KOMUNIKAT PRASOWY

EDPS/2016/08

Bruksela, dnia 21 marca 2016 r.

Wytyczne EIOD w zakresie zabezpieczenia informacji i ciągłości działania

W niniejszych, opublikowanych dzisiaj **Wytycznych** *w zakresie zarządzania ryzykiem bezpieczeństwa informacji,* Europejski Inspektor Ochrony Danych przekazuje instytucjom unijnym wskazówki dotyczące zapewnienia bezpiecznego i zaufanego środowiska cyfrowego dla informacji o kluczowym znaczeniu dla funkcjonowania jej służb.

Zastępca Inspektora Wojciech Wiewiórowski powiedział: *„Bezpieczeństwo danych osobowych stanowi nie tylko wymóg prawa, lecz jest konieczne także w interesie organizacji, których codzienna praca zależy od wykorzystywania informacji. Niezmiernie ważne jest, by utrzymywały one odpowiedni poziom bezpieczeństwa informacji, ponieważ od tego zależy wartość i wydajność ich pracy. Apeluję do struktur instytucji unijnych o zaangażowanie się w dostosowane do potrzeb opracowywanie i wykorzystywanie procesów zarządzania ryzykiem bezpieczeństwa informacji w celu spełnienia konkretnych potrzeb poszczególnych instytucji."*

Poszczególne struktury organizacyjne muszą stawić czoła różnym rodzajom ryzyka dla bezpieczeństwa wykorzystywanych przez nie informacji. Wydajnym narzędziem identyfikacji rozwiązań odpowiadających konkretnym rodzajom ryzyka, jakim stawia czoła dana instytucja, są nowoczesne metody oceny ryzyka, które stanowią także uzasadniony cel wykorzystania zasobów finansowych i informatycznych w celu ich opracowania.

Zarządzanie ryzykiem bezpieczeństwa informacji w zakresie danych osobowych wymaga specjalistycznej wiedzy w dziedzinie bezpieczeństwa informacji i bezpieczeństwa informatycznego, a także ochrony danych. Inspektorzy ochrony danych (DPO) powinni wspierać ekspertów bezpieczeństwa informacji i bezpieczeństwa informatycznego w opracowywaniu takich procesów.

Wyłącznie techniczne rozwiązania w zakresie bezpieczeństwa nie rozwiążą jednak problemu bezpieczeństwa informacji. Za wyegzekwowanie decyzji, które mają wpływa na aplikacje i obsługującą je infrastrukturę informatyczną, ostateczną odpowiedzialność ponosi struktura kierownicza danej organizacji. Kierownictwo musi wspierać opracowywanie i wdrażanie polityk oraz mobilizować zasoby wymagane do tego, by przeciwdziałać konkretnym ryzykom dla informacji, które występują dla danej organizacji.

Choć niniejsze Wytyczne są zasadniczo skierowane do instytucji UE, mogą okazać się przydatne dla wszystkich osób zainteresowanych problematyką ochrony danych osobowych; rozporządzenie o ochronie danych (rozporządzenie (WE) nr 45/2001) jest pod wieloma względami zbliżone do dyrektywy (WE) 95/46; której przepisy wdrożono w ustawodawstwie krajowym państw członkowskich UE, a także Islandii, Liechtensteinu i Norwegii.

Niniejsze wytyczne będą mieć w dalszym ciągu zastosowanie po wejściu w życie nowego ogólnego rozporządzenia o ochronie danych, które utrzymuje zasadę zarządzania ryzykiem dla bezpieczeństwa i wzmacnia wymagania w zakresie ogólnej odpowiedzialności oraz zarządzania, bezpośrednio wprowadzając zasadę **odpowiedzialności** dotyczącej respektowania zobowiązań w zakresie ochrony danych.

Informacje ogólne

Zasady ochrony danych w instytucjach UE, jak również obowiązki Europejskiego Inspektora Ochrony Danych (EIOD) określono w **rozporządzeniu (WE) nr 45/2001**. EIOD jest względnie nowym, ale coraz bardziej wpływowym niezależnym organem nadzorczym odpowiedzialnym za monitorowanie przetwarzania danych osobowych przez instytucje i organy UE, doradztwo w zakresie polityki i ustawodawstwa mającego wpływ na ochronę prywatności oraz współpracę z podobnymi organami w celu zapewnienia spójnego poziomu ochrony danych.

Członkami tej instytucji są **Giovanni Buttarelli** (EIOD) oraz **Wojciech Wiewiórowski** (zastępca EIOD), którzy na mocy wspólnej decyzji Parlamentu Europejskiego i Rady zostali mianowani na pięcioletnią kadencję i objęli urząd w dniu 4 grudnia 2014 r.

Dane osobowe: Wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania (żyjącej) osoby fizycznej. Przykładami są nazwiska, daty urodzenia, fotografie, nagrania wideo, adresy e-mail i numery telefonów. Inne dane, takie jak adresy IP i treść komunikacji – związane z użytkownikami końcowymi usług komunikacyjnych lub dostarczone przez nich – są również uważane za dane osobowe.

Prywatność: prawo jednostki do spokoju oraz kontroli nad dotyczącymi jej informacjami. Prawo do prywatności lub życia prywatnego jest zapisane w Powszechnej deklaracji praw człowieka (art. 12), europejskiej konwencji praw człowieka (art. 8) oraz Karcie praw podstawowych Unii Europejskiej (art. 7). W Karcie zapisano także wyraźnie prawo do ochrony danych osobowych (art. 8).

Przetwarzanie danych osobowych: Zgodnie z art. 2 lit. b) rozporządzenia (WE) nr 45/2001 przetwarzanie danych osobowych oznacza „każdą operację lub zestaw operacji, dokonywanych na danych osobowych przy pomocy środków zautomatyzowanych lub innych, jak np.: gromadzenie, nagrywanie, porządkowanie, przechowywanie, adaptacja lub modyfikacja, odzyskiwanie, konsultowanie, wykorzystywanie, ujawnienie przez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, układanie lub kompilowanie, blokowanie, usuwanie lub niszczenie". Zob. glosariusz na stronie internetowej EIOD.

Artykuł 22 rozporządzenia nr 45/2001: zawiera wymóg zobowiązujący instytucje unijne do ograniczenia rodzajów ryzyka występujących podczas przetwarzania danych osobowych;

- Analiza stanowiąca element zarządzania ryzykiem bezpieczeństwa informacji musi także obejmować ryzyka bezpieczeństwa informacji dotyczące danych osobowych;
- Na podstawie analizy można zdefiniować i wdrożyć pakiet odpowiednich środków bezpieczeństwa.

Środków bezpieczeństwa dotyczących ochrony danych osobowych nie można zdefiniować na poziomie ogólnym, ponieważ muszą pochodzić z procesu zarządzania ryzykiem bezpieczeństwa informacji, który uwzględni konkretny kontekst, w którym przetwarzane są dane osobowe.

Eksperci ds. bezpieczeństwa informacji specjalizują się w opracowywaniu sposobów ochrony informacji i systemów informacji przed nieautoryzowanym dostępem, wykorzystaniem, ujawnieniem, zakłóceniem, modyfikacją lub zniszczeniem.

Eksperci ds. bezpieczeństwa informatycznego specjalizują się w opracowywaniu sposobów ochrony informacji przed nieautoryzowanym dostępem, nadużyciem, niesprawnością, modyfikacją, zniszczeniem lub niewłaściwym ujawnieniem, z wykorzystaniem różnych form technologii służących do tworzenia, przechowywania, wykorzystywania i wymiany takich informacji.

Europejski Inspektor Ochrony Danych (EIOD) jest niezależnym organem nadzorczym odpowiedzialnym za ochronę danych osobowych i prywatności oraz krzewienie dobrych praktyk w instytucjach i organach UE. Swoje zadania realizuje:

- monitorując przetwarzanie danych osobowych przez administrację UE;
- doradzając w zakresie polityki i ustawodawstwa mających wpływ na prywatność;
- współpracując z podobnymi organami w celu zapewnienia spójnej ochrony danych.

Dokument wytycznych EIOD dostępny jest na stronie internetowej EIOD.

Pytania można kierować na adres: press@edps.europa.eu

EIOD – europejski strażnik ochrony danych osobowych

www.edps.europa.eu.

Obserwuj nas na Twitterze:

@EU_EDPS