DECYZJA KOMISJI (UE) 2021/2243

z dnia 15 grudnia 2021 r.

ustanawiająca przepisy wewnętrzne dotyczące przekazywania informacji osobom, których dane dotyczą, oraz ograniczenia niektórych ich praw w kontekście przetwarzania danych osobowych do celów bezpieczeństwa systemów teleinformatycznych Komisji

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 249 ust. 1,

a także mając na uwadze, co następuje:

(1) Przy wykonywaniu swoich zadań Komisja jest zobowiązana do poszanowania praw osób fizycznych w związku z przetwarzaniem danych osobowych zgodnie z art. 8 ust. 1 Karty praw podstawowych Unii Europejskiej i art. 16 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej. Komisja musi również przestrzegać praw przewidzianych w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2018/1725 ([1]). Jednocześnie Komisja musi zajmować się incydentami związanymi z bezpieczeństwem IT zgodnie z zasadami określonymi w art. 15 decyzji (UE, Euratom) 2017/46 ([2]).

(2) W celu zapewnienia bezpieczeństwa IT, tj. zachowania poufności, integralności i dostępności systemów teleinformatycznych oraz zbiorów danych, które są w nich przetwarzane, w odniesieniu do osób, mienia i informacji, Komisja, w szczególności za pośrednictwem Dyrekcji Generalnej ds. Informatyki, wprowadziła środki przewidziane w decyzji (UE, Euratom) 2017/46 i w decyzji C(2017) 8841 final ([3]). Środki te obejmują monitorowanie ryzyka związanego z bezpieczeństwem IT i wdrożonych środków bezpieczeństwa IT, zwracanie się do właścicieli systemów o wprowadzenie konkretnych środków bezpieczeństwa IT w celu ograniczenia ryzyka dla bezpieczeństwa IT dla systemów teleinformatycznych Komisji, a także zarządzanie incydentami związanymi z bezpieczeństwem IT.

(3) Dyrekcja Generalna ds. Informatyki realizuje działania i usługi w zakresie bezpieczeństwa IT Komisji i musi przetwarzać kilka kategorii danych osobowych w celu:

— przekazywania alarmów i ostrzeżeń dotyczących zdarzeń i incydentów związanych z bezpieczeństwem IT,

— reagowania na zdarzenia i incydenty związane z bezpieczeństwem IT oraz ich opanowania,

— ułatwiania dostępu do narzędzi i działań poprzez audyty bezpieczeństwa, oceny bezpieczeństwa i zarządzanie lukami w zabezpieczeniach,

— zwiększania świadomości pracowników Komisji w dziedzinie cyberbezpieczeństwa,

— monitorowania i wykrywania zdarzeń i incydentów związanych z bezpieczeństwem IT oraz zapobiegania im,

— dokonywania przeglądu kont użytkowników uprzywilejowanych.

(4) W każdej operacji przetwarzania danych prowadzonej przez Komisję mogą wystąpić incydenty związane z bezpieczeństwem IT, które mogłyby zagrozić bezpieczeństwu systemów teleinformatycznych Komisji. Mogą one dotyczyć dowolnej kategorii danych osobowych przetwarzanych przez Komisję.

([1]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz.U. L 295 z 21.11.2018, s. 39).

([2]) Decyzja Komisji (UE, Euratom) 2017/46 z dnia 10 stycznia 2017 r. w sprawie bezpieczeństwa systemów teleinformatycznych w Komisji Europejskiej (Dz.U. L 6 z 11.1.2017, s. 40).

([3]) Decyzja Komisji (C(2017) 8841) z dnia 13 grudnia 2017 r. ustanawiająca przepisy wykonawcze do art. 3, 5, 7–12, 14 i 15 decyzji Komisji (UE, Euratom) 2017/46 w sprawie bezpieczeństwa systemów teleinformatycznych w Komisji.

(5) W określonych sytuacjach może okazać się konieczne pogodzenie praw osób, których dane dotyczą, na podstawie rozporządzenia (UE) 2018/1725 z potrzebą skutecznego wykonywania przez Komisję jej zadań w zakresie zapewnienia bezpieczeństwa IT osób, mienia i informacji w Komisji na podstawie decyzji (UE, Euratom) 2017/46, a także z pełnym poszanowaniem podstawowych praw i wolności innych osób, których dane dotyczą. W tym celu art. 25 ust. 1 rozporządzenia (UE) 2018/1725 uprawnia Komisję do ograniczenia zastosowania art. 14–17, 19, 20 i 35 tego rozporządzenia, a także zasady przejrzystości określonej w jego art. 4 ust. 1 lit. a), o ile ich przepisy odpowiadają prawom i obowiązkom przewidzianym w art. 14–17, 19 i 20 tego rozporządzenia.

(6) Niniejsza decyzja powinna mieć zastosowanie do wszystkich operacji przetwarzania danych przeprowadzanych przez Komisję jako administratora danych w ramach wykonywania jej zadań polegających na zapewnieniu bezpieczeństwa IT osób, mienia i informacji w Komisji zgodnie z decyzją (UE, Euratom) 2017/46. W związku z tym powinna ona dotyczyć osób, których dotyczą dane należące do kategorii danych osobowych objętych wszystkimi tymi operacjami przetwarzania, tj. osób, które wchodzą w interakcję z dowolnymi systemami teleinformatycznymi Komisji.

(7) Dane osobowe są przechowywane w zabezpieczonym środowisku elektronicznym w celu zapobieżenia bezprawnemu dostępowi do danych osobom spoza Komisji. Do różnych operacji przetwarzania mają zastosowanie różne okresy zatrzymywania danych, w zależności od rodzaju danych osobowych. Kwestię zatrzymywania dokumentacji w Komisji reguluje wspólny wykaz zatrzymywanych danych na poziomie Komisji (SEC(2019) 900), dokument regulacyjny w formie harmonogramu, w którym określono okresy zatrzymywania różnych rodzajów dokumentacji Komisji w celu ograniczenia zatrzymywania danych do tego, co jest konieczne.

(8) Komisja może być zmuszona do ograniczenia stosowania praw osób, których dane dotyczą, w celu ochrony swojego bezpieczeństwa wewnętrznego zgodnie z art. 25 ust. 1 lit. d) rozporządzenia (UE) 2018/1725 (tj. w celu zachowania poufności, integralności i dostępności swoich systemów teleinformatycznych oraz zbiorów danych, które są w nich przetwarzane, swojego mienia i informacji). W szczególności Komisja może być zmuszona do uczynienia tego podczas:

— przekazywania alarmów i ostrzeżeń dotyczących zdarzeń i incydentów związanych z bezpieczeństwem IT,

— reagowania na zdarzenia i incydenty związane z bezpieczeństwem IT oraz ich opanowania; ułatwiania dostępu do narzędzi i działań poprzez audyty bezpieczeństwa, oceny bezpieczeństwa i zarządzanie lukami w zabezpieczeniach,

— zwiększania świadomości pracowników Komisji w dziedzinie cyberbezpieczeństwa,

— monitorowania i wykrywania zdarzeń i incydentów związanych z bezpieczeństwem IT oraz zapobiegania im,

— dokonywania przeglądu kont użytkowników uprzywilejowanych.

(9) Do celów postępowania w przypadku incydentów związanych z bezpieczeństwem IT, o których mowa w art. 15 decyzji (UE, Euratom) 2017/46, Dyrekcja Generalna ds. Informatyki może wymieniać informacje z zespołem reagowania na cyberataki Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa.

(10) Aby zapewnić zgodność z art. 14–16 rozporządzenia (UE) 2018/1725, Komisja powinna informować wszystkie osoby fizyczne o działaniach, które wiążą się z przetwarzaniem ich danych osobowych i które mają wpływ na ich prawa. Powinna to uczynić w sposób przejrzysty i spójny, publikując na stronie internetowej Komisji notę o ochronie danych. W stosownych przypadkach Komisja powinna wprowadzić dodatkowe środki ochronne, aby indywidualnie i w odpowiedni sposób poinformować osoby, których dane dotyczą.

(11) Zastosowanie się do art. 14–16 rozporządzenia (UE) 2018/1725 ustanowionych na podstawie art. 15 decyzji (UE, Euratom) 2017/46 mogłoby ujawnić istnienie środków bezpieczeństwa IT, luk w zabezpieczeniach lub incydentów. Ujawnienie tych środków bezpieczeństwa IT, luk w zabezpieczeniach i incydentów zwiększa ryzyko obejścia ujawnionego środka bezpieczeństwa IT, wykorzystania ujawnionej luki oraz możliwości podważenia trwającej analizy incydentów związanych z bezpieczeństwem IT, ponieważ użytkownik lub podmiot działający w złych zamiarach mógłby przypadkowo lub celowo manipulować artefaktami. Mogłoby to poważnie zaszkodzić zdolności Komisji do zapewnienia bezpieczeństwa swoich systemów IT, a w szczególności do skutecznego reagowania w przyszłości na incydenty związane z bezpieczeństwem IT.

(12) Na podstawie art. 25 ust. 1 lit. h) rozporządzenia (UE) 2018/1725 Komisja jest również uprawniona do ograniczenia stosowania praw osób, których dane dotyczą, w celu ochrony praw i wolności innych osób w związku ze zdarzeniami związanymi z bezpieczeństwem IT, które mogłyby zagrozić działaniom w zakresie bezpieczeństwa IT.

(13) Komisja może również być zmuszona do ograniczenia udzielania informacji osobom, których dane dotyczą, i ograniczenia stosowania innych praw tych osób w odniesieniu do danych osobowych otrzymywanych od państw niebędącymi członkiem UE lub organizacji międzynarodowych, aby wywiązać się z obowiązku współpracy z tymi państwami lub organizacjami. Stanowi to część spoczywającego na Komisji obowiązku ochrony ważnego celu leżącego w ogólnym interesie publicznym UE, o którym mowa w art. 25 ust. 1 lit. c) rozporządzenia (UE) 2018/1725. W pewnych okolicznościach konieczność ochrony praw podstawowych osoby, której dane dotyczą, może jednak przeważać nad interesem współpracy międzynarodowej.

(14) W związku z tym Komisja określiła powody wymienione w art. 25 ust. 1 lit. c), d) i h) rozporządzenia (UE) 2018/1725 jako podstawę ograniczeń, których zastosowanie może być konieczne do operacji przetwarzania danych przeprowadzanych przez Dyrekcję Generalną ds. Informatyki w związku z realizacją działań i usług związanych z bezpieczeństwem IT na rzecz Komisji.

(15) Wszelkie ograniczenia, stosowane na podstawie niniejszej decyzji, powinny być konieczne i proporcjonalne, biorąc pod uwagę zagrożenia dla praw i wolności osób, których dane dotyczą.

(16) Komisja powinna rozpatrywać wszystkie ograniczenia w sposób przejrzysty i każde zastosowanie ograniczeń odnotować w odpowiednim systemie rejestracji.

(17) Na podstawie art. 25 ust. 8 rozporządzenia (UE) 2018/1725 administratorzy danych mogą wstrzymać przekazanie informacji, pominąć je lub go odmówić w oparciu o powody zastosowania ograniczenia w stosunku do osoby, której dane dotyczą, jeżeli przekazanie tych informacji mogłoby w jakikolwiek sposób podważyć skutek tego ograniczenia. Dotyczy to w szczególności ograniczeń obowiązków przewidzianych w art. 16 i 35 rozporządzenia (UE) 2018/1725. Komisja powinna regularnie dokonywać przeglądu nałożonych ograniczeń w celu zapewnienia, aby prawa osoby, której dane dotyczą, do uzyskania informacji zgodnie z art. 16 i 35 rozporządzenia (UE) 2018/1725 były ograniczone tylko tak długo, jak długo takie ograniczenia są konieczne, aby umożliwić Komisji zapewnienie swojego bezpieczeństwa systemów IT i w szczególności zajęcie się incydentami związanymi z bezpieczeństwem IT.

(18) W przypadku gdy Komisja ogranicza stosowanie praw osób, których dane dotyczą, innych niż te, o których mowa w art. 16 i 35 rozporządzenia (UE) 2018/1725, administrator danych powinien ocenić w poszczególnych przypadkach, czy powiadomienie o ograniczeniu naruszyłoby cel ograniczenia.

(19) Inspektor ochrony danych Komisji powinien przeprowadzić niezależny przegląd stosowania ograniczeń w celu zapewnienia zgodności z niniejszą decyzją.

(20) Aby umożliwić Komisji natychmiastowe ograniczenie stosowania niektórych praw i obowiązków zgodnie z art. 25 rozporządzenia (UE) 2018/1725, niniejsza decyzja powinna wejść w życie dwudziestego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

(21) Europejski Inspektor Ochrony Danych wydał opinię w dniu 16 września 2021 r.,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

Przedmiot i zakres

1. Niniejsza decyzja ustanawia zasady obowiązujące Komisję w zakresie informowania osób, których dane dotyczą, o przetwarzaniu ich danych osobowych zgodnie z art. 14–16 rozporządzenia (UE) 2018/1725, kiedy realizuje ona swoje zadania zgodnie z decyzją (UE, Euratom) 2017/46.

Decyzja określa również warunki, na jakich Komisja może ograniczyć stosowanie art. 4, 14–17, 19, 20 i 35 rozporządzenia (UE) 2018/1725, zgodnie z jego art. 25 ust. 1 lit. c), d) i h), kiedy realizuje ona swoje zadania zgodnie z decyzją (UE, Euratom) 2017/46.

2. Niniejsza decyzja ma zastosowanie do przetwarzania danych osobowych przez Komisję lub w jej imieniu do celów działań zmierzających do zapewnienia bezpieczeństwa IT osób, mienia i informacji w Komisji zgodnie z decyzją (UE, Euratom) 2017/46 lub w związku z takimi działaniami.

Artykuł 2

Obowiązujące wyjątki i ograniczenia

1. Wykonując swoje obowiązki w odniesieniu do praw osób, których dane dotyczą, na podstawie rozporządzenia (UE) 2018/1725, Komisja uwzględnia, czy zastosowanie mają jakiekolwiek wyjątki określone w tym rozporządzeniu.

2. Z zastrzeżeniem art. 3–7 niniejszej decyzji, w przypadku gdy wykonywanie praw i obowiązków przewidzianych w art. 14–17, 19, 20 i 35 rozporządzenia (UE) 2018/1725 w odniesieniu do danych osobowych przetwarzanych przez Komisję zagrażałoby celowi realizacji działań i usług w zakresie bezpieczeństwa IT, między innymi przez ujawnienie czynności dochodzeniowych, luk w zabezpieczeniach i metod Komisji, lub mogłoby mieć niekorzystny wpływ na prawa i wolności oraz bezpieczeństwo innych osób, których dane dotyczą, w szczególności w odniesieniu do przetwarzania danych osobowych w celu:

— przekazywania alarmów i ostrzeżeń dotyczących zdarzeń i incydentów związanych z bezpieczeństwem IT,

— reagowania na zdarzenia i incydenty związane z bezpieczeństwem IT oraz ich opanowania,

— ułatwiania dostępu do narzędzi i działań poprzez audyty bezpieczeństwa, oceny bezpieczeństwa i zarządzanie lukami w zabezpieczeniach,

— zwiększania świadomości pracowników Komisji w dziedzinie cyberbezpieczeństwa,

— monitorowania i wykrywania zdarzeń i incydentów związanych z bezpieczeństwem IT oraz zapobiegania im,

— dokonywania przeglądu kont użytkowników uprzywilejowanych.

Komisja może ograniczyć stosowanie:

a) art. 14–17, art. 19, 20 i 35 rozporządzenia (UE) 2018/1725;

b) zasady przejrzystości określonej w art. 4 ust. 1 lit. a) rozporządzenia (UE) 2018/1725 w zakresie, w jakim jego przepisy odpowiadają prawom i obowiązkom przewidzianym w art. 14–17, 19 i 20 rozporządzenia (UE) 2018/1725.

Komisja może to uczynić zgodnie z art. 25 ust. 1 lit. c), d) i h) rozporządzenia (UE) 2018/1725.

3. Z zastrzeżeniem art. 3–7 Komisja może ograniczyć prawa i obowiązki, o których mowa w ust. 2 niniejszego artykułu:

a) gdy wykonywanie tych praw i obowiązków w odniesieniu do danych osobowych uzyskanych od innych instytucji, organów i jednostek organizacyjnych UE mogłoby zostać ograniczone przez tę inną instytucję, organ lub jednostkę organizacyjną UE na podstawie aktów prawnych, o których mowa w art. 25 rozporządzenia (UE) 2018/1725, lub zgodnie z rozdziałem IX tego rozporządzenia lub zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/794 ([4]) lub zgodnie z rozporządzeniem Rady (UE) 2017/1939 ([5]);

b) gdy wykonywanie tych praw i obowiązków w odniesieniu do danych osobowych uzyskanych od właściwego organu państwa członkowskiego mogłoby zostać ograniczone przez właściwe organy tego państwa członkowskiego na podstawie aktów prawnych, o których mowa w art. 23 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 ([6]) lub na podstawie środków krajowych transponujących art. 13 ust. 3, art. 15 ust. 3 lub art. 16 ust. 3 dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 ([7]);

([4]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/794 z dnia 11 maja 2016 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol), zastępujące i uchylające decyzje Rady 2009/371/WSiSW, 2009/934/WSiSW, 2009/935/WSiSW, 2009/936/WSiSW i 2009/968/WSiSW (Dz.U. L 135 z 24.5.2016, s. 53).

([5]) Rozporządzenie Rady (UE) 2017/1939 z dnia 12 października 2017 r. wdrażające wzmocnioną współpracę w zakresie ustanowienia Prokuratury Europejskiej (Dz.U. L 283 z 31.10.2017, s. 1).

([6]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1).

([7]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz.U. L 119 z 4.5.2016, s. 89).

c) gdy wykonywanie tych praw i obowiązków naruszyłoby współpracę Komisji z państwami niebędącymi członkiem UE lub organizacjami międzynarodowymi w zakresie wspólnych zagrożeń cyberbezpieczeństwa.

Przed zastosowaniem ograniczeń w okolicznościach, o których mowa w akapicie pierwszym lit. a) i b), Komisja konsultuje się z odpowiednimi instytucjami, organami, agencjami, jednostkami organizacyjnymi UE lub władzami państw członkowskich w sprawie potencjalnych podstaw nałożenia ograniczeń oraz konieczności i proporcjonalności takich ograniczeń, chyba że zagroziłoby to działalności Komisji a dla Komisji jest jasne, że jeden z aktów, o których mowa w tych punktach przewiduje stosowanie ograniczenia, lub konsultacje podważyły cel jej działalności przewidzianej na podstawie decyzji (UE, Euratom) 2017/46.

Akapit pierwszy lit. c) nie ma zastosowania, w przypadku gdy interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, przeważają nad interesem Komisji dotyczącym współpracy z państwami niebędącymi członkiem UE lub organizacjami międzynarodowymi.

4. Ustępy 1, 2 i 3 pozostają bez uszczerbku dla stosowania innych decyzji Komisji ustanawiających przepisy wewnętrzne regulujące przekazywanie informacji osobom, których dane dotyczą, oraz dla ograniczeń stosowania niektórych praw wynikających z art. 25 rozporządzenia (UE) 2018/1725.

5. Wszelkie ograniczenia praw i obowiązków, o których mowa w ust. 2, powinny być konieczne i proporcjonalne do zagrożeń dla praw i wolności osób, których dane dotyczą.

6. Analizę konieczności i proporcjonalności przeprowadza się indywidualnie w poszczególnych przypadkach przed zastosowaniem ograniczeń, a ograniczenia nie wykraczają poza to, co jest absolutnie niezbędne do osiągnięcia zamierzonego celu.

Artykuł 3

Przekazywanie informacji osobom, których dane dotyczą

1. Komisja publikuje na swojej stronie internetowej notę o ochronie danych, w którym informuje wszystkie osoby, których dane dotyczą, o swoich działaniach wiążących się z przetwarzaniem ich danych osobowych do celów wykonywania zadań Komisji wynikających z decyzji (UE, Euratom) 2017/46, w tym opis kategorii takich danych osobowych. Jeśli jest to możliwe bez szkody dla bezpieczeństwa IT, Komisja zapewnia, aby osoby, których dane dotyczą, były we właściwy sposób indywidualnie informowane.

2. W przypadku gdy Komisja ogranicza, w całości lub w części, przekazywanie informacji osobom, których dane osobowe przetwarza do celów wykonywania swoich zadań na mocy decyzji (UE, Euratom) 2017/46, odnotowuje ona i rejestruje powody ograniczenia zgodnie z art. 6 tej decyzji.

Artykuł 4

Prawo dostępu dla osób, których dane dotyczą, prawo do usunięcia danych oraz prawo do ograniczenia przetwarzania danych

1. W przypadku gdy Komisja ogranicza, w całości lub w części, prawo dostępu do danych osobowych osób, których dane dotyczą, prawo do usunięcia danych lub prawo do ograniczenia przetwarzania danych, o których to prawach mowa w art. 17, 19 i 20 rozporządzenia (UE) 2018/1725, informuje ona zainteresowaną osobę, której dane dotyczą, w odpowiedzi na wniosek o dostęp, usunięcie lub ograniczenie przetwarzania danych:

a) o zastosowanym ograniczeniu i jego głównych przyczynach oraz

b) o tym, jak złożyć skargę za pośrednictwem Europejskiego Inspektora Ochrony Danych lub jak odwołać się do Trybunału Sprawiedliwości Unii Europejskiej.

2. Komisja może wstrzymać lub pominąć przekazywanie informacji dotyczących przyczyn zastosowania ograniczenia, o których mowa w akapicie pierwszym, lub odmówić przekazywania takich informacji, w zakresie, w jakim podważyłoby to cel nałożonego ograniczenia.

3. Zgodnie z art. 6 Komisja odnotowuje i rejestruje powody ograniczenia.

4. W przypadku gdy prawo dostępu jest w całości lub w części ograniczone, osoby, których dane dotyczą, mogą skorzystać z prawa dostępu kontaktując się z Europejskim Inspektorem Ochrony Danych zgodnie z art. 25 ust. 6, 7 i 8 rozporządzenia (UE) 2018/1725.

Artykuł 5

Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych

W przypadku gdy Komisja ogranicza zawiadomienie o naruszeniu ochrony danych osobowych osoby, której dane dotyczą, o którym to zawiadomieniu mowa w art. 35 rozporządzenia (UE) 2018/1725, odnotowuje ona i rejestruje powody ograniczenia zgodnie z art. 6 niniejszej decyzji. Komisja przekazuje protokół Europejskiemu Inspektorowi Ochrony Danych w momencie zgłoszenia naruszenia ochrony danych osobowych.

Artykuł 6

Odnotowywanie i rejestrowanie ograniczeń

1. Komisja odnotowuje przyczyny wszelkich ograniczeń zastosowanych na podstawie niniejszej decyzji, dodając odniesienie do podstaw prawnych ograniczeń oraz ocenę konieczności i proporcjonalności tych ograniczeń, z uwzględnieniem odpowiednich elementów określonych w art. 25 ust. 2 rozporządzenia (UE) 2018/1725.

2. W zapisie określa się, w jaki sposób wykonywanie prawa przez osobę, której dane dotyczą, podważyłoby cel realizacji działań i usług w zakresie bezpieczeństwa IT na rzecz Komisji zgodnie z decyzją (UE, Euratom) 2017/46 lub cel stosowania ograniczeń na podstawie art. 2 ust. 2 lub 3 niniejszej decyzji, lub wpłynęłoby negatywnie na prawa i wolności innych osób, których dane dotyczą.

3. Komisja rejestruje te wpisy i wszelkie dokumenty zawierające elementy faktyczne i prawne leżące u podstaw tych ograniczeń. Udostępnia się je na żądanie Europejskiemu Inspektorowi Ochrony Danych.

Artykuł 7

Okres obowiązywania ograniczeń

1. Ograniczenia, o których mowa w art. 3–5, mają zastosowanie tak długo, jak długo istnieją powody uzasadniające ich zastosowanie.

2. Jeżeli powody ograniczenia, o którym mowa w art. 3–5, tracą ważność, Komisja:

a) znosi ograniczenie;

b) informuje osobę, której dane dotyczą, o głównych powodach ograniczenia;

c) informuje o tym, jak można złożyć, w dowolnym momencie, skargę za pośrednictwem Europejskiego Inspektora Ochrony Danych lub o tym, jak odwołać się do Trybunału Sprawiedliwości Unii Europejskiej.

Artykuł 8

Zabezpieczenia i okresy przechowywania

1. Komisja dokonuje przeglądu stosowania ograniczeń, o których mowa w art. 3–5, sześć miesięcy po ich przyjęciu i oraz z chwilą zamknięcia poszczególnego działania w zakresie bezpieczeństwa IT. Następnie raz w roku Komisja poddaje przeglądowi i monitoruje konieczność podtrzymania jakiegokolwiek ograniczenia.

Przegląd obejmuje ocenę konieczności i proporcjonalności ograniczenia, z uwzględnieniem odpowiednich elementów określonych w art. 25 ust. 2 rozporządzenia (UE) 2018/1725.

2. Komisja przyjęła środki techniczne i organizacyjne, aby uniknąć przypadkowego lub bezprawnego zniszczenia, utraty, zmiany, nieuprawnionego ujawnienia lub dostępu do danych osobowych przekazywanych, przechowywanych lub przetwarzanych w inny sposób, takich jak zarządzanie prawami dostępu, polityka tworzenia kopii zapasowych i wszelkie inne środki zgodne z decyzją (UE, Euratom) 2017/46.

3. Komisja odnotowuje mające zastosowanie okresy zatrzymywania zgodnie ze wspólnym wykazem zatrzymywanych danych na poziomie Komisji i udostępnia osobom, których dane dotyczą, informacje o odpowiednich okresach zatrzymywania tych czynności przetwarzania w swojej nocie o ochronie danych.

Artykuł 9

Przegląd dokonywany przez inspektora ochrony danych Komisji

1. Inspektor ochrony danych Komisji jest niezwłocznie informowany, ilekroć prawa osób, których dane dotyczą, są ograniczone zgodnie z niniejszą decyzją. Inspektor ochrony danych otrzymuje, na żądanie, dostęp do zapisu oraz wszelkich dokumentów zawierających elementy faktyczne i prawne leżące u podstaw tych ograniczeń.

2. Inspektor ochrony danych może zwrócić się o dokonanie przeglądu ograniczeń i jest informowany o wyniku wnioskowanego przeglądu.

3. Komisja dokumentuje działania inspektora ochrony danych, ilekroć prawa osób, których dane dotyczą, są ograniczone zgodnie z niniejszą decyzją.

Artykuł 10

Wejście w życie

Niniejsza decyzja wchodzi w życie dwudziestego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Sporządzono w Brukseli dnia 15 grudnia 2021 r.

W imieniu Komisji
Ursula VON DER LEYEN
Przewodnicząca