Kontrola przestrzegania przepisów o ochronie danych osobowych

zasady, zakres, przebieg

Piotr Glen

Inspektor ochrony danych

Kontrola, a postępowanie administracyjne

CEL KONTROLI – ustalenie stanu faktycznego – weryfikacja przestrzegania przepisów o ochronie danych osobowych

CEL POSTĘPOWANIA - jeżeli na podstawie informacji zgromadzonych w postępowaniu kontrolnym Prezes Urzędu uzna, że mogło dojść do naruszenia przepisów o ochronie danych osobowych, obowiązany jest do niezwłocznego wszczęcia postępowania, o którym mowa w art. 60 uodo, celem wydania decyzji administracyjnej

Naruszenia przepisów o ochronie danych osobowych - naruszenie każdego wymogu, obowiązku prawnego (np. obowiązku informacyjnego)

Naruszenia ochrony danych osobowych - oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Pojęcie naruszenia ochrony danych osobowych dotyczy wyłącznie aspektu bezpieczeństwa: poufności; integralności; dostępności.

Plik Edycja Widok Historia Zakładki Narzędzia Pomoc

Według zagadnień - UODO

https://uodo.gov.pl/234

Często odwiedzane Zaloguj

Urząd Ochrony Danych Osobowych

Infolinia Urzędu 606-950-000

Wpisz frazę której szukasz

Prezes i Urząd | Prawo | Edukacja | Współpraca | Wydarzenia

Akty prawne

Decyzje

Wytyczne

» Prawo » Decyzje » Według zagadnień

- Rekrutacja
- Pracodawca
- Pracownik
- Administrator
- Współadministrator
- Podmiot przetwarzający
  - ZSOŚS.440.140.2018
  - ZSOŚS.440.115.2018
- Powierzenie przetwarzania
- Podstawy prawne
  - ZSOŚS.440.140.2018
  - ZSOŚS.440.115.2018

Zakres kontroli

Zakres kontroli jest dość szeroki. Organ nadzorczy może kontrolować między innymi następujące kwestie:

- **zgodność z prawem, rzetelność, przejrzystość**, **źródła pozyskiwania danych**
- ograniczenie celu,
- **minimalizacja danych**,
- prawidłowość,
- **ograniczenie przechowywania**,
- **integralność i poufność**,
- **rozliczalność – zakres uprawnień do przetwarzania danych**
- przetwarzanie szczególnych kategorii danych,
- **warunki wyrażenia zgody i jej wycofania**,
- warunki wyrażenia zgody przez dziecko dla potrzeb usług społeczeństwa informacyjnego,
- **obowiązki informacyjne**,

- **prawo dostępu do danych**,
- **sprostowanie danych**,
- **usunięcie danych** (prawo do bycia zapomnianym),
- **prawo do ograniczenia przetwarzania**,
- obowiązek powiadamiania o sprostowaniu lub usunięciu danych lub ograniczeniu przetwarzania,
- prawo do przenoszenia danych,
- **prawo do sprzeciwu**,
- zautomatyzowane podejmowanie decyzji
- **profilowanie**,
- faza projektowania,
- domyślna ochrona danych,
- **bezpieczeństwo przetwarzania**,
- **rejestrowanie czynności przetwarzania**,
- zgłaszanie organowi nadzorczemu naruszeń ochrony danych,
- zawiadamianie osoby, której dane dotyczą, o naruszeniu,
- ocena skutków dla ochrony danych,
- **inspektor ochrony danych**,
- **umowne powierzenie przetwarzania** (podmiot przetwarzający),

- przekazywanie danych do państw trzecich lub organizacji międzynarodowych: (i) z zastrzeżeniem odpowiednich zabezpieczeń; (ii) wiążące reguły korporacyjne – proces zatwierdzania,
- wspólne kontrole
- **rejestr czynności przetwarzania danych** i rejestr kategorii czynności przetwarzania
- wytyczne dotyczące klasyfikacji naruszeń
- procedura zgłaszania naruszeń ochrony danych do organu nadzorczego
- procedurę informowania osób, których dane dotyczą, w razie naruszenia mogącego powodować wysokie ryzyko naruszenia ich praw lub wolności osób, w tym o działaniach jakie powinni wykonać, aby ryzyko to ograniczyć
- procedurę prowadzenia wewnętrznej dokumentacji stanowiącej rejestr naruszeń ochrony danych
- **raport z ogólnej analizy ryzyka**
- **raport z ocen skutków dla ochrony danych**
- procedury związane z pseudonimizacją i szyfrowaniem
- plan ciągłości działania
- procedury odtwarzania systemu po awarii, oraz ich testowania.
- **polityki ochrony danych**
- dokumentacja technicznych i organizacyjnych środków ochrony danych

TRYBY KONTROLI

Zgodnie z art. 78 ust. 2 uodo, Kontrolę prowadzi się:

- zgodnie z zatwierdzonym przez Prezesa Urzędu planem kontroli lub

- na podstawie uzyskanych przez Prezesa Urzędu informacji (doraźne) lub

- w ramach monitorowania przestrzegania stosowania rozporządzenia 2016/679.

Przepis nie przewiduje obowiązku informowania o kontroli

Roczny plan kontroli sektorowych UODO na 2019 rok

Sektor publiczny

I. Miejski monitoring wizyjny (kontynuacja kontroli sektorowych z 2018 r.)

II. Udostępnianie danych w Biuletynie Informacji Publicznej oraz sposób wysyłania korespondencji zawierającej dane osobowe

III. Sposób prowadzenia rejestru czynności przetwarzania danych osobowych i sposób dokumentowania przez administratora danych naruszeń ochrony danych osobowych

IV. System identyfikacji i monitoringu odpadów

V. Sposób prowadzenia i zabezpieczenia przez spółdzielnie mieszkaniowe rejestru członków

Sektor prywatny

I. Telemarketing

II. Brokerzy danych w zakresie podstaw prawnych przetwarzania danych osobowych

III. Profilowanie w sektorze bankowym i ubezpieczeniowym.

Sektor zdrowia, zatrudnienia i szkolnictwa

I. Szkoły i placówki oświatowe - przetwarzanie danych osobowych rejestrowanych za pomocą systemu monitoringu wizyjnego (cd. sektora rozpoczętego w IV kwartale 2018 r.).

II. Pracodawcy - przetwarzanie danych osobowych rejestrowanych za pomocą systemu monitoringu wizyjnego. Przetwarzanie danych w związku z rekrutacją.

III. Podmioty udzielające świadczeń zdrowotnych - przetwarzanie danych osobowych w związku z udostępnianiem dokumentacji medycznej w ramach realizacji praw pacjenta do dostępu do dokumentacji medycznej dotyczącej jego stanu zdrowia oraz udzielonych mu świadczeń zdrowotnych.

Kontrolujący

Zgodnie z art. 81 uodo, kontrolę przeprowadza się po okazaniu imiennego upoważnienia wraz z legitymacją służbową, a w przypadku kontrolującego, o którym mowa w art. 79 ust. 1 pkt 2 uodo, po okazaniu imiennego upoważnienia wraz z dokumentem potwierdzającym tożsamość.

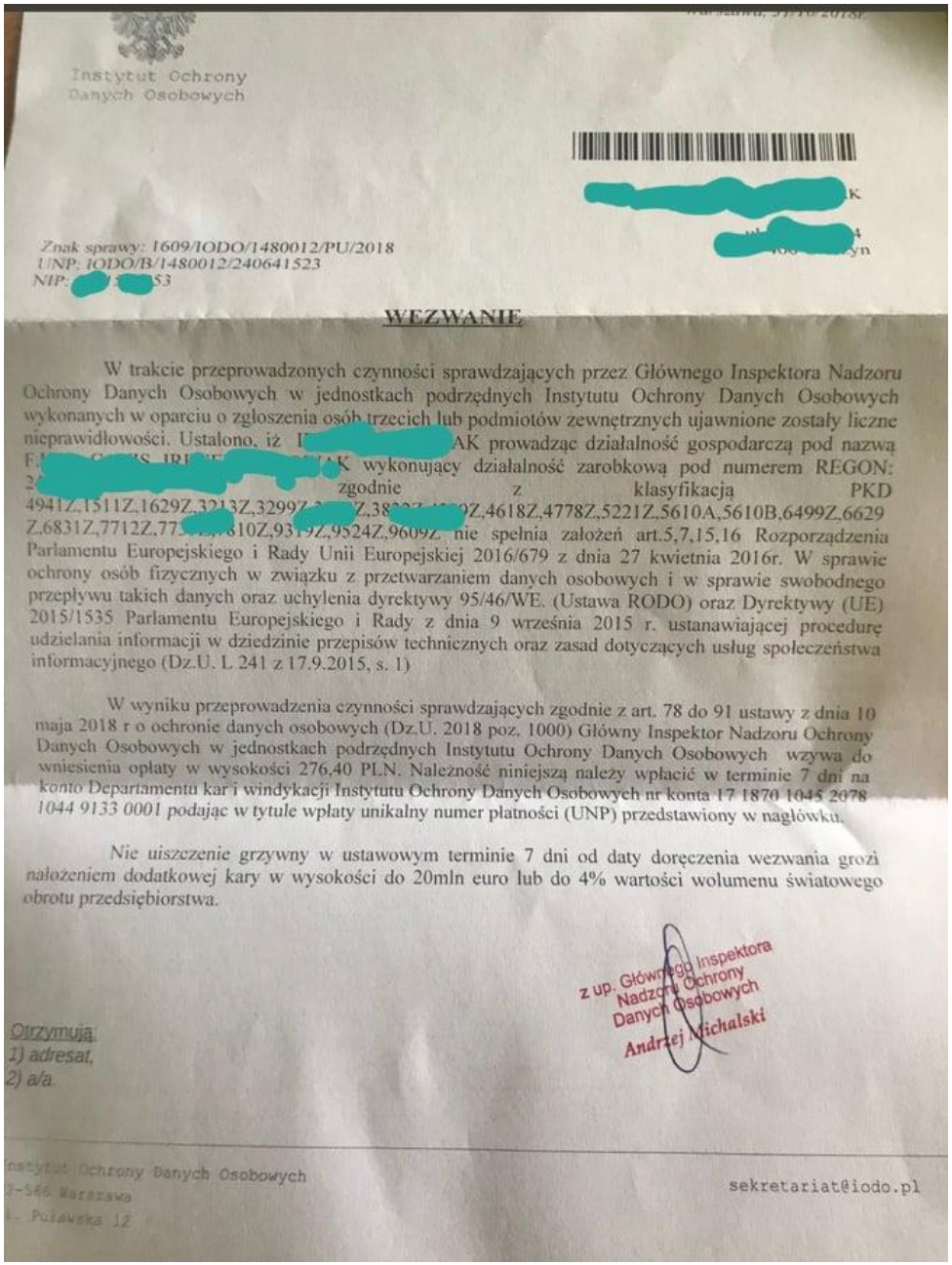
Zgodnie z art. 79 uodo, kontrolę przeprowadza upoważniony przez Prezesa Urzędu:

1) pracownik Urzędu,

2) członek lub pracownik organu nadzorczego państwa członkowskiego Unii Europejskiej w przypadku, o którym mowa w art. 62 rozporządzenia 2016/679 –

zwany dalej „kontrolującym”.

3) osoba upoważniona posiadająca wiedzę specjalistyczną.



Instytut Ochrony
Danych Osobowych

Znak sprawy: 1609/IODO/1480012/PU/2018
UNP: IODO/B/1480012/240641523
NIP: [redacted]53

WEZWANIE

W trakcie przeprowadzonych czynności sprawdzających przez Głównego Inspektora Nadzoru Ochrony Danych Osobowych w jednostkach podrzędnych Instytutu Ochrony Danych Osobowych wykonanych w oparciu o zgłoszenia osób trzecich lub podmiotów zewnętrznych ujawnione zostały liczne nieprawidłowości. Ustalono, iż [redacted]AK prowadząc działalność gospodarczą pod nazwą [redacted]K wykonujący działalność zarobkową pod numerem REGON: [redacted] zgodnie z klasyfikacją PKD 4941Z,1511Z,1629Z,3213Z,3299Z,[redacted]Z,38[redacted]Z,4618Z,4778Z,5221Z,5610A,5610B,6499Z,6629Z,6831Z,7712Z,77[redacted]810Z,9319Z,9524Z,9609Z nie spełnia założeń art.5,7,15,16 Rozporządzenia Parlamentu Europejskiego i Rady Unii Europejskiej 2016/679 z dnia 27 kwietnia 2016r. W sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE. (Ustawa RODO) oraz Dyrektywy (UE) 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiającej procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego (Dz.U. L 241 z 17.9.2015, s. 1)

W wyniku przeprowadzenia czynności sprawdzających zgodnie z art. 78 do 91 ustawy z dnia 10 maja 2018 r o ochronie danych osobowych (Dz.U. 2018 poz. 1000) Główny Inspektor Nadzoru Ochrony Danych Osobowych w jednostkach podrzędnych Instytutu Ochrony Danych Osobowych wzywa do wniesienia opłaty w wysokości 276,40 PLN. Należność niniejszą należy wpłacić w terminie 7 dni na konto Departamentu kar i windykacji Instytutu Ochrony Danych Osobowych nr konta 17 1870 1045 2078 1044 9133 0001 podając w tytule wpłaty unikalny numer płatności (UNP) przedstawiony w nagłówku.

Nie uiszczenie grzywny w ustawowym terminie 7 dni od daty doręczenia wezwania grozi nałożeniem dodatkowej kary w wysokości do 20mln euro lub do 4% wartości wolumenu światowego obrotu przedsiębiorstwa.

z up. Głównego Inspektora
Nadzoru Ochrony
Danych Osobowych
Andrzej Michalski

Otrzymują:
1) adresat,
2) a/a.

Instytut Ochrony Danych Osobowych
[redacted]-566 Warszawa
[redacted]. Puławska 12

sekretariat@iodo.pl

Instytut Ochrony Danych Osobowych rozsyła do przedsiębiorców pisma informujące o złamaniu ustawy RODO i domaga się zapłaty 276,40 zł grzywny. Nie daj się nabrać – to próba oszustwa. Oszuści podszywają się pod faktycznie działającą firmę.

Upoważnienie do kontroli

Artykuł 81 ust. 2 u.o.d.o. wymienia enumeratywnie, z czego składa się imienne upoważnienie do przeprowadzenia kontroli. Musi ono zawierać:

1) wskazanie podstawy prawnej przeprowadzenia kontroli,

2) oznaczenie organu,

3) imię i nazwisko, stanowisko służbowe kontrolującego oraz numer legitymacji służbowej,

4) określenie zakresu przedmiotowego kontroli,

5) oznaczenie kontrolowanego,

6) wskazanie daty rozpoczęcia i przewidywanego terminu zakończenia czynności kontrolnych,

7) podpis Prezesa Urzędu,

8) pouczenie kontrolowanego o jego prawach i obowiązkach,

9) datę i miejsce jego wystawienia.

Upoważnienie do przeprowadzenia kontroli oraz legitymację służbową lub dokument potwierdzający tożsamość (w przypadku członka lub pracownika organu nadzorczego państwa członkowskiego UE) należy okazać:

– kontrolowanemu lub

– osobie przez niego uprawnionej

W przypadku ich nieobecności osobie czynnej w lokalu przedsiębiorstwa.

Rodzaje kontroli

Kotrolujący mogą prowadzić kontrolę:

a) przy biurku: analiza zebranej dokumentacji oraz informacji z ankiet, rejestrów i innych zasobów informacyjnych,

b) na miejscu: dostęp do wszystkich pomieszczeń administratora, do danych, wszystkich informacji, sprzętu i środków służących do przetwarzania danych.

Prawo dostępu i oględzin nie oznacza prawa do przeszukania

Zasady kontroli

- Czynności kontrolnych dokonuje się w obecności kontrolowanego lub osoby przez niego upoważnionej. Kontrolowany jest zobowiązany do pisemnego wskazania osoby upoważnionej do reprezentowania go w trakcie kontroli.

- W uzasadnionych przypadkach przebieg kontroli lub poszczególne czynności w jej toku, po uprzednim poinformowaniu kontrolowanego, mogą być utrwalane przy pomocy urządzeń rejestrujących obraz lub dźwięk. Informatyczne nośniki danych, na których zarejestrowano przebieg kontroli lub poszczególne czynności w jej toku, stanowią załącznik do protokołu kontroli.

- Kontrolowany zapewnia kontrolującemu oraz osobom upoważnionym do udziału w kontroli warunki i środki niezbędne do sprawnego przeprowadzenia kontroli, a w szczególności sporządza we własnym zakresie kopie lub wydruki dokumentów oraz informacji zgromadzonych na nośnikach, w urządzeniach lub systemach;

- Kontrolowany dokonuje potwierdzenia za zgodność z oryginałem sporządzonych kopii lub wydruków.

W przypadku odmowy potwierdzenia za zgodność z oryginałem kontrolujący czyni o tym wzmiankę w protokole kontroli.

Kontrolujący ma prawo:

1) wstępu w godzinach od 6:00 do 22:00 na grunt oraz do budynków, lokali lub innych pomieszczeń;

2) wglądu do dokumentów i informacji mających bezpośredni związek z zakresem przedmiotowym kontroli;

3) przeprowadzania oględzin miejsc, przedmiotów, urządzeń, nośników oraz systemów informatycznych lub teleinformatycznych służących do przetwarzania danych;

4) żądać złożenia pisemnych lub ustnych wyjaśnień oraz przesłuchiwać w charakterze świadka osoby w zakresie niezbędnym do ustalenia stanu faktycznego;

5) zlecać sporządzanie ekspertyz i opinii.

Przebieg czynności kontrolnych kontrolujący przedstawia w protokole kontroli (art. 88 u.o.d.o.)

Protokół kontroli podpisuje kontrolujący i przekazuje kontrolowanemu w celu podpisania.

Kontrolowany w terminie 7 dni od dnia przedstawienia protokołu kontroli do podpisu podpisuje go albo składa pisemne zastrzeżenia do jego treści.

W przypadku złożenia zastrzeżeń, kontrolujący dokonuje ich analizy i, w razie potrzeby, podejmuje dodatkowe czynności kontrolne, a w przypadku stwierdzenia zasadności zastrzeżeń zmienia lub uzupełnia odpowiednią część protokołu kontroli w formie aneksu do protokołu kontroli.

Brak doręczenia kontrolującemu podpisanego protokołu kontroli i niezgłoszenie zastrzeżeń do jego treści w terminie uznaje się za odmowę podpisania protokołu kontroli.

Protokół kontroli sporządza się w postaci elektronicznej albo w postaci papierowej w dwóch egzemplarzach. Protokół kontroli kontrolujący doręcza kontrolowanemu.

Czas trwania kontroli

Kontrolę prowadzi się nie dłużej niż 30 dni od dnia okazania kontrolowanemu imiennego upoważnienia do przeprowadzenia kontroli oraz legitymacji służbowej.

Do terminu nie wlicza się terminów przewidzianych na zgłoszenie zastrzeżeń do protokołu kontroli lub podpisanie i doręczenie protokołu kontroli przez kontrolowanego.

Terminem zakończenia kontroli jest dzień podpisania protokołu kontroli przez kontrolowanego.

Podejście do kontroli

Zasada ROZLICZALNOŚCI - wykazanie zgodności z zasadami ochrony danych – to Administrator ma wykazać, że jest zgodny z przepisami.

Podejście oparte na analizie ryzyka.

Za utrudnianie kontroli grozi odpowiedzialność karna

Dziękuję za uwagę

Piotr Glen

Zapraszam do zadawania pytań