Weryfikacja przestrzegania przepisów dotyczących inspektora ochrony danych – Norwegia

W ostatnich miesiąca nie cichną komentarze po kontroli przeprowadzonej przez UODO w zakresie sprawdzenia sposobu działań IOD-ów, na podstawie listy 27 pytań. Ich treść można poznać na stronie Urzędu (link: https://uodo.gov.pl/pl/138/2336), a także na naszym blogu (link: https://www.isecure.pl/blog/uodo-sprawdza-jak-pracuje-iod-czyli-o-co-chodzi-z-lista-27-pytan/).

Z ciekawości przejrzałem strony innych organów ochrony danych osobowych i ciekawe wyniki swojej kontroli/ankiety przedstawił w ubiegłym roku norweski organ Datatilsynet. Jednak sama ankieta nie dotyczyła weryfikacji realizacji zadań Inspektora, jednak na końcu podano 5 wytyczne w jaki sposób można dbać o jego rolę i jak powinien sprawować swoją funkcję.

Co wynika z ankiety?

Na wstępie nie powiem nic odkrywczego - Inspektorzy ochrony danych mają kluczowe znaczenie dla przestrzegania przez przedsiębiorstwa przepisów o ochronie danych. Rolą inspektora jest doradzanie, jak najlepiej chronić interesy, prawa, wolności i obowiązki podmiotów, których dane są przetwarzane, a także zapewnienie zgodności tego przetwarzania z odpowiednimi przepisami.

Dlatego ze smutkiem należy przyjąć, że spośród Inspektorów, którzy udzielili odpowiedzi – aż 11% stwierdza, że w ogóle nie poświęca czasu na pełnienie dodatkowej funkcji, a jedynie 17% pracuje na wspomnianym stanowisku w pełnym wymiarze godzin.

Co jest problemem? Trzech na dziesięciu Inspektorów stwierdza, że nie ma wystarczająco czasu, aby poświęcić się wypełnianiu funkcji Inspektora Ochrony Danych. Zgodnie z art. 38 ust 2 RODO, administrator danych jest zobowiązany dostarczyć Inspektorowi odpowiednich zasobów do pełnienia swojej roli. Obowiązek ten jest interpretowany jako zapewnienie nie tylko zasobów technicznych czy organizacyjnych, ale również czasowych. Podejrzewam, że nasz Urząd nie byłby ukontentowany z zastanej sytuacji.

> *Art. 38 ust. 2. RODO*
>
> *Administrator oraz podmiot przetwarzający wspierają inspektora ochrony danych w wypełnianiu przez niego zadań, o których mowa w art. 39, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej.*

Dodatkowo 1/3 IOD-ów uważa, że kierownictwo w bardzo małym stopniu jest informowane o i wyraża zainteresowanie rolą i obowiązkami Inspektora, co według norweskiego organu mogło by oznaczać, że wielu administratorów nie jest informowana na bieżąco o działaniach swoich Inspektorów.

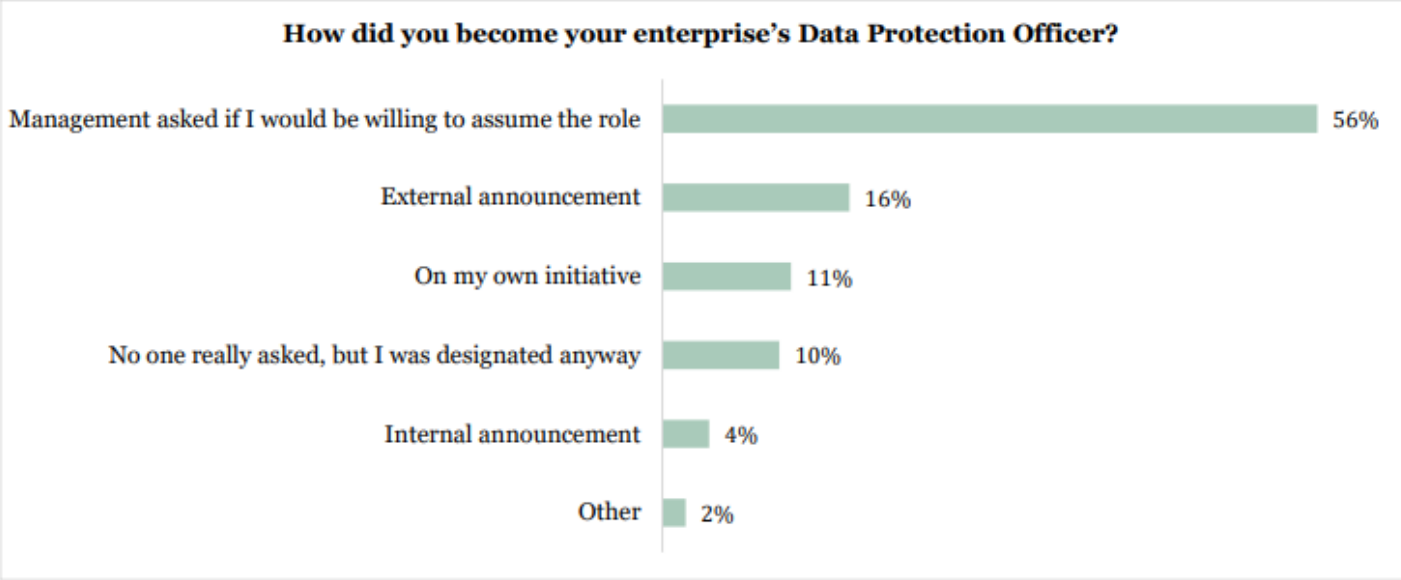
Kim są norwescy Inspektorzy?

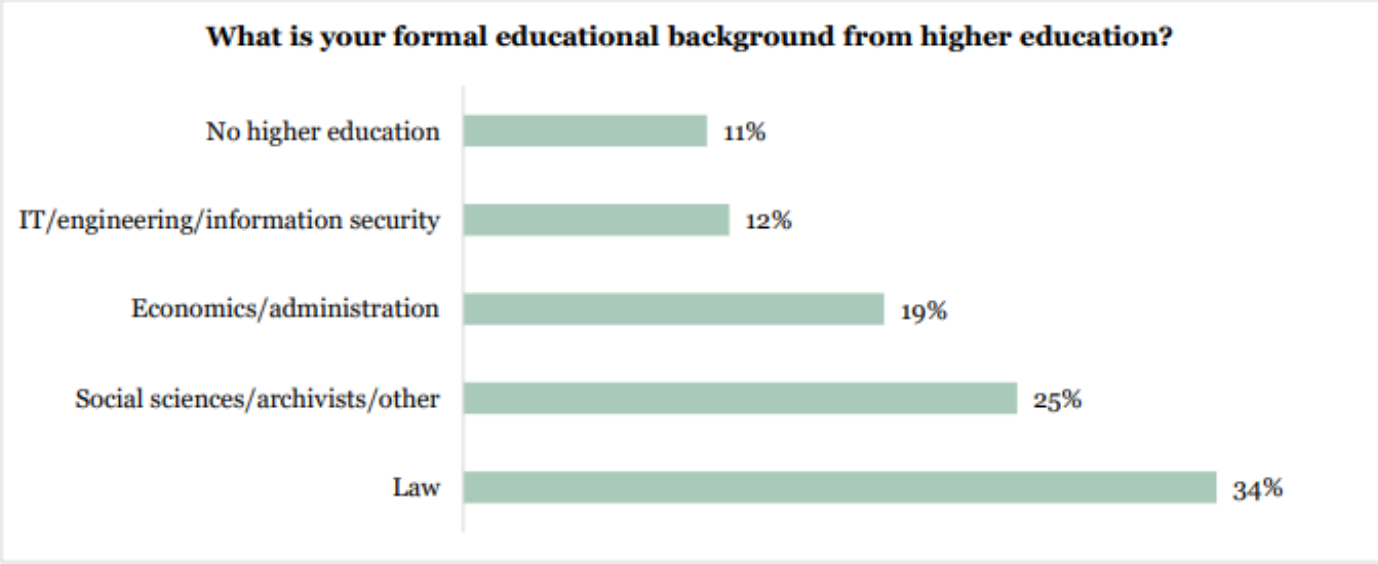
Na podstawie jakich kwalifikacji administrator wyznaczył IOD (np. wykształcenie, doświadczenie, wiedza)?

– tak brzmiało jedno z 27 pytań zadanych przez UODO polskim podmiotom, które były przez niego audytowane. Na swojej stronie polski organ wskazuje w jaki sposób można ocenić kwalifikacje osoby kandydującej do pełnienia funkcji IOD (link: https://uodo.gov.pl/pl/223/612), w tym powołuje się na wytyczne EROD (dawniej Grupa Robocza art. 29) dotyczące Inspektorów Ochrony Danych link:

https://uodo.gov.pl/pl/10/7). Można więc zauważyć, że administrator musi uzasadnić wybór danej osoby na Inspektora w swojej organizacji. A wskazana osoba powinna posiadać odpowiednie doświadczenie czy wiedzę do sprawowania powierzonej jej funkcji.

Tymczasem możemy zauważyć, że w Norwegii do pełnienia roli Inspektorów Ochrony Danych powoływani są pracownicy danego podmiotu – aż 56%. Czy może to świadczyć o przemyślanym wyborze? Pytanie pozostawiam bez odpowiedzi, prezentując poniżej dokładne statystyki:





Komu podlegają Inspektorzy?

Inspektor Ochrony Danych powinien podlegać najwyższemu kierownictwu. Zwraca na to uwagę polski UODO (link: https://uodo.gov.pl/pl/223/713), jak również mówią o tym wprost przepisy art. 38 ust. 3

RODO. W ostatnim audycie wykonywania funkcji IOD w przedsiębiorstwach także kwestia ta podlegała sprawdzeniu, przez zadanie następujących pytań UODO przedsiębiorcom:

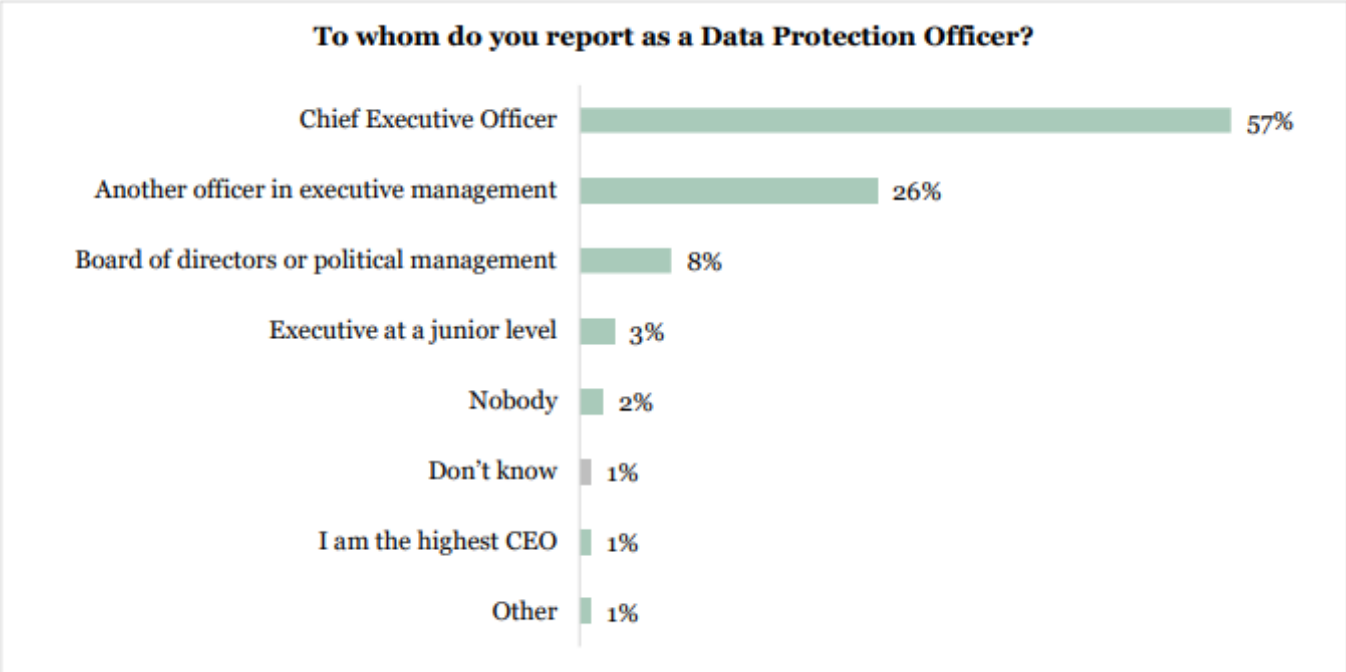
- Jakie stanowisko zajmuje IOD i komu podlega w strukturze organizacyjnej administratora?

- Czy w zakresie wykonywania innych zadań IOD podlega innym osobom niż najwyższe kierownictwo administratora?

> *Art. 38 ust. 3. RODO*
>
> *Administrator oraz podmiot przetwarzający zapewniają, by inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania tych zadań. Nie jest on odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań. Inspektor ochrony danych bezpośrednio podlega najwyższemu kierownictwu administratora lub podmiotu przetwarzającego.*

Odpowiedzi udzielone przez ankietowanych Inspektorów w Norwegii ukazują, że:

- Ponad połowa podlega dyrektorom,
- 26% podlega innemu członkowi kierownictwa przedsiębiorstwa,
- Natomiast aż 5% nie wie komu podlegają, albo nie mają komu podlegać, a
- 3% podlega kierownictwu niższego szczebla.



Jak sam norweski organ zauważa – nie jest to zgodne z wymogami RODO. Ponieważ wyższa kadra kierownicza przedsiębiorstwa ponosi ostateczną i formalną odpowiedzialność za zapewnienie zgodności z przepisami RODO. Dlatego ważne jest, aby przedstawiono im zalecenia Inspektora Ochrony Danych, aby mogli rozważyć te zalecenia i porównać je z innymi aspektami. Odpowiedzi

pokazują, że większość Inspektorów podlega kierownictwu wykonawczemu, co wskazuje, że najwyższe kierownictwo jest często informowane o pracy inspektora ochrony danych.
Problematyczne jest jednak to, że tak wielu funkcjonariuszy nie podlega kierownictwu wykonawczemu. W konsekwencji kierownictwo wykonawcze nie jest informowane o pracach związanych z zapewnieniem zgodności z RODO, za które jest odpowiedzialne. Oznacza to również, że kierownictwo wykonawcze niekoniecznie musi posiadać wiedzę niezbędną do podejmowania świadomych decyzji dotyczących wykorzystania danych osobowych w przedsiębiorstwie.

Czy Inspektor ma kontakt z kierownictwem?

Dobra komunikacja między IOD a kierownictwem jest niezbędna do ustalenia priorytetów środków ochrony danych w przedsiębiorstwie. Sprawozdawczość, raporty i spotkania wskazują na to, w jakim stopniu przedsiębiorstwo jest świadome zadań i znaczenia roli Inspektora. Formalne procedury sprawozdawcze mogą być konieczne do ustanowienia dobrych ram dialogu. Norweski organ zapytał Inspektorów czy mają jakąkolwiek formę dostarczania regularnych, pisemnych raportów dla kierownictwa przedsiębiorstwa.

Aż 65% Inspektorów odpowiedziało, że nie przygotowuje żadnych regularnych pisemnych raportów do przedstawienia kierownictwu. Wynik daleki od idealnego, a nasz polski organ również zwraca na to uwagę, pytając administratorów:

- *Czy IOD opracował (systematycznie opracowuje) plan swojej pracy np. w zakresie szkoleń, 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?*

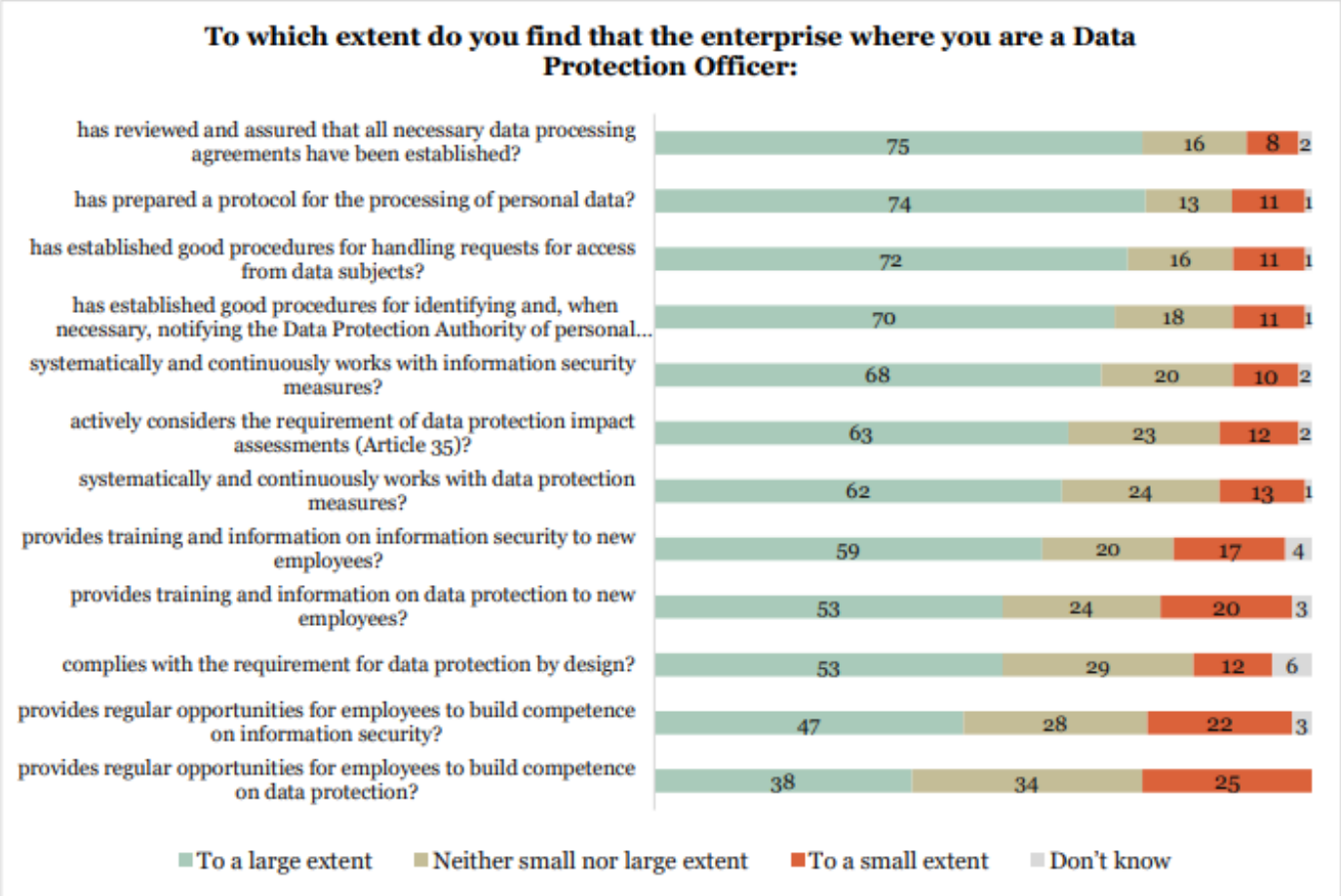
- *Jak często i w jaki sposób IOD przekazuje administratorowi wyniki przeprowadzonych audytów?*

Dlatego należy pamiętać, że komunikacja i raportowanie do najwyższego kierownictwa to nie tylko zalecenia, ale również zobowiązanie wynikające z RODO, które może podlegać weryfikacji przez organy nadrzędne ds. ochrony danych osobowych.

Z jakimi problemami spotykają się przedsiębiorstwa w Norwegii?

Chociaż wielu Inspektorów Ochrony Danych stwierdza, że ich przedsiębiorstwa generalnie przestrzegają odpowiednich przepisów RODO, tak samo rozporządzenie zawiera kilka szczegółowych wymagań, które muszą być aktywnie spełniane. Dlatego norweski urząd zapytał, w jakim stopniu

Inspektorzy uznają, że w reprezentowanych przez nich przedsiębiorstwach spełniono główne wymagania i warunki zgodności wynikające z przepisów o ochronie danych osobowych.



Możemy zauważyć, że większość Inspektorów potwierdza zawarcie wszelkich niezbędnych umów dotyczących przetwarzania danych osobowych czy wdrożono odpowiednie procedury obsługi żądań osób, których dane dotyczą. Zgodnie z ich zdaniem większość przedsiębiorstw systematycznie weryfikuje stosowane środki, uwzględniając wpływ na ochronę danych osobowych (DPIA), czy prowadzi szkolenia z zakresu bezpieczeństwa informacji dla nowych pracowników. Po drugiej stronie znajduje się sytuacja aktualnych pracowników, w których już administratorzy nie inwestują – ani w szkolenia z zakresu ochrony danych osobowych, ani z bezpieczeństwa informacji. Pamiętajmy, że zgodnie ze statystykami (np. Związku Firm Ochrony Danych Osobowych, ZFODO link: https://www.zfodo.org.pl/wp-content/uploads/2020/02/raport_zfodo_naruszenia-16.02.20.pdf) wynika, że większość naruszeń wynika z błędu (nieumyślnego) pracowników (ponad 70%), a przyczyną naruszenia jest tzw. czynnik ludzki (89%), nie technologiczny (11%).

Jakie zalecenia daje norweski urząd Inspektorom?

Na samym końcu podsumowania przeprowadzonej w 2021 r. ankiety możemy znaleźć 5 zaleceń, a w zasadzie wskazówek którymi obdarowuje Inspektorów norweski urząd. Zgodnie z nimi:

1) Należy ustalić opis pracy Inspektora oraz jego roli w przedsiębiorstwie – co powinno zostać uzgodnione z osobą z wyższego szczebla kierowniczego,
2) Należy ustalić formalne struktury, które zapewnią zaangażowanie i wymianę informacji/raportów między Inspektorem a najwyższym kierownictwem,
3) Powinno budować się świadomość roli Inspektora Ochrony Danych w przedsiębiorstwie, podwyższać jego kompetencje oraz innych pracowników w zakresie ochrony danych osobowych,
4) Zalecane jest nawiązanie kontaktu z innymi Inspektorami, w celu wymiany informacji i aktualizacji wiedzy z zakresu ochrony danych osobowych,
5) Istnieje możliwość kontaktu z norweskim organem w celu uzyskania porady i wskazówek z zakresu RODO, do czego organ namawia.

Podsumowanie

Nie tylko w Polsce organ ochrony danych osobowych weryfikuje sposób sprawowania funkcji IOD. Norweski urząd w ubiegłym roku wysłał kwestionariusze do Inspektorów Ochrony Danych. Na podstawie udzielonych odpowiedzi stworzył raport, z którego możemy wyczytać, że aż 65% Inspektorów nie przygotowuje żadnych regularnych pisemnych raportów dla kierownictwa przedsiębiorstwa, a 5% Inspektorów nie wie komu podlega bądź nie ma komu raportować swojej pracy. Dodatkowo 3% potwierdziło, że podlega kierownictwu niższego szczebla. Dodatkowo ponad połowa Inspektorów została wybrana wśród załogi przedsiębiorstwa, przez co aż 11% stwierdza, że w ogóle nie poświęca czasu na pełnienie dodatkowej funkcji Inspektora, a jedynie 17% pracuje jako IOD w pełnym wymiarze godzin.

Podane statystyki i grafiki pochodzą ze strony
https://www.datatilsynet.no/contentassets/b5f70248207a4768a3295aaffac78edc/data-protection-officer-survey-2020-21.pdf

Przemysław Siarka – specjalista ds. ochrony danych osobowych w iSecure Sp. z o.o.