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.
IOD W TUT. STACJI ZOSTAŁ POWOŁANY ORAZ PRZESZKOLONY. SZKOLENIA WYMIENIONO W ODPOWIEDZI NA KOLEJNE PYTANIE.

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?
IOD NIE POSIADA WYKSZTAŁCENIA PRAWNICZEGO. IOD ODBYŁ SZKOLENIE Z ZAKRESU OCHRONY DANYCH OSOBOWYCH, SZKOLENIE Z ZAKRESU SZACOWANIA RYZYKA W PROCESIE „ANALIZY RYZYKA OGÓLNEGO" ORAZ „OCENY SKUTKÓW DLA PRZETWARZANIA DANYCH (DPIA)" W OPARCIU O WYTYCZNE RODO, GRUPY ROBOCZEJ ART.29, ISO 27001, 27002 ORAZ 27005, SZKOLENIE Z EUROPEJSKIEGO ROZPORZĄDZENIA O OCHRONIE DANYCH OSOBOWYCH (RODO). IOD UZYSKAŁ CERTYFIKATY Z POWYŻSZYCH SZKOLEŃ. IOD UCZESTNICZYŁ RÓ1)NIEŻ W SZKOLENIU „OCENA SKUTKÓW ORAZ ANALIZA RYZYKA W 5 KROKACH".

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

5. 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
TAK - BIP

6. 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?

ADMINISTRATOR UMOŻLIWIŁ UCZESTNICTWO IOD W WYBRANYCH SZKOLENIACH.

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

ADMINISTRATOR UMOŻLIWIŁ UCZESTNICTWO IOD W WYBRANYCH SZKOLENIACH.

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

STARSZY ASYSTENT W SEKCJI EPIDEMIOLOGII, PODLEGA KIEROWNIKOWI SEKCJI ORAZ DYREKTOROWI STACJI.

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

POPRZEZ NIEZWŁOCZNE PRZEKAZANIE MU INFORMACJI.

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

ADMINISTRATOR WYDAŁ UPOWAŻNIENIE UPRAWNIAJĄCE IOD DO WGLĄDU DO PRZETWARZANEJ W STACJI DOKUMENTACJI.

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

TAK – ZARZĄDZENIA ORAZ REGULAMIN ORGANIZACYJNY.

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

TAK

- 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?

TAK

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

NIE

- 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?

NIE DOTYCZY

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

NIE DOTYCZY

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

NIE

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).

IOD PROWADZI SZKOLENIA DLA NOWO ZATRUDNIONYCH PRACOWNIKÓW, PRZECHOWUJE PODPISANE DEKLARACJE POUFNOŚCI, PRZYGOTOWUJE I PROWADZI REJESTRACJĘ NADAWANYCH UPOWAŻNIEŃ DO PRZYTWARZANIA DOKUMENTÓW I REJESTRÓW ZAWIERAJĄCYCH DANE OSOBOWE. W DNIU 01.02.2018 R. PRZEPROWADZONO SZKOLENIE WSTĘPNE DLA NOWO ZATRUDNIONEGO PRACOWNIKA. W DNIU 07.05.2018 R. PRZEPROWADZONO SZKOLENIE WSTĘPNE DLA NOWO ZATRUDNIONEGO PRACOWNIKA. W DNIU 10.09.2018 R. PRZEPROWADZONO SZKOLENIE WSTĘPNE DLA NOWO ZATRUDNIONEGO PRACOWNIKA. W DNIU 10.09.2018 R. PRZEPROWADZONO SZKOLENIE WSTĘPNE DLA NOWO ZATRUDNIONEGO PRACOWNIKA. W DNIU 01.03.2019 R. PRZEPROWADZONO SZKOLENIE WSTĘPNE DLA NOWO ZATRUDNIONEGO PRACOWNIKA. W DNIU 19.12.2019 R. ODBYŁO SIĘ SZKOLENIE W ZAKRESIE „OCHRONY DANYCH OSOBOWYCH”, W SZKOLENIU UDZIAŁ WZIĘŁO 13 OSÓB. W DNIU 31.12.2019 R. PRZEPROWADZONO SZKOLENIE WSTĘPNE DLA NOWO ZATRUDNIONEGO PRACOWNIKA. W DNIU 07.01.2020 R. PRZEPROWADZONO SZKOLENIE WSTĘPNE DLA NOWO ZATRUDNIONEGO PRACOWNIKA. W DNIU 01.04.2020 R. PRZEPROWADZONO SZKOLENIE WSTĘPNE DLA NOWO ZATRUDNIONEGO PRACOWNIKA. W DNIU 01.03.2021 R. PRZEPROWADZONO SZKOLENIE WSTĘPNE DLA NOWO ZATRUDNIONEGO PRACOWNIKA. W DNIU 01.06.2021 R. PRZEPROWADZONO SZKOLENIE WSTĘPNE DLA NOWO ZATRUDNIONEGO PRACOWNIKA.
W DNIU 04.05.2022 R. PRZEPROWADZONO SZKOLENIE WSTĘPNE DLA NOWO ZATRUDNIONEGO PRACOWNIKA. W DNIU 26.01.2022 R. ODBYŁO SIĘ SZKOLENIE W ZAKRESIE „PRZETWARZANIE I OCHRONA DANYCH OSOBOWYCH W PRACY W SYSTEMACH INFORMATYCZNYCH”, W SZKOLENIU UDZIAŁ WZIĘŁO 11 OSÓB.

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

TAK. PROCEDURA PO/PSSE-02 ZACHOWANIE POUFNOŚCI INFORMACJI, OCHRONA PRAW WŁASNOŚCI KLIENTA ORAZ OCHRONA INFORMACJI NIEJAWNYCH.

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

15.04.2019 r. WPROWADZONO Analizę Ryzyka Ogólnego i Ocenę Skutków dla Przetwarzania Danych (DPIA) w organizacji o nazwie: POWIATOWA STACJA SANITARNO-EPIDEMIOLOGICZNA W ŻARACH

10. W jaki sposób w roku 2023 były 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)
PRZEPROWADZANE SĄ SZKOLENIA DLA NOWO ZATRUDNIONYCH PRACOWNIKÓW Z ZAKRESU OCHRONY DANYCH OSOBOWYCH. W ROKU 2023 PRZEPROWADZONO DWA TAKIE SZKOLENIA. W LISTOPADZIE ORAZ GRUDNIU 2023 R. CZĘŚĆ PRACOWNIKÓW ZAKWALIFIKOWAŁA SIĘ DO UCZESTNICTWA W SZKOLENIACH Z CYBERBEZPIECZEŃSTWA ORGANIZOWANYCH W RAMACH PROJEKTU UE.

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.)
NIE. ADYTY PRZEPROWADZANE SĄ PRZEZ ADITORÓW WEWNĘTRZNYCH WG ROCZNEGO PLANU ADITÓW.

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

TAK. W JEDNOSTCE OBOWIĄZUJE PROCEDURA PO/PSSE-02 ZACHOWANIE POUFNOŚCI INFORMACJI, OCHRONA PRAW WŁASNOŚCI KLIENTA ORAZ OCHRONA INFORMACJI NIEJAWNYCH, ZGODNIE Z KTÓRĄ SYSTEM BEZPIECZEŃSTWA DANYCH OSOBOWYCH PODLEGA PRZEGLĄDOWI POD KĄTEM AKTUALNOŚCI I STOSOWALNOŚCI W ODSTĘPACH SZEŚCIOMIESIĘCZNYCH. PONADTO W WW. OBSZARZE RAZ W ROKU PRZEPROWADZANY JEST AUDIT, ZGODNIE Z COROCZNIE OPRACOWYWANYM PLANEM AUDITÓW

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.

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).

ZGODNIE Z PROJEKTEM USTAWY O SYGNALISTACH Z 2021 R., W PIERWSZEJ KOLEJNOŚCI DO WDROŻENIA WEWNĘTRZNYCH REGULACJI SŁUŻĄCYCH OCHRONIE SYGNALISTÓW, ZOBOWIĄZANI MIELI BYĆ PRZEDSIĘBIORCY ZATRUDNIAJĄCY CO NAJMNIEJ 250 PRACOWNIKÓW. DOPIERO W KOLEJNYM KROKU, PRZEDMIOTOWE REGULACJE OBJĄĆ MIAŁY RÓWNIEŻ TYCH PRZEDSIĘBIORCÓW, KTÓRZY ZATRUDNIAJĄ OD 50 DO 249 PRACOWNIKÓW. CO JEDNAK ISTOTNE, W PROJEKCIE USTAWY O SYGNALISTACH Z 2023 R. ZREZYGNOWANO ZE STOPNIOWEGO WDRAŻANIA USTAWOWYCH REGULACJI I WSKAZANO WPROST (W TREŚCI ART. 23 UST. 1 PROJEKTU), ŻE PRZEPISY DOT. PROCEDURY ZGŁOSZEŃ WEWNĘTRZNYCH STOSUJE SIĘ DO PODMIOTU

PRAWNEGO, NA RZECZ KTÓREGO WYKONUJE LUB ŚWIADCZY PRACĘ CO NAJMNIEJ 50 OSÓB. W PSSE W ŻARACH ZATRUDNIONYCH JEST MNIEJ NIŻ 50 OSÓB.

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

PATRZ – ODPOWIEDŹ NA PYTANIE 2

4. Kto dokonuje obsługi zgłoszeń dt. sygnalistów?

PATRZ – ODPOWIEDŹ NA PYTANIE 2

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)?
TAK