1. Czy Państwa jednostka wyznaczyła Inspektora Ochrony Danych osobowych (dalej: IOD)

   TAK

2. Na podstawie jakich kwalifikacji administrator wyznaczył IOD (np. wykształcenie prawnicze, doświadczenie, wiedza)? 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. 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, a zwłaszcza w firmach prywatnych - proces ten nadal przebiegał zbyt wolno - często są to osoby przypadkowe lub informatycy. Brak wyznaczenia IOD zgodnie z kwalifikacjami zmusi nas do powiadomienia odpowiednich organów.

   Informatyk z fachową wiedzą w zakresie RODO (studia podyplomowe).

3. 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?

   - Studia Podyplomowe – Inspektor Ochrony Danych Osobowych
   - Szkolenie Mastere dla Audytorów i Pełnomocników Zarządu
   - Certyfikat Kompetencji Inspektora Ochrony Danych wydany przez Zontek i Wspólnicy
   - Certyfikat RBDO – rejestracja i bezpieczeństwo danych osobowych

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

   Jeszcze nie.

   Przepisy ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (art. 11 ustawy) 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

   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.

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

Funkcje IOD pełni podmiot zewnętrzny, który sam dba o niezbędne zasoby.

W jaki sposób administrator zapewnia zasoby na utrzymanie wiedzy fachowej IOD?

jw

Jakie stanowisko zajmuje IOD i komu podlega w strukturze organizacyjnej administratora?

Podlega bezpośrednio pod administratora. Jest to podmiot zewnętrzny.

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

Dyskusja, konsultacja.

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

IOD uzyskuje dostęp do danych osobowych podczas audytu.

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

Umowa z IOD dot. obowiązków oraz częstości dokonywania audytów.

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

Brak konfliktu – podmiot zewnętrzny.

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?

Kontakt email, telefon, wizyty bezpośrednio w siedzibie.

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

Tak, zapisany w umowie.

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?

TAK

Jak często i w jaki sposób IOD przekazuje administratorowi wyniki przeprowadzonych audytów

Raz na kwartał.

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

Rozmowa.

7. 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)

Sprawozdania z audytów.

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

Wdrożono regulamin przetwarzania danych.

9. Wnosimy o opisanie aktualizacji dokumentacji RODO od 2018r.? W szczególności interesuje nas aktualizacja dokumentacji od roku 2022r. (stanowiska ENISA)

Dokumentacja RODO jest dostosowywana do zmieniających się przepisów.

10. W jaki sposób w roku 2023 były realizowane szkolenia z zakresu

a) RODO

Prelekcja bezpośrednia lub szkolenie online.

b) KRI bezpieczeństwa informacji

Nie dotyczy.

c) Cyberbezpieczeństwa

Podnoszenie świadomości podczas szkolenia z RODO.

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

Szkolenia są prowadzone głównie na początku roku szkolnego (wrzesień) lub doraźnie wg potrzeb.

11. 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.)

Audyt raz na kwartał.

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

TAK, nie ma raportu.

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 ORAZ POZOSTAŁYCH USTAW

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). "Podmioty są zobowiązane, zgodnie z § 20 ust. 2 pkt 14 Rozporządzenia KRI do zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji nie rzadziej niż raz na rok

1. 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 2020 – 2023)

NIE

ROK

Data audytu

Koszt audytu (jeśli audyt był prowadzony przez podmiot zewnętrzny)

Nazwa podmiotu prowadzącego audyt (jeśli audyt był prowadzony przez podmiot zewnętrzny)

2020

2021

2022

2023

2. 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? Przypominamy, iż dyrektywa unijna jest stosowana bezpośrednio.

TAK

Oznacza to konieczność bezpośredniego stosowania dyrektywy w tych wszystkich przypadkach relacji wertykalnych: obywatel – podmiot, którego działalność stanowi „emanacje funkcji państwa”. Wynika

to z utrwalonego stanowiska TSUE. W orzecznictwie TSUE ugruntowało się stanowisko dopuszczające bezpośrednie stosowanie dyrektyw w relacjach wertykalnych (obywatel -> władza publiczna) m.in. w przypadku braku terminowej implementacji dyrektyw. W takiej sytuacji dyrektywa znajdzie bezpośrednie zastosowanie, o ile jej przepisy będą bezwarunkowe oraz wystarczająco jasne i precyzyjne (zob. wyrok z 4 grudnia 1974 r., Van Duyn).

3. Czy jednostka wdrożyła odpowiednie kanały zgłoszeń zapewniające anonimowość sygnalisty np. system informatyczny dt. zgłoszeń?

TAK

4. Kto dokonuje obsługi zgłoszeń dt. sygnalistów?

Dyrektor

5. 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)?

NIE