony danych dla personelu mającego stały lub regularny dostęp do danych osobowych (...).

2a. Europejska Rada Ochrony Danych doradza Komisji w sprawie formatu i procedur wymiany informacji między administratorami, podmiotami przetwarzającymi oraz organami nadzorczymi do celów wiążących reguł korporacyjnych.

3. (...)



4. Komisja może określić format i procedury wymiany informacji (...) między administratorami, podmiotami przetwarzającymi i organami nadzorczymi do celów wiążących reguł korporacyjnych w rozumieniu niniejszego artykułu. Akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 87 ust. 2.

#### *Artykuł 44*

#### ***Odstępstwa w szczególnych sytuacjach***

1. W razie braku decyzji stwierdzającej odpowiedni poziom ochrony określonej w art. 41 ust. 3 lub braku odpowiednich gwarancji określonych w art. 42, w tym wiążących reguł korporacyjnych (...), przekazanie danych osobowych lub kategoria takiego przekazania do (...) państwa trzeciego lub organizacji międzynarodowej mogą nastąpić wyłącznie pod warunkiem, że:
- a) podmiot danych, poinformowany, że ze względu na brak decyzji stwierdzającej odpowiedni poziom ochrony oraz na brak odpowiednich gwarancji takie przekazania mogą wiązać się z zagrożeniami dla podmiotu danych, wyrażnie udzielił zgody na proponowane przekazanie; lub
  - b) przekazanie jest niezbędne do wykonania umowy między podmiotem danych a administratorem lub do wprowadzenia w życie środków przedumownych podejmowanych na wniosek podmiotu danych; lub
  - c) przekazanie jest niezbędne do zawarcia lub wykonania umowy zawartej w interesie podmiotu danych między administratorem a inną osobą fizyczną lub prawną; lub
  - d) przekazanie jest niezbędne ze względu na ważne przesłanki interesu publicznego; lub
  - e) przekazanie jest niezbędne do ustalenia, realizacji lub ochrony roszczeń prawnych; lub
  - f) przekazanie jest niezbędne do ochrony żywotnych interesów podmiotu danych lub innych osób, jeżeli podmiot danych jest fizycznie lub prawnie niezdolny do udzielenia zgody; lub
  - g) przekazanie następuje z rejestru, który zgodnie z prawem Unii lub prawem państwa członkowskiego ma służyć za źródło informacji dla ogółu obywateli i który pozostaje do wglądu dla ogółu obywateli lub dla każdej osoby mogącej wykazać uzasadniony interes – ale wyłącznie w zakresie, w jakim w danym przypadku spełnione zostały warunki takiego wglądu określone prawem Unii lub prawem państwa członkowskiego; lub

- h) przekazanie, które nie ma dużego zakresu ani nie jest częste, jest niezbędne ze względu na uzasadnione interesy realizowane przez administratora – wobec których charakteru nadrzędnego nie mają interesy lub prawa i wolności podmiotu danych – a administrator (...) ocenił wszelkie okoliczności związane z operacją przekazania danych lub operacjami przekazania danych i (...) na podstawie tej oceny przewidział odpowiednie gwarancje ochrony danych osobowych.
2. Przekazanie na mocy ust. 1 lit. g) nie obejmuje całości danych osobowych ani całych kategorii danych osobowych zawartych w rejestrze. Jeżeli rejestr służy do wglądu osobom mającym uzasadniony interes, przekazanie następuje wyłącznie wtedy, gdy osoby te o nie wystąpiły lub gdy mają one być odbiorcami.
3. (...)
4. Ustęp 1 lit. a), b), c) i h) nie ma zastosowania do działalności prowadzonej przez organy publiczne w ramach wykonywania przysługujących im uprawnień publicznych.
5. Interes publiczny, o którym mowa w ust. 1 lit. d), musi być uznany prawem Unii lub prawem krajowym państwa członkowskiego, któremu podlega administrator. (...)
- 5a. W razie braku decyzji stwierdzającej odpowiedni poziom ochrony prawo Unii lub prawo państwa członkowskiego mogą ze względu na ważne przesłanki interesu publicznego wyraźnie nakładać ograniczenia na przekazywanie konkretnych kategorii danych osobowych do państwa trzeciego lub organizacji międzynarodowej. Państwa członkowskie powiadamiają Komisję o takich przepisach.
6. Administrator lub podmiot przetwarzający dokumentują ocenę oraz odpowiednie gwarancje (...), o których mowa w ust. 1 lit. h), w rejestrach, o których mowa w art. 28 (...).
- 6a. (...)
7. (...)

## ***Artykuł 45***

### *Międzynarodowa współpraca na rzecz ochrony danych osobowych*

1. Komisja i organy nadzorcze podejmują wobec państw trzecich i organizacji międzynarodowych odpowiednie działania na rzecz:
  - a) wypracowania mechanizmów współpracy międzynarodowej ułatwiających *skuteczne* egzekwowanie przepisów o ochronie danych osobowych;
  - b) zapewnienia wzajemnej pomocy międzynarodowej w egzekwowaniu przepisów o ochronie danych osobowych, w tym poprzez (...) przekazywanie skarg, pomoc dochodzeniową oraz wymianę informacji – z zastrzeżeniem odpowiednich gwarancji ochrony danych osobowych i innych podstawowych praw i wolności;
  - c) włączenia stosownych zainteresowanych stron w dyskusję i działalność mające na celu propagowanie międzynarodowej współpracy w dziedzinie egzekwowania przepisów o ochronie danych osobowych;
  - d) propagowania wymiany i dokumentowania przepisów i praktyk w dziedzinie ochrony danych osobowych.
2. (...)

## ROZDZIAŁ VI

### NIEZALEŻNE ORGANY NADZORCZE

#### SEKCJA 1

#### NIEZALEŻNY STATUS

##### *Artykuł 46*

##### ***Organ nadzorczy***

1. Każde państwo członkowskie stanowi, że za monitorowanie stosowania niniejszego rozporządzenia odpowiada co najmniej jeden niezależny organ publiczny.
- 1a. Każdy organ nadzorczy przyczynia się do spójnego stosowania niniejszego rozporządzenia w całej Unii (...). W tym celu organy nadzorcze współpracują ze sobą i z Komisją zgodnie z rozdziałem VII.
2. Jeżeli w państwie członkowskim ustanowiono więcej niż jeden organ nadzorczy, państwo to wyznacza organ nadzorczy, który reprezentuje te organy w Europejskiej Radzie Ochrony Danych, oraz ustala mechanizm zapewniający przestrzeganie przez pozostałe organy przepisów dotyczących mechanizmu spójności, o którym mowa w art. 57.
3. Najpóźniej w terminie określonym w art. 91 ust. 2 każde państwo członkowskie zawiadamia Komisję o przepisach przyjętych na mocy niniejszego rozdziału, a następnie niezwłocznie o każdej kolejnej zmianie mającej na nie wpływ.

##### *Artykuł 47*

##### ***Niezależność***

1. Każdy organ nadzorczy działa w sposób w pełni niezależny podczas wykonywania obowiązków i korzystania z uprawnień powierzonych mu zgodnie z niniejszym rozporządzeniem.

2. Członek lub członkowie każdego organu nadzorczego podczas wykonywania swoich obowiązków i korzystania ze swoich uprawnień zgodnie z niniejszym rozporządzeniem pozostają wolni od bezpośrednich i pośrednich wpływów zewnętrznych, nie zwracają się do nikogo o instrukcje ani ich od nikogo nie przyjmują.
3. (...)
4. (...)
5. Każde państwo członkowskie dopilnowuje, by każdy organ nadzorczy został wyposażony w (...) zasoby kadrowe, techniczne i finansowe, pomieszczenia i infrastrukturę niezbędne do skutecznego wykonywania swoich obowiązków i korzystania ze swoich uprawnień, w tym w kontekście wzajemnej pomocy, współpracy i uczestnictwa w pracach Europejskiej Rady Ochrony Danych.
6. Każde państwo członkowskie dopilnowuje, by każdy organ nadzorczy miał własny personel, (...) działający pod kierownictwem członka lub członków organu nadzorczego.
7. Państwa członkowskie dopilnowują, by każdy organ nadzorczy podlegał kontroli finansowej, nienaruszającej jego niezależności. Państwa członkowskie dopilnowują, by każdy organ nadzorczy dysponował odrębnym, publicznym budżetem rocznym, który może być częścią ogólnego budżetu państwowego lub krajowego.

#### *Artykuł 48*

#### ***Ogólne warunki dotyczące członków organu nadzorczego***

1. Państwa członkowskie stanowią, że członek lub członkowie każdego z organów nadzorczych muszą zostać mianowani (...) przez parlament, rząd lub głowę danego państwa członkowskiego lub przez niezależny organ, któremu prawo państwa członkowskiego powierzyło zadanie mianowania drogą przejrzystej procedury.

2. Członek lub członkowie posiadają kwalifikacje, doświadczenie i umiejętności potrzebne do wykonywania swoich obowiązków i korzystania ze swoich uprawnień (...).
3. W razie upływu kadencji, rezygnacji lub przymusowego pozbawienia funkcji członek organu przestaje pełnić swoje obowiązki zgodnie z prawem danego państwa członkowskiego.
4. (...)
5. (...).

#### *Artykuł 49*

#### ***Zasady ustanawiania organu nadzorczego***

1. Każde państwo członkowskie stanowi prawem:
  - a) ustanowienie (...) każdego z organów nadzorczych;
  - b) kwalifikacje (...) wymagane do wykonywania obowiązków członka organu nadzorczego;
  - c) zasady i procedury mianowania członka lub członków każdego z organów nadzorczych (...);
  - d) okres kadencji członka lub członków każdego z organów nadzorczych, nie krótszy (...) niż cztery lata, z wyjątkiem pierwszej kadencji po wejściu w życie niniejszego rozporządzenia, która częściowo może trwać krócej, jeżeli jest to niezbędne, aby chronić niezależność organu nadzorczego za pomocą procedury stopniowej wymiany członków;
  - e) czy członek lub członkowie każdego z organów nadzorczych mogą zostać mianowani ponownie, a jeżeli tak – na ile kadencji;
  - f) (...) warunki regulujące zobowiązania członka lub członków oraz personelu każdego z organów nadzorczych, zakaz podejmowania w trakcie kadencji lub po jej zakończeniu działań i zajęć sprzecznych z tymi zobowiązaniami, a także przepisy regulujące ustanie stosunku zatrudnienia;
  - g) (...).

2. Członek lub członkowie oraz personel każdego z organów nadzorczych podlegają zgodnie z prawem Unii lub prawem państwa członkowskiego obowiązkowi dochowania tajemnicy służbowej – *zarówno w trakcie kadencji, jak i po jej zakończeniu* – w odniesieniu do wszelkich poufnych informacji, które uzyskali w toku wykonywania obowiązków (...) lub korzystania ze swoich uprawnień.

*Artykuł 50*

***Tajemnica służbowa***

(...)

**SEKCJA 2**  
**WŁAŚCIWOŚĆ, ZADANIA I UPRAWNIENIA**

*Artykuł 51*

***Właściwość***

1. Każdy organ nadzorczy jest właściwy do wykonywania zadań i korzystania z uprawnień powierzonych mu zgodnie z niniejszym rozporządzeniem na terytorium własnego państwa członkowskiego. (...)
2. Jeżeli przetwarzania dokonują organy publiczne lub podmioty prywatne działające na podstawie art. 6 ust. 1 lit. c) lub e), organem właściwym jest organ nadzorczy danego państwa członkowskiego. W takich przypadkach nie ma zastosowania art. 51a.
3. Organy nadzorcze nie są właściwe do nadzorowania operacji przetwarzania dokonywanych przez sądy w toku sprawowania przez nie wymiaru sprawiedliwości. (...).

*Artykuł 51a*

***Właściwość głównego organu nadzorczego***

1. Bez uszczerbku dla art. 51 organ nadzorczy głównej siedziby lub pojedynczej siedziby administratora lub podmiotu przetwarzającego jest właściwy do podejmowania działań jako główny organ nadzorczy – zgodnie z procedurą przewidzianą w art. 54a – na potrzeby przetwarzania transnarodowego prowadzonego przez tego administratora lub ten podmiot przetwarzający.
2. (...)
- 2a. W drodze odstępstwa od ust. 1 każdy organ nadzorczy jest właściwy do rozpatrzenia skargi, którą do niego wniesiono, lub zajęcia się ewentualnym naruszeniem niniejszego rozporządzenia, jeżeli sprawa dotyczy wyłącznie siedziby w jego państwie członkowskim lub znacznie wpływa na podmioty danych wyłącznie w jego państwie członkowskim.



- 2b. W przypadkach, o których mowa w ust. 2a, organ nadzorczy niezwłocznie informuje o danej sprawie główny organ nadzorczy. W terminie trzech tygodni od otrzymania informacji główny organ nadzorczy postanawia, czy zajmie się daną sprawą zgodnie z procedurą przewidzianą w art. 54a, uwzględniając, czy w państwie członkowskim, którego organ nadzorczy przekazał mu informacje, znajduje się siedziba administratora lub podmiotu przetwarzającego.
- 2c. Jeżeli główny organ nadzorczy postanowi zająć się daną sprawą, zastosowanie ma procedura przewidziana w art. 54a. Organ nadzorczy, który przekazał informacje głównemu organowi nadzorczemu, może przedłożyć temu organowi nadzorczemu projekt decyzji. Główny organ nadzorczy w jak największym stopniu uwzględnia ten projekt, przygotowując projekt decyzji, o którym mowa w art. 54a ust. 2.
- 2d. Jeżeli główny organ nadzorczy postanowi nie zajmować się daną sprawą, sprawą zajmuje się – zgodnie z art. 55 i 56 – organ nadzorczy, który przekazał informacje głównemu organowi nadzorczemu.
3. Główny organ nadzorczy jest jedynym partnerem kontaktowym administratora lub podmiotu przetwarzającego w sprawach dotyczących prowadzonego przez nich przetwarzania transnarodowego.
4. (...).

*Artykuł 51b*

**Określanie organu nadzorczego właściwego względem głównej siedziby**

(...)

*Artykuł 51c*

**Rejestr kompleksowej obsługi**

(...)

## Artykuł 52

### Zadania

1. Bez uszczerbku dla innych zadań określonych na mocy niniejszego rozporządzenia każdy organ nadzorczy na swoim terytorium:
  - a) monitoruje i egzekwuje stosowanie niniejszego rozporządzenia;
  - aa) upowszechnia w społeczeństwie wiedzę o zagrożeniach, przepisach, gwarancjach i prawach związanych z przetwarzaniem danych osobowych oraz rozumienie tych zjawisk. Szczególną uwagę poświęca działaniom skierowanym do dzieci;
  - ab) doradza, zgodnie z prawem krajowym, parlamentowi narodowemu, rządowi oraz innym instytucjom i organom w sprawie ustawodawczych i administracyjnych środków dotyczących ochrony praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych;
  - ac) upowszechnia wśród administratorów i podmiotów przetwarzających wiedzę o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia;
  - ad) zapewnia podmiotom danych na ich wniosek informacje o możliwości korzystania z praw przysługujących im na mocy niniejszego rozporządzenia, a w stosownym przypadku współpracuje w tym celu z organami nadzorczymi innych państw członkowskich;
  - b) rozpatruje skargi wniesione przez podmiot danych lub organ, organizację lub stowarzyszenie reprezentujące podmiot danych zgodnie z art. 73, w odpowiednim zakresie prowadzi dochodzenia w przedmiocie tych skarg i w racjonalnym terminie informuje podmiot danych lub organ, organizację lub stowarzyszenie o postępach i wynikach tego dochodzenia, w szczególności jeżeli niezbędne są dalsze dochodzenie lub koordynacja działań z innym organem nadzorczym;
  - c) współpracuje z innymi organami nadzorczymi, w tym dzieli się informacjami, oraz świadczy im wzajemną pomoc w celu zapewnienia spójnego stosowania i egzekwowania niniejszego rozporządzenia;
  - d) prowadzi dochodzenia w sprawie stosowania niniejszego rozporządzenia, w tym na podstawie informacji otrzymanych od innego organu nadzorczego lub innego organu publicznego;
  - e) monitoruje zmiany w stosownych dziedzinach, o ile mają one wpływ na ochronę danych osobowych, w szczególności rozwój technologii informacyjno-komunikacyjnych i praktyk handlowych;

- f) przyjmuje standardowe klauzule umowne, o których mowa w art. 26 ust. 2c;
- fa) ustanawia i prowadzi wykaz związany z wymogiem dokonania oceny skutków pod kątem ochrony danych na mocy art. 33 ust. 2a;
- g) udziela porad, o których mowa w art. 34 ust. 3, co do operacji przetwarzania;
- ga) zachęca do sporządzania kodeksów postępowania na mocy art. 38, wydaje opinie na ich temat oraz zatwierdza te kodeksy, w których znajdują się odpowiednie gwarancje, na mocy art. 38 ust. 2;
- gb) propaguje ustanawianie mechanizmów certyfikacji w dziedzinie ochrony danych oraz pieczęci i oznaczeń z tej dziedziny, a także zatwierdza kryteria certyfikacji zgodnie z art. 39 ust. 2a;
- gc) w stosownym przypadku zgodnie z art. 39 ust. 4 okresowo weryfikuje udzielone certyfikacje;
- h) opracowuje i publikuje kryteria akredytacji podmiotu monitorującego kodeksy postępowania na mocy art. 38a oraz podmiotu certyfikującego na mocy art. 39a;
- ha) akredytuje podmiot monitorujący kodeksy postępowania na mocy art. 38a oraz podmiot certyfikujący na mocy art. 39a;
- hb) zezwała na klauzule umowne, o których mowa w art. 42 ust. 2a lit. a);
- i) zatwierdza wiążące reguły korporacyjne na mocy art. 43;
- j) wnosi wkład w działalność Europejskiej Rady Ochrony Danych;
- k) wypełnia inne zadania związane z ochroną danych osobowych.

2. (...)

3. (...).

4. Każdy organ nadzorczy ułatwia wnoszenie skarg, o których mowa w ust. 1 lit. b), za pomocą takich środków, jak udostępnienie formularza skargi, który można wypełnić także elektronicznie, przy czym nie wyklucza innych sposobów komunikacji.

5. Każdy organ nadzorczy wykonuje zadania na rzecz podmiotów danych i inspektora ochrony danych, jeżeli istnieje, w sposób wolny od opłat.

6. Jeżeli wnioski są ewidentnie nieuzasadnione lub nadmierne, zwłaszcza ze względu na swój ustawiczny się charakter, organ nadzorczy może odmówić podjęcia działań względem wniosku. Obowiązek wykazania, że wniosek ma ewidentnie nieuzasadniony lub nadmierny charakter, spoczywa na organie nadzorczym.

### *Artykuł 53*

#### ***Uprawnienia***

1. Każde państwo członkowskie stanowi prawem, że jego organ nadzorczy posiada co najmniej następujące uprawnienia dochodzeniowe:
  - a) nakazuje administratorowi i podmiotowi przetwarzającemu, a w stosownym przypadku przedstawicielowi administratora dostarczyć wszelkich informacji potrzebnych mu do wykonania zadań;
  - aa) prowadzi dochodzenia w formie audytu w dziedzinie ochrony danych;
  - ab) weryfikuje udzielone certyfikacje na mocy art. 39 ust. 4;
  - b) (...)
  - c) (...)
  - d) zawiadamia administratora lub podmiot przetwarzający o domniemanym naruszeniu niniejszego rozporządzenia;
  - da) uzyskuje od administratora i podmiotu przetwarzającego dostęp do wszelkich danych osobowych i wszelkich informacji niezbędnych mu do wykonania zadań;
  - db) uzyskuje dostęp do wszelkich pomieszczeń administratora i podmiotu przetwarzającego, w tym do wszelkiego sprzętu i wszelkich środków służących do przetwarzania danych, zgodnie z prawem Unii lub prawem procesowym państwa członkowskiego.
- 1a. (...).
- 1b. Każde państwo członkowskie stanowi prawem, że jego organ nadzorczy posiada następujące uprawnienia korekcyjne:
  - a) wydaje ostrzeżenia skierowane do administratora lub podmiotu przetwarzającego, że planowane operacje przetwarzania mogą skutkować naruszeniem przepisów niniejszego rozporządzenia;

- b) udziela upomnień administratorowi lub podmiotowi przetwarzającemu, jeżeli operacje przetwarzania poskutkowały naruszeniem przepisów niniejszego rozporządzenia;
- c) (...);
- ca) nakazuje administratorowi lub podmiotowi przetwarzającemu wykonać wniosek podmiotu danych o możliwość skorzystania z praw przysługujących mu na mocy niniejszego rozporządzenia;
- d) nakazuje administratorowi lub podmiotowi przetwarzającemu dostosować operacje przetwarzania do przepisów niniejszego rozporządzenia – a w stosownym przypadku wskazuje konkretny sposób i konkretny termin – zwłaszcza nakazując poprawić, ograniczyć lub usunąć dane na mocy art. 16, 17 i 17a oraz powiadomić o tym odbiorców, którym ujawniono dane, na mocy art. 17 ust. 2a i art. 17b;
- e) wprowadza czasowe lub ostateczne ograniczenia przetwarzania (...);
- f) nakazuje zawiesić przepływ danych do odbiorcy w państwie trzecim lub do organizacji międzynarodowej;
- g) oprócz lub zamiast środków, o których mowa w niniejszym ustępie, nakłada grzywnę administracyjną na mocy art. 79 i 79a, zależnie od okoliczności konkretnej sprawy.
- 1c. Każde państwo członkowskie stanowi prawem, że jego organ nadzorczy posiada następujące uprawnienia autoryzacyjne i doradcze:
  - a) udziela porad administratorowi zgodnie z procedurą uprzednich konsultacji, o której mowa w art. 34;
  - aa) z własnej inicjatywy lub na wniosek wydaje opinie przeznaczone dla parlamentu narodowego, rządu państwa członkowskiego lub – zgodnie z prawem krajowym – innych instytucji i organów oraz opinii publicznej we wszelkich sprawach związanych z ochroną danych osobowych;
  - ab) zezwała na przetwarzanie zgodnie z art. 34 ust. 7a, jeżeli prawo państwa członkowskiego wymaga takiego uprzedniego zezwolenia;
  - ac) zaopiniowuje i zatwierdza projekty kodeksów postępowania zgodnie z art. 38 ust. 2;
  - ad) akredytuje podmioty certyfikujące na warunkach art. 39a;
  - ae) udziela certyfikacji i zatwierdza kryteria certyfikacji zgodnie z art. 39 ust. 2a;
    - (b) przyjmuje standardowe klauzule ochrony danych, o których mowa w art. 42 ust. 2 lit. c);
    - (c) zezwała na klauzule umowne, o których mowa w art. 42 ust. 2a lit. a);

ca) zezwała na porozumienia administracyjne, o których mowa w art. 42 ust. 2a lit. d);

d) zatwierdza wiążące reguły korporacyjne na mocy art. 43.

2. Korzystanie z uprawnień powierzonych organowi nadzorczemu na mocy niniejszego artykułu podlega odpowiednim gwarancjom – w tym prawu do skutecznego środka ochrony prawnej i sprawiedliwości proceduralnej – określonym w prawie Unii i prawie państw członkowskich zgodnie z Kartą praw podstawowych Unii Europejskiej.

3. Każde państwo członkowskie stanowi prawem, że jego organ nadzorczy może zgłosić organom wymiaru sprawiedliwości naruszenie niniejszego rozporządzenia oraz (...) w stosownym przypadku wszcząć lub w inny sposób uczestniczyć w postępowaniu sądowym, po to by wyegzekwować przepisy niniejszego rozporządzenia.

4. (...)

5. (...)

#### *Artykuł 54*

#### ***Sprawozdanie z działalności***

Każdy organ nadzorczy sporządza roczne sprawozdanie ze swojej działalności. Sprawozdanie jest przekazywane parlamentowi narodowemu, rządowi i innym organom wskazanym prawem krajowym. Sprawozdanie udostępniane jest opinii publicznej, Komisji Europejskiej oraz Europejskiej Radzie Ochrony Danych.

**ROZDZIAŁ VII**  
**WSPÓŁPRACA I SPÓJNOŚĆ**  
**SEKCJA 1**  
**WSPÓŁPRACA**

*Artykuł 54a*

**Współpraca między głównym organem nadzorczym a innymi zainteresowanymi organami nadzorczymi**

1. Główny organ nadzorczy (...) współpracuje z innymi zainteresowanymi organami nadzorczymi zgodnie z niniejszym artykułem w celu osiągnięcia porozumienia (...). Główny organ nadzorczy i zainteresowane organy nadzorcze wymieniają się wszelkimi istotnymi informacjami.
  - 1a. Główny organ nadzorczy może w dowolnym momencie zwrócić się do innych zainteresowanych organów nadzorczych o wzajemną pomoc zgodnie z art. 55 i może prowadzić wspólne operacje zgodnie z art. 56, zwłaszcza w celu przeprowadzenia dochodzenia lub monitorowania wdrażania środka względem administratora lub podmiotu przetwarzającego mającego siedzibę w innym państwie członkowskim.
2. Główny organ nadzorczy niezwłocznie przekazuje innym zainteresowanym organom nadzorczym istotne informacje o danej sprawie. Niezwłocznie przedkłada innym zainteresowanym organom nadzorczym projekt decyzji w celu uzyskania ich opinii i należytego uwzględnienia ich uwag.
3. Jeżeli w terminie czterech tygodni od otrzymania wniosku o opinię zgodnie z ust. 2 którykolwiek z innych zainteresowanych organów nadzorczych zgłosi istotny i zasadny sprzeciw wobec projektu decyzji, główny organ nadzorczy – jeżeli nie przychyli się do sprzeciwu lub sądzi, że sprzeciw nie jest istotny i zasadny – poddaje sprawę pod mechanizm spójności, o którym mowa w art. 57. (...)

3a. Jeżeli główny organ nadzorczy zamierza przychylić się do zgłoszonego sprzeciwu, przedkłada innym zainteresowanym organom nadzorczym zmieniony projekt decyzji w celu uzyskania ich opinii. Zmieniony projekt decyzji jest poddawany procedurze, o której mowa w ust. 3, w terminie dwóch tygodni.

4. Jeżeli w terminie, o którym mowa w ust. 3 i 3a, żaden inny zainteresowany organ nadzorczy nie zgłosi sprzeciwu wobec projektu decyzji przedłożonego przez główny organ nadzorczy, uznaje się, że główny organ nadzorczy i zainteresowane organy nadzorcze porozumiały się w sprawie projektu decyzji i są nią związane.

4a. Główny organ nadzorczy przyjmuje decyzję i notyfikuje ją odpowiednio głównej siedzibie lub pojedynczej siedzibie administratora lub podmiotu przetwarzającego oraz informuje o przedmiotowej decyzji inne zainteresowane organy nadzorcze i Europejską Radę Ochrony Danych, dołączając streszczenie stanu faktycznego i powodów decyzji. Organ nadzorczy, do którego wniesiono skargę, informuje skarżącego o decyzji.

4b. W drodze odstępstwa od ust. 4a, jeżeli skarga zostaje oddalona lub odrzucona, organ nadzorczy, do którego wniesiono skargę, przyjmuje decyzję i notyfikuje ją skarżącemu oraz informuje o niej administratora.

4bb. Jeżeli główny organ nadzorczy i zainteresowane organy nadzorcze porozumiały się co do oddalenia lub odrzucenia części skargi oraz co do podjęcia działań względem innych części tej skargi, dla każdej z tych części przyjmuje się odrębną decyzję. Główny organ nadzorczy przyjmuje decyzję w sprawie części dotyczącej działań względem administratora i notyfikuje ją głównej siedzibie lub pojedynczej siedzibie administratora lub podmiotu przetwarzającego na terytorium swojego państwa członkowskiego i informuje o niej skarżącego, a organ nadzorczy skarżącego przyjmuje decyzję w sprawie części dotyczącej oddalenia lub odrzucenia tej skargi, notyfikuje ją skarżącemu oraz informuje o niej administratora lub podmiot przetwarzający.



4c. Po tym jak administratorowi lub podmiotowi przetwarzającemu notyfikowana zostanie decyzja głównego organu nadzorczego zgodnie z ust. 4a i 4bb, przedsiębiorą oni niezbędne środki, by zastosować się do tej decyzji, jeżeli chodzi o czynności przetwarzania w ramach wszystkich swoich siedzib w Unii. Administrator lub podmiot przetwarzający zawiadamiają główny organ nadzorczy o środkach przedsięwziętych w celu zastosowania się do decyzji, ten zaś informuje o nich inne zainteresowane organy nadzorcze.

4d. Jeżeli w wyjątkowych okolicznościach zainteresowany organ nadzorczy ma powody sądzić, że istnieje pilna potrzeba podjęcia działań w celu ochrony interesów podmiotów danych, zastosowanie ma tryb pilny, o którym mowa w art. 61.

5. Główny organ nadzorczy i inne zainteresowane organy nadzorcze dostarczają sobie nawzajem informacji wymaganych na mocy niniejszego artykułu (...) drogą elektroniczną w standardowym formacie.

#### *Artykuł 54b*

#### ***Współpraca między głównym organem nadzorczym a innymi zainteresowanymi organami nadzorczymi w poszczególnych przypadkach nieprzestrzegania rozporządzenia***

(...)

## Artykuł 55

### ***Wzajemna pomoc***

1. Organy nadzorcze przekazują sobie stosowne informacje i świadczą sobie wzajemną pomoc w celu spójnego wdrażania i stosowania niniejszego rozporządzenia oraz wprowadzają środki na rzecz skutecznej wzajemnej współpracy. Wzajemna pomoc obejmuje w szczególności wnioski o udzielenie informacji oraz środki nadzorcze, takie jak wnioski o udzielenie uprzednich zezwoleń i przeprowadzenie uprzednich konsultacji oraz o przeprowadzenie kontroli i dochodzeń. (...)
2. Każdy organ nadzorczy przedsięwzię wszelkie odpowiednie środki, by odpowiedzi na wniosek innego organu nadzorczego udzielić bez zbędnej zwłoki i nie później niż w terminie jednego miesiąca od otrzymania wniosku. Środki takie mogą obejmować w szczególności przekazanie odpowiednich informacji o przebiegu dochodzenia (...).
3. Wniosek o pomoc zawiera wszelkie niezbędne informacje, w tym cel i uzasadnienie wniosku. Uzyskane informacje są wykorzystywane wyłącznie do celu, w którym o nie wystąpiono.
4. Organ nadzorczy będący adresatem wniosku o pomoc nie może odmówić jego wykonania, chyba że:
  - a) nie jest organem właściwym w przedmiocie wniosku lub środków, o których wykonanie wystąpiono; lub
  - b) wykonanie wniosku byłoby niezgodne z przepisami niniejszego rozporządzenia lub z prawem Unii lub prawem państwa członkowskiego, któremu podlega organ nadzorczy będący adresatem wniosku.
5. Organ nadzorczy będący adresatem wniosku informuje organ nadzorczy, od którego wniosek pochodzi, o rezultatach lub w stosownym przypadku o postępach lub środkach przedsięwziętych w celu udzielenia odpowiedzi na ten wniosek. W razie odmowy na mocy ust. 4 wyjaśnia jej powody.

6. Informacji żądanych przez inne organy nadzorcze organ nadzorczy zasadniczo dostarcza drogą elektroniczną w standardowym formacie.
7. Działania podejmowane w wyniku wniosku o wzajemną pomoc są wolne od opłat. Organy nadzorcze mogą uzgodnić z innymi organami nadzorczymi zasady rekompensowania przez inne organy nadzorcze konkretnych wydatków poniesionych w wyniku świadczenia wzajemnej pomocy w wyjątkowych okolicznościach.
8. Jeżeli organ nadzorczy nie dostarczy informacji, o których mowa w ust. 5, w terminie jednego miesiąca od otrzymania wniosku innego organu nadzorczego, organ nadzorczy, od którego wniosek pochodzi, może przyjąć tymczasowy środek na terytorium swojego państwa członkowskiego zgodnie z art. 51 ust. 1 i przedkłada sprawę Europejskiej Radzie Ochrony Danych (...) zgodnie z mechanizmem spójności, o którym mowa w art. 57.
9. Organ nadzorczy określa termin obowiązywania takiego środka tymczasowego, przy czym nie jest on dłuższy niż trzy miesiące. Organ nadzorczy niezwłocznie informuje o tym środku i o powodach jego przyjęcia Europejską Radę Ochrony Danych (...) zgodnie z mechanizmem spójności, o którym mowa w art. 57.
10. Komisja może określić formułę i procedurę wzajemnej pomocy, o której mowa w niniejszym artykule, oraz zasady wymiany informacji drogą elektroniczną między organami nadzorczymi oraz między organami nadzorczymi a Europejską Radą Ochrony Danych, w szczególności standardowy format, o którym mowa w ust. 6. Akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 87 ust. 2.

***Wspólne operacje organów nadzorczych***

1. Organy nadzorcze mogą w stosownym przypadku prowadzić wspólne operacje, w tym wspólne dochodzenia i wspólne środki egzekucyjne, w których uczestniczą członkowie lub personel organów nadzorczych innych państw członkowskich.
2. Jeżeli administrator lub podmiot przetwarzający mają siedziby w kilku państwach członkowskich lub jeżeli operacje przetwarzania mogą znacznie wpłynąć na istotną liczbę podmiotów danych w więcej niż jednym państwie członkowskim, organ nadzorczy każdego z tych państw członkowskich ma prawo uczestniczyć w stosownym przypadku we wspólnych operacjach. Właściwy organ nadzorczy zaprasza organ nadzorczy każdego z tych państw członkowskich do uczestnictwa w danych wspólnych operacjach i niezwłocznie odpowiada na wniosek organu nadzorczego o możliwość uczestnictwa.
3. Organ nadzorczy może zgodnie z prawem własnego państwa członkowskiego i za zgodą wysyłającego organu nadzorczego przyznać uprawnienia, w tym uprawnienia dochodzeniowe, członkom lub personelowi wysyłającego organu nadzorczego uczestniczącym we wspólnych operacjach lub – jeżeli zezwala na to prawo państwa członkowskiego przyjmującego organu nadzorczego – pozwolić członkom lub personelowi wysyłającego organu nadzorczego korzystać z ich własnych uprawnień dochodzeniowych zgodnie z prawem państwa członkowskiego wysyłającego organu nadzorczego. Z takich uprawnień dochodzeniowych można korzystać wyłącznie pod kierownictwem i w obecności członków lub personelu przyjmującego organu nadzorczego. Członkowie lub personel wysyłającego organu nadzorczego podlegają prawu krajowemu przyjmującego organu nadzorczego. (...)

3a. Jeżeli zgodnie z ust. 1 personel wysyłającego organu nadzorczego działa w innym państwie członkowskim, państwo członkowskie przyjmującego organu nadzorczego odpowiada za wszelkie szkody wyrządzone przez ten personel w trakcie operacji, zgodnie z prawem państwa członkowskiego, na którego terytorium ten personel działa.

3b. Państwo członkowskie, na którego terytorium została wyrządzona szkoda, naprawia taką szkodę zgodnie z warunkami mającymi zastosowanie do szkód wyrządzonych przez jego własny personel. Państwo członkowskie wysyłającego organu nadzorczego, którego personel wyrządził szkodę wobec osoby na terytorium innego państwa członkowskiego, zwraca temu państwu całość kwot, które zapłaciło ono osobom uprawnionym w jego imieniu.

3c. Bez uszczerbku dla możliwości dochodzenia swoich praw wobec osób trzecich i z wyłączeniem ust. 3b każde państwo członkowskie powstrzymuje się w przypadku określonym w ust. 1 od żądania zwrotu za szkody, których doznało od innego państwa członkowskiego.

4. (...)

5. Jeżeli planowana jest wspólna operacja, a organ nadzorczy nie wywiąże się w terminie jednego miesiąca z obowiązku ustanowionego w ust. 2 zdanie drugie, inne organy nadzorcze moga przyjąć środek tymczasowy na terytorium swojego państwa członkowskiego zgodnie z art. 51 ust. 1.

6. Organ nadzorczy określa termin obowiązywania środka tymczasowego, o którym mowa w ust. 5, przy czym nie jest on dłuższy niż trzy miesiące. Organ nadzorczy niezwłocznie informuje o tych środku i o powodach jego przyjęcia Europejską Radę Ochrony Danych (...) zgodnie z mechanizmem spójności, o którym mowa w art. 57.

## SEKCJA 2

### SPÓJNOŚĆ

#### *Artykuł 57*

#### ***Mechanizm spójności***

1. Do celów określonych w art. 46 ust. 1a organy nadzorcze współpracują ze sobą, stosując mechanizm spójności określony w niniejszej sekcji.
2. Europejska Rada Ochrony Danych wydaje opinię, ilekroć właściwy organ nadzorczy zamierza przyjąć któryś ze środków wymienionych poniżej. W tym celu właściwy organ nadzorczy zgłasza Europejskiej Radzie Ochrony Danych projekt decyzji, jeżeli:
  - a) (...);
  - b) (...);
  - c) służy ona przyjęciu na mocy art. 33 ust. 2a wykazu operacji przetwarzania podlegających wymogowi dokonania oceny skutków pod kątem ochrony danych; lub
  - ca) dotyczy ona kwestii podlegającej art. 38 ust. 2b, tzn. czy projekt kodeksu postępowania, zmiana kodeksu lub jego poszerzenie są zgodne z niniejszym rozporządzeniem; lub
  - cb) służy zatwierdzeniu kryteriów akredytacji podmiotu na mocy art. 38a ust. 3 lub podmiotu certyfikującego na mocy (...) art. 39a ust. 3;

- d) służy ona określeniu standardowych klauzul ochrony danych, o których mowa w art. 42 ust. 2 lit. c);

lub

- e) służy ona zezwoleniu na klauzule umowne, o których mowa w art. 42 ust. 2 lit. d); lub

- f) służy ona zatwierdzeniu wiążących reguł korporacyjnych w rozumieniu art. 43.

3. Europejska Rada Ochrony Danych przyjmuje wiążącą decyzję w następujących przypadkach:

- a) Jeżeli w przypadku, o którym mowa w art. 54a ust. 3, zainteresowany organ nadzorczy zgłosił istotny i zasadny sprzeciw wobec projektu decyzji głównego organu nadzorczego, a główny organ nadzorczy odrzucił sprzeciw jako nieistotny lub niezasadny. Wiążąca decyzja dotyczy wszystkich spraw, które są przedmiotem istotnego i zasadnego sprzeciwu, w szczególności tego, czy doszło do naruszenia niniejszego rozporządzenia;
- b) Jeżeli panują sprzeczne opinie co to tego, który z zainteresowanych organów nadzorczych jest właściwy względem głównej siedziby;
- c) (...)
- d) Jeżeli właściwy organ nadzorczy nie wystąpił o opinię do Europejskiej Rady Ochrony Danych w przypadkach, o których mowa w ust. 2 niniejszego artykułu, lub nie zastosował się do opinii Europejskiej Ochrony Danych wydanej w myśl art. 58. W takim przypadku każdy zainteresowany organ nadzorczy lub Komisja mogą zgłosić sprawę Europejskiej Radzie Ochrony Danych.

4. Każdy organ nadzorczy, przewodniczący Europejskiej Rady Ochrony Danych lub Komisja mogą wystąpić o to, by Europejska Rada Ochrony Danych przeanalizowała w celu wydania opinii dowolną sprawę mającą charakter ogólny lub wywołującą skutki w więcej niż jednym państwie członkowskim, zwłaszcza jeżeli właściwy organ nadzorczy nie wywiązuje się z obowiązków wzajemnej pomocy zgodnie z art. 55 lub wspólnych operacji zgodnie z art. 56.

5. Organy nadzorcze i Komisja przekazują Europejskiej Radzie Ochrony Danych drogą elektroniczną w standardowym formacie wszelkie stosowne informacje, w tym w stosownym przypadku streszczenie stanu faktycznego, projekt decyzji, powody przemawiające za przyjęciem takiego środka oraz opinię innych zainteresowanych organów nadzorczych.

6. Przewodniczący Europejskiej Rady Ochrony Danych bez zbędnej zwłoki przekazuje drogą elektroniczną członkom Europejskiej Rady Ochrony Danych i Komisji wszelkie stosowne informacje otrzymane w standardowym formacie. W razie potrzeby sekretariat Europejskiej Rady Ochrony Danych zapewnia tłumaczenie stosownych informacji.

#### *Artykuł 58*

#### ***Opinia Europejskiej Rady Ochrony Danych***

1. (...)

2. (...)

3. (...)



4. (...)

5. (...)

6. (...)

7. W przypadkach, o których mowa w art. 57 ust. 2 i 4, Europejska Rada Ochrony Danych wydaje opinię w sprawie jej przedłożonej, o ile już wcześniej nie wydała opinii w tej samej sprawie. Opinia ta zostaje przyjęta w terminie jednego miesiąca zwykłą większością głosów członków Europejskiej Rady Ochrony Danych. Okres ten można przedłużyć o jeden miesiąc ze względu na złożony charakter sprawy. Jeżeli chodzi o projekt decyzji przekazanej członkom Europejskiej Rady Ochrony Danych zgodnie z art. 57 ust. 6, uznaje się, że członek, który w terminie wskazanym przez przewodniczącego nie wyraził sprzeciwu, zgadza się z projektem decyzji.

7a. W terminie, o którym mowa w ust. 7, właściwy organ nadzorczy nie przyjmuje projektu decyzji, o której mowa w art. 57 ust. 2.

7b. Przewodniczący Europejskiej Rady Ochrony Danych bez zbędnej zwłoki informuje o opinii organ nadzorczy, o którym mowa odpowiednio w art. 57 ust. 2 i 4, i Komisję oraz podaje tę opinię do wiadomości publicznej.

8. Organ nadzorczy, o którym mowa w art. 57 ust. 2, w jak największym stopniu uwzględnia opinię Europejskiej Rady Ochrony Danych i w terminie dwóch tygodni po otrzymaniu tej opinii informuje drogą elektroniczną przewodniczącego Europejskiej Rady Ochrony Danych, czy podtrzymuje czy też zmienia projekt decyzji, a w stosownym przypadku przekazuje mu w standardowym formacie zmieniony projekt decyzji.

9. Jeżeli zainteresowany organ nadzorczy w terminie, o którym mowa w ust. 8, poinformuje przewodniczącego Europejskiej Rady Ochrony Danych, że nie zamierza w całości lub w części zastosować się do opinii, podając istotną przyczynę, zastosowanie ma art. 57 ust. 3.

10. (...)

11. (...)

#### Artykuł 58a

#### **Decyzje Europejskiej Rady Ochrony Danych**

1. W przypadkach, o których mowa w art. 57 ust. 3, Europejska Rada Ochrony Danych przyjmuje decyzję w przedłożonej jej sprawie, po to by zapewnić w poszczególnych sytuacjach właściwe i spójne stosowanie niniejszego rozporządzenia. Decyzja zostaje uzasadniona i skierowana do głównego organu nadzorczego oraz wszystkich zainteresowanych organów nadzorczych i jest dla nich wiążąca.
2. Decyzja, o której mowa w ust. 1, jest przyjmowana większością dwóch trzecich głosów członków Europejskiej Rady Ochrony Danych w terminie jednego miesiąca od wpłynięcia sprawy. Okres ten można przedłużyć o jeden miesiąc ze względu na złożony charakter sprawy.
3. Jeżeli Europejska Rada Ochrony Danych nie jest w stanie przyjąć decyzji w terminach, o których mowa w ust. 2, przyjmuje decyzję w terminie dwóch tygodni po upływie drugiego miesiąca, o którym mowa w ust. 2, zwykłą większością głosów swoich członków. Jeżeli głosy członków Europejskiej Rady Ochrony Danych rozkładają się po równo, decyduje głos przewodniczącego.
4. W terminach, o których mowa w ust. 2 i 3, zainteresowane organy nadzorcze nie przyjmują decyzji w sprawie przedłożonej Europejskiej Radzie Ochrony Danych na mocy ust. 1.
5. (...)

6. Przewodniczący Europejskiej Rady Ochrony Danych bez zbędnej zwłoki notyfikuje zainteresowanym organom nadzorczym decyzję, o której mowa w ust. 1. Informuje o niej Komisję. Decyzja jest niezwłocznie publikowana na stronie internetowej Europejskiej Rady Ochrony Danych, po tym jak organ nadzorczy notyfikował ostateczną decyzję, o której mowa w ust. 7.
7. Bez zbędnej zwłoki i najpóźniej w terminie jednego miesiąca po tym, jak Europejska Rada Ochrony Danych notyfikuje swoją decyzję, główny organ nadzorczy lub w stosownym przypadku organ nadzorczy, do którego wniesiono skargę, przyjmują ostateczną decyzję na podstawie decyzji, o której mowa w ust. 1. Główny organ nadzorczy lub w stosownym przypadku organ nadzorczy, do którego wniesiono skargę, informują Europejską Radę Ochrony Danych o terminie, w którym notyfikowały ostateczną decyzję odpowiednio administratorowi lub podmiotowi przetwarzającemu i podmiotowi danych. Ostateczna decyzja zainteresowanych organów nadzorczych zostaje przyjęta w trybie art. 54a ust. 4a, 4b i 4bb. Ostateczna decyzja zawiera informacje o decyzji, o której mowa w ust. 1, i wskazuje, że decyzja, o której mowa w ust. 1, zostanie opublikowana na stronie internetowej Europejskiej Rady Ochrony Danych zgodnie z ust. 6. Do ostatecznej decyzji załączona zostaje decyzja, o której mowa w ust. 1.

*Artykuł 59*

***Opinia Komisji***

(...)

*Artykuł 60*

***Zawieszenie projektu środka***

(...)

## *Artykuł 61*

### *Tryb pilny*

1. W wyjątkowych okolicznościach, jeżeli zainteresowany organ nadzorczy uzna, że istnieje pilna potrzeba podjęcia działań w celu ochrony praw i wolności podmiotów danych, może w drodze odstępstwa od mechanizmu spójności, o którym mowa w art. 57, lub procedury, o której mowa w art. 54a, niezwłocznie przyjąć środki tymczasowe mające wywołać skutki prawne na terytorium własnego państwa członkowskiego o konkretnym terminie obowiązywania. Organ nadzorczy niezwłocznie informuje o tych środkach i o powodach ich przyjęcia inne zainteresowane organy nadzorcze, Europejską Radę Ochrony Danych i Komisję.
2. Jeżeli organ nadzorczy przedsięwziął środek na mocy ust. 1 i uznaje, że należy pilnie przyjąć środki ostateczne, może zwrócić się z wnioskiem o wydanie opinii lub wiążącej decyzji w trybie pilnym do Europejskiej Rady Ochrony Danych, uzasadniając swój wniosek o opinię lub decyzję.
3. Każdy organ nadzorczy może zwrócić się do Europejskiej Rady Ochrony Danych z wnioskiem o wydanie opinii lub w stosownym przypadku wiążącej decyzji w trybie pilnym, uzasadniając swój wniosek o opinię lub decyzję, w tym pilną potrzebę podjęcia działań – jeżeli właściwy organ nadzorczy nie przedsięwziął odpowiedniego środka w sytuacji, w której istnieje pilna potrzeba podjęcia działań w celu ochrony praw i wolności podmiotów danych.
4. W drodze odstępstwa od art. 58 ust. 7 i art. 58a ust. 2 opinię lub wiążącą decyzję wydawane w trybie pilnym, o których mowa w ust. 2 i 3 niniejszego artykułu, przyjmuje się w terminie dwóch tygodni zwykłą większością głosów członków Europejskiej Rady Ochrony Danych.

*Artykuł 62*  
***Akty wykonawcze***

1. Komisja może przyjmować akty wykonawcze o zasięgu ogólnym, aby:

a) (...);

b) (...);

c) (...);

d) określić zasady wymiany informacji drogą elektroniczną między organami nadzorczymi oraz między organami nadzorczymi a Europejską Radą Ochrony Danych, w szczególności standardowy format, o którym mowa w art. 57 ust. 5 i 6 oraz w art. 58 ust. 8.

Akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 87 ust. 2.

2. (...)

3. (...)

*Artykuł 63*  
***Egzekwowanie***

(...)

**Sekcja 3**  
**Europejska Rada Ochrony Danych**

*Artykuł 64*  
***Europejska Rada Ochrony Danych***

1a. Niniejszym ustanawia się Europejską Radę Ochrony Danych jako organ Unii mający osobowość prawną.

1b. Europejską Radę Ochrony Danych reprezentuje jej przewodniczący.

2. W skład Europejskiej Rady Ochrony Danych wchodzi szefowie jednego z organów nadzorczych każdego państwa członkowskiego lub ich przedstawiciele oraz Europejski Inspektor Ochrony Danych.

3. Jeżeli w państwie członkowskim za monitorowanie stosowania przepisów na mocy niniejszego rozporządzenia jest odpowiedzialny więcej niż jeden organ nadzorczy, (...) to zgodnie z prawem krajowym tego państwa członkowskiego wyznaczony zostaje wspólny przedstawiciel.

4. Komisja oraz Europejski Inspektor Ochrony Danych lub jego przedstawiciel mają prawo uczestniczyć w działaniach i posiedzeniach Europejskiej Rady Ochrony Danych bez prawa głosu. Komisja wyznacza swojego przedstawiciela. Przewodniczący Europejskiej Rady Ochrony Danych informuje Komisję (...) o działaniach Europejskiej Rady Ochrony Danych.

## *Artykuł 65*

### ***Niezależność***

1. W toku wykonywania swoich zadań lub korzystania ze swoich uprawnień na mocy art. 66 (...) i 67 Europejska Rada Ochrony Danych działa w sposób niezależny.
2. Bez uszczerbku dla wniosków Komisji, o których mowa w art. 66 ust. 1 lit. b) i ust. 2, Europejska Rada Ochrony Danych podczas wykonywania swoich zadań lub korzystania ze swoich uprawnień nie zwraca się do nikogo o instrukcje ani ich od nikogo nie przyjmuje.

## *Artykuł 66*

### ***Zadania Europejskiej Rady Ochrony Danych***

1. Europejska Rada Ochrony Danych propaguje spójne stosowanie niniejszego rozporządzenia. W tym celu z własnej inicjatywy lub na wniosek Komisji podejmuje w szczególności następujące działania:
  - aa) monitoruje i zapewnia właściwe stosowanie niniejszego rozporządzenia w przypadkach, o których mowa w art. 57 ust. 3, bez uszczerbku dla zadań krajowych organów nadzorczych;
  - a) doradza Komisji w każdej sprawie związanej z ochroną danych osobowych w Unii, w tym w sprawie wszelkich proponowanych zmian do niniejszego rozporządzenia;

b) z własnej inicjatywy lub na wniosek jednego ze swoich członków lub Komisji bada wszelkie kwestie dotyczące stosowania niniejszego rozporządzenia i opracowuje wytyczne, zalecenia oraz wzorcowe rozwiązania, by zachęcić do spójnego stosowania niniejszego rozporządzenia;

ba) opracowuje wytyczne dla organów nadzorczych w sprawie stosowania środków, o których mowa w art. 53 ust. 1, 1b i 1c, oraz w sprawie ustalania grzywien administracyjnych na mocy art. 79 i 79a;

c) weryfikuje praktyczne stosowanie wytycznych, zaleceń i wzorcowych rozwiązań, o których mowa w lit. b) i ba);

ca) zachęca do sporządzania kodeksów postępowania oraz do ustanawiania mechanizmów certyfikacji w dziedzinie ochrony danych oraz pieczęci i oznaczeń w tej dziedzinie na mocy art. 38 i 39;

cb) akredytuje podmioty certyfikujące i okresowo weryfikuje certyfikację na mocy art. 39a oraz prowadzi publiczny rejestr podmiotów akredytowanych na mocy art. 39a ust. 6 i akredytowanych administratorów i podmiotów przetwarzających mających siedzibę w państwach trzecich na mocy art. 39 ust. 4;

cd) precyzuje wymogi, o których mowa w art. 39a ust. 3, z myślą o akredytacji podmiotów certyfikujących na mocy art. 39;

ce) wydaje opinie dla Komisji na temat poziomu ochrony danych osobowych w państwach trzecich lub organizacjach międzynarodowych, zwłaszcza w przypadkach, o których mowa w art. 41;

d) wydaje opinie w sprawie projektów decyzji zgłoszonych przez organy nadzorcze zgodnie z mechanizmem spójności, o którym mowa w ust. 2, i w sprawach przedłożonych jej zgodnie z art. 57 ust. 4;



- e) propaguje współpracę oraz skuteczną dwustronną i wielostronną wymianę informacji i praktyk między organami nadzorczymi;
- f) propaguje wspólne programy szkoleń oraz ułatwia wymianę personelu między organami nadzorczymi, a w stosownym przypadku – z organami nadzorczymi państw trzecich lub organizacji międzynarodowych;
- g) propaguje wymianę wiedzy i dokumentów na temat ustawodawstwa i praktyki w dziedzinie ochrony danych z organami nadzorczymi odpowiedzialnymi za ochronę danych na świecie;
- h) (...);
- i) prowodzi publicznie dostępny elektroniczny rejestr decyzji podjętych przez organy nadzorcze i sądy w sprawach rozpatrywanych w ramach mechanizmu spójności.

2. Jeżeli Komisja zwraca się z wnioskiem o poradę do Europejskiej Rady Ochrony Danych, może – uwzględniając pilność sprawy – wskazać termin.

3. Europejska Rada Ochrony Danych przekazuje swoje opinie, wytyczne, zalecenia i wzorcowe rozwiązania Komisji i komitetowi, o którym mowa w art. 87, oraz podaje je do wiadomości publicznej.

*Artykuł 67*  
***Sprawozdania***

1. (...)
2. Europejska Rada Ochrony Danych sporządza roczne sprawozdanie na temat ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w Unii, a w stosownym przypadku w państwach trzecich i organizacjach międzynarodowych. Sprawozdanie jest podawane do wiadomości publicznej oraz przekazywane Parlamentowi Europejskiemu, Radzie i Komisji.
3. W rocznym sprawozdaniu przedstawia się praktyczne stosowanie wytycznych, zaleceń i wzorcowych rozwiązań, o których mowa w art. 66 ust. 1 lit. c), oraz wiążących decyzji, o których mowa w art. 57 ust. 3.

*Artykuł 68*  
***Procedura***

1. Europejska Rada Ochrony Danych przyjmuje wiążące decyzje, o których mowa w art. 57 ust. 3, zgodnie z wymogami większościowymi, o których mowa w art. 58a ust. 2 i 3. Decyzje związane z innymi zadaniami wymienionymi w art. 66 podejmuje zwykłą większością głosów swoich członków.
2. Europejska Rada Ochrony Danych przyjmuje swój regulamin wewnętrzny większością dwóch trzecich głosów swoich członków i ustala swoje zasady działania.

*Artykuł 69*  
***Przewodniczący***

1. Europejska Rada Ochrony Danych wybiera zwykłą większością głosów spośród swoich członków przewodniczącego i dwóch wiceprzewodniczących (...).
2. Kadencja przewodniczącego i wiceprzewodniczących trwa pięć lat i jest jednokrotnie odnawialna.

*Artykuł 70*  
***Zadania przewodniczącego***

1. Przewodniczący ma następujące zadania:
  - a) zwołuje posiedzenia Europejskiej Rady Ochrony Danych i sporządza porządek obrad;
  - aa) notyfikuje głównemu organowi nadzorczemu i zainteresowanym organom nadzorczym decyzje przyjęte przez Europejską Radę Ochrony Danych na mocy art. 58a;
  - b) zapewnia terminowe wykonanie zadań Europejskiej Rady Ochrony Danych, w szczególności w odniesieniu do mechanizmu spójności, o którym mowa w art. 57.
2. Europejska Rada Ochrony Danych w swoim regulaminie wewnętrznym określa podział zadań między przewodniczącego a wiceprzewodniczących.

## *Artykuł 71*

### ***Sekretariat***

1. Europejską Radę Ochrony Danych wspiera sekretariat, którego obsługę zapewnia sekretariat Europejskiego Inspektora Ochrony Danych (...).

1a. Sekretariat wykonuje swoje zadania wyłącznie pod kierunkiem przewodniczącego Europejskiej Rady Ochrony Danych.

1b. Personel Europejskiego Inspektora Ochrony Danych wykonujący zadania, które powierza Europejskiej Radzie Ochrony Danych niniejsze rozporządzenie, jest oddzielony organizacyjnie od personelu wykonującego zadania powierzone Europejskiemu Inspektorowi Ochrony Danych i podlega oddzielnej hierarchii służbowej.

1c. W razie potrzeby Europejska Rada Ochrony Danych w konsultacji z Europejskim Inspektorem Ochrony Danych opracowuje i publikuje kodeks postępowania wdrażający niniejszy artykuł i mający zastosowanie do personelu sekretariatu Europejskiego Inspektora Ochrony Danych wykonującego zadania powierzone Europejskiej Radzie Ochrony Danych niniejszym rozporządzeniem.

2. Sekretariat zapewnia Europejskiej Radzie Ochrony Danych wsparcie analityczne, administracyjne i logistyczne.

3. Sekretariat jest w szczególności odpowiedzialny za:

a) bieżącą działalność Europejskiej Rady Ochrony Danych;

b) przekazywanie informacji między członkami Europejskiej Rady Ochrony Danych, jej przewodniczącym i Komisją oraz komunikację z innymi instytucjami i opinią publiczną;

- c) stosowanie metod elektronicznych do komunikacji wewnętrznej i zewnętrznej;
- d) dokonywanie tłumaczeń stosownych informacji;
- e) przygotowywanie posiedzeń Europejskiej Rady Ochrony Danych oraz działania następcze;
- f) przygotowywanie, redagowanie i publikowanie opinii, decyzji w sprawie rozstrzygnięcia sporu między organami nadzorczymi oraz innych tekstów przyjmowanych przez Europejską Radę Ochrony Danych.

*Artykuł 72*

***Poufność***

1. Obrady Europejskiej Rady Ochrony Danych są poufne.
2. Dostęp do dokumentów przedłożonych członkom Europejskiej Rady Ochrony Danych, ekspertom i przedstawicielom stron trzecich jest regulowany rozporządzeniem (WE) nr 1049/2001.

## ROZDZIAŁ VIII

### ŚRODKI OCHRONY PRAWNEJ, ODPOWIEDZIALNOŚĆ PRAWNA I SANKCJE

#### *Artykuł 73*

#### ***Prawo wniesienia skargi do organu nadzorczego***

1. Bez uszczerbku dla innych administracyjnych lub sądowych środków ochrony prawnej każdy podmiot danych ma prawo wnieść skargę do jednego organu nadzorczego, w szczególności w państwie członkowskim, w którym znajduje się miejsce jego zwykłego pobytu, miejsce pracy lub miejsce domniemanego naruszenia, jeżeli sądzi, że przetwarzanie danych osobowych go dotyczących nie jest zgodne z niniejszym rozporządzeniem.
2. (...)
3. (...)
4. (...)
5. Organ nadzorczy, do którego wniesiono skargę, informuje skarżącego o postępach i efektach rozpatrywania skargi, w tym o możliwości skorzystania z sądowego środka ochrony prawnej na mocy art. 74 (...).

#### *Artykuł 74*

#### ***Prawo do skutecznego sądowego środka ochrony prawnej przeciwko organowi nadzorczemu***

1. Bez uszczerbku dla innych administracyjnych lub pozasądowych środków ochrony prawnej każda osoba fizyczna lub prawna ma prawo do skutecznego sądowego środka ochrony prawnej przeciwko prawnie wiążącej decyzji organu nadzorczego jej dotyczącej.

2. Bez uszczerbku dla innych administracyjnych lub pozasądowych środków ochrony prawnej każdy podmiot danych ma prawo do skutecznego sądowego środka ochrony prawnej, jeżeli organ nadzorczy właściwy zgodnie z art. 51 i 51a nie rozpatrzył skargi lub nie poinformował podmiotu danych w terminie trzech miesięcy – lub w terminie krótszym przewidzianym prawem Unii lub prawem państwa członkowskiego – o postępach lub efektach rozpatrywania skargi wniesionej na mocy art. 73.

3. (...) Postępowanie przeciwko (...) organowi nadzorczemu zostaje wszczęte przed sądem państwa członkowskiego, w którym organ nadzorczy ma siedzibę.

3a. Jeżeli postępowanie zostało wszczęte przeciwko decyzji organu nadzorczego, którą poprzedziła opinia lub decyzja Europejskiej Rady Ochrony Danych w ramach mechanizmu spójności, organ nadzorczy przekazuje sądowi tę opinię lub decyzję.

4. (...)

5. (...)

#### *Artykuł 75*

#### ***Prawo do skutecznego sądowego środka ochrony prawnej przeciwko administratorowi lub podmiotowi przetwarzającemu***

1. Bez uszczerbku dla dostępnych administracyjnych lub pozasądowych środków ochrony prawnej, w tym prawa wniesienia skargi do organu nadzorczego na mocy art. 73, podmioty danych mają prawo do skutecznego sądowego środka ochrony prawnej, jeżeli sądzą, że prawa przysługujące im na mocy niniejszego rozporządzenia zostały naruszone w wyniku przetwarzania ich danych osobowych niezgodnie z niniejszym rozporządzeniem.

2. Postępowanie przeciwko administratorowi lub podmiotowi przetwarzającemu zostaje wszczęte przed sądem państwa członkowskiego, w którym administrator lub podmiot przetwarzający mają siedzibę (...). Ewentualnie postępowanie takie może zostać wszczęte przed sądem państwa członkowskiego, w którym podmiot danych ma miejsce zwykłego pobytu, chyba że administrator lub podmiot przetwarzający są organami publicznymi wykonującymi swoje uprawnienia publiczne.

3. (...)

4. (...)

## *Artykuł 76*

### **Reprezentowanie podmiotów danych**

1. Podmiot danych ma prawo zlecić organowi, organizacji lub stowarzyszeniu, które zostały należycie ustanowione zgodnie z prawem państwa członkowskiego i które wśród swoich statutowych celów mają ochronę praw i wolności podmiotów danych w związku z ochroną ich danych osobowych, wniesienie skargi w swoim imieniu oraz skorzystanie z praw, o których mowa w art. 73, 74 i 75, w jego imieniu.
  - 1a. (...)
2. Państwa członkowskie mogą przewidzieć, że organ, organizacja lub stowarzyszenie, o których mowa w ust. 1, niezależnie od zlecenia otrzymanego od podmiotu danych (...) mają w tym państwie członkowskim prawo wnieść skargę do organu nadzorczego właściwego zgodnie z art. 73 oraz skorzystać z praw, o których mowa w art. 73, 74 i 75, jeżeli uznają, że w wyniku przetwarzania danych osobowych niezgodnie z niniejszym rozporządzeniem naruszone zostały prawa podmiotu danych.
3. (...)
4. (...)

## *Artykuł 76a*

### **Zawieszenie postępowania**

1. Jeżeli właściwy sąd państwa członkowskiego ma informacje, że przed sądem w innym państwie członkowskim toczy się postępowanie w tej samej sprawie w odniesieniu do przetwarzania (...) przez tego samego administratora lub ten sam podmiot przetwarzający, kontaktuje się z tym sądem w innym państwie członkowskim, aby potwierdzić istnienie takiego postępowania.
2. Jeżeli przed sądem w innym państwie członkowskim toczy się postępowanie w tej samej sprawie w odniesieniu do przetwarzania (...) przez tego samego administratora lub ten sam podmiot przetwarzający, każdy właściwy sąd inny niż sąd, przed którym jako pierwszym wszczęto postępowanie, może zawiesić swoje postępowanie.



2a. Jeżeli postępowanie toczy się w pierwszej instancji, każdy sąd inny niż sąd, przed którym jako pierwszym wszczęto postępowanie, może także – na wniosek jednej ze stron – stwierdzić brak swojej jurysdykcji, jeżeli sąd, przed którym jako pierwszym wszczęto postępowanie, ma jurysdykcję względem przedmiotowych spraw, a jego prawo dopuszcza ich połączenie.

3. (...).

### *Artykuł 77*

#### ***Prawo do odszkodowania i odpowiedzialność prawna***

1. Każda osoba, która poniosła szkodę materiałną lub niematerialną w wyniku przetwarzania niezgodnego z niniejszym rozporządzeniem, ma prawo otrzymać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę.
2. Każdy administrator (...) uczestniczący w przetwarzaniu odpowiada prawnie za szkody spowodowane przetwarzaniem niezgodnym z niniejszym rozporządzeniem. Podmiot przetwarzający odpowiada prawnie za (...) szkody spowodowane przetwarzaniem wyłącznie wtedy, gdy nie dopełnił obowiązków, które niniejsze rozporządzenie nakłada bezpośrednio na podmiot przetwarzający, lub gdy działał poza zgodnymi z prawem instrukcjami administratora lub wbrew tym instrukcjom.
3. Administrator lub podmiot przetwarzający zostają zwolnieni z odpowiedzialności prawnej, zgodnie z ust. 2, jeżeli udowodnią, że w żadnym razie nie ponoszą winy (...) za zdarzenie, które doprowadziło do powstania szkody.
4. Jeżeli w tym samym przetwarzaniu uczestniczy więcej niż jeden administrator lub podmiot przetwarzający lub uczestniczą w nim i administrator, i podmiot przetwarzający i zgodnie z warunkami określonymi w ust. 2 i 3 odpowiadają za jakąkolwiek szkodę spowodowaną przetwarzaniem, każdy z nich odpowiada prawnie (...) za całą szkodę.

5. Administrator lub podmiot przetwarzający, który zgodnie z ust. 4 wypłacił pełne odszkodowanie za wyrządzoną szkodę, ma prawo domagać się od pozostałych administratorów lub podmiotów przetwarzających, którzy uczestniczyli w tym samym przetwarzaniu, części odszkodowania odpowiadającej ich części odpowiedzialności za szkodę zgodnie z warunkami określonymi w ust. 2.
6. Postępowanie sądowe dotyczące korzystania z prawa do odszkodowania jest wszczynane przed sądem właściwym na mocy prawa krajowego państwa członkowskiego, o którym mowa w art. 75 ust. 2.

#### *Artykuł 78*

##### ***Kary***

(...)

#### *Artykuł 79*

##### **Ogólne warunki nakładania grzywien administracyjnych**

1. Każdy organ nadzorczy (...) dopilnowuje, by nakładanie grzywien administracyjnych na mocy niniejszego artykułu za naruszenia niniejszego rozporządzenia, o których mowa w art. 79a, (...) było w każdym przypadku skuteczne, proporcjonalne i odstraszające.
2. (...)
- 2a. Grzywny administracyjne nakłada się, zależnie od okoliczności danej sprawy, oprócz lub zamiast środków, o których mowa w art. 53 ust. 1b lit. a)–f). Decydując, czy nałożyć grzywnę administracyjną, (...) oraz ustalając jej kwotę, w każdym przypadku zwraca się należyta uwagę na:

- a) charakter, wagę i czas trwania naruszenia w odniesieniu do charakteru, zakresu lub celu danego przetwarzania, liczbę podmiotów danych, na które wpłynęło naruszenie, oraz zakres poniesionej przez nie szkody;
  - b) umyślny lub lekkomyślny charakter naruszenia;
  - c) (...);
  - d) działania podjęte przez administratora lub podmiot przetwarzający w celu zminimalizowania szkody poniesionej przez podmioty danych;
  - e) stopień odpowiedzialności administratora lub podmiotu przetwarzającego z uwzględnieniem środków technicznych i organizacyjnych wdrożonych przez nich na mocy art. 23 i 30;
  - f) wszelkie odnośne wcześniejsze naruszenia ze strony administratora lub podmiotu przetwarzającego;
  - g) (...);
  - h) sposób, w jaki organ nadzorczy dowiedział się o naruszeniu, w szczególności, czy i w jakim stopniu administrator lub podmiot przetwarzający zgłosili naruszenie;
  - i) jeżeli wobec zainteresowanego administratora lub podmiotu przetwarzającego wcześniej orzeczone zostały w tej samej sprawie środki, o których mowa w (...) art. 53 ust. 1b lit. a), d), e) i f) – przestrzeganie tych środków;
  - j) stosowanie zatwierdzonych kodeksów postępowania na mocy art. 38 lub zatwierdzonych mechanizmów certyfikacji na mocy art. 39;
  - k) (...);
  - l) (...);
  - m) wszelkie inne obciążające lub łagodzące czynniki mające zastosowanie do okoliczności sprawy.
3. (...)
- 3a. (...)

- 3b. Każde państwo członkowskie może ustalić, czy i w jakim zakresie grzywny administracyjne można nakładać na organy i podmioty publiczne ustanowione w tym państwie członkowskim.
4. Korzystanie przez organ nadzorczy (...) z uprawnień przyznanych mu niniejszym artykułem podlega odpowiednim gwarancjom proceduralnym zgodnym z prawem Unii i prawem państwa członkowskiego, w tym skutecznemu sądowemu środkowi ochrony prawnej i sprawiedliwości proceduralnej.
5. Państwa członkowskie mogą nie przewidywać przepisów o grzywnach administracyjnych, o których mowa w art. 79a ust. 1, 2 i 3, jeżeli ich system prawny nie przewiduje grzywien administracyjnych, a za naruszenia, o których mowa we wspomnianym artykule, do [data z art. 91 ust. 2] ich prawo krajowe będzie już przewidywać sankcje karne, a jednocześnie państwa te dopilnują, by sankcje te były skuteczne, proporcjonalne i odstrasżające, uwzględniając poziom grzywien administracyjnych przewidzianych w niniejszym rozporządzeniu.

W takim przypadku państwa członkowskie szczegółowo notyfikują Komisji odnośne przepisy swojego prawa karnego.

#### *Artykuł 79a*

##### **Grzywny administracyjne**

1. Organ nadzorczy (...) może nałożyć grzywnę w wysokości nieprzekraczającej 250 000 EUR lub w przypadku przedsiębiorstwa 0,5% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego na administratora, który umyślnie lub lekkomyślnie:
- (a) nie odpowie w terminie, o którym mowa w art. 12 ust. 2, na wnioski podmiotu danych;
  - (b) pobiera opłatę, naruszając art. 12 ust. 4 zdanie pierwsze.
2. Organ nadzorczy (...) może nałożyć grzywnę w wysokości nieprzekraczającej 500 000 EUR lub w przypadku przedsiębiorstwa 1% jego całkowitego rocznego światowego (...) obrotu z poprzedniego roku obrotowego na administratora lub podmiot przetwarzający, którzy umyślnie lub lekkomyślnie:

- a) nie podają informacji podmiotowi danych zgodnie z art. 12 ust. 3, art. 14 i 14a, (...) podają informacje niepełne lub nie podają informacji [na czas lub] w [dostatecznie] przejrzysty sposób;
- b) nie zapewniają dostępu podmiotowi danych lub nie poprawiają danych osobowych zgodnie z artykułami 15 i 16 (...);
- c) nie usuwają danych osobowych, naruszając prawo do usunięcia danych i do „bycia zapomnianym”, o którym mowa w art. 17 ust. 1 lit. a), 17 ust. 1 lit. b), 17 ust. 1 lit. d) lub 17 ust. 1 lit. e);
- d) (...)
- da) przetwarzają dane osobowe z naruszeniem prawa do ograniczenia przetwarzania na mocy art. 17a lub nie informują podmiotu danych przed uchyleniem tego ograniczenia zgodnie z art. 17a ust. 4;
- db) nie informują o poprawieniu, usunięciu lub ograniczeniu przetwarzania każdego odbiorcy, któremu administrator ujawnił dane osobowe, z naruszeniem art. 17b;
- dc) nie dostarczają podmiotowi danych danych osobowych jego dotyczących (...) z naruszeniem art. 18;
- dd) przetwarzają dane osobowe po sprzeciwie podmiotu danych na mocy art. 19 ust. 1 i nie wykazują istnienia ewidentnych uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności podmiotu danych, lub do ustalenia, realizacji lub obrony roszczeń prawnych;
- de) nie podają podmiotowi danych informacji o prawie do sprzeciwu wobec przetwarzania do celów marketingu bezpośredniego na mocy z art. 19 ust. 2 lub nadal przetwarzają dane do celów marketingu bezpośredniego po sprzeciwie podmiotu danych, z naruszeniem art. 19 ust. 2a;
- e) nie określają wcale lub wystarczająco podziału zadań, o którym mowa w art. 24, między współadministratorami;

- f) nie prowadzą żadnej lub wystarczającej dokumentacji, o której mowa w art. 28 i art. 31 ust. 4.
- g) (...)

3. Organ nadzorczy (...) może nałożyć grzywnę w wysokości nieprzekraczającej 1 000 000 EUR lub w przypadku przedsiębiorstwa 2% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego na administratora lub podmiot przetwarzający, którzy umyślnie lub lekkomyślnie:

- a) przetwarzają dane osobowe bez (...) podstawy prawnej przetwarzania lub nie przestrzegają warunków zgody, o której mowa w art. 6, 7, 8 i 9;
- b) (...);
- c) (...);
- d) nie przestrzegają warunków (...) automatycznego zindywidualizowanego podejmowania decyzji, w tym profilowania, wynikających z art. 20;
  - da) nie (...) wdrażają odpowiednich środków lub nie są w stanie wykazać przestrzegania przepisów art. 22 (...) i 30;
  - db) nie wyznaczają przedstawiciela, naruszając art. 25;
  - dc) przetwarzają lub polecają przetwarzać dane osobowe z naruszeniem (...) art. 26;
  - dd) nie ostrzegają lub nie powiadamiają organu nadzorczego lub podmiotu danych o naruszeniu ochrony danych osobowych, lub nie zgłaszają go [na czas lub] w całości, naruszając art. 31 i 32;
  - de) nie dokonują oceny skutków pod kątem ochrony danych, naruszając art. 33, lub przetwarzają dane osobowe bez uprzednich konsultacji z organem nadzorczym, naruszając art. 34 ust. 2;
- e) (...);

- f) nadużywają pieczęci lub oznaczenia w dziedzinie ochrony danych w rozumieniu art. 39 lub nie przestrzegają warunków i procedur ustanowionych w art. 38a i 39a;
- g) przekazują lub polecają przekazać dane odbiorcy w państwie trzecim lub organizacji międzynarodowej, naruszając art. 41–44;
- h) nie przestrzegają nakazu, tymczasowego lub ostatecznego ograniczenia przetwarzania lub zawieszenia przepływu danych wydanego przez organ nadzorczy na podstawie art. 53 ust. 1b lub nie zapewniają dostępu, naruszając art. 53 ust. 1.
- i) (...)
- j) (...).
- 3a. Jeżeli administrator lub podmiot przetwarzający umyślnie lub lekkomyślnie naruszają kilka przepisów niniejszego rozporządzenia wymienionych w ust. 1, 2 lub 3, całkowita kwota grzywny nie może przekroczyć kwoty za najpoważniejsze naruszenie.
4. (...)

#### *Artykuł 79b*

##### ***Kary***

1. *Na wypadek naruszeń (...) niniejszego rozporządzenia, w szczególności naruszeń niepodlegających grzywnom administracyjnym na mocy (...) art. 79a, państwa członkowskie ustalają przepisy o karach mających zastosowanie do takich naruszeń oraz przedsiębiorzą wszelkie środki niezbędne do ich wdrożenia (...). Kary te są skuteczne, proporcjonalne i odstraszające.*
2. (...).
3. *Najpóźniej w terminie określonym w art. 91 ust. 2 każde państwo członkowskie zawiadamia Komisję o swoich przepisach przyjętych na mocy ust. 1, a następnie niezwłocznie o każdej kolejnej zmianie mającej na nie wpływ.*

## ROZDZIAŁ IX

### PRZEPISY DOTYCZĄCE SZCZEGÓLNYCH SYTUACJI ZWIĄZANYCH Z PRZETWARZANIEM DANYCH

#### *Artykuł 80*

##### ***Przetwarzanie danych osobowych a wolność wypowiedzi i informacji***

1. Prawo krajowe państw członkowskich (...) godzi prawo do ochrony danych osobowych na mocy niniejszego rozporządzenia z prawem do wolności wypowiedzi i informacji, w tym do przetwarzania danych osobowych do celów dziennikarskich oraz do celów wypowiedzi akademickiej, artystycznej lub literackiej.
2. Dla przetwarzania danych osobowych do celów dziennikarskich lub do celów wypowiedzi akademickiej, artystycznej lub literackiej państwa członkowskie przewidują wyjątki lub odstępstwa od przepisów rozdziału II (Zasady), rozdziału III (Prawa podmiotu danych), rozdziału IV (Administrator i podmiot przetwarzający), rozdziału V (Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych), rozdziału VI (Niezależne organy nadzorcze), rozdziału VII (Współpraca i spójność), jeżeli są one niezbędne, by pogodzić prawo do ochrony danych osobowych z wolnością wypowiedzi i informacji (...).

#### *Artykuł 80a*

##### ***Przetwarzanie danych osobowych a publiczny dostęp do dokumentów urzędowych***

Dane osobowe zawarte w dokumentach urzędowych posiadanych przez organ lub podmiot publiczny lub podmiot prywatny w celu wykonania zadania realizowanego w interesie publicznym mogą zostać przez ten organ lub podmiot ujawnione zgodnie z prawem Unii lub prawem państwa członkowskiego, któremu podlegają ten organ lub podmiot, po to by pogodzić publiczny dostęp do dokumentów urzędowych z prawem do ochrony danych osobowych na mocy niniejszego rozporządzenia.



Artykuł 80aa

**Przetwarzanie danych osobowych a ponowne wykorzystywanie informacji sektora publicznego**

Dane osobowe zawarte w informacjach sektora publicznego posiadanych przez organ lub podmiot publiczny lub podmiot prywatny w celu wykonania zadania realizowanego w interesie publicznym mogą zostać przez ten organ lub podmiot ujawnione zgodnie z prawem Unii lub prawem państwa członkowskiego, któremu podlegają ten organ lub podmiot, po to by pogodzić ponowne wykorzystanie takich dokumentów urzędowych i informacji sektora publicznego z prawem do ochrony danych osobowych na mocy niniejszego rozporządzenia.

Artykuł 80b

**Przetwarzanie krajowego numeru identyfikacyjnego**

Państwa członkowskie mogą określić szczegółowe warunki przetwarzania krajowego numeru identyfikacyjnego lub innego identyfikatora o zasięgu ogólnym. W takim przypadku krajowy numer identyfikacyjny lub inny identyfikator o zasięgu ogólnym są używane wyłącznie z zastrzeżeniem odpowiednich gwarancji dla praw i wolności podmiotu danych na mocy niniejszego rozporządzenia.

Artykuł 81

**Przetwarzanie danych osobowych do celów zdrowotnych**

(...)

Artykuł 81a

**Przetwarzanie danych genetycznych**

(...)

*Artykuł 82*

***Przetwarzanie w kontekście zatrudnienia***

1. Państwa członkowskie mogą przewidzieć prawem lub umowami zbiorowymi bardziej szczegółowe przepisy mające zapewnić ochronę praw i wolności w przypadku przetwarzania danych osobowych pracowników w kontekście zatrudnienia, w szczególności do celów rekrutacji, wykonania umowy o pracę, w tym wykonania obowiązków określonych prawem lub umowami zbiorowymi, zarządzania, planowania i organizacji pracy, równości i różnorodności w miejscu pracy, bezpieczeństwa i higieny pracy, ochrony własności pracodawcy lub klienta oraz do celów indywidualnego lub zbiorowego wykonywania praw i korzystania ze świadczeń związanych z zatrudnieniem, a także do celów zakończenia stosunku pracy. (...)
2. Najpóźniej w terminie określonym w art. 91 ust. 2 każde państwo członkowskie zawiadamia Komisję o swoich przepisach przyjętych na mocy ust. 1, a następnie niezwłocznie o każdej kolejnej zmianie mającej na nie wpływ.
3. Państwa członkowskie mogą określić prawem warunki, na których dane osobowe w kontekście zatrudnienia można przetwarzać za zgodą pracownika.

*Artykuł 82a*

***Przetwarzanie do celów ochrony socjalnej***

(...)

**Odstępstwa mające zastosowanie do przetwarzania danych osobowych do celów archiwizacyjnych w interesie publicznym lub do celów naukowych, statystycznych i historycznych**

1. Jeżeli dane osobowe są przetwarzane do celów naukowych, statystycznych lub historycznych, prawo Unii lub prawo państwa członkowskiego mogą przewidywać – z zastrzeżeniem odpowiednich gwarancji dla praw i wolności podmiotów danych – odstępstwa od art. 14a ust. 1 i 2, art. 15, 16, 17, 17a, 17b, 18 i 19, o ile takie odstępowstwo jest niezbędne do wypełnienia tych konkretnych celów.
- 1a. Jeżeli dane osobowe są przetwarzane do celów archiwizacyjnych w interesie publicznym, prawo Unii lub prawo państwa członkowskiego mogą przewidywać – z zastrzeżeniem odpowiednich gwarancji dla praw i wolności podmiotów danych – odstępstwa od art. 14a ust. 1 i 2, art. 15, 16, 17, 17a, 17b, 18, 19, 23, 32, 33 i art. 53 ust. 1b lit. d) i e), o ile takie odstępowstwo jest niezbędne do wypełnienia tych konkretnych celów.
- 1b. Jeżeli przetwarzanie, o którym mowa w ust. 1 i 1a, służy równocześnie innemu celowi, dopuszczalne odstępowstwa mają zastosowanie wyłącznie do przetwarzania do celów, o których mowa w tych ustępach.
2. Odpowiednie gwarancje, o których mowa w ust. 1 i 1a, zostają ustanowione w prawie Unii lub prawie państwa członkowskiego i służą temu, by do danych osobowych stosowane były techniczne lub organizacyjne środki ochrony zgodne z niniejszym rozporządzeniem (...) w celu ograniczenia przetwarzania danych osobowych w myśl zasady proporcjonalności i zasady konieczności, np. pseudonimizacja danych, chyba że środki te uniemożliwiają realizację celu przetwarzania, a celu tego nie można zrealizować w inny sposób racjonalnymi środkami.
3. (...).

#### *Artykuł 84*

##### ***Obowiązek dochowania tajemnicy***

1. (...) Państwa członkowskie mogą przyjąć przepisy szczegółowe określające uprawnienia (...) organów nadzorczych ustanowione w art. 53 ust. 1 lit. da) i db) wobec administratorów lub podmiotów przetwarzających, którzy podlegają – na mocy prawa Unii lub prawa państwa członkowskiego lub przepisów ustanowionych przez właściwe organy krajowe – obowiązkowi dochowania tajemnicy służbowej, innym równoważnym obowiązkowi dochowania tajemnicy lub kodeksowi etyki zawodowej nadzorowanemu i egzekwowanemu przez organy zawodowe, jeżeli jest to niezbędne i proporcjonalne w celu pogodzenia prawa do ochrony danych osobowych z obowiązkiem dochowania tajemnicy. Przepisy te mają zastosowanie wyłącznie do danych osobowych, które administrator lub podmiot przetwarzający otrzymali lub pozyskali w ramach działania objętego tym obowiązkiem dochowania tajemnicy.
2. Najpóźniej w terminie określonym w art. 91 ust. 2 każde państwo członkowskie zawiadamia Komisję o swoich przepisach przyjętych na mocy ust. 1, a następnie niezwłocznie o każdej kolejnej zmianie mającej na nie wpływ.

#### *Artykuł 85*

##### ***Obowiązujące przepisy kościołów i stowarzyszeń religijnych o ochronie danych***

1. Jeżeli w państwie członkowskim w momencie wejścia w życie niniejszego rozporządzenia kościoły i stowarzyszenia lub wspólnoty religijne stosują kompleksowe przepisy dotyczące ochrony osób fizycznych w związku z przetwarzaniem danych osobowych, przepisy takie mogą być nadal stosowane, pod warunkiem że zostaną dostosowane do przepisów niniejszego rozporządzenia.
2. Kościoły i stowarzyszenia religijne, które stosują kompleksowe przepisy zgodnie z ust. 1, podlegają kontroli niezależnego organu nadzorczego, który może być organem specjalnym, z zastrzeżeniem że spełnia warunki ustanowione w rozdziale VI niniejszego rozporządzenia.

## ROZDZIAŁ X

### AKTY DELEGOWANE I AKTY WYKONAWCZE

#### *Artykuł 86*

#### ***Korzystanie z przekazanych uprawnień***

1. Uprawnienie do przyjmowania aktów delegowanych zostaje powierzone Komisji na warunkach określonych w niniejszym artykule.
2. Uprawnienie do przyjmowania aktów delegowanych, o których mowa w art. 39a ust. 7, (...) zostaje powierzone Komisji na czas nieokreślony od dnia wejścia w życie niniejszego rozporządzenia.
3. Uprawnienie do przyjmowania aktów delegowanych, o których mowa w art. 39a ust. 7, (...) może zostać w dowolnym momencie odwołane przez Parlament Europejski lub przez Radę. Decyzja o odwołaniu kończy przekazanie określonych w niej uprawnień. Decyzja o odwołaniu staje się skuteczna następnego dnia po opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej* lub w późniejszym terminie określonym w tej decyzji. Nie wpływa ona na ważność jakichkolwiek już obowiązujących aktów delegowanych.
4. Niezwłocznie po przyjęciu aktu delegowanego Komisja powiadamia o nim równocześnie Parlament Europejski i Radę.

5. Akt delegowany przyjęty na mocy art. 39a ust. 7 (...) wchodzi w życie wyłącznie wtedy, gdy ani Parlament Europejski, ani Rada w terminie dwóch miesięcy od otrzymania powiadomienia o nim nie wyrażą sprzeciwu lub gdy przed upływem tego terminu zarówno Parlament Europejski, jak i Rada poinformują Komisję, że nie wniosą sprzeciwu. Termin ten zostaje przedłużony o dwa miesiące z inicjatywy Parlamentu Europejskiego lub Rady.

#### *Artykuł 87*

#### ***Procedura komitetowa***

1. Komisję wspomaga komitet. Komitet ten jest komitetem w rozumieniu rozporządzenia (UE) nr 182/2011.
2. W przypadku odesłania do niniejszego ustępu zastosowanie ma art. 5 rozporządzenia (UE) nr 182/2011.
3. W przypadku odesłania do niniejszego ustępu zastosowanie ma art. 8 rozporządzenia (UE) nr 182/2011 w związku z jego art. 5.

## ROZDZIAŁ XI

### PRZEPISY KOŃCOWE

#### *Artykuł 88*

#### ***Uchylenie dyrektywy 95/46/WE***

1. Uchyla się dyrektywę 95/46/WE.
2. Odesłania do uchylonej dyrektywy należy interpretować jako odesłania do niniejszego rozporządzenia. Odesłania do Grupy Roboczej ds. Ochrony Osób Fizycznych w zakresie Przetwarzania Danych Osobowych, ustanowionej w art. 29 dyrektywy 95/46/WE, należy interpretować jako odesłania do Europejskiej Rady Ochrony Danych, ustanowionej niniejszym rozporządzeniem.

#### *Artykuł 89*

#### ***Stosunek do dyrektywy 2002/58/WE i jej zmiana***

1. Niniejsze rozporządzenie nie nakłada dodatkowych obowiązków na osoby fizyczne ani prawne co do przetwarzania danych osobowych w związku ze świadczeniem ogólnodostępnych usług łączności elektronicznej w publicznych sieciach łączności w Unii w sprawach, w których podmioty te podlegają szczegółowym obowiązkom mającym ten sam cel określonym w dyrektywie 2002/58/WE.
2. (...)

*Artykuł 89a*

***Stosunek do uprzednio zawartych porozumień***

*Międzynarodowe porozumienia, które obejmują przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych i które zostały zawarte przez państwa członkowskie przed wejściem w życie niniejszego rozporządzenia, i które są zgodne z dyrektywą 95/46/WE, pozostają w mocy do czasu ich zmiany, zastąpienia lub uchylecia*

*Artykuł 90*

***Ocena***

1. Komisja regularnie przedkłada Parlamentowi Europejskiemu i Radzie sprawozdania z oceny i przeglądu niniejszego rozporządzenia.
2. W ramach oceny Komisja sprawdza w szczególności stosowanie i funkcjonowanie przepisów rozdziału VII o współpracy i spójności.
3. Pierwsze sprawozdanie zostaje przedłożone najpóźniej cztery lata po wejściu w życie niniejszego rozporządzenia. Kolejne sprawozdania są przedkładane co cztery lata. Sprawozdania są podawane do wiadomości publicznej.
4. W razie potrzeby Komisja przedkłada odpowiednie propozycje zmian do niniejszego rozporządzenia oraz propozycje dostosowania innych instrumentów prawnych, uwzględniając w szczególności rozwój technologii informacyjnych oraz postęp w społeczeństwie informacyjnym.



*Artykuł 91*

***Wejście w życie i stosowanie***

1. Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.
2. Niniejsze rozporządzenie ma zastosowanie od dnia [*dwa lata od daty, o której mowa w ust. 1*].

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich.

Sporządzono w Brukseli dnia [...]

*W imieniu Parlamentu Europejskiego*

*W imieniu Rady*

*Przewodniczący*

*Przewodniczący*