**Urząd Ochrony Danych Osobowych nałożył administracyjną karę pieniężną w wysokości niemal 52 tys. złotych na spółdzielnię mieszkaniową za niezgłoszenie organowi nadzorczemu naruszenia ochrony danych osobowych oraz za niezawiadomienie o naruszeniu osoby, której dane dotyczą. Nakazał również administratorowi zawiadomienie o naruszeniu ochrony danych osobowych podmiotu tych danych.**Do UODO wpłynęła wiadomość od osoby trzeciej informująca, iż udostępniono jej jako osobie nieuprawnionej informacje dotyczące członka spółdzielni mieszkaniowej.

W związku z tym i karami nałożonymi na spółdzielnie mieszkaniowe przez Urząd Ochrony Danych <https://uodo.gov.pl/pl/138/2658> nasza fundacja działając w interesie publicznym wnioskuje o udzielenie informacji publicznej w zakresie:

**Zgodnie z ustawą o dostępie do informacji publicznej podmiot ma obowiązek udzielenia odpowiedzi na zadane pytania! W przeciwnym razie skierujemy sprawę do Sądu na bezczynność.**

Na podstawie art. 61 w związku z art. 8 ust. 2 Konstytucji Rzeczpospolitej Polskiej oraz art.2 ust.1 Ustawy o dostępie do informacji publicznej z dnia 6 września 2001 r. składamy wniosek o udzielenie następującej informacji publicznej.

Pozwalamy sobie przypomnieć, że  ipso iure art. 2 ust. 2 Ustawy o dostępie do informacji publicznej “ (…) Od osoby wykonującej prawo do informacji publicznej nie wolno żądać wykazania interesu prawnego lub faktycznego. Przedmiotowy wniosek/wnioski  - nie powinny być rozpatrywane w trybie KPA.  Celem naszych wniosków jest - sensu largo - usprawnienie, naprawa - na miarę istniejących możliwości - funkcjonowania struktur Administracji Publicznej - głownie w Gminach/Miastach/szkołach  - gdzie jak wynika z naszych wniosków - stan faktyczny wymaga wszczęcia procedur sanacyjnych, publikacji wyników na naszej stronie internetowej oraz zgłoszenia nieprawidłowości odpowiednim organom.

W przypadku braku odpowiedzi na informację publiczną złożymy wniosek do Wojewódzkiego Sądu Administracyjnego skargę na bezczynność.

Treść wniosku

1.  Czy Państwa jednostka korzysta z usług osób fizycznych lub podmiotów zewnętrznych w zakresie pełnienia obowiązków Inspektora Ochrony Danych, a jeżeli tak prosimy o podanie:

·       w przypadku wyznaczenia Inspektora Ochrony Danych spośród pracowników Administratora proszę o informację czy Inspektor Ochrony Danych wykonuje inne zadania niezwiązane z pełnieniem funkcji Inspektora Ochrony Danych (jakie?; Inne stanowiska, jakie?) Czy IOD ma wykształcenie prawnicze lub odpowiednie kwalifikacje o których mowa w art. 37 ust.5 RODO ( wiedza prawnicza i dogłębna znajomość RODO i przepisów sektorowych)? Wnosimy o potwierdzenie w/w kwalifikacji.

·       wnosimy o podanie przepisów wewnętrznych i dokumentów, z których zapisów wynika, w jaki sposób IOD został włączony w bieżące funkcjonowanie jednostki.

·       na podstawie jakich kwalifikacji administrator wyznaczył IOD (np. wykształcenie, doświadczenie, wiedza)?

·       jakie niezbędne zasoby, o których mowa w art. 38 ust. 2 rozporządzenia 2016/679 administrator zapewnia IOD?

·       w jaki sposób administrator zapewnia zasoby na utrzymanie wiedzy fachowej IOD?

·       jakie stanowisko zajmuje IOD i komu podlega w strukturze organizacyjnej administratora?

·       czy administrator powołał zastępcę IOD, jeżeli tak, to kiedy?

·       w jaki sposób administrator zapewnia by IOD był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych?

·       w jaki sposób administrator zapewnia IOD dostęp do danych osobowych i operacji przetwarzania?

·       czy administrator przyjął jakiekolwiek regulacje wewnętrzne dotyczące funkcjonowania IOD (...) a jeżeli tak, to w jakim akcie wewnętrznym zostały one przewidziane?

·       w jaki sposób administrator zapewnia, aby IOD nie były wydawane instrukcje co do wykonywania zdań przez IOD?

·       W jaki sposób administrator zapewnia, aby IOD nie były karany i odwoływany za wykonywanie swoich zadań?

·       w jaki sposób ADO postępuje w przypadku, gdy nie uwzględnia wskazówek lub rekomendacji IOD, np. czy dokumentuje powody niezastosowania tych wskazówek?

·       czy administrator opracował politykę zarządzania konfliktem interesów lub wprowadził inny mechanizm zapewniający niewystępowanie konfliktu interesów?

·       czy IOD wykonuje swoje zadania jedynie w siedzibie administratora, a jeżeli nie, to w jakim miejscu i w jaki sposób zapewniona jest stała dostępność IOD dla kierownictwa i pracowników administratora?

·       czy IOD opracował (systematycznie opracowuje) plan swojej pracy np. w zakresie szkoleń i planów audytów?

·       czy taki plan był prezentowany administratorowi w celu umożliwienia dokonania oceny, czy IOD dysponuje wystarczającymi zasobami i uprawnieniami w obszarach, które IOD obejmuje swoimi zadaniami?

·       jak często i w jaki sposób IOD przekazuje administratorowi wyniki przeprowadzonych audytów

·       czy administrator kontroluje pracę inspektora, jeżeli tak, to w jaki sposób?

·       czy w jednostce przeprowadzony został audyt, o którym mowa w § 20 ust. 2 pkt. 14 Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych? (Informacji proszę udzielić w rozbiciu na lata w zakresie 2015 – 2023)

|  |  |  |  |
| --- | --- | --- | --- |
| ROK | Data audytu | Koszt audytu (jeśli audyt był prowadzony przez podmiot zewnętrzny) | Nazwa podmiotu prowadzącego audyt (jeśli audyt był prowadzony przez podmiot zewnętrzny) |
| 2015 |  |  |  |
| 2016 |  |  |  |
| 2017 |  |  |  |
| 2018 |  |  |  |
| 2019 |  |  |  |
| 2020 |  |  |  |
| 2021 |  |  |  |
| 2022 |  |  |  |
| 2023 |  |  |  |

2.      Czy podmiot- zgodnie ze stanowiskiem UODO <https://uodo.gov.pl/pl/495/2342> -upublicznił dane Inspektora Ochrony Danych na swojej stronie internetowej?

 Przepisy ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (art. 11) wprost zobowiązują podmiot, który wyznaczył IOD, by udostępnił jego dane na swojej stronie internetowej. Administrator, który wyznaczył IOD powinien opublikować jego następujące dane: imię i nazwisko oraz adres poczty elektronicznej lub numer telefonu

3.  Art 37 ust. 5 RODO inspektor ochrony danych jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39 RODO. Według UODO Karami administracyjnymi obwarowane są zatem zarówno poszczególne obowiązki administratorów danych dotyczące także [wyznaczania IOD](https://uodo.gov.pl/pl/121/193). To na administratorze spoczywa ciężar wyznaczenia IOD zgodnie z kwalifikacjami i wiedzą prawniczą: <https://uodo.gov.pl/pl/225/637>  Jednakże warto zrealizować rekonesans - w tym obszarze i dokonać stosownej analizy - wykazując troskę o bezpieczeństwo danych oraz wyznaczanie IOD zgodnie z kwalifikacjami. Tymczasem często na IOD są wybierani osoby nie mające odpowiednich kwalifikacji, wiedzy prawniczej. Co gorsza często takie funkcje piastują osoby z wykształceniem informatycznym. Dzięki kontrolom NIK i UODO oraz działaniom sfer Rządowych (w skali makro) w ostatnim czasie sytuacja ulega  poprawie, jednakże bez szybkiej sanacji tego obszaru  (w skali mikro) również w Gminach  i jednostkach oświatowych - proces ten  będzie w dalszym ciągu przebiegał zbyt wolno   -często są to osoby przypadkowe lub informatycy, zewnętrzni IOD nie mający wiedzy prawniczej.

W związku z powyższym wnosimy o wykazanie kwalifikacji IOD w zakresie wiedzy prawniczej? Czy IOD jest prawnikiem? Jakie posiada doświadczenie? Kto i w jaki sposób weryfikował kwalifikacje IOD?

 Nadmieniamy, iż powyższe pytania o informację publiczną -  wydają się szczególnie istotne z punktu widzenia interesu publicznego pro publico bono - nawiązując do art. 3 ust. 1 pkt. 1 Ustawy z dnia 6 września o dostępie do informacji publicznej (Dz.U.2018.1330 t.j. z 2018.07.10) - gdyż ten obszar  RODO i kwalifikacji IOD a zwłaszcza doświadczenia i wiedzy prawniczej wydaje się (jak wynika z uprzednio uzyskanych przez nas odpowiedzi) - szczególnie wymagać - wdrożenia procedur aby takie „przypadkowe” osoby nie pełniły takich funkcji.

4.     Czy na bieżąco przekazywane są IOD do akceptacji pod względem prawidłowości w zakresie ochrony danych osobowych projekty dokumentów tj. projekty umów, informacji udostępnianych w Biuletynie Informacji Publicznych, projekty przepisów wewnętrznych związanych z udostępnianiem bądź pozyskiwaniem danych osobowych.

5.     W jaki sposób IOD realizuje swoje zadania ( audyty, szkolenia, konsultacje). Wnosimy o dokumentację  potwierdzająca realizację zadań przez IOD lub opis jego działań od dnia 25 maja 2018 roku (zadań wynikających z art. 39 rozporządzenia RODO)

6.     Czy zostały opracowane i wdrożone przepisy wewnętrzne, procedury, instrukcje i inne dokumenty dotyczące przetwarzania danych osobowych oraz bezpieczeństwa informacji. Jeśli tak to jakie?

7.     Wnosimy o opisanie aktualizacji dokumentacji RODO od 2018r.?

Czy dokumentacja została zaktualizowana o stanowisko EROD z 202or:<https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_pl.pdf>?

8.     Wnosimy o informację czy podmiot opracował i wdrożył procedury dotyczących oceny skali naruszeń według ENISA? <https://www.enisa.europa.eu/publications/report-files/ETL-translations/pl/etl2020-data-breach-ebook-en-pl.pdf>

9.     W jaki sposób są realizowane szkolenia z zakresu

a)     RODO

b)    KRI bezpieczeństwa informacji

c)     Cyberbezpieczeństwa

Wnosimy o informację na temat częstotliwości szkoleń, ponadto (informacje tj. data szkolenia, zakres szkolenia, osoba prowadząca, listy obecności, czas trwania)

10.  Wnosimy o przedłożenie dokumentu potwierdzającego zapoznanie się pracowników z treścią obowiązujących przepisów wewnętrznych, ewentualnie wskazanie w jaki sposób zostali oni zapoznani.

11.  W jaki sposób realizowany jest obowiązek informacyjny – art. 13 RODO? Opisać.

12.  W jaki sposób realizowany jest obowiązek informacyjny – art. 14 RODO?

13. Czy IOD w ramach monitorowania przeprowadza regularne i systematyczne sprawdzenia/audyty w zakresie prawidłowości przetwarzania danych osobowych oraz przestrzegania rozporządzenia RODO, ustawy o.d.o. oraz regulacji wewnętrznych? Dokumentacja w tym zakresie  (plany, sprawozdania, raporty, itp.)

14.  Czy IOD dokonuje audytów z zakresu ochrony danych osobowych z ZFSS? Czy z audytu ZFSS jest sporządzany raport?

Art. 8 1d. Ustawa o ZFSS

*Pracodawca dokonuje przeglądu danych osobowych, o których mowa w ust. 1a, nie rzadziej niż raz w roku kalendarzowym w celu ustalenia niezbędności ich dalszego przechowywania. Pracodawca usuwa dane osobowe, których dalsze przechowywanie jest zbędne do realizacji celu określonego w ust. 1a i 1c.*

**PYTANIA Z KRAJOWYCH RAM INTEROPERACYJNOŚCI**

 Zgodnie z Rozporządzeniem R. M. z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych                        (Dz. U. z 2012r. poz. 526) "każdy podmiot publiczny zobowiązany jest do zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok (§ 20 ust.2 pkt 14). "

1.     Kto dokonuje corocznych audytów z KRI?

2.     Czy IOD realizuje zadania w związku z KRIO?

3.     Kto przeprowadza audyt bezpieczeństwa?

SYGNALIŚCI:

1.     Czy jednostka opracowała i wdrożyła procedury w zakresie obsługi sygnalistów na podstawie **Dyrektywy Parlamentu Europejskiego i rady (UE) 2019/1937 z dnia 23 października 2019 w sprawie ochrony osób zgłaszających naruszenia prawa Unii która obowiązuje bezpośrednio w państwach członkowskich?**

2.     **Jaki system informatyczny zapewniający sygnaliście anonimowość został wdrożony i umieszczony na stronie www?**

3.     **Kto dokonuje obsługi zgłoszeń dt. sygnalistów?**

4.     **Czy jednostka dokonała zgłoszenia osób kontaktowych właściwemu CSIRT na podstawie  ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560)?**

**PYTANIA-MONITORING WIZYJNY**

Temat monitoringu wizyjnego jest przedmiotem naszego zainteresowania. O jego funkcjonowaniu w Państwa podmiocie wiemy wciąż niewiele. Informacja o monitoringu jest informacją publiczną np. koszt, cel, spełnienie wymogów związanych z instalacją, okres przechowywania.

Właśnie dlatego postanowiliśmy zgłębić temat wysyłając wnioski o udostępnienie informacji publicznej z prośbą o udzielenie następujących odpowiedzi:

1.     Czy podmiot posiada monitoring wizyjny?

2.     Jakie obowiązki przeprowadził administrator w związku z zainstalowaniem monitoringu ( ocena skutków, obowiązki informacyjne, konsultacje z organem prowadzący, zapoznanie pracowników)

3.     Czy jednostki oświatowe przeprowadziły konsultacje z organem prowadzącym?

Art.  108a.  [Monitoring placówek oświatowych]1.

*Jeżeli jest to niezbędne do zapewnienia bezpieczeństwa uczniów i pracowników lub ochrony mienia dyrektor szkoły lub placówki, w uzgodnieniu z organem prowadzącym szkołę lub placówkę oraz po przeprowadzeniu konsultacji z radą pedagogiczną, radą rodziców i samorządem uczniowskim, może wprowadzić szczególny nadzór nad pomieszczeniami szkoły lub placówki lub terenem wokół szkoły lub placówki w postaci środków technicznych umożliwiających rejestrację obrazu (monitoring).*

4.     Czy w związku z monitoringiem wizyjnym miejsc publicznych prowadzonym przez Państwa jednostkę była prowadzona była ocena skutków w rozumieniu art. 35 ust. 1 rodo stosownie do treści tego przepisu:

*„Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może spowodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę”.*

Natomiast zgodnie z art. 35 ust. 3 rodo:

„*Ocena skutków dla ochrony danych, o której mowa w ust. 1, wymagana w szczególności w przypadku systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie”.*

*Jednocześnie zgodnie z art. 35 ust. 7 rodo ocena skutków obligatoryjnie zawiera co najmniej*

*a)systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora;*

*b)ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;*

*c)ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą, o którym mowa w ust. 1; oraz*

*d)środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie niniejszego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy”.*

Jeżeli ocena skutków (stosownie do treści art. 35 ust. 1 rodo) była prowadzona to wnosimy przesłanie tej oceny.

* rozporządzenie Rady Ministrów z 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2012 r. poz. 526).

 Na podstawie art. 14 ust. 1 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej prosimy o przesłanie informacji w ustawowym terminie, we wskazanym powyżej zakresie, wyłącznie pocztą elektroniczną mój adres mail.

 W przypadku braku szczegółowych odpowiedzi będziemy zmuszeni skierować skargę na bezczynność do Sądu!