Rada
Unii Europejskiej

Bruksela, 2 października 2015 r.
(OR. en)

12555/15

Międzyinstytucjonalny numer referencyjny:
2012/0010 (COD)

DATAPROTECT 154
JAI 707
DAPIX 163
FREMP 202
COMIX 456
CODEC 1279

NOTA

Od:	Prezydencja
Do:	Rada
Nr poprz. dok.:	12266/15
Nr dok. Kom.:	5833/12
Dotyczy:	Wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich, ścigania lub wykonywania kar kryminalnych oraz w sprawie swobodnego przepływu takich danych - Podejscie ogólne

I. WPROWADZENIE

1. W dniu 27 stycznia 2012 r. Komisja przedstawiła wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania albo wykonywania kar kryminalnych oraz swobodnego przepływu tych danych (dalej „projekt dyrektywy”)[1]. Dyrektywa ta miałaby zastąpić decyzję ramową 2008/977/WSiSW[2].

[1] Dok. 5833/12.
[2] Dz.U. L 350 z 30.12.2008, s. 60–71.

2. Wraz z projektem dyrektywy Komisja przedstawiła wniosek w sprawie ogólnego rozporządzenia o ochronie danych (dalej „projekt rozporządzenia") [3]; miałoby ono zastąpić dyrektywę 95/46/WE[4]. Proponowana dyrektywa i proponowane rozporządzenie stanowią pakiet reformujący ramy prawne w dziedzinie ochrony danych.

3. Parlament Europejski przyjął stanowisko w sprawie projektu dyrektywy w dniu 12 marca 2014 r. w pierwszym czytaniu w ramach zwykłej procedury ustawodawczej[5].

4. Europejski Inspektor Ochrony Danych wydał opinię w sprawie wniosku Komisji w dniu 8 marca 2012 r.[6]

5. Grupa Robocza ds. Wymiany Informacji i Ochrony Danych (DAPIX) rozpoczęła analizę tekstu na posiedzeniu w dniu 16 kwietnia 2012 r. za prezydencji duńskiej. Od tego czasu omawiała go za każdej prezydencji.

6. Za prezydencji luksemburskiej – od lipca 2015 r. – grupa DAPIX oraz Grupa Przyjaciół Prezydencji omawiały projekt dyrektywy w dniach 2–3 lipca, 15–16 lipca, 22 lipca, 3–4 września, 9 września, 16 września i 21–22 września, radcy ds. WSiSW w dniu 28 września, a Coreper w dniach 24 września i 1 października 2015 r.

7. Rada Europejska zaapelowała w konkluzjach z 25–26 czerwca 2015 r., by pakiet z zakresu ochrony danych przyjąć do końca 2015 r.[7]

8. Na posiedzeniu w dniu 15 czerwca 2015 r. Rada przyjęła podejście ogólne do projektu rozporządzenia. Negocjacje w jego sprawie z Parlamentem Europejskim przebiegają w szybkim tempie i w duchu kompromisu.

---

3 Wniosek w sprawie rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych) (dok. 5853/12).

4 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 (Dz.U. L 281 z 23.11.1995, s. 31–50).

5 Dok. 7428/14.

6 Dok. 7375/12.

7 Zob. dok. EUCO 22/15 pkt 12 ppkt a.

9. Wobec powyższego prezydencja postanowiła do końca 2015 r. zamknąć prace nad oboma projektami z pakietu.

10. Od lipca 2015 r. w pracach nad projektem dyrektywy poczyniono znaczne postępy. Prezydencja uważa, że tekst można już przedłożyć ministrom, tak by przyjęli podejście ogólne, a następnie na tej podstawie można było przystąpić do negocjacji z Parlamentem Europejskim.

II. TEKST KOMPROMISOWY

11. Tekst projektu dyrektywy, który prezydencja przedstawia jako podstawę podejścia ogólnego, znajduje się w załączniku. Wszelkie zmiany wobec pierwotnego wniosku Komisji zaznaczono podkreśleniem, skreślenia – nawiasem (…), a tekst przeniesiony – *kursywą*. Uwagi delegacji do tekstu dyrektywy – niezawierającego jeszcze zmian w motywach 18, 27, 36, 57 i 71 oraz w art. 61 i 62 – znajdują się w dokumencie prezentującym wyniki posiedzenia Komitetu Stałych Przedstawicieli z dnia 1 października 2015 r. (dok. 12643/15).

12. Mając na uwadze wyniki posiedzenia Komitetu Stałych Przedstawicieli z dnia 1 października 2015 r. oraz chcąc uwzględnić wciąż aktualne uwagi delegacji, prezydencja wprowadziła do tekstu dyrektywy następujące zmiany:

i. w motywie 18 skreślono słowa „do celów określonych w niniejszej dyrektywie”;
ii. w motywie 27 słowo „oraz” zastąpiono słowem „lub”;
iii. w motywie 36 skreślono słowo „czasowe”, a dodano słowa „w takim przypadku”;
iv. w motywie 57 dodano zdanie mówiące, że uprawnienia organów nadzorczych nie powinny kolidować ze szczegółowymi przepisami o postepowaniu karnym ani z niezależnością wymiaru sprawiedliwości.

v. zmieniono art. 61, aby zaznaczyć, że podczas oceny stosowania dyrektywy Komisja powinna też ocenić w szczególności funkcjonowanie art. 36aa;

vi. okres wdrażania dyrektywy, przewidziany w art. 62 (i motywie 71), przedłużono do trzech lat.

III. PODSUMOWANIE

13. Wobec powyższego i w duchu kompromisu Rada jest proszona o zatwierdzenie – w celu udzielenia prezydencji mandatu do negocjacji z przedstawicielami Parlamentu Europejskiego – podejścia ogólnego do projektu dyrektywy w załączonej wersji.

ZAŁĄCZNIK

Wniosek

DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich lub ścigania, wykonywania kar kryminalnych lub do celów ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom oraz w sprawie swobodnego przepływu takich danych

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,

po zasięgnięciu opinii Europejskiego Inspektora Ochrony Danych[8],

[8] Dz.U. C […] z [...], s. [...].

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą,

a także mając na uwadze, co następuje:

(1) Ochrona osób fizycznych w zakresie przetwarzania danych osobowych jest jednym z praw podstawowych. Artykuł 8 ust. 1 Karty praw podstawowych Unii Europejskiej oraz art. 16 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej 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.

(3) Szybki rozwój technologiczny i globalizacja skutkują nowymi wyzwaniami w dziedzinie ochrony danych osobowych. Skala zbierania i wymiany danych niezwykle wzrosła. Dzięki technologii (...) można na niespotykaną dotąd skalę wykorzystywać dane osobowe do (...) czynności takich, jak zapobieganie przestępstwom, prowadzenie dochodzeń w ich sprawie, wykrywanie ich lub ściganie lub wykonywanie kar kryminalnych.

(4) W związku z tym należy ułatwić swobodny przepływ danych między właściwymi organami do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich lub ścigania*, wykonywania kar kryminalnych* lub do celów ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom na terytorium Unii oraz przekazywanie danych do państw trzecich i organizacji międzynarodowych, a równocześnie zagwarantować wysoki poziom ochrony danych osobowych. Przemiany te wymagają budowy stabilnych, spójniejszych ram ochrony danych w Unii oraz zdecydowanego egzekwowania ich przepisów.

(5) 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[9] ma zastosowanie do wszystkich czynności przetwarzania danych w państwach członkowskich, zarówno w sektorze publicznym, jak i prywatnym. Nie ma ona jednak zastosowania do przetwarzania danych osobowych „w ramach działalności wykraczającej poza zakres prawa Wspólnoty", takiej jak działalność w ramach współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej.

[9] Dz.U. L 281, z 23.11.1995, s. 31.

(6) Decyzja ramowa Rady 2008/977/WSiSW z dnia 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych[10] ma zastosowanie do współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej. Jednak zakres zastosowania tej decyzji ramowej jest ograniczony do przetwarzania danych osobowych przekazywanych lub udostępnianych pomiędzy państwami członkowskimi.

(7) Zapewnienie spójnego, wysokiego poziomu ochrony danych osobowych osób fizycznych oraz ułatwienie wymiany danych osobowych między właściwymi organami państw członkowskich ma zasadnicze znaczenie dla zagwarantowania skutecznej współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej. Zatem należy we wszystkich państwach członkowskich zapewnić równorzędny poziom ochrony praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich lub ścigania*, wykonywania kar kryminalnych* lub do celów ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom. Aby ochrona danych osobowych w Unii była skuteczna, należy wzmocnić prawa podmiotów danych oraz obowiązki podmiotów przetwarzających dane osobowe, ale też zapewnić równorzędne uprawnienia do monitorowania i egzekwowania przepisów o ochronie danych osobowych w państwach członkowskich.

(8) Artykuł 16 ust. 2 Traktatu o funkcjonowaniu Unii Europejskiej powierza Parlamentowi Europejskiemu i Radzie określenie zasad ochrony osób fizycznych w związku z przetwarzaniem danych osobowych oraz zasad swobodnego przepływu takich danych.

(9) Na tej podstawie rozporządzenie Parlamentu Europejskiego i Rady UE …../XXX w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (ogólne rozporządzenie o ochronie danych) ustanawia ogólne przepisy mające chronić osoby fizyczne w związku z przetwarzaniem danych osobowych oraz zagwarantować swobodny przepływ danych osobowych w Unii.

---

10 Dz.U. L 350 z 30.12.2008, s. 60.

(10) W deklaracji 21 w sprawie ochrony danych osobowych w dziedzinie współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej – załączonej do Aktu końcowego konferencji międzyrządowej, która przyjęła Traktat z Lizbony – konferencja uznała, że ze względu na szczególny charakter współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej konieczne może okazać się przyjęcie – na podstawie art. 16 Traktatu o funkcjonowaniu Unii Europejskiej – szczególnych przepisów o ochronie danych osobowych i ich swobodnym przepływie w tych dziedzinach.

(11) Dlatego szczególny charakter tych dziedzin należy uwzględnić w odrębnej dyrektywie, ustanawiając przepisy o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich lub ścigania *lub wykonywania kar kryminalnych*. Takimi właściwymi organami mogą być nie tylko organy publiczne – takie jak organy wymiaru sprawiedliwości, policja lub inne organy egzekwowania prawa – ale też m.in. wszelkie organy/podmioty, którym prawo krajowe powierza realizację obowiązków publicznych lub uprawnień publicznych na potrzeby zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich lub ścigania lub *wykonywania kar kryminalnych*. Jeżeli jednak taki organ/podmiot przetwarza dane osobowe do celów innych niż realizacja obowiązków publicznych lub uprawnień publicznych na potrzeby zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich lub ścigania *lub wykonywania kar kryminalnych*, zastosowanie ma rozporządzenie UE/XXX. Zatem rozporządzenie UE/XXX ma zastosowanie wtedy, gdy organ/podmiot zbiera dane osobowe do innych celów, a następnie dalej te dane przetwarza z uwagi na obowiązek prawny, któremu podlega, *np.* gdy instytucje finansowe zatrzymują na potrzeby dochodzenia, wykrywania i ścigania określone przetwarzane przez siebie dane i udostępniają je tylko właściwym organom krajowym w konkretnych sytuacjach i w zgodzie z prawem krajowym. Organ/podmiot, który w imieniu takich organów przetwarza dane osobowe w ramach niniejszej dyrektywy, powinien podlegać umowie lub innemu aktowi o mocy prawnej oraz przepisom mającym zgodnie z niniejszą dyrektywą zastosowanie do podmiotu przetwarzającego, podczas gdy we wszelkich czynnościach przetwarzania spoza zakresu niniejszej dyrektywy podmiot przetwarzający powinien nadal podlegać rozporządzeniu UE/XXX.

(11a) Czynności policji lub innych organów egzekwowania prawa koncentrują się na zapobieganiu przestępstwom, prowadzeniu dochodzeń w ich sprawie, wykrywaniu ich lub ściganiu, w tym na działaniach, przy których nie wiadomo jeszcze, czy dane zdarzenie jest przestępstwem. Czynności te mogą też polegać na sprawowaniu władzy środkami przymusu, np. gdy policja podejmuje działania podczas demonstracji, dużych imprez sportowych czy zamieszek.
Czynności te, wykonywane przez wymienione wyżej organy, obejmują też utrzymywanie prawa i porządku jako zadanie powierzone policji lub innym organom egzekwowania prawa, gdy jest to konieczne do ochrony przed zagrożeniami dla bezpieczeństwa publicznego i do zapobiegania takim zagrożeniom i ma zapobiegać zachowaniom mogącym zagrażać podstawowym, prawnie chronionym interesom społecznym i skutkować przestępstwem.

Państwa członkowskie mogą powierzyć właściwym organom inne zadania, które niekoniecznie służą zapobieganiu przestępstwom, prowadzeniu dochodzeń w ich sprawie, ich wykrywaniu lub ściganiu, lub ochronie przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganiu takim zagrożeniom; tym sposobem przetwarzanie danych osobowych w związku z tymi innymi zadaniami – o ile mieści się w zakresie prawa Unii – będzie wchodzić w zakres (…) rozporządzenia (…) UE/XXX.

(11aa) Pojęcie „przestępstwa” w rozumieniu niniejszej dyrektywy powinno być autonomicznym pojęciem prawa unijnego, zgodnie z wykładnią Trybunału Sprawiedliwości Unii Europejskiej.

(11b) Niniejsza dyrektywa nie powinna mieć zastosowania do przetwarzania danych osobowych w toku działalności wykraczającej poza zakres prawa Unii, dlatego nie należy czynności w zakresie bezpieczeństwa narodowego, czynności agencji lub jednostek zajmujących się bezpieczeństwem narodowym ani przetwarzania danych osobowych przez państwa członkowskie podczas czynności, które wchodzą zakres zastosowania tytułu V rozdział 2 Traktatu o Unii Europejskiej, (…) uznawać za czynności mieszczące się w zakresie niniejszej dyrektywy.

(12) Aby zagwarantować jednakowy poziom ochrony osób fizycznych poprzez prawnie egzekwowalne prawa obowiązujące w całej Unii oraz aby zapobiec różnicom utrudniającym wymianę danych osobowych między właściwymi organami, niniejsza dyrektywa powinna przewidywać zharmonizowane przepisy o ochronie i swobodnym przepływie danych osobowych przetwarzanych do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich lub ścigania, *wykonywania kar kryminalnych* lub do celów ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom. Zbliżenie przepisów państw członkowskich nie powinno skutkować osłabieniem gwarantowanej przez nie ochrony danych, a wręcz przeciwnie – powinno służyć zapewnieniu wysokiego poziomu ochrony w całej Unii. Państwa członkowskie powinny także móc ustanawiać gwarancje wyższe od przewidzianych w niniejszej dyrektywie dla ochrony praw i wolności podmiotu danych w związku z przetwarzaniem danych osobowych przez właściwe organy.

(13) Niniejsza dyrektywa nie narusza **(...)** zasady publicznego dostępu do dokumentów urzędowych (...). (...) W myśl rozporządzenia UE/XXX dane osobowe zawarte w dokumentach urzędowych posiadanych przez organ lub podmiot publiczny lub podmiot prywatny do 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 (...).

(14) Niniejsza dyrektywa zapewnia ochronę osobom fizycznym – niezależnie od ich obywatelstwa czy miejsca zamieszkania – w związku z przetwarzaniem ich danych osobowych.

(15) Ochrona osób fizycznych powinna być technologicznie neutralna i niezależna od stosowanych technologii (...); w przeciwnym razie zachodziłoby 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 zorganizowane według określonych kryteriów, nie powinny wchodzić w zakres niniejszej dyrektywy.

(...)

(15a) Do przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne Unii ma zastosowanie rozporządzenie (WE) nr 45/2001[11]. Rozporządzenie (WE) nr 45/2001 oraz inne unijne akty prawne mające zastosowanie do takiego przetwarzania danych osobowych należy dostosować do zasad i przepisów rozporządzenia UE/XXX.

---

11 Dz.U. L 8 z 12.1.2001, s. 1.

(15b) **(…)** Niniejsza dyrektywa nie powinna stanowić dla państw członkowskich przeszkody w określaniu – w krajowym prawie karnym procesowym – operacji i procedur przetwarzania danych osobowych przez sądy i inne organy wymiaru sprawiedliwości, zwłaszcza danych osobowych ujmowanych w orzeczeniach sądowych lub aktach związanych z postępowaniem karnym.

(16) Zasady ochrony danych powinny mieć zastosowanie do wszelkich informacji o zidentyfikowanych lub możliwych do zidentyfikowania osobach fizycznych. Aby stwierdzić, czy dana osoba fizyczna 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 technologię 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 nie można już zidentyfikować.

(16a) Dane genetyczne należy zdefiniować jako dane osobowe o odziedziczonych lub nabytych cechach genetycznych osoby fizycznej, **(...)** ujawniające niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i wynikające w szczególności z analizy chromosomów, kwasu dezoksyrybonukleinowego (DNA) lub kwasu rybonukleinowego (RNA) lub z analizy wszelkich innych materiałów umożliwiających pozyskanie równoważnych informacji. (...)

(17) 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, niezależnie od ich źródła, którym może być na przykład lekarz lub inny pracownik służby zdrowia, szpital, urządzenie medyczne lub badanie diagnostyczne *in vitro*.

(18) Wszelkie przetwarzanie danych osobowych musi być (...) zgodne z prawem i rzetelne względem zainteresowanej osoby fizycznej oraz służyć wyłącznie konkretnym celom określonym prawem. Sama zasada rzetelnego przetwarzania nie zabrania organom egzekwowania prawa prowadzić czynności takich, jak niejawne dochodzenie czy nadzór wideo. Czynności takie można prowadzić do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich lub ścigania, wykonywania kar kryminalnych lub do celów ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom, jeżeli czynności te są określone prawem i stanowią niezbędne i proporcjonalne działanie w społeczeństwie demokratycznym – przy należytym uwzględnieniu uzasadnionych interesów danej osoby fizycznej. Zasada rzetelnego przetwarzania obowiązująca w ochronie danych jest pojęciem odrębnym względem prawa do rzetelnego procesu, które jest zdefiniowane w art. 6 europejskiej „Konwencji o ochronie praw człowieka i podstawowych wolności" i w art. 47 Karty praw podstawowych. Osobom fizycznym należy uświadomić zagrożenia, zasady, gwarancje i prawa związane z przetwarzaniem ich danych osobowych oraz sposoby korzystania z praw przysługujących im w związku z tym przetwarzaniem. Jednoznaczne, uzasadnione i określone w momencie zbierania danych powinny być w szczególności konkretne cele ich przetwarzania. Dane powinny być ilościowo i treściowo (...) odpowiednie do celów przetwarzania; w szczególności należy dopilnować, by zebrane dane nie były nadmierne i by okres ich przechowywania był nie dłuższy, niż jest to niezbędne do osiągnięcia celu ich przetwarzania (...). 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. Państwa członkowskie powinny ustanowić odpowiednie gwarancje dla danych osobowych przechowywanych dłużej do użytku archiwizacyjnego w interesie publicznym, naukowego, statystycznego lub historycznego.

(19) Zapobieganie przestępstwom, prowadzenie dochodzeń w ich sprawie i ich ściganie wymaga, aby właściwe organy (...) przetwarzały dane osobowe – zebrane w kontekście zapobiegania konkretnym przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich lub ścigania – w kontekście szerszym, tak by zrozumieć zjawiska i tendencje przestępcze, zbierać informacje wywiadowcze o zorganizowanych sieciach przestępczych oraz wzajemnie kojarzyć różne wykryte przestępstwa.

(19a) Aby zapewnić bezpieczeństwo przetwarzania i zapobiegać przetwarzaniu niezgodnemu z niniejszą dyrektywą, dane osobowe należy przetwarzać tak, by zapewnić odpowiedni poziom bezpieczeństwa i poufności, w tym chronić przed nieuprawnionym dostępem do nich samych i do sprzętu służącego ich przetwarzaniu lub przed nieuprawnionym korzystaniem z tych danych i tego sprzętu, biorąc pod uwagę najnowsze zmiany w odnośnej dziedzinie, technologię i koszty wdrożeniowe względem ryzyka i charakteru danych osobowych wymagających ochrony.

(20) (...)

(20a) Dane osobowe należy zbierać w konkretnych, jednoznacznych i uzasadnionych celach mieszczących się w zakresie zastosowania niniejszej dyrektywy i nie należy ich przetwarzać w celach niezgodnych z zapobieganiem przestępstwom, prowadzeniem dochodzeń w ich sprawie, wykrywaniem ich lub ściganiem, wykonywaniem kar kryminalnych lub z ochroną przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganiem takim zagrożeniom. Jeżeli dane osobowe przetwarza ten sam lub inny administrator do celu mieszczącego się w zakresie zastosowania niniejszej dyrektywy, ale innego niż cel, w którym dane zostały zebrane, przetwarzanie takie jest zgodne z niniejszą dyrektywą, o ile jest dozwolone na mocy mających zastosowanie przepisów prawa oraz jest niezbędne i proporcjonalne do tego innego celu.

(21) Zasadę ścisłości danych należy stosować, uwzględniając charakter i cel odnośnego przetwarzania. Ponieważ przetwarza się dane dotyczące różnych kategorii podmiotów danych, *właściwe **(...)** organy (...) powinny w jak największym stopniu rozróżniać dane osobowe różnych kategorii tych podmiotów, takich jak osoby skazane za przestępstwo, osoby podejrzane, (...) ofiary i strony trzecie*. W szczególności w postępowaniu sądowym oświadczenia zawierające dane osobowe opierają się na subiektywnym osądzie osób fizycznych i są w pewnych przypadkach nieweryfikowalne. Dlatego wymóg ścisłości danych nie powinien odnosić się do ścisłości oświadczenia, lecz jedynie do faktu, że dane oświadczenie zostało złożone.

(22) Interpretując i stosując przepisy niniejszej dyrektywy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich, ścigania*, wykonywania kar kryminalnych* lub do celów ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom, właściwe organy (...) powinny uwzględniać specyfikę sektora, w tym konkretne wytyczone cele.

(23) (…)

(24) (...) Właściwe organy powinny dopilnować, by nieścisłe, niekompletne lub nieaktualne dane osobowe nie były przekazywane ani udostępniane. (…) Aby zapewnić ochronę osób fizycznych oraz ścisłość, kompletność, aktualność (...) i rzetelność przekazywanych lub udostępnianych danych osobowych, (...) właściwe organy powinny w miarę możliwości opatrywać wszelkie przekazywane dane osobowe niezbędnymi informacjami.

(24a) Ilekroć w niniejszej dyrektywie 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.

(24b) Pojęcie „przetwarzanie danych osobowych przez właściwe organy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich lub ścigania, wykonywania kar kryminalnych lub do celów ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom" powinno obejmować każdą operację lub każdy zestaw operacji, które wykonuje się do wspomnianych celów na danych osobowych lub na ich zestawach w sposób zautomatyzowany lub nie, takie jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie. W szczególności przepisy niniejszej dyrektywy powinny mieć zastosowanie do przekazywania danych osobowych, które służy celom określonym w niniejszej dyrektywie, do odbiorców niepodlegających niniejszej dyrektywie. (…) „Odbiorca" powinien tu oznaczać osobę fizyczną lub prawną, organ publiczny, jednostkę organizacyjną lub inny podmiot, któremu właściwy organ ujawnia te dane (…) zgodnie z prawem. Jeżeli właściwy organ pierwotnie zebrał dane do jednego z celów określonych w niniejszej dyrektywie, to do przetwarzania tych danych do celów innych niż określone w niniejszej dyrektywie – jeżeli przetwarzanie to jest dozwolone przez prawo Unii lub prawo państwa członkowskiego – powinno mieć zastosowanie rozporządzenie UE/XXX **(…)**.
W szczególności przepisy rozporządzenia UE/XXX powinny mieć zastosowanie do przekazywania danych osobowych do celów niemieszczących się w zakresie zastosowania niniejszej dyrektywy.
Do przetwarzania danych osobowych przez odbiorcę, który nie stanowi lub nie pełni funkcji właściwego organu w rozumieniu niniejszej dyrektywy i któremu właściwy organ ujawnia dane osobowe zgodnie z prawem, zastosowanie powinno mieć (…) rozporządzenie (…) UE/XXX.
Transponując niniejszą dyrektywę, państwa członkowskie mogą też doprecyzować zastosowanie przepisów rozporządzenia UE/XXX pod warunkami określonymi w rozporządzeniu UE/XXX.

(25) Aby przetwarzanie danych osobowych w ramach niniejszej dyrektywy było zgodne z prawem, powinno ono być niezbędne do (...) wykonania zadania realizowanego przez właściwy organ w interesie publicznym na podstawie prawa Unii lub prawa państwa członkowskiego do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich lub ścigania , *wykonywania kar kryminalnych* lub do celów ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom, co dotyczy też przetwarzania niezbędnego (...) do ochrony żywotnych interesów podmiotu danych lub innej osoby **(...)**. Wykonywanie zadania polegającego na zapobieganiu przestępstwom, prowadzeniu dochodzeń w ich sprawie, wykrywaniu ich lub ściganiu, instytucjonalnie powierzonego na mocy prawa właściwym organom, pozwala tym organom wymagać/nakazywać, aby osoby fizyczne zastosowały się do stawianych żądań. W takich przypadkach zgoda podmiotu danych (określona w rozporządzeniu UE/XXX) nie powinna stanowić podstawy prawnej przetwarzania danych osobowych przez właściwe organy (...). Ilekroć podmiot danych musi wywiązać się z obowiązku prawnego, nie ma on faktycznego, swobodnego wyboru, zatem jego reakcji nie należy traktować jako swobodnego wyrazu jego woli. Nie powinno to stanowić dla państw członkowskich przeszkody w stanowieniu prawem, że (…) podmiot danych może (…) wyrazić zgodę na przetwarzanie jego danych osobowych do celów określonych w niniejszej dyrektywie – przetwarzanie takie jak badania DNA w dochodzeniu karnym czy (…) monitorowanie miejsca pobytu podmiotu danych za pomocą aparatury elektronicznej w ramach kary kryminalnej. (…)

(25a) Państwa członkowskie powinny przewidzieć prawem, że ilekroć prawo unijne lub krajowe mające zastosowanie do właściwego organu przekazującego (...) stawia w określonych sytuacjach szczególne wymogi co do przetwarzania danych osobowych, jak np. stosowanie kodeksów postępowania, organ przekazujący (...) powinien o takich wymogach i o obowiązku ich przestrzegania poinformować odbiorcę, któremu przekazuje dane. Wymogi takie mogą np. przewidywać, że odbiorca, któremu przekazuje się dane, nie przekazuje tych danych dalej, nie wykorzystuje ich do innych celów ani nie informuje podmiotu danych o ograniczeniu prawa do informacji bez uprzedniej zgody właściwego organu przekazującego. Wymogi te dotyczą także przekazywania danych odbiorcom w państwach trzecich lub organizacjach międzynarodowych. Państwa członkowskie powinny przewidzieć prawem, że właściwy organ przekazujący (...) nie stosuje względem odbiorców w innych państwach członkowskich ani w organach i jednostkach organizacyjnych ustanowionych na mocy tytułu V rozdział IV i V Traktatu o funkcjonowaniu Unii Europejskiej wymogów **(...)** innych niż mające zastosowanie do podobnego (...) przekazywania danych w obrębie państwa członkowskiego właściwego organu przekazującego.

(26) 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 niniejszej dyrektywie terminu „pochodzenie rasowe" nie oznacza, że Unia Europejska akceptuje teorie sugerujące istnienie osobnych ras ludzkich. Danych takich nie należy przetwarzać, chyba że przetwarzanie podlega odpowiednim, określonym prawem gwarancjom dla praw i wolności podmiotu danych i jest dozwolone w (…) przypadkach dopuszczonych prawem (...), a jeżeli nie jest dopuszczone takim prawem – jest niezbędne do ochrony żywotnych interesów podmiotu danych lub innej osoby, (...) albo też dotyczy danych ewidentnie upublicznionych przez sam podmiot danych. (...) Odpowiednie gwarancje dla praw i wolności podmiotu danych mogą m.in. polegać na tym, że odnośne dane wolno zbierać tylko w połączeniu z innymi danymi zainteresowanej osoby fizycznej, że zebrane dane należy właściwie zabezpieczyć, że dostęp pracowników właściwego organu (...) do danych jest rygorystyczniej regulowany lub że danych tych nie wolno przekazywać. Przetwarzanie takich danych powinno być także dozwolone prawem, jeżeli ich podmiot udzielił wyraźnej zgody, w przypadkach gdy przetwarzanie danych jest szczególnie inwazyjne dla osób fizycznych. Niemniej sama zgoda podmiotu danych nie powinna stanowić podstawy prawnej przetwarzania takich newralgicznych danych osobowych przez właściwe organy (...).

(27) 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 niekorzystne skutki prawne lub znacznie na niego wpływa. Przetwarzanie takie powinno zawsze podlegać odpowiednim gwarancjom, w tym konkretnemu informowaniu podmiotu danych i prawu do uzyskania interwencji ludzkiej, a zwłaszcza prawu do wyrażenia własnego stanowiska, prawu do uzyskania wyjaśnienia co do decyzji wynikłej z takiej oceny lub prawu do zakwestionowania takiej decyzji.

(28) Aby podmiot danych mógł korzystać ze swoich praw, wszelkie kierowane do niego informacje powinny być łatwo dostępne (m.in. na stronie internetowej administratora) i zrozumiałe (sformułowane jasnym i prostym językiem).

(29) Należy przewidzieć tryb ułatwiający podmiotowi danych korzystanie z jego praw na mocy przepisów przyjętych zgodnie z niniejszą dyrektywą – w tym mechanizmy bezpłatnego składania wniosków (...) o dostęp do danych czy o ich poprawienie, usunięcie i ograniczenie ich przetwarzania. Administrator powinien mieć obowiązek odpowiadać na wnioski podmiotu danych bez zbędnej zwłoki. 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. (…)

(30) (...) Podmiotowi danych należy udostępnić przynajmniej informacje o: (...) tożsamości administratora, prowadzeniu operacji przetwarzania, (...) celach przetwarzania (...) oraz (...) prawie do wniesienia skargi. (...) Można to uczynić na stronie internetowej właściwego organu.

(31) (...)

(32) Każda osoba fizyczna powinna mieć prawo dostępu do zebranych danych jej dotyczących oraz powinna móc łatwo korzystać z tego prawa w rozsądnych odstępach czasu, by wiedzieć o przetwarzaniu danych i móc zweryfikować jego zgodność z prawem. Dlatego każdy podmiot danych powinien mieć prawo, by znać w szczególności cele przetwarzania danych, (...) okres ich przetwarzania, ich odbiorców (także w państwach trzecich) oraz by otrzymywać odnośne informacje. (...) Aby prawo to wypełnić, wystarczy przekazać wnioskodawcy pełne podsumowanie tych danych w zrozumiałej formie, czyli w formie pozwalającej mu poznać te dane, sprawdzić ich ścisłość oraz zweryfikować zgodność ich przetwarzania z niniejszą dyrektywą, tak by w stosownym przypadku mógł on skorzystać z praw przysługujących mu na mocy niniejszej dyrektywy.

(33) Należy zezwolić państwom członkowskim na przyjmowanie środków legislacyjnych pozwalających opóźnić, ograniczyć lub pominąć informowanie podmiotów danych lub ich dostęp do własnych danych osobowych w takim zakresie i przez taki czas, w jakim (...) odnośny środek jest działaniem niezbędnym i proporcjonalnym w społeczeństwie demokratycznym – przy należytym uwzględnieniu uzasadnionych interesów danej osoby fizycznej – tak aby uniemożliwić utrudnianie urzędowych lub prawnych dochodzeń, śledztw lub procedur, aby uniemożliwić szkodzenie zapobieganiu przestępstwom, ich wykrywaniu, prowadzeniu dochodzeń w ich sprawie, ich ściganiu lub wykonywaniu kar kryminalnych, aby chronić bezpieczeństwo publiczne lub narodowe lub aby chronić (...) prawa i wolności innych osób.

(34) O wszelkiej odmowie lub wszelkim ograniczeniu dostępu należy zasadniczo powiadomić podmiot danych na piśmie, podając również faktyczne i prawne powody decyzji.

(35) (...)

(36) Każda osoba fizyczna powinna mieć prawo spowodować, by dotyczące jej nieścisłe dane osobowe – zwłaszcza faktograficzne – zostały poprawione, a jeżeli przetwarzanie jej danych osobowych jest niezgodne z przepisami niniejszej dyrektywy – by zostały usunięte. Niemniej prawo do poprawienia danych nie powinno dotyczyć na przykład treści zeznania świadka. Każda osoba fizyczna (...) może też mieć prawo spowodować, by przetwarzanie elementu jej danych osobowych zostało ograniczone, jeżeli jego ścisłość jest kwestionowana. W szczególności należy zamiast usuwania danych osobowych ograniczyć ich przetwarzanie, jeżeli w konkretnym przypadku racjonalne przesłanki sugerują, że usunięcie mogłoby wpłynąć na uzasadnione interesy podmiotu danych. W takim przypadku dane o ograniczonym przetwarzaniu należy przetwarzać tylko w celu, który uniemożliwił ich usunięcie. Wśród metod pozwalających ograniczyć przetwarzanie danych osobowych mogą się znaleźć między innymi: (…) przeniesienie wybranych danych do innego systemu przetwarzania – np. do celów archiwizacyjnych – lub uniemożliwienie użytkownikom dostępu do wybranych danych. 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.

(36a) Jeżeli administrator odmawia podmiotowi danych prawa do dostępu, poprawienia, usunięcia lub ograniczenia przetwarzania danych, (...) podmiot danych powinien mieć prawo wystąpienia z wnioskiem, by (...) krajowy organ nadzorczy sprawdził zgodność przetwarzania z prawem. O prawie tym należy poinformować podmiot danych. Jeżeli (...) organ nadzorczy podejmie interwencję w imieniu podmiotu danych, powinien on poinformować ten podmiot przynajmniej o fakcie przeprowadzenia wszelkich niezbędnych weryfikacji lub kontroli. (...)

(36aa) *Jeżeli dane osobowe przetwarza się w toku dochodzenia karnego i* sądowego *postępowania* karnego*, (...) korzystanie z prawa do informacji, dostępu, poprawienia, usunięcia i ograniczenia przetwarzania może się odbywać zgodnie z krajowymi przepisami o postępowaniu sądowym.*

(37) 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 przepisami przyjętymi na podstawie niniejszej dyrektywy. Środki te powinny uwzględniać charakter, zakres, kontekst i cele przetwarzania oraz zagrożenie dla praw i wolności podmiotów danych. Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, wśród środków tych powinna się znaleźć realizacja odpowiednich strategii ochrony danych. Strategie te powinny przewidywać stosowanie przepisów, które w dziedzinie ochrony danych przyjęto na podstawie niniejszej dyrektywy.

(37a) (...) Z przetwarzania danych mogą wynikać zagrożenia, o różnym prawdopodobieństwie i różnej powadze, dla praw i wolności podmiotu danych, to zaś może 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; 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, przekonania religijne lub światopoglądowe, 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.

(37b) 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 podmiotów danych.

(38) Ochrona praw i wolności podmiotów danych w kontekście przetwarzania danych osobowych wymaga wdrożenia odpowiednich środków technicznych i organizacyjnych, by zapewnić spełnienie wymogów dyrektywy. Aby móc wykazać przestrzeganie przepisów przyjętych na podstawie niniejszej dyrektywy, 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. Środki takie mogą polegać między innymi na stosowaniu jak najszybszej pseudonimizacji. Stosowanie pseudonimizacji do celów niniejszej dyrektywy może być […] narzędziem ułatwiającym zwłaszcza swobodny przepływ odnośnych danych w przestrzeni wolności, bezpieczeństwa i sprawiedliwości.

(39) 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 niniejszej dyrektywy 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.

(39a) Przetwarzanie przez podmiot przetwarzający powinno być regulowane aktem o mocy prawnej, na przykład umową, wiążącym podmiot przetwarzający z administratorem i przewidującym w szczególności, że podmiot przetwarzający (...) powinien działać wyłącznie na polecenie administratora.

(40) Administrator (...) i podmiot przetwarzający powinni rejestrować kategorie czynności przetwarzania danych osobowych – w tym przekazywanie danych pod odpowiednimi gwarancjami i w określonych sytuacjach – by umożliwić monitorowanie przestrzegania niniejszej dyrektywy. Każdy administrator i każdy podmiot przetwarzający powinni mieć obowiązek współpracować z organem nadzorczym i na żądanie udostępniać mu wspomniane rejestry do monitorowania operacji przetwarzania.

(40a) Ewidencjonować należy przynajmniej operacje dokonywane w zautomatyzowanych systemach przetwarzania, takie jak zbieranie, modyfikowanie, przeglądanie, ujawnianie, łączenie i usuwanie. Ewidencji należy używać do weryfikacji zgodności przetwarzania danych z prawem, do monitorowania własnej działalności oraz do gwarantowania integralności i bezpieczeństwa danych. (...) Nie stanowi to zakazu używania takiej ewidencji (...) zgodnie z prawem państwa członkowskiego do celów operacyjnych w trakcie dochodzeń i postępowań karnych.

(41) Aby zapewnić skuteczną ochronę praw i wolności podmiotów danych, (...), administrator lub podmiot przetwarzający powinni w określonych przypadkach konsultować się z organem nadzorczym przed zamierzonym przetwarzaniem.

(42) 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, naruszenie dobrego imienia, niedozwolone cofnięcie pseudonimizacji, naruszenie poufności danych chronionych tajemnicą służbową lub wszelkie inne znaczne szkody gospodarcze lub społeczne. Dlatego zaraz po stwierdzeniu (...) naruszenia ochrony danych osobowych, które może przysporzyć (...) szkód fizycznych, materialnych lub moralnych, administrator powinien bez zbędnej zwłoki zgłosić naruszenie organowi nadzorczemu. Osoby, na których (...) prawa i wolności (...) naruszenie takie mogłoby poważnie wpłynąć, należy bez zbędnej zwłoki zawiadomić, tak by mogły podjąć niezbędne środki ostrożności (...).

(43) Zawiadomienie podmiotu danych o naruszeniu ochrony danych osobowych nie powinno być wymagane, jeżeli administrator wdrożył odpowiednie techniczne środki ochrony i środki te były 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. Zawiadomienie podmiotu danych nie jest również wymagane, jeżeli administrator przedsięwziął późniejsze środki, by wyeliminować prawdopodobieństwo dużego zagrożenia dla praw i wolności odnośnych podmiotów danych (...).

(44) (...) Administratora lub podmiot przetwarzający może wspomagać w monitorowaniu wewnętrznego przestrzegania przepisów przyjętych na podstawie niniejszej dyrektywy osoba dysponująca wiedzą fachową na temat prawa i praktyk w dziedzinie ochrony danych. Osoba ta może dostarczać administratorowi lub podmiotowi przetwarzającemu oraz pracownikom, którzy przetwarzają dane osobowe, informacji i porad na temat spoczywających na nich obowiązków ochrony danych. Kilka właściwych organów lub podmiotów (...) może, uwzględniając swoją strukturę organizacyjną i wielkość, wspólnie wyznaczyć jednego inspektora ochrony danych (...). Taki inspektor ochrony danych musi być w stanie wykonywać swoje obowiązki i zadania w sposób niezależny (...).

(45) Państwa członkowskie powinny zadbać o to, by dane były przekazywane do państwa trzeciego lub organizacji międzynarodowej tylko wtedy, gdy jest to konieczne do zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich lub ścigania*, wykonywania kar kryminalnych* lub (...) do ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom i gdy administrator w państwie trzecim lub w organizacji międzynarodowej jest organem właściwym w rozumieniu niniejszej dyrektywy. Przekazanie może nastąpić w przypadkach, w których Komisja zdecydowała, że dane państwo trzecie lub organizacja międzynarodowa zapewniają odpowiedni poziom ochrony albo gdy wprowadzono odpowiednie gwarancje lub mają zastosowanie odstępstwa w szczególnych sytuacjach.

(45a) Przekazywanie danych osobowych z któregokolwiek państwa członkowskiego do państw trzecich lub (...) organizacji międzynarodowych powinno zasadniczo odbywać się wyłącznie za zgodą państwa członkowskiego, od którego te dane uzyskano. Jeżeli zagrożenie dla bezpieczeństwa publicznego państwa członkowskiego lub państwa trzeciego lub dla ważnych interesów państwa członkowskiego jest tak nagłe, że nie da się na czas uzyskać uprzedniej zgody, wtedy z uwagi na efektywność współpracy w dziedzinie egzekwowania prawa właściwy organ (...) *powinien móc przekazać odnośne dane osobowe do danego państwa trzeciego lub danej organizacji międzynarodowej bez takiej uprzedniej zgody.* Państwa członkowskie powinny przewidzieć prawem, że należy informować państwa trzecie lub organizacje międzynarodowe o wszelkich specjalnych wymogach dotyczących przekazania.

(46) Jeżeli Komisja nie przyjęła decyzji, o której mowa w art. 41 rozporządzenia (UE) XXX, może ona stwierdzić ze skutkiem dla całej Unii, że niektóre państwa trzecie – albo też terytorium lub co najmniej jeden określony sektor w państwie trzecim – bądź organizacja międzynarodowa zapewniają 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.

(47) Zgodnie z podstawowymi wartościami, na których opiera się Unia, w szczególności z ochroną praw człowieka, Komisja powinna wziąć pod uwagę stopień, w jakim 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.

(48) Komisja powinna mieć również możliwość uznania, że państwo trzecie – albo 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. 35–36. Należy przewidzieć procedury konsultacji 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.

(49) Przekazanie, które nie opiera się na decyzji stwierdzającej odpowiedni poziom ochrony, powinno być dopuszczalne jedynie wtedy, gdy w prawnie wiążącym (...) akcie wprowadzono odpowiednie gwarancje zapewniające ochronę danych osobowych lub gdy administrator (...) ocenił wszystkie okoliczności towarzyszące (...) przekazaniu danych (...) i na podstawie tej oceny stwierdza, że istnieją odpowiednie gwarancje ochrony danych osobowych. Takim prawnie wiążącym aktem może być np. prawnie wiążąca umowa dwustronna, która została zawarta przez państwo członkowskie i wprowadzona przez nie do jego porządku prawnego, która może być egzekwowana przez jego podmioty danych i która zapewnia (...) przestrzeganie wymogów ochrony danych oraz praw podmiotów danych, w tym prawa do skutecznych administracyjnych lub sądowych środków ochrony prawnej. Oceniając wszystkie okoliczności towarzyszące przekazaniu danych, administrator może wziąć pod uwagę umowy o współpracy zawarte przez Europol lub Eurojust z państwami trzecimi, przewidujące wymianę danych osobowych. Administrator może też wziąć pod uwagę to, czy przekazane dane osobowe będą podlegać wymogom poufności i zasadzie celowości, tak że nie będą przetwarzane do celów innych niż cele, w których zostały przekazane. Ponadto administrator powinien wziąć pod uwagę to, czy dane osobowe nie posłużą do zażądania, orzeczenia lub wykonania kary śmierci ani do żadnego innego okrutnego lub nieludzkiego traktowania. Kryteria te można uznać za odpowiednie gwarancje umożliwiające przekazanie danych, niemniej administrator może zażądać gwarancji dodatkowych.

(49a) (...)

(49aa) Jeżeli nie ma decyzji stwierdzającej odpowiedni poziom ochrony ani nie ma odpowiednich gwarancji, przekazanie lub określona kategoria przekazań może nastąpić tylko w szczególnych sytuacjach, gdy jest to konieczne, by chronić żywotne interesy podmiotu danych lub innej osoby lub by zabezpieczyć uzasadnione interesy podmiotu danych zgodnie z wymogami prawa państwa członkowskiego przekazującego dane osobowe, lub gdy jest to niezbędne, by zapobiec bezpośredniemu, poważnemu zagrożeniu dla bezpieczeństwa publicznego państwa członkowskiego lub państwa trzeciego, lub niezbędne, by w indywidualnych przypadkach zapobiegać przestępstwom, prowadzić dochodzenia w ich sprawie, wykrywać je lub ścigać, *wykonywać kary kryminalne* (...) lub prowadzić ochronę przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegać takim zagrożeniom, lub niezbędne, by w indywidualnych przypadkach (...) ustalić roszczenia prawne, realizować je i ich bronić.

(49b) Właściwe organy państw członkowskich stosują (…) obowiązujące dwu- lub wielostronne umowy międzynarodowe zawarte z państwami trzecimi w dziedzinie współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej, by wymieniać (...) istotne informacje do wykonywania prawnie ciążących na nich obowiązków. Odbywa się to zasadniczo dzięki reagowaniu właściwych organów odnośnych państw trzecich lub przynajmniej we współpracy z tymi organami. Niemniej w (...) konkretnych indywidualnych przypadkach może się zdarzyć, że procedury przewidziane w mających zastosowanie umowach międzynarodowych nie pozwalają szybko wymieniać (...) istotnych informacji, tak że właściwe organy państw członkowskich muszą dane osobowe przekazywać bezpośrednio odbiorcom mającym siedzibę w państwach trzecich. Tak może być (...), gdy przestępstwo zostało popełnione przy pomocy elektronicznej technologii komunikacyjnej (np. sieci społecznościowej) lub gdy dane wygenerowane technologią komunikacyjną są istotne jako dowód popełnienia przestępstwa, lub gdy zachodzi pilna potrzeba przekazania danych osobowych w celu ratowania życia osobie mogącej paść ofiarą przestępstwa. Nawet jeżeli taka wymiana (...) między właściwymi organami a odbiorcami mającymi siedzibę w państwach trzecich (…) miałaby się odbywać tylko w (...) konkretnych, indywidualnych przypadkach, niniejsza dyrektywa powinna wskazać (...) zasady służące uregulowaniu takich (...) przypadków. Odnośnych zasad nie należy traktować jak odstępstw od obowiązujących dwu- lub wielostronnych umów międzynarodowych w dziedzinie współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej. (...) Zasady te (...) powinny obowiązywać jako dodatek do pozostałych przepisów dyrektywy, zwłaszcza (…) przepisów o zgodności przetwarzania z prawem i (…) przepisów rozdziału V.

(50) (...)

(51) Zasadniczym elementem ochrony osób fizycznych w związku z przetwarzaniem danych osobowych jest ustanowienie w państwach członkowskich organów nadzorczych, wykonujących swoje funkcje w sposób całkowicie niezależny. Organy nadzorcze powinny monitorować stosowanie przepisów przyjętych na podstawie niniejszej dyrektywy oraz przyczyniać się do ich spójnego stosowania w całej Unii, po to by chronić osoby fizyczne w związku z przetwarzaniem ich danych osobowych. W tym celu organy nadzorcze powinny współpracować ze sobą oraz z Komisją.

(52) Odpowiedzialność za zadania, które mają być realizowane przez krajowe organy nadzorcze ustanowione na podstawie niniejszej dyrektywy, państwa członkowskie mogą powierzyć organowi nadzorczemu ustanowionemu już (...) na mocy rozporządzenia UE/XXX.

(53) Aby odzwierciedlić swoją strukturę konstytucyjną, organizacyjną i administracyjną, państwa członkowskie powinny móc utworzyć więcej niż jeden organ nadzorczy. 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.

(53a) (...) Organy nadzorcze powinny (...) pod względem swoich wydatków finansowych podlegać (...) niezależnej kontroli lub mechanizmom monitorującym, pod warunkiem że taka kontrola finansowa nie wpływa na ich niezależność. (...).

(54) 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 danego państwa członkowskiego lub niezależny organ, któremu prawo państwa członkowskiego powierzyło zadanie mianowania drogą przejrzystej procedury (...).

(55) Niniejsza dyrektywa ma zastosowanie także do działalności sądów krajowych i innych organów wymiaru sprawiedliwości, niemniej właściwość organów nadzorczych nie powinna obejmować przetwarzania danych osobowych przez sądy w ramach sprawowania wymiaru sprawiedliwości – tak by chronić niezawisłość sędziów w wykonywaniu zadań sądowych. Wyjątek ten powinien być (…) ograniczony do (...) czynności wymiaru sprawiedliwości w sprawach sądowych i nie powinien mieć zastosowania do innych czynności, w których sędziowie mogą brać udział zgodnie z prawem krajowym. (…) Państwa członkowskie mogą również przewidzieć prawem, że właściwość organu nadzorczego może nie obejmować przetwarzania danych osobowych przez inne niezależne organy wymiaru sprawiedliwości w ramach sprawowania wymiaru sprawiedliwości, np. przez prokuraturę. Niemniej przestrzeganie przepisów niniejszej dyrektywy przez sądy i inne niezależne organy wymiaru sprawiedliwości powinno zawsze podlegać niezależnej kontroli zgodnie z art. 8 ust. 3 Karty praw podstawowych UE.

(56) *Każdy organ nadzorczy powinien rozpatrywać skargi wnoszone przez podmioty danych oraz prowadzić stosowne dochodzenia. Dochodzenie na podstawie skargi powinno być prowadzone – z zastrzeżeniem kontroli sądowej – w zakresie odpowiednim do konkretnej sprawy. 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.*

(57) Aby niniejsza dyrektywa była spójnie monitorowana i egzekwowana w całej Unii, organy nadzorcze powinny mieć w *każdym państwie członkowskim* te same zadania i faktyczne uprawnienia, w tym uprawnienia dochodzeniowe (...), (…) korekcyjne (...) (…) i doradcze. Ich uprawnienia nie powinny jednak kolidować ze szczegółowymi przepisami o postępowaniu karnym, w tym o prowadzeniu dochodzeń w sprawie przestępstw oraz o ich ściganiu, ani z niezależnością wymiaru sprawiedliwości.(…) Bez uszczerbku dla uprawnień organów prokuratorskich na mocy prawa krajowego organy nadzorcze powinny również mieć uprawnienie do zgłaszania naruszeń niniejszej dyrektywy organom wymiaru sprawiedliwości i/lub do udziału w postępowaniu sądowym. (…)

Ze swoich uprawnień organ nadzorczy powinien korzystać zgodnie z odpowiednimi gwarancjami proceduralnymi przewidzianymi w prawie Unii i prawie państw członkowskich, bezstronnie, sprawiedliwie i w racjonalnym terminie. W szczególności każdy środek powinien być odpowiedni, niezbędny i proporcjonalny, aby zapewnić przestrzeganie niniejszej dyrektywy – 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 prawa krajowego, takimi jak wymóg uzyskania uprzedniego zezwolenia sądu. (…)
(…) Przyjęcie (...) prawnie wiążącej decyzji (...) powinno podlegać (...) kontroli sądowej w państwie członkowskim organu nadzorczego, który ją przyjął.

(58) Organy nadzorcze powinny wspierać się wzajemnie w wykonywaniu swoich zadań oraz świadczyć sobie wzajemną pomoc, by zapewnić spójne stosowanie i egzekwowanie przepisów przyjętych na podstawie niniejszej dyrektywy.

(59) Europejska Rada Ochrony Danych ustanowiona rozporządzeniem UE/XXX powinna przyczyniać się do spójnego stosowania niniejszej dyrektywy w całej Unii, m.in. poprzez doradzanie Komisji i propagowanie współpracy organów nadzorczych w całej Unii.

(60) Każdy podmiot danych powinien (...) mieć prawo wnieść skargę do pojedynczego organu nadzorczego (...), a jeżeli uzna, że jego prawa wynikające z przepisów przyjętych na podstawie niniejszej dyrektywy są naruszane, lub jeżeli organ nadzorczy nie reaguje na skargę, w części lub w całości ją odrzuca lub oddala lub nie podejmuje działania, choć jest ono niezbędne do ochrony praw tego podmiotu danych – powinien mieć prawo do skutecznego sądowego środka ochrony prawnej, zgodnie z art. 47 Karty praw podstawowych. Dochodzenie na podstawie skargi powinno być prowadzone – z zastrzeżeniem kontroli sądowej – w zakresie odpowiednim do konkretnej sprawy. Właściwy 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.

(61) Każda osoba fizyczna lub prawna powinna mieć prawo skorzystać przed właściwym sądem krajowym ze skutecznego sądowego 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 bądź odrzucania skarg. Prawo to nie dotyczy jednak innych niewiążących prawnie środków organów nadzorczych, takich jak wydawane przez nie opinie czy porady. Pozew przeciwko organowi nadzorczemu należy wnieść do sądu państwa członkowskiego, w którym organ nadzorczy ma siedzibę, a postępowanie powinno się toczyć zgodnie z krajowym prawem (...) 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.

(62) Jeżeli podmiot danych uznа, że naruszane są jego prawa wynikające z niniejszej dyrektywy, 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.* (…) Prawo podmiotu danych do bycia reprezentowanym nie powinno powodować uszczerbku dla krajowego prawa procesowego, które może wymagać, by podmiot danych był przed krajowymi sądami obowiązkowo reprezentowany przez „prawnika**”** zdefiniowanego w dyrektywie 77/249/EWG.

(63) (…)

(64) Za szkodę, którą dana osoba poniosła wskutek (...) przetwarzania niezgodnego z przepisami przyjętymi na podstawie niniejszej dyrektywy, powinno przysługiwać odszkodowanie od administratora lub innego organu właściwego w świetle prawa krajowego **(...).** Pojęcie szkody należy interpretować szeroko, w świetle orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej, w sposób w pełni zgodny z celami niniejszej dyrektywy. Pozostaje to bez uszczerbku dla wszelkich roszczeń z tytułu szkód wynikających z naruszenia innych przepisów prawa Unii lub prawa państwa członkowskiego.

Jeżeli jest mowa o przetwarzaniu niezgodnym z prawem lub niezgodnym z przepisami przyjętymi na podstawie niniejszej dyrektywy, dotyczy to także przetwarzania, które jest niezgodne z aktami **(...)** wykonawczymi przyjętymi w myśl niniejszej dyrektywy. Podmiot danych powinien uzyskać pełne i skuteczne odszkodowanie na poniesioną szkodę. (...)

(65) Każda osoba fizyczna lub prawna, która nie przestrzega przepisów przyjętych na podstawie niniejszej dyrektywy, niezależnie od tego czy działa na podstawie prawa prywatnego czy publicznego, powinna podlegać karze. Państwa członkowskie powinny zagwarantować, że kary będą skuteczne, proporcjonalne i odstraszające, oraz przedsięwziąć wszelkie środki służące wykonaniu kar.

(66) (…)

(67) Aby zapewnić jednolite warunki wdrażania niniejszej dyrektywy, należy powierzyć Komisji uprawnienia wykonawcze co do: (...) stwierdzania odpowiedniego poziomu ochrony zapewnianego przez państwo trzecie, terytorium lub określony sektor w tym państwie trzecim, bądź organizację międzynarodową; określania formuły i trybu *wzajemnej pomocy* oraz ustalania zasad 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[12].

(68) Ponieważ – jeżeli chodzi o (...) stwierdzanie odpowiedniego poziomu ochrony zapewnianego przez państwo trzecie, terytorium lub określony sektor w tym państwie trzecim, bądź organizację międzynarodową; o określanie formuły i trybu wzajemnej pomocy oraz o ustalanie zasad wymiany informacji drogą elektroniczną między organami nadzorczymi oraz między organami nadzorczymi a Europejską Radą Ochrony Danych – odnośne akty wykonawcze mają zasięg ogólny, należy je przyjmować zgodnie z procedurą sprawdzającą.

(69) Komisja powinna przyjmować akty wykonawcze o natychmiastowym zastosowaniu, jeżeli jest to szczególnie pilne w należycie uzasadnionych przypadkach dotyczących państwa trzeciego, terytorium lub określonego sektora w tym państwie trzecim, bądź organizacji międzynarodowej, które nie zapewniają już odpowiedniego poziomu ochrony.

(70) Ponieważ celów niniejszej dyrektywy – którymi są ochrona podstawowych praw i wolności podmiotów danych, w szczególności ich prawa do ochrony danych osobowych, oraz zapewnienie swobodnego przepływu danych osobowych między właściwymi organami w ramach 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 niniejsza dyrektywa nie wykracza poza zakres niezbędny do osiągnięcia tego celu.

---

[12] Dz.U. L 55 z 28.2.2011, s. 13.

(71) Niniejszą dyrektywą należy uchylić decyzję ramową 2008/977/WSiSW. Przetwarzanie, które w dniu wejścia niniejszej dyrektywy w życie już się toczy, powinno w terminie trzech lat od jej wejścia w życie zostać dostosowane do jej przepisów. Jeżeli jednak takie przetwarzanie jest zgodne z unijnym prawem mającym zastosowanie przed wejściem niniejszej dyrektywy w życie, wymogi niniejszej dyrektywy dotyczące uprzednich konsultacji z organem nadzorczym nie powinny mieć zastosowania do operacji przetwarzania, które przed wejściem niniejszej dyrektywy w życie już się toczyły, gdyż wymogów tych z uwagi na ich charakter należy dopełnić przed przetwarzaniem.

(72) Dyrektywa nie wpływa na szczegółowe przepisy aktów unijnych przyjętych w dziedzinie współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej (…), które zostały przyjęte przed datą przyjęcia niniejszej dyrektywy i regulują przetwarzanie danych osobowych między państwami członkowskimi lub dostęp wyznaczonych organów państw członkowskich do systemów informacyjnych ustanowionych na mocy traktatów – przepisy takie, jak np. szczegółowe przepisy o ochronie danych osobowych stosowane na mocy decyzji Rady 2008/615/WSiSW[13] czy art. 23 Konwencji o pomocy prawnej w sprawach karnych pomiędzy państwami członkowskimi Unii Europejskiej (2000/C 197/01)[14]. Komisja powinna ocenić sytuację pod kątem stosunku niniejszej dyrektywy do aktów, które zostały przyjęte przed datą przyjęcia niniejszej dyrektywy i regulują przetwarzanie danych osobowych między państwami członkowskimi lub dostęp wyznaczonych organów państw członkowskich do systemów informacyjnych ustanowionych na mocy traktatów, i ustalić, czy należy te szczegółowe przepisy dostosować do niniejszej dyrektywy.

(73) Aby ochrona danych osobowych w Unii była całościowa i spójna, międzynarodowe porozumienia, które zostały zawarte przez państwa członkowskie przed wejściem niniejszej dyrektywy w życie (...) i są zgodne z odnośnym prawem Unii *mającym zastosowanie* przed wejściem niniejszej dyrektywy w życie, powinny pozostać w mocy do czasu ich zmiany, zastąpienia lub uchylenia.

(74) Niniejsza dyrektywa pozostaje bez uszczerbku dla przepisów o zwalczaniu niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz o zwalczaniu pornografii dziecięcej ustanowionych w dyrektywie 2011/93/UE Parlamentu Europejskiego i Rady z dnia 13 grudnia 2011 r.[15]

---

[13] Decyzja Rady 2008/615/WSiSW z dnia 23 czerwca 2008 r. w sprawie intensyfikacji współpracy transgranicznej, szczególnie w zwalczaniu terroryzmu i przestępczości transgranicznej, Dz.U. L 210 z 6.8.2008, s. 1.

[14] Akt Rady z dnia 29 maja 2000 r. ustanawiający zgodnie z art. 34 Traktatu o Unii Europejskiej Konwencję o pomocy prawnej w sprawach karnych pomiędzy państwami członkowskimi Unii Europejskiej (Dz.U. C 197 z 12.7.2000, s. 1).

[15] Dz.U. L 335 z 17.12.2011, s. 1.

(75) Zgodnie z art. 6a Protokołu w sprawie stanowiska Zjednoczonego Królestwa i Irlandii w odniesieniu do przestrzeni wolności, bezpieczeństwa i sprawiedliwości, który jest załączony do Traktatu o Unii Europejskiej i Traktatu o funkcjonowaniu Unii Europejskiej, Zjednoczone Królestwo i Irlandia nie są związane przepisami ustanowionymi w niniejszej dyrektywie, dotyczącymi przetwarzania danych osobowych przez państwa członkowskie w ramach wykonywania działań wchodzących w zakres zastosowania części trzeciej tytuł V rozdział 4 lub rozdział 5 Traktatu o funkcjonowaniu Unii Europejskiej, jeżeli państwa te nie są związane zasadami regulującymi formy współpracy wymiarów sprawiedliwości w sprawach karnych lub współpracy policyjnej, w ramach której należy przestrzegać przepisów ustanowionych na podstawie art. 16 Traktatu o funkcjonowaniu Unii Europejskiej.

(76) Zgodnie z art. 2 i 2a Protokołu w sprawie stanowiska Danii, który jest załączony do Traktatu o Unii Europejskiej i Traktatu o funkcjonowaniu Unii Europejskiej, Dania nie jest związana przepisami ustanowionymi w niniejszej dyrektywie ani im podlega, o ile przepisy te dotyczą przetwarzania danych osobowych przez państwa członkowskie w ramach wykonywania działań wchodzących w zakres zastosowania części trzeciej tytuł V rozdział 4 lub rozdział 5 Traktatu o funkcjonowaniu Unii Europejskiej. Ponieważ niniejsza dyrektywa stanowi rozwinięcie przepisów dorobku Schengen w rozumieniu części trzeciej tytuł V Traktatu o funkcjonowaniu Unii Europejskiej, Dania zgodnie z art. 4 tego protokołu podejmuje w terminie sześciu miesięcy od daty przyjęcia niniejszej dyrektywy decyzję, czy dokona jej transpozycji do swojego prawa krajowego.

(77) W odniesieniu do Islandii i Norwegii niniejsza dyrektywa stanowi rozwinięcie przepisów dorobku Schengen w rozumieniu Umowy zawartej przez Radę Unii Europejskiej i Republikę Islandii oraz Królestwo Norwegii dotyczącej włączenia tych dwóch państw we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen[16].

(78) W odniesieniu do Szwajcarii niniejsza dyrektywa stanowi rozwinięcie przepisów dorobku Schengen w rozumieniu Umowy zawartej między Unią Europejską, Wspólnotą Europejską a Konfederacją Szwajcarską dotyczącej włączenia Konfederacji Szwajcarskiej we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen[17].

[16] Dz.U. L 176 z 10.7.1999, s. 36.
[17] Dz.U. L 53 z 27.2.2008, s. 52.

(79) W odniesieniu do Liechtensteinu niniejsza dyrektywa stanowi rozwinięcie przepisów dorobku Schengen w rozumieniu Protokołu między Unią Europejską, Wspólnotą Europejską, Konfederacją Szwajcarską i Księstwem Liechtensteinu w sprawie przystąpienia Księstwa Liechtensteinu do Umowy między Unią Europejską, Wspólnotą Europejską i Konfederacją Szwajcarską dotyczącej włączenia Konfederacji Szwajcarskiej we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen[18].

(80) Niniejsza dyrektywa nie narusza praw podstawowych i jest zgodna z zasadami uznanymi w Karcie praw podstawowych Unii Europejskiej umocowanej Traktatem, w szczególności z prawem do poszanowania życia prywatnego i rodzinnego, prawem do ochrony danych osobowych oraz prawem do skutecznego środka ochrony prawnej i rzetelnego procesu. Ograniczenia tych praw są zgodne z art. 52 ust. 1 karty, ponieważ są niezbędne do realizacji celów leżących w interesie ogólnym i uznanych przez Unię lub do ochrony praw i wolności innych osób.

(81) Zgodnie ze wspólną deklaracją polityczną państw członkowskich i Komisji z dnia 28 września 2011 r. dotyczącą dokumentów wyjaśniających państwa członkowskie zobowiązały się w uzasadnionych przypadkach dołączać do zawiadomienia o swoich środkach transpozycji przynajmniej jeden dokument wyjaśniający związek między elementami dyrektywy a odpowiadającymi im częściami krajowych instrumentów transpozycyjnych. W odniesieniu do niniejszej dyrektywy prawodawca uznaje przekazywanie takich dokumentów za uzasadnione.

(82) Niniejsza dyrektywa nie powinna stanowić dla państw członkowskich przeszkody, by w krajowych przepisach o postępowaniu karnym umożliwić podmiotom danych korzystanie z prawa do informacji, dostępu, poprawienia, usunięcia i ograniczenia przetwarzania swoich danych osobowych w toku postępowania karnego oraz by określić ewentualne ograniczenia tych praw.

---

18 Dz.U. L 160 z 18.6.2011, s. 19.

ROZDZIAŁ I
PRZEPISY OGÓLNE

Artykuł 1
Przedmiot i cele

1. Niniejsza dyrektywa ustanawia przepisy o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich lub ścigania, *wykonywania kar kryminalnych* lub do celów ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom.

1a. Niniejsza dyrektywa nie wyklucza ustanowienia przez państwa członkowskie gwarancji wyższych niż przewidziane w niniejszej dyrektywie dla ochrony praw i wolności podmiotu danych w związku z przetwarzaniem danych osobowych przez właściwe organy.

2. Zgodnie z niniejszą dyrektywą państwa członkowskie:

a) chronią prawa podstawowe i wolności osób fizycznych, w szczególności ich prawo do ochrony danych osobowych; oraz

b) dopilnowują, by wymiana danych osobowych przez właściwe organy w Unii – jeżeli jest podyktowana prawem unijnym lub krajowym – nie była ograniczana ani zakazywana z przyczyn związanych z ochroną osób fizycznych w związku z przetwarzaniem danych osobowych.

Artykuł *2*

Zakres zastosowania

1. Niniejsza dyrektywa ma zastosowanie do przetwarzania danych osobowych przez właściwe organy do celów, o których mowa w art. 1 ust. 1.

2. Niniejsza dyrektywa 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.

3. Niniejsza dyrektywa nie ma zastosowania do przetwarzania danych osobowych:

a) w toku działalności nieobjętej prawem Unii (…);

(...)

b) przez instytucje, organy i jednostki organizacyjne Unii.

Artykuł 3

Definicje

Do celów niniejszej dyrektywy:

(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 dotyczące lokalizacji, identyfikator internetowy lub co najmniej jeden znak szczególny związany z jej tożsamością fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną;

(2) (…)

(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;

(4) „ograniczenie przetwarzania” oznacza ocechowanie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;

(4a) „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;

(5) „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;

(6) „administrator” oznacza właściwy (...) organ, 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;

(7) „podmiot przetwarzający” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę organizacyjną lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

(8) „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 „odbiorcą” nie jest organ publiczny, który może otrzymywać dane w ramach konkretnego dochodzenia;

(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) (...);

(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;

(…)

(14) „właściwy organ (...)" oznacza każdy organ publiczny właściwy w państwie członkowskim do zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich lub ścigania, *wykonywania kar kryminalnych* lub do ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom lub każdy organ/podmiot, któremu prawo krajowe powierza realizację obowiązków publicznych lub uprawnień publicznych do celów określonych w art. 1 ust. 1 (...);

(15) „organ nadzorczy" oznacza niezależny organ publiczny ustanowiony przez państwo członkowskie na mocy art. 39;

(16) „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, a także Interpol.

ROZDZIAŁ II
ZASADY

Artykuł 4

Zasady przetwarzania danych osobowych

1. Państwa członkowskie stanowią prawem, że dane osobowe muszą być:

a) przetwarzane zgodnie z prawem i *rzetelnie*;

b) zbierane w konkretnych, jednoznacznych i uzasadnionych celach (…) i nie mogą być (…) przetwarzane w sposób (…) z tymi celami niezgodny (…);

c) ilościowo i treściowo odpowiednie oraz nienadmierne w stosunku do celów, w których są przetwarzane;

d) ścisłe i w razie potrzeby uaktualniane; (...)

e) przechowywane w formie umożliwiającej identyfikację podmiotów danych przez okres nie dłuższy, niż jest to niezbędne do celów, w których są przetwarzane;

ee) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych.

(…)

1a. (...)

2. (...) Przetwarzanie przez tego samego lub innego administratora do celów określonych w art. 1 ust. 1, ale innych niż cel, w którym dane zostały zebrane (...), jest dozwolone, o ile:

(…)

b) administratorowi wolno przetwarzać takie dane osobowe w takim celu na mocy mających zastosowanie przepisów prawa; oraz

c) przetwarzanie jest niezbędne i proporcjonalne do tego innego celu.

3. Przetwarzanie przez tego samego lub innego administratora (...) może obejmować (...) użytkowanie archiwizacyjne w interesie publicznym, *naukowe, statystyczne lub historyczne* do celów, o których mowa w art. 1 ust. 1 (...), o ile podlega ono odpowiednim gwarancjom dla praw i wolności podmiotów danych.

4. Za przestrzeganie przepisów ust. 1, 2 i 3 odpowiada administrator.

Artykuł 5

Rozróżnianie poszczególnych kategorii podmiotów danych

(…)

Artykuł 6

Weryfikacja jakości przekazywanych lub udostępnianych danych

1. Państwa członkowskie stanowią prawem, że właściwe organy podejmują wszelkie racjonalne działania, tak aby nieścisłe, niekompletne lub nieaktualne dane osobowe nie były przekazywane ani udostępniane. W tym celu każdy właściwy organ weryfikuje w maksymalnym praktycznie stopniu jakość danych osobowych przed ich przekazaniem lub udostępnieniem. W miarę możliwości, ilekroć przekazuje się dane osobowe, dołącza się do nich (...) niezbędne informacje, które pozwalają właściwemu organowi odbierającemu ocenić stopień ich ścisłości, kompletności, aktualności i rzetelności.

2. Jeżeli stwierdzi się, że przekazano dane nieprawidłowe lub że dane przekazano niezgodnie z prawem, należy o tym bezzwłocznie powiadomić odbiorcę. W takim przypadku dane osobowe należy poprawić, usunąć lub ograniczyć ich przetwarzanie zgodnie z art. 15.

Artykuł 7

Zgodność przetwarzania z prawem

Państwa członkowskie stanowią prawem, że przetwarzanie danych osobowych jest zgodne z prawem jedynie wtedy, gdy – i w tylko w takim zakresie, w jakim – jest ono niezbędne (…) do wykonania zadania realizowanego przez właściwy organ (...) w celach określonych w art. 1 ust. 1 i ma podstawę w prawie Unii lub prawie państwa członkowskiego (...).

b) (...)
c) (…)

d) (…)

Artykuł 7a

Szczególne wymogi przetwarzania

1. Danych osobowych zbieranych przez właściwe organy do celów określonych w art. 1 ust. 1 nie przetwarza się do celów innych niż określone w art. 1 ust. 1, chyba że takie przetwarzanie jest dozwolone prawem Unii lub prawem państwa członkowskiego (…).
W takim przypadku zastosowanie do takiego przetwarzania ma rozporządzenie UE/XXX, chyba że przetwarzanie odbywa się w toku działalności nieobjętej prawem Unii.
1a. Jeżeli prawo państwa członkowskiego powierza właściwym organom wykonywanie zadań do celów innych niż cele określone w art. 1 ust. 1, to do przetwarzania w takich celach – w tym do (…) użytkowania archiwizacyjnego w interesie publicznym, (…) naukowego, statystycznego lub historycznego – ma zastosowanie rozporządzenie UE/XXX, chyba że przetwarzanie odbywa się w toku działalności nieobjętej prawem Unii.
1b Państwa członkowskie przewidują prawem, że ilekroć prawo unijne lub krajowe mające zastosowanie do właściwego organu przekazującego (...) stawia szczególne wymogi (...) co do przetwarzania danych osobowych, właściwy organ przekazujący informuje o takich wymogach i o obowiązku ich przestrzegania odbiorcę, któremu przekazuje dane.
2. Państwa członkowskie przewidują prawem, że właściwy organ przekazujący (...) nie stosuje względem odbiorców w innych państwach członkowskich ani w organach i jednostkach organizacyjnych ustanowionych na mocy tytułu V rozdział IV i V Traktatu o funkcjonowaniu Unii Europejskiej wymogów, o których mowa w ust. 1b, innych niż mające zastosowanie do podobnego (...) przekazywania danych w obrębie państwa członkowskiego właściwego organu przekazującego.
2a. (...)

Artykuł 8

Przetwarzanie danych osobowych szczególnych kategorii

(…) Dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne lub dane dotyczące zdrowia lub seksualności wolno przetwarzać wyłącznie wtedy, gdy jest to ściśle niezbędne i podlega odpowiednim gwarancjom dla praw i wolności podmiotu danych i gdy:
a) (…) jest dopuszczone prawem Unii lub prawem państwa członkowskiego **(…)**; lub (…);

b) (...) służy ochronie żywotnych interesów podmiotu danych lub innej osoby; lub

(…)

c) dotyczy danych osobowych ewidentnie upublicznionych przez podmiot danych.

Artykuł 9

(...) ***Automatyczne zindywidualizowane podejmowanie decyzji***(...)

[...] Państwa członkowskie stanowią prawem, że decyzje, które opierają się wyłącznie na automatycznym przetwarzaniu, **w** tym profilowaniu, i wywołują wobec podmiotu danych niekorzystne skutki prawne lub poważnie na niego wpływają, są zakazane, chyba że dopuszcza je prawo Unii lub prawo państwa członkowskiego, któremu podlega administrator i które przewiduje odpowiednie gwarancje dla praw i wolności podmiotu danych, a co najmniej prawo do uzyskania interwencji ludzkiej ze strony administratora (...).

1a. (...)

ROZDZIAŁ III
PRAWA PODMIOTU DANYCH

Artykuł 10

Komunikacja oraz tryb korzystania z praw przez podmiot danych

1. (…)

2. Państwa członkowskie stanowią prawem, że administrator podejmuje (...) wszelkie racjonalne kroki, aby w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem udzielić podmiotowi danych wszelkich informacji, o których mowa w art. 10a (...), oraz prowadzić z nim wszelką komunikację na mocy art. 12, 15 i 29 w sprawie przetwarzania danych osobowych. Informacji udziela się wszelkimi stosownymi sposobami, w tym (...) elektronicznie. Zasadniczo administrator udziela informacji w takiej samej formie, jaką posłużył się wnioskodawca (...).

3. Państwa członkowskie stanowią prawem, że administrator podejmuje wszelkie racjonalne kroki, by (...) ułatwić podmiotowi danych korzystanie z praw przysługujących mu na mocy art. 12 i 15 (...).

4. (...)

5. Państwa członkowskie stanowią prawem, że informacje udzielone na mocy art. 10a (...) oraz wszelka komunikacja podjęta na mocy art. 12, 15 i 29 są (...) wolne od opłat. Jeżeli wnioski 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 (...).

5a. Jeżeli administrator ma uzasadnione wątpliwości co do tożsamości osoby składającej wniosek, o którym mowa w art. (…) 12 i 15, może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości podmiotu danych.

Artykuł 10a

Informacje dla podmiotu danych

1. Państwa członkowskie stanowią prawem, że administrator udostępnia podmiotowi danych przynajmniej następujące informacje:

a) *tożsamość i dane kontaktowe administratora*; administrator podaje też dane kontaktowe inspektora ochrony danych, *jeżeli istnieje*;

b) *cele przetwarzania, do których mają posłużyć dane osobowe*;

c) (...)

d) (...)

e) *informacje o prawie do wniesienia skargi do organu nadzorczego* (…).

2. Państwa członkowskie stanowią prawem (…), że oprócz informacji, o których mowa w ust. 1, administrator podaje podmiotowi danych informacje niezbędne (…) w konkretnym przypadku i umożliwiające mu skorzystanie z jego praw, zwłaszcza (...) gdy dane są zbierane bez jego wiedzy.

3. Państwa członkowskie mogą przyjąć środki legislacyjne pozwalające opóźnić, ograniczyć lub pominąć informowanie podmiotu danych przewidziane w ust. 2 (...) w *takim zakresie i przez taki czas, w jakim odnośny środek jest działaniem koniecznym i proporcjonalnym w społeczeństwie demokratycznym – przy należytym uwzględnieniu uzasadnionych interesów danej osoby fizycznej – aby:*

a) uniemożliwić utrudnianie urzędowych lub prawnych dochodzeń, śledztw lub procedur;
b) uniemożliwić szkodzenie zapobieganiu przestępstwom, ich wykrywaniu, prowadzeniu dochodzeń w ich sprawie, ich ściganiu lub wykonywaniu kar kryminalnych;
c) chronić *bezpieczeństwo publiczne*;
d) chronić *bezpieczeństwo narodowe*;
e) chronić *prawa i wolności innych osób*.

Artykuł 11

Informacje podawane w przypadku zbierania danych od podmiotu danych

(...)

Artykuł 11a

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

(...)

Artykuł 11b

Ograniczenia prawa do informacji

(...)

Artykuł 12

Prawo dostępu przysługujące podmiotowi danych

1. Z zastrzeżeniem art. 13 państwa członkowskie stanowią prawem, że podmiot danych ma prawo w sposób wolny od opłat, w racjonalnych odstępach czasu uzyskiwać od administratora potwierdzenie, czy dotyczące go dane osobowe są przetwarzane, a jeżeli takie dane są przetwarzane – uzyskać dostęp do nich i stosownymi sposobami następujące informacje:

a) cele przetwarzania;

b) (…)

c) informacje o odbiorcach lub kategoriach odbiorców (…), którym dane osobowe zostały (...) ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;

d) (...) planowany okres przechowywania danych lub zasady obliczania tego okresu;

e) informacje o prawie do tego, by zwrócić się do administratora o poprawienie, usunięcie lub ograniczenie przetwarzania danych osobowych dotyczących podmiotu danych;

f) informacje o prawie do wniesienia skargi do organu nadzorczego (…);

g) wskazanie, jakie dane osobowe podlegają przetwarzaniu, oraz w razie potrzeby wszelkie dostępne informacje o ich źródle.

h) (...)

1a. (...)

2. (...)

2a. (...)

Artykuł 13

Ograniczenia prawa do dostępu

1. Państwa członkowskie mogą przyjąć środki legislacyjne pozwalające ograniczyć w całości lub w części prawo dostępu podmiotu danych w takim stopniu, w jakim takie częściowe lub całkowite ograniczenie jest działaniem niezbędnym i proporcjonalnym w społeczeństwie demokratycznym – przy należytym uwzględnieniu uzasadnionych interesów danej osoby fizycznej – aby:

a) uniemożliwić utrudnianie urzędowych lub prawnych dochodzeń, śledztw lub procedur;

b) uniemożliwić szkodzenie zapobieganiu przestępstwom, ich wykrywaniu, prowadzeniu dochodzeń w ich sprawie, ich ściganiu lub wykonywaniu kar kryminalnych;

c) chronić bezpieczeństwo publiczne;

d) chronić bezpieczeństwo narodowe;

e) chronić prawa i wolności innych osób.

2. (...)

3. W przypadkach, o których mowa w ust. 1 (...), państwa członkowskie stanowią prawem, że administrator informuje podmiot danych na piśmie o każdej odmowie lub każdym ograniczeniu dostępu i (...) o przyczynach tej odmowy lub tego ograniczenia. (...) Nie ma to zastosowania, (...) jeżeli udzielenie takich informacji godziłoby w którykolwiek z celów, o których mowa w ust. 1. Państwa członkowskie stanowią prawem, że administrator informuje podmiot danych o możliwościach wniesienia skargi do organu nadzorczego lub możliwościach skorzystania z sądowych środków ochrony prawnej.

4. Państwa członkowskie dopilnowują, by administrator dokumentował (...) faktyczne lub prawne przyczyny swojej decyzji.

Artykuł 14

Dodatkowy tryb korzystania z prawa do dostępu

(...)

Artykuł 15

Prawo do poprawienia danych, ich usunięcia oraz ograniczenia ich przetwarzania

1. Państwa członkowskie stanowią prawem, że podmiot danych ma prawo spowodować, by administrator bez zbędnej zwłoki poprawił dane osobowe go dotyczące, jeżeli są one nieścisłe. *Uwzględniając* (...) *cel odnośnego przetwarzania*, (...) państwa członkowskie stanowią prawem, że podmiot danych ma prawo spowodować, by niekompletne dane osobowe zostały uzupełnione, w tym poprzez przedstawienie dodatkowego oświadczenia.

1a. *Państwa członkowskie stanowią prawem, że administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, a pomiot danych ma prawo spowodować, by administrator bez zbędnej zwłoki usunął dotyczące go dane osobowe, jeżeli przetwarzanie jest niezgodne z przepisami przyjętymi na podstawie art. 4* (...)*, 7 i 8 niniejszej dyrektywy lub jeżeli dane muszą zostać usunięte w myśl obowiązku prawnego ciążącego na administratorze.*

1b. (…) Jeżeli podmiot danych kwestionuje ścisłość dowolnego elementu swoich danych osobowych, ale nie da się stwierdzić ich ścisłości bądź nieścisłości, można ograniczyć przetwarzanie tego elementu.

2. Państwa członkowskie stanowią prawem, że administrator informuje podmiot danych na piśmie o każdej odmowie poprawienia, usunięcia lub ograniczenia przetwarzania danych oraz o przyczynach tej odmowy (…). Państwa członkowskie mogą przyjmować środki legislacyjne, które w całości lub w części ograniczają obowiązek udzielania takich informacji, (…) jeżeli takie ograniczenie jest działaniem niezbędnym i proporcjonalnym w społeczeństwie demokratycznym – przy należytym uwzględnieniu uzasadnionych interesów danej osoby fizycznej – aby:

a) uniemożliwić utrudnianie urzędowych lub prawnych dochodzeń, śledztw lub procedur;

b) uniemożliwić szkodzenie zapobieganiu przestępstwom, ich wykrywaniu, prowadzeniu dochodzeń w ich sprawie, ich ściganiu lub wykonywaniu kar kryminalnych;

c) chronić bezpieczeństwo publiczne;

d) chronić bezpieczeństwo narodowe;

e) chronić prawa i wolności innych osób.

Państwa członkowskie stanowią prawem, że administrator informuje podmiot danych o możliwościach wniesienia skargi do organu nadzorczego lub możliwościach skorzystania z sądowych środków ochrony prawnej.

3. Państwa członkowskie stanowią prawem, że w przypadkach, o których mowa w ust. 1, 1a i 1b, administrator powiadamia odbiorców, a odbiorcy w swojej gestii poprawiają dane osobowe, usuwają je lub ograniczają ich przetwarzanie.

Artykuł 15a

Korzystanie z prawa przez podmiot danych oraz weryfikacja dokonywana przez organ nadzorczy

1. (…)

1a. W odniesieniu do przypadków, o których mowa w art. 13 ust. 3 i art. 15 ust. 2, państwa członkowskie mogą przyjąć środki przewidujące, że ze swoich praw podmiot danych może korzystać za pośrednictwem właściwego organu nadzorczego.

2. (…)

3. Jeżeli dochodzi do skorzystania z prawa określonego w ust. 1a, organ nadzorczy informuje podmiot danych przynajmniej o fakcie przeprowadzenia wszelkich niezbędnych weryfikacji lub kontroli. (…)

Artykuł 16

Prawo do usunięcia danych

(…)

Artykuł 17

Prawa podmiotu danych w dochodzeniu i postępowaniu karnym

Państwa członkowskie mogą ustanowić prawem, że z praw (...) określonych w art. **(...)** 10a, 12 i 15 korzysta się zgodnie z (…) prawem krajowym, jeżeli dane osobowe są ujęte w orzeczeniu sądowym, protokole lub akcie sprawy przetwarzanym w toku dochodzenia lub postępowania karnego.

ROZDZIAŁ IV

ADMINISTRATOR I PODMIOT PRZETWARZAJĄCY

SEKCJA 1

OBOWIĄZKI OGÓLNE

Artykuł 18

Obowiązki administratora

1. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz prawdopodobieństwo i powagę zagrożenia dla praw i wolności osób fizycznych, państwa członkowskie stanowią prawem, że administrator wdraża odpowiednie środki i jest w stanie wykazać, że przetwarzanie danych osobowych odbywa się zgodnie z przepisami przyjętymi na podstawie niniejszej dyrektywy.

1a. 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, w których to strategiach przewiduje się stosowanie krajowych przepisów o ochronie danych (…) służących wdrożeniu niniejszej dyrektywy.

2. (…)

Artykuł 19

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, państwa członkowskie przewidują prawem, że administrator wdraża (…) środki techniczne i organizacyjne (…) odpowiednie do wykonywanej czynności przetwarzania i do jej celów – np. pseudonimizację – w taki sposób, by przetwarzanie było zgodne z wymogami przepisów przyjętych na podstawie niniejszej dyrektywy oraz chroniło prawa podmiotów danych.

2. Państwa członkowskie stanowią prawem, że administrator wdraża odpowiednie środki (…) – zwłaszcza względem automatycznego przetwarzania – aby domyślnie przetwarzane były wyłącznie (...) te dane osobowe, które są niezbędne do każdego konkretnego celu przetwarzania; dotyczy to ilości (…) zbieranych danych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności.

Artykuł 20

Współadministratorzy

1. Państwa członkowskie stanowią prawem, że jeżeli dwaj administratorzy lub większa ich liczba wspólnie ustalają cele i sposoby przetwarzania danych osobowych, są oni współadministratorami. W przejrzysty sposób (...) określają oni podział zadań w zakresie przestrzegania przepisów przyjętych na podstawie niniejszej dyrektywy – w szczególności odnośnie do (…) korzystania przez podmiot danych z przysługujących mu praw – oraz podział obowiązków w zakresie podawania informacji, o których mowa w art. 10a **(...)**, chyba że – i w takim zakresie, w jakim – przypadające każdemu z nich obowiązki określa prawo Unii lub prawo państwa członkowskiego, któremu administratorzy ci podlegają. (...) Państwa członkowskie mogą wskazać, który ze współadministratorów może pełnić funkcję pojedynczego punktu kontaktowego wobec podmiotów danych chcących skorzystać ze swoich praw.

1a. (...) Bez uszczerbku dla art. 17 państwa członkowskie mogą ustanowić prawem, że z praw przysługujących na mocy przepisów przyjętych na podstawie niniejszej dyrektywy podmiot danych może korzystać wobec każdego z administratorów i przeciwko każdemu z nich.

Artykuł 21

Podmiot przetwarzający

1. Państwa członkowskie stanowią prawem, że administrator korzysta z usług wyłącznie (...) takich podmiotów przetwarzających, które dają wystarczające gwarancje wdrożenia odpowiednich środków (…) technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom przepisów przyjętych na podstawie niniejszej dyrektywy (…).

1a. Państwa członkowskie stanowią prawem, że 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.

2. Państwa członkowskie stanowią prawem, że przetwarzanie przez podmiot przetwarzający jest regulowane aktem o mocy prawnej (w tym umową), który podlega prawu Unii lub prawu państwa członkowskiego, wiąże podmiot przetwarzający z administratorem, określa przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie podmiotów danych, prawa administratora i przewiduje w szczególności, że podmiot przetwarzający działa wyłącznie na polecenie administratora (...).

3. (…)

Artykuł 22

Przetwarzanie z upoważnienia administratora i podmiotu przetwarzającego

(…)

Artykuł 23

Rejestrowanie kategorii czynności przetwarzania danych osobowych

1. Państwa członkowskie stanowią prawem, że każdy administrator **(...)** 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 inspektora ochrony danych – jeżeli istnieje;

b) cele przetwarzania;

c) (…) *kategorie odbiorców*, którym dane osobowe zostały lub zostaną ujawnione, w szczególności odbiorców w państwach trzecich;

ca) opis kategorii danych osobowych dotyczących (…) podmiotów danych;

d) w odpowiednim przypadku kategorie przekazań danych osobowych do *państwa trzeciego lub organizacji międzynarodowej* (…);

e) w miarę możliwości planowane terminy usunięcia poszczególnych kategorii danych;

f) w miarę możliwości ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 27 ust. 1.

2. (…)

2a. Państwa członkowskie stanowią prawem, że 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 (…);

b) imię i nazwisko/nazwa oraz dane kontaktowe inspektora ochrony danych – jeżeli istnieje;

c) kategorie przetwarzań dokonywanych w imieniu każdego z administratorów;

d) (...)

e) (...)

f) w miarę możliwości ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 27 ust. 1.

2b 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 udostępniają rejestr organowi nadzorczemu.

Artykuł 24

Ewidencja czynności

1. Państwa członkowskie dopilnowują, by o ile jest to możliwe i nie wymaga niewspółmiernie dużego wysiłku, (…) ewidencjonowano przynajmniej następujące czynności przetwarzania *prowadzone w zautomatyzowanych systemach przetwarzania*: zbieranie, modyfikowanie, przeglądanie, ujawnianie, łączenie lub usuwanie. Ewidencja przeglądania i ujawniania wskazuje: (...) ich cel, datę i godzinę oraz w miarę możliwości tożsamość osoby, która przeglądała lub ujawniła dane osobowe.

2. Ewidencja (...) jest używana do **(...)** weryfikacji zgodności przetwarzania danych z prawem, do monitorowania własnej działalności oraz do gwarantowania integralności i bezpieczeństwa danych.

Artykuł 25

Współpraca z organem nadzorczym

(…)

Artykuł 26

Uprzednie konsultacje z organem nadzorczym

1. Państwa członkowskie stanowią prawem, że przed przetworzeniem danych osobowych, które będą należeć do mającego powstać nowego zbioru danych, administrator lub podmiot przetwarzający konsultują się z organem nadzorczym, jeżeli:

a) przetwarzane mają być szczególne kategorie danych osobowych, o których to kategoriach mowa w art. 8;

b) odnośny rodzaj przetwarzania – zwłaszcza z użyciem nowych technologii, mechanizmów lub procedur – niesie duże zagrożenie dla (...) (...) praw i wolności (...) podmiotów danych.

1a. (...) Państwa członkowskie stanowią prawem, że konsultacja z organem nadzorczym następuje podczas przygotowywania projektu środka ustawodawczego lub środka regulacyjnego, jeżeli środek przewiduje przetwarzanie danych osobowych, o którym mowa w ust. 1.

2. Państwa członkowskie mogą ustanowić prawem, że organ nadzorczy sporządza wykaz operacji przetwarzania, które wymagają uprzednich konsultacji zgodnie z ust. 1.

3. Państwa członkowskie stanowią prawem, że jeżeli zdaniem organu nadzorczego zamierzone przetwarzanie, o którym mowa w ust. 1, nie jest zgodne z przepisami przyjętymi na podstawie niniejszej dyrektywy – w szczególności jeżeli zagrożenie jest niedostatecznie zidentyfikowane lub zminimalizowane – to najpóźniej sześć tygodni po wpłynięciu wniosku o konsultacje organ nadzorczy udziela administratorowi porady na piśmie. Okres ten można przedłużyć o jeden miesiąc 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.

SEKCJA 2

BEZPIECZEŃSTWO DANYCH

Artykuł 27

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, państwa członkowskie stanowią prawem, że administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić poziom bezpieczeństwa odpowiadający temu zagrożeniu (...).

2. Odnośnie do zautomatyzowanego przetwarzania danych każde państwo członkowskie stanowi prawem, że po ocenie zagrożeń administrator lub podmiot przetwarzający wdrażają środki, które:

a) uniemożliwią osobom nieuprawnionym dostęp do sprzętu używanego do przetwarzania danych osobowych (kontrola dostępu do sprzętu);

b) zapobiegną nieuprawnionemu odczytywaniu, kopiowaniu, zmienianiu lub usuwaniu nośników danych (kontrola nośników danych);

c) zapobiegną nieuprawnionemu wprowadzaniu danych oraz nieuprawnionemu oglądaniu, zmienianiu lub usuwaniu przechowywanych danych osobowych (kontrola przechowywania);

d) zapobiegną korzystaniu z systemów zautomatyzowanego przetwarzania danych przez osoby nieuprawnione, używające sprzętu do przesyłu danych (kontrola użytkowników);

e) zagwarantują, że osoby uprawnione do korzystania z systemu zautomatyzowanego przetwarzania danych będą mieć dostęp wyłącznie do danych objętych posiadanym przez siebie uprawnieniem (kontrola dostępu do danych);

f) pozwolą zweryfikować i ustalić, którym organom dane osobowe zostały lub mogą zostać przekazane lub udostępnione za pomocą sprzętu do przesyłu danych (kontrola przesyłu danych);

g) pozwolą następczo zweryfikować i stwierdzić, które dane osobowe zostały wprowadzone do systemów zautomatyzowanego przetwarzania danych, kiedy i przez kogo (kontrola wprowadzania danych);

h) zapobiegną nieuprawnionemu odczytywaniu, kopiowaniu, zmienianiu lub usuwaniu danych osobowych podczas ich przekazywania lub podczas przenoszenia nośników danych (kontrola transportu);

i) zagwarantują, że w razie awarii można będzie przywrócić zainstalowane systemy (odzyskiwanie);

j) zagwarantują działanie funkcji systemu, zgłaszanie występujących w nich błędów (niezawodność) oraz odporność przechowywanych danych na uszkodzenia powodowane błędnym działaniem systemu (integralność).

3. (…)

Artykuł 28

Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu

1. Państwa członkowskie stanowią prawem, że jeżeli dojdzie do naruszenia ochrony danych osobowych mogącego nieść duże zagrożenie dla praw i wolności podmiotów danych, (...) administrator bez zbędnej zwłoki (...) – jeżeli to wykonalne, nie później niż w ciągu 72 godzin po stwierdzeniu naruszenia – zgłasza naruszenie ochrony danych osobowych organowi nadzorczemu (...). 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. 29 ust. 3 lit. a) i b) nie jest wymagane zawiadomienie podmiotu danych. (…)

2. Podmiot przetwarzający bez zbędnej zwłoki po stwierdzeniu naruszenia ochrony danych osobowych ostrzega i informuje administratora.

3. Zgłoszenie, o którym mowa w ust. 1, musi co najmniej:

a) opisywać charakter naruszenia ochrony danych osobowych;

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. Państwa członkowskie stanowią prawem, że administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, o których mowa w ust. 1, w tym okoliczności naruszenia, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu zweryfikować przestrzeganie niniejszego artykułu. (...)

4a. Z zastrzeżeniem ust. 1a *państwa członkowskie stanowią prawem, że jeżeli naruszenie ochrony danych dotyczy danych osobowych przekazanych przez* lub do administratora *innego państwa członkowskiego, informacje, o których mowa w* ust. 3, *dostarcza się bez zbędnej zwłoki* administratorowi *tego państwa członkowskiego.*

5. (…)

6. (…)

Artykuł 29

Zawiadamianie podmiotu danych o naruszeniu ochrony danych osobowych

1. Z zastrzeżeniem ust. 3 i 4 niniejszego artykułu państwa członkowskie stanowią prawem, że jeżeli naruszenie ochrony danych osobowych może nieść duże zagrożenie dla praw i wolności (...) podmiotu danych, (...) 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, o których mowa w art. 28 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 danych; lub

b) administrator przedsięwziął późniejsze środki, by wyeliminować 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. Wtedy zostaje w zamian wydany publiczny komunikat lub przedsięwzięty podobny środek, za pomocą którego podmioty danych informuje się w równie skuteczny sposób.

4. Zawiadomienie, o którym mowa w ust. 1, można opóźnić, ograniczyć lub pominąć z przyczyn, o których mowa w art. 10a ust. 3.

SEKCJA 3

INSPEKTOR OCHRONY DANYCH

Artykuł 30

Wyznaczenie inspektora ochrony danych

1. Państwa członkowskie mogą lub gdy wymaga tego *prawo Unii* (...), muszą ustanowić prawem, że administrator lub podmiot przetwarzający wyznaczają inspektora ochrony danych.

2. Inspektora ochrony danych wyznacza się 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. 32, a zwłaszcza braku konfliktu interesów.

3. Można wyznaczyć jednego inspektora ochrony danych dla kilku właściwych organów (...), uwzględniając ich strukturę organizacyjną (...) i wielkość.

4. *Państwa członkowskie stanowią prawem, że administrator lub podmiot przetwarzający dopilnowują, by inspektor ochrony danych był właściwie i terminowo angażowany we wszystkie sprawy dotyczące ochrony danych osobowych.*

5. *Administrator lub podmiot przetwarzający dopilnowują, by inspektor ochrony danych otrzymał zasoby niezbędne to skutecznego wykonywania (...) zadań, o których mowa w art. 32, i by w ramach wykonywania swoich zadań mógł działać w sposób niezależny (...).*

Artykuł 31

Status inspektora ochrony danych

(…)

Artykuł 32

Zadania inspektora ochrony danych

Państwa członkowskie stanowią prawem, że administrator lub podmiot przetwarzający powierzają inspektorowi ochrony danych (...) następujące zadania:

a) informowanie administratora lub podmiotu przetwarzającego (...) **o** ich obowiązkach wynikających z przepisów przyjętych na podstawie niniejszej dyrektywy i z innych przepisów Unii lub państw członkowskich o ochronie danych oraz doradzanie im w tej sprawie (…);

b) monitorowanie przestrzegania przepisów przyjętych na podstawie niniejszej dyrektywy, przestrzegania innych przepisów Unii lub państw członkowskich o ochronie danych oraz przestrzegania (...) 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) (…)

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. 26, oraz w stosownym przypadku udzielanie konsultacji we wszelkich innych sprawach (...).

ROZDZIAŁ V
PRZEKAZYWANIE DANYCH OSOBOWYCH DO PAŃSTW TRZECICH LUB ORGANIZACJI MIĘDZYNARODOWYCH

Artykuł 33

Ogólne zasady przekazywania danych osobowych

1. Państwa członkowskie stanowią prawem, że przekazanie danych osobowych (...) przez właściwe organy do państwa trzeciego lub do organizacji międzynarodowej, w tym dalsze, wtórne ich przekazanie do innego państwa trzeciego lub innej organizacji międzynarodowej, może nastąpić wyłącznie wtedy, gdy:
   a) przekazanie jest niezbędne do celów, o których mowa w art. 1 ust. 1; oraz
   b) (…)
   c) administrator w państwie trzecim lub organizacji międzynarodowej jest organem właściwym do realizacji celów określonych w art. 1 ust. 1; oraz
   d) w przypadku przekazywania lub udostępniana danych od innego państwa członkowskiego to inne państwo członkowskie wyraziło na przekazanie uprzednią zgodę odpowiednio do swojego prawa krajowego; oraz
   e) Komisja stwierdziła zgodnie z art. 34, że dane państwo trzecie lub dana organizacja międzynarodowa zapewniają odpowiedni poziom ochrony, bądź – w razie braku stwierdzenia odpowiedniego poziomu ochrony wskazanego w art. 34 – oferowane są lub istnieją odpowiednie gwarancje zgodnie z art. 35. (…)

2. Państwa członkowskie stanowią prawem, że przekazanie danych osobowych bez uprzedniej zgody innego państwa członkowskiego, o której mowa w lit. d), jest dozwolone tylko wtedy, gdy odnośne przekazanie jest niezbędne do zapobieżenia nagłemu, poważnemu zagrożeniu dla bezpieczeństwa publicznego w państwie członkowskim lub państwie trzecim bądź dla ważnych interesów państwa członkowskiego, a uprzedniej zgody nie da się uzyskać na czas. Organ odpowiadający za wydanie uprzedniej zgody zostaje bezzwłocznie powiadomiony.

3. Państwa członkowskie stanowią prawem, że w razie braku decyzji stwierdzającej odpowiedni poziom ochrony wskazany w art. 34 lub braku odpowiednich gwarancji wskazanych w art. 35 przekazanie może nastąpić tylko wtedy, gdy zastosowanie mają odstępstwa w szczególnych sytuacjach zgodnie z art. 36 oraz gdy zachodzą warunki określone w ust. 1 lit. a), c) i d) oraz – odpowiednio do przypadku – (…) w ust. 2 niniejszego artykułu.

Artykuł 34

Przekazywanie na podstawie decyzji stwierdzającej odpowiedni poziom ochrony

1. Państwa członkowskie stanowią prawem, że dane osobowe wolno przekazać do państwa trzeciego – albo też terytorium lub co najmniej jednemu określonemu sektorowi w państwie trzecim – lub do organizacji międzynarodowej, jeżeli Komisja stwierdziła w decyzji zgodnie z art. 41 rozporządzenia UE/XXX lub zgodnie z ust. 3 niniejszego artykułu, że państwo trzecie, terytorium lub określony sektor w tym państwie trzecim lub dana organizacja międzynarodowa zapewniają odpowiedni poziom ochrony. Takie przekazanie nie wymaga specjalnego zezwolenia.
2. W razie braku decyzji na mocy art. 41 rozporządzenia UE/XXX (…) Komisja ocenia, czy oferowany poziom ochrony jest odpowiedni, uwzględniając w szczególności [...] następujące elementy:
   a) praworządność, poszanowanie praw człowieka i podstawowych wolności, stosowne ustawodawstwo (zarówno ogólne, jak i sektorowe), przepisy o ochronie danych (...) (w tym dotyczące bezpieczeństwa publicznego, obrony, bezpieczeństwa narodowego i prawa karnego) oraz (...) środki bezpieczeństwa (w tym zasady wtórnego przekazywania danych osobowych do kolejnego państwa trzeciego lub organizacji międzynarodowej) stosowane w tym państwie trzecim lub w tej organizacji międzynarodowej, a także istniejące skuteczne i egzekwowalne prawa podmiotów danych, a w przypadku podmiotów (...) przekazywanych danych osobowych – prawa 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 dysponującego odpowiednim uprawnieniem do nakładania sankcji – oraz pomagać i doradzać (...) podmiotom danych w korzystaniu z przysługujących im praw, a także współpracować z organami nadzorczymi Unii i państw członkowskich; oraz
   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 w ramach niniejszej dyrektywy przyjąć decyzję stwierdzającą, że państwo trzecie, terytorium lub co najmniej jeden określony sektor 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 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. 57 ust. 2.

4. (…)

4a. Komisja monitoruje funkcjonowanie decyzji przyjętych na mocy ust. 3 (…).

5. Komisja może w ramach niniejszej dyrektywy 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. Odnośne akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 57 ust. 2, lub w przypadkach wyjątkowo pilnych zgodnie z procedurą, o której mowa w art. 57 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. Państwa członkowskie dopilnowują, by jeżeli zapadnie decyzja na mocy ust. 5, decyzja ta (...) nie powodowała 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. 35 i 36 (…).

7. Komisja publikuje w *Dzienniku Urzędowym Unii Europejskiej* wykaz tych państw trzecich, terytoriów i określonych sektorów w państwach trzecich oraz tych organizacji międzynarodowych, co do których zapadły decyzje na mocy ust. 3 (…) i 5.

8. (…)

Artykuł 35

Przekazywanie na podstawie odpowiednich gwarancji

1. (...) *Na wypadek braku decyzji określonej w art. 34 ust. 3* państwa członkowskie stanowią prawem, że (…) dane osobowe wolno przekazać do państwa trzeciego lub organizacji międzynarodowej, jeżeli:

   a) w prawnie wiążącym (…) akcie wprowadzono odpowiednie gwarancje co do ochrony danych osobowych; lub

   b) administrator (...) ocenił wszystkie okoliczności związane z przekazaniem danych osobowych i stwierdził, że istnieją odpowiednie gwarancje co do ochrony danych osobowych. Taka ocena może uwzględniać obowiązujące umowy o współpracy między Europolem lub Eurojustem a państwami trzecimi przewidujące wymianę danych osobowych.

2. (…)

Artykuł 36

Odstępstwa w (...) szczególnych sytuacjach

1. (...) *Na wypadek braku decyzji stwierdzającej odpowiedni poziom ochrony wskazanej w art. 34 lub braku odpowiednich gwarancji wskazanych w art. 35* państwa członkowskie stanowią prawem, że przekazanie lub określona kategoria przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej może nastąpić wyłącznie wtedy, gdy:

   a) przekazanie jest niezbędne do ochrony żywotnych interesów podmiotu danych lub innej osoby; lub

   b) przekazanie jest niezbędne do zabezpieczenia uzasadnionych interesów podmiotu danych (…), jeżeli prawo państwa członkowskiego przekazującego dane osobowe tak stanowi; lub

   c) przekazanie jest niezbędne do zapobieżenia nagłemu, poważnemu zagrożeniu dla bezpieczeństwa publicznego państwa członkowskiego lub państwa trzeciego; lub

d) przekazanie jest niezbędne w indywidualnym przypadku do celów, o których mowa w art. 1 ust. 1; lub

e) przekazanie jest niezbędne w indywidualnym przypadku, by ustalić roszczenia prawne, realizować je lub ich bronić w związku z celami, o których mowa w art. 1 ust. 1.

2. Danych osobowych nie przekazuje się, jeżeli właściwy organ przekazujący stwierdzi, że (...) podstawowe prawa i wolności (…) odnośnego podmiotu danych są nadrzędne wobec interesu publicznego przemawiającego za przekazaniem, o którym mowa w ust. 1 lit. d) i e).

Artykuł 36a

(…)

Artykuł 36aa

Przekazywanie danych osobowych (…) **odbiorcom** (…) **mającym siedzibę w państwach trzecich**

1. Na zasadzie odstępstwa od art. 33 ust. 1 lit. c) i bez uszczerbku dla umów międzynarodowych, o których mowa w ust. 2, prawo Unii lub prawo państwa członkowskiego może stanowić, że właściwe organy mogą w indywidualnych, (...) konkretnych przypadkach przekazywać dane osobowe bezpośrednio (…) odbiorcom (…) mającym siedzibę w państwach trzecich, o ile tylko zachowane są pozostałe przepisy niniejszej dyrektywy i spełnione następujące warunki:

   (a) przekazanie jest (…) ściśle niezbędne do wykonania zadania właściwego organu zgodnie z prawem Unii lub prawem państwa członkowskiego do celów, o których mowa w art. 1 ust. 1; oraz

   (b) (…)

   (c) (…)

   (d) właściwy organ przekazujący stwierdza, że podstawowe prawa (…) i wolności odnośnego podmiotu danych nie są nadrzędne wobec interesu publicznego przemawiającego za przedmiotowym przekazaniem.

2. Umowa międzynarodowa, o której mowa w ust. 1, może oznaczać jakąkolwiek dwu- lub wielostronną umowę międzynarodową obowiązującą między państwami członkowskimi a państwami trzecimi o współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej. (…)

Artykuł 37

Szczególne warunki przekazania danych osobowych

Artykuł 38

Międzynarodowa współpraca na rzecz ochrony danych osobowych

(…)

ROZDZIAŁ VI

NIEZALEŻNE ORGANY NADZORCZE

SEKCJA 1

NIEZALEŻNY STATUS

Artykuł 39

Organ nadzorczy

1. Każde państwo członkowskie stanowi prawem, że za monitorowanie stosowania przepisów przyjętych na podstawie niniejszej dyrektywy odpowiada co najmniej jeden niezależny organ publiczny.

1a. Każdy organ nadzorczy przyczynia się do spójnego stosowania niniejszej dyrektywy w całej Unii. (...) W tym celu organy nadzorcze współpracują ze sobą i z Komisją zgodnie z rozdziałem VII.

2. Państwa członkowskie mogą ustanowić prawem, że organem nadzorczym, o którym mowa w niniejszej dyrektywie i na którym spoczywa odpowiedzialność za wypełnianie zadań organu nadzorczego mającego powstać na mocy ust. 1, może być organ nadzorczy ustanowiony (...) na mocy rozporządzenia UE/XXX.

3. Jeżeli w państwie członkowskim ustanowiono więcej niż jeden organ nadzorczy, państwo to wyznacza organ nadzorczy, który (...) reprezentuje te organy w Europejskiej Radzie Ochrony Danych.

Artykuł 40

Niezależność

1. Państwa członkowskie dopilnowują, by każdy organ nadzorczy działał w sposób całkowicie niezależny podczas wykonywania zadań i korzystania z uprawnień mu powierzonych.

2. (...) Państwa członkowskie stanowią prawem, że członek lub **(...)** członkowie **(...)** każdego organu nadzorczego pozostają – podczas wykonywania swoich zadań i korzystania ze swoich uprawnień zgodnie z niniejszą dyrektywą – wolni od bezpośrednich i pośrednich wpływów zewnętrznych, nie zwracają się do nikogo o instrukcje ani ich od nikogo nie przyjmują.

3. (…)

4. (…)

5. (...) Państwa członkowskie dopilnowują, by każdy organ nadzorczy otrzymał (…) zasoby kadrowe, techniczne i finansowe, pomieszczenia i infrastrukturę niezbędne do skutecznego wykonywania swoich zadań i korzystania ze swoich uprawnień, w tym w kontekście wzajemnej pomocy, współpracy i aktywnego uczestnictwa w pracach Europejskiej Rady Ochrony Danych.

6. (...) Państwa członkowskie dopilnowują, 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 41

Ogólne warunki dotyczące członków organu nadzorczego

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

2. Członek lub członkowie posiadają kwalifikacje, doświadczenie i umiejętności niezbędne 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 42

Zasady ustanawiania organu nadzorczego

1**.** Państwa członkowskie stanowią prawem:

a) ustanowienie każdego z organów nadzorczych (...);

b) (...) kwalifikacje (...) niezbędne 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 niniejszej dyrektywy, która to kadencja może częściowo 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) (…)

1a. *Państwa członkowskie stanowią prawem, że* 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 43

Tajemnica służbowa

(…)

SEKCJA 2

ZADANIA **I UPRAWNIENIA**

Artykuł 44

Właściwość

1. Państwa członkowskie stanowią prawem, że każdy organ nadzorczy jest *na terytorium swojego państwa członkowskiego* właściwy do wykonywania zadań i korzystania (...) z uprawnień powierzonych mu zgodnie z niniejszą dyrektywą. (…)
2. Państwa członkowskie stanowią prawem, że organ nadzorczy nie jest właściwy do nadzorowania operacji przetwarzania dokonywanych przez (...) sądy w toku sprawowania przez nie wymiaru sprawiedliwości. Państwa członkowskie mogą ustanowić prawem, że organ nadzorczy nie jest właściwy do nadzorowania operacji przetwarzania dokonywanych przez inne niezależne organy sądowe w toku sprawowania przez nie wymiaru sprawiedliwości sprawiedliwości.

Artykuł 45

Zadania

1. Państwa członkowskie stanowią prawem, że każdy organ nadzorczy na swoim terytorium:
   a) monitoruje i egzekwuje stosowanie przepisów przyjętych na podstawie niniejszej dyrektywy oraz stosowanie odnośnych środków wykonawczych;
   aa) upowszechnia w społeczeństwie wiedzę o zagrożeniach, przepisach, gwarancjach i prawach związanych z przetwarzaniem danych osobowych oraz rozumienie tych zjawisk;
   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 podmiotów danych w związku z przetwarzaniem danych osobowych;
   ac) upowszechnia wśród administratorów i podmiotów przetwarzających wiedzę o ich obowiązkach wynikających z przepisów przyjętych na podstawie niniejszej dyrektywy;
   ad) zapewnia podmiotom danych na ich wniosek informacje o możliwości skorzystania z praw przysługujących im na mocy przepisów przyjętych na podstawie niniejszej dyrektywy, 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 i stosownie przez ten podmiot upoważnione (…), prowadzi w odpowiednim zakresie 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) sprawdza zgodność przetwarzania z prawem na mocy art. 15a (…) oraz informuje podmiot danych w rozsądnym terminie o wynikach tej kontroli – zgodnie z art. 15a ust. 3 – lub o powodach jej nieprzeprowadzenia;

d) współpracuje z innymi organami nadzorczymi, w tym dzieląc się informacjami, oraz świadczy im wzajemną pomoc w celu zapewnienia spójnego stosowania i egzekwowania przepisów przyjętych na podstawie niniejszej dyrektywy;

e) prowadzi dochodzenia w sprawie stosowania przepisów przyjętych na podstawie niniejszej dyrektywy (...), m.in. na podstawie informacji otrzymanych od innego organu nadzorczego lub innego organu publicznego (...) (...);

f) monitoruje zmiany w odpowiednich dziedzinach w zakresie, w jakim mają one wpływ na ochronę danych osobowych, w szczególności rozwój technologii informacyjno-komunikacyjnych (…);

g) (…)

h) udziela porad, o których mowa w art. 26, co do operacji przetwarzania;

i) wnosi wkład w działalność Europejskiej Rady Ochrony Danych.

2. (…)

3. (…)

4. (…)

5. Państwa członkowskie stanowią prawem, że każdy organ nadzorczy wykonuje zadania na rzecz podmiotów danych i inspektora ochrony danych, jeżeli istnieje, w sposób wolny od opłat.

6. Państwa członkowskie stanowią prawem, że (…) jeżeli wnioski są ewidentnie nieuzasadnione lub nadmierne, zwłaszcza ze względu na swój ustawiczny charakter, organ nadzorczy może odmówić podjęcia działań względem wniosku. Obowiązek wykazania, że wniosek ma ewidentnie nieuzasadniony lub nadmierny charakter, spoczywa na organie nadzorczym.

Artykuł 46

Uprawnienia

1. Każde państwo członkowskie stanowi prawem, że jego organ nadzorczy posiada (…) skuteczne uprawnienia *dochodzeniowe*, (…) przynajmniej uprawnienie, by uzyskiwać od administratora i podmiotu przetwarzającego dostęp do wszelkich przetwarzanych danych osobowych i wszelkich informacji niezbędnych mu do wykonania zadań.

1a. Każde państwo członkowskie stanowi prawem, że (...) jego organ nadzorczy posiada skuteczne uprawnienia korekcyjne, takie np. jak (…):

a) uprawnienie, by wydawać ostrzeżenia skierowane do administratora lub podmiotu przetwarzającego, że zamierzone operacje przetwarzania mogą skutkować naruszeniem przepisów przyjętych na podstawie niniejszej dyrektywy;

b) (…)

c) (…)

d) uprawnienie, by nakazać administratorowi lub podmiotowi przetwarzającemu dostosować operacje przetwarzania do przepisów przyjętych na podstawie niniejszej dyrektywy – w stosownym przypadku wskazując konkretny sposób i konkretny termin – a zwłaszcza by nakazać poprawić dane, ograniczyć ich przetwarzania lub usunąć je na mocy art. 15;

e) uprawnienie, by wprowadzać czasowe lub ostateczne ograniczenia przetwarzania.

f) (…)

1b. Każde państwo członkowskie stanowi prawem, że jego organ nadzorczy posiada (…) skuteczne uprawnienia doradcze, by udzielać porad administratorowi zgodnie z procedurą uprzednich konsultacji, o której mowa w art. 26, oraz by z własnej inicjatywy lub na wniosek wydawać 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.

2. Korzystanie z uprawnień powierzonych organowi nadzorczemu na mocy niniejszego artykułu podlega odpowiednim gwarancjom – w tym prawu do skutecznego sądowego 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 jest uprawniony, by (…) zgłaszać (…) organom wymiaru sprawiedliwości naruszenia przepisów przyjętych na podstawie niniejszej dyrektywy oraz w stosownym przypadku wszczynać lub w inny sposób *angażować się w postępowanie sądowe*, po to by wyegzekwować przepisy przyjęte na podstawie niniejszej dyrektywy.

Artykuł 47

Sprawozdanie z działalności

Państwa członkowskie stanowią prawem, że każdy organ nadzorczy sporządza roczne sprawozdanie z działalności. Sprawozdanie jest przekazywane parlamentowi narodowemu, rządowi i innym organom wskazanym prawem krajowym. Jest udostępniane opinii publicznej, Komisji Europejskiej oraz Europejskiej Radzie Ochrony Danych.

ROZDZIAŁ VII

WSPÓŁPRACA

Artykuł 48

Wzajemna pomoc

1. Państwa członkowskie stanowią prawem, że organy nadzorcze świadczą sobie wzajemną pomoc w celu spójnego wdrażania i stosowania przepisów przyjętych na podstawie niniejszej dyrektywy, (...) oraz wprowadzają środki na rzecz skutecznej wzajemnej współpracy. Wzajemna pomoc obejmuje w szczególności wnioski o udzielenie informacji oraz środki nadzorcze, takie jak wnioski o przeprowadzenie (...) kontroli i dochodzeń.
2. Państwa członkowskie stanowią prawem, że organ nadzorczy przedsiębierze 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. (…)

(…)

2b. Państwa członkowskie stanowią prawem, że 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 przyjętymi na podstawie niniejszej dyrektywy lub z prawem Unii, lub prawem państwa członkowskiego, któremu podlega organ nadzorczy będący adresatem wniosku.

3. Organ nadzorczy będący adresatem wniosku informuje organ nadzorczy, od którego wniosek pochodzi, o wynikach lub w stosownym przypadku o postępach lub środkach przedsięwziętych w celu udzielenia odpowiedzi na ten wniosek. Jeżeli odmawia na mocy ust. 2b, wyjaśnia powody odmowy.

3a. Informacji żądanych przez inne organy nadzorcze organ nadzorczy zasadniczo dostarcza drogą elektroniczną. (…)

3b. 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.

3c. 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 **(…)**. Odnośne akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 57 ust. 2.

Artykuł 49

Zadania Europejskiej Rady Ochrony Danych

1. Europejska Rada Ochrony Danych ustanowiona rozporządzeniem (UE) …./XXX wykonuje następujące zadania w odniesieniu do przetwarzania wchodzącego w zakres zastosowania niniejszej dyrektywy:

a) doradza Komisji w każdej sprawie związanej z ochroną danych osobowych w Unii, w tym w sprawie wszelkich proponowanych zmian do niniejszej dyrektywy;

b) *z własnej inicjatywy* lub *na wniosek jednego ze swoich członków* lub Komisji bada wszelkie kwestie dotyczące stosowania przepisów przyjętych na podstawie niniejszej dyrektywy i opracowuje wytyczne, zalecenia oraz wzorcowe rozwiązania (...), by zachęcić do spójnego stosowania tych przepisów;

ba) opracowuje wytyczne dla organów nadzorczych w sprawie stosowania środków, o których mowa w art. 46 ust. 1 i 1b (…);

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

d) wydaje opinie dla Komisji na temat poziomu ochrony w państwach trzecich lub organizacjach międzynarodowych;

e) propaguje współpracę oraz skuteczną dwu- i wielostronną wymianę informacji i rozwiązań 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.

2. Jeżeli Komisja występuje do Europejskiej Rady Ochrony Danych z wnioskiem o poradę, 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. 57 ust. 1, oraz podaje je do wiadomości publicznej.

4. Komisja informuje Europejską Radę Ochrony Danych o swoich działaniach w odniesieniu do opinii, wytycznych, zaleceń i wzorcowych rozwiązań opracowanych przez Europejską Radę Ochrony Danych.

ROZDZIAŁ VIII

ŚRODKI OCHRONY PRAWNEJ, ODPOWIEDZIALNOŚĆ PRAWNA I SANKCJE

Artykuł 50

Prawo do wniesienia skargi do organu nadzorczego

1. Bez uszczerbku dla innych administracyjnych lub sądowych środków ochrony prawnej państwa członkowskie stanowią prawem, że każdy podmiot danych ma prawo wnieść skargę do jednego (...) organu nadzorczego, jeżeli (...) sądzi, że przetwarzanie danych osobowych go dotyczących nie jest zgodne z przepisami przyjętymi na podstawie niniejszej dyrektywy.

1a. Państwa członkowskie stanowią prawem, że jeżeli skarga nie zostaje wniesiona do organu nadzorczego właściwego zgodnie z art. 44 ust. 1, organ nadzorczy, do którego wniesiono skargę, przekazuje ją bez zbędnej zwłoki właściwemu organowi nadzorczemu. O przekazaniu skargi zostaje poinformowany podmiot danych.

1b. Państwa członkowskie stanowią prawem, że organ nadzorczy, do którego wniesiono skargę, udziela podmiotowi danych dalszej pomocy na jego żądanie.

2. (…)

2a. (…) Właściwy organ nadzorczy informuje podmiot danych o postępach i efektach rozpatrywania skargi, w tym o możliwości skorzystania z sądowego środka ochrony prawnej na mocy art. 51.

3. (…)

Artykuł 51

Prawo do skutecznego sądowego środka ochrony prawnej przeciwko organowi nadzorczemu

1. Bez uszczerbku dla innych administracyjnych lub pozasądowych środków ochrony prawnej państwa członkowskie stanowią prawem, że 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. 44 ust. 1 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. 50.

3. Państwa członkowskie stanowią prawem, że postępowanie przeciwko organowi nadzorczemu zostaje wszczęte przed sądem państwa członkowskiego, w którym organ nadzorczy ma siedzibę.

Artykuł 52

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

Bez uszczerbku dla dostępnych administracyjnych lub pozasądowych środków ochrony prawnej, w tym prawa do wniesienia skargi do organu nadzorczego na mocy art. 50, państwa członkowskie stanowią prawem, że podmiot danych ma prawo do skutecznego sądowego środka ochrony prawnej, jeżeli sądzi, że jego prawa wynikające z przepisów przyjętych na podstawie niniejszej dyrektywy zostały naruszone w wyniku przetwarzania jego danych osobowych niezgodnie z tymi przepisami.

Artykuł 53

(...) Reprezentowanie podmiotu danych

1. Państwa członkowskie stanowią prawem zgodnie z krajowym prawem procesowym, że 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 jego imieniu* oraz skorzystanie z praw, o których mowa w art. 50, 51 i 52, w jego imieniu.
2. (…)
3. (…)

Artykuł 54

(...) Prawo do odszkodowania (…)

1. Państwa członkowskie stanowią prawem, że każda osoba, która poniosła szkodę (…) w wyniku (...) operacji przetwarzania niezgodnej z prawem lub w wyniku czynności niezgodnej z krajowymi (…) przepisami przyjętymi na podstawie niniejszej dyrektywy, ma prawo otrzymać od administratora lub innego organu właściwego w świetle prawa krajowego odszkodowanie za poniesioną szkodę.
2. (…)
3. (…)
4. (…)
5. (…)

Artykuł 55

Kary

Państwa członkowskie ustanawiają przepisy o karach za naruszenie przepisów przyjętych na podstawie niniejszej dyrektywy i przedsiębiorą wszelkie niezbędne środki w celu zapewnienia ich wdrożenia. Przewidziane kary muszą być skuteczne, proporcjonalne i odstraszające.

ROZDZIAŁ IX

(...) AKTY WYKONAWCZE

Artykuł 56

Korzystanie z przekazanych uprawnień

(…)

Artykuł 57

Procedura komitetowa

1. Komisję wspomaga komitet ustanowiony na mocy art. 87 rozporządzenia (UE) XXX. 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 X
PRZEPISY KOŃCOWE

Artykuł 58

Przepisy uchylające

1. Uchyla się decyzję ramową Rady 2008/977/WSiSW ze skutkiem od daty, o której mowa w art. 62 ust. 1.
2. Odesłania do uchylonej decyzji ramowej, o której mowa w ust. 1, należy interpretować jako odesłania do niniejszej dyrektywy.

Artykuł 59

Stosunek do uprzednio przyjętych aktów Unii o współpracy wymiarów sprawiedliwości w sprawach karnych oraz o współpracy policyjnej

Dyrektywa nie wpływa na szczegółowe przepisy o ochronie danych osobowych **(…)** – przewidziane w aktach Unii przyjętych w dziedzinie współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej przed datą przyjęcia niniejszej dyrektywy – regulujące przetwarzanie danych osobowych między państwami członkowskimi lub dostęp wyznaczonych organów państw członkowskich do systemów informacyjnych ustanowionych na mocy traktatów w ramach zastosowania niniejszej dyrektywy.

Artykuł 60

Stosunek do uprzednio zawartych umów międzynarodowych o współpracy wymiarów sprawiedliwości w sprawach karnych oraz o współpracy policyjnej

Umowy międzynarodowe, które obejmują przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych i które zostały zawarte przez państwa członkowskie przed wejściem niniejszej dyrektywy w życie, i które są zgodne z prawem Unii mającym zastosowanie przed wejściem niniejszej dyrektywy w życie, pozostają w mocy do czasu ich zmiany, zastąpienia lub uchylenia. (…)

Artykuł 61

Ocena

1. Komisja ocenia stosowanie niniejszej dyrektywy. W kontekście tej oceny Komisja analizuje w szczególności stosowanie i funkcjonowanie art. 36aa.

2. W ciągu pięciu lat po wejściu niniejszej dyrektywy w życie Komisja dokonuje przeglądu innych przyjętych przez Unię Europejską aktów regulujących przetwarzanie danych osobowych przez właściwe organy do celów określonych w art. 1 ust. 1 – w tym przyjętych przez Unię aktów określonych w art. 59 – by ocenić potrzebę dostosowania ich do niniejszej dyrektywy, i w razie potrzeby przedstawia niezbędne propozycje ich zmiany celem zapewnienia spójnego podejścia do ochrony danych osobowych wchodzących w zakres zastosowania niniejszej dyrektywy.

3. Komisja regularnie przedkłada Parlamentowi Europejskiemu i Radzie sprawozdania z oceny i przeglądu niniejszej dyrektywy na mocy ust. 1. Pierwsze sprawozdania przedkłada najpóźniej cztery lata po wejściu niniejszej dyrektywy w życie. Kolejne sprawozdania przedkłada co cztery lata. W razie potrzeby Komisja przedkłada odpowiednie propozycje zmian do niniejszej dyrektywy oraz propozycje dostosowania innych instrumentów prawnych. Sprawozdanie jest podawane do wiadomości publicznej.

Artykuł 62

Wdrożenie

1. Państwa członkowskie przyjmują i publikują najpóźniej do dnia [data/trzy lata po wejściu w życie] przepisy ustawowe, wykonawcze i administracyjne niezbędne do wykonania niniejszej dyrektywy. Tekst tych przepisów przekazują niezwłocznie Komisji. Państwa członkowskie stosują te przepisy od dnia xx.xx.201x [data/trzy lata po wejściu w życie]. Przepisy przyjęte przez państwa członkowskie zawierają odniesienie do niniejszej dyrektywy lub odniesienie takie towarzyszy ich urzędowej publikacji. Metody dokonywania takiego odniesienia określane są przez państwa członkowskie.
2. Państwa członkowskie przekazują Komisji tekst podstawowych przepisów prawa krajowego przyjętych w dziedzinie objętej niniejszą dyrektywą.

Artykuł 63

Wejście w życie (...)

Niniejsza dyrektywa wchodzi w życie pierwszego dnia po opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Artykuł 64

Adresaci

Niniejsza dyrektywa jest skierowana do państw członkowskich.