Ochrona sygnalistów zgodna z RODO. Obowiązkowe zmiany w dokumentacji

Obowiązujące od 25 września br. przepisy o ochronie sygnalistów powodują, że podmioty obowiązane np. brokerzy czy agenci ubezpieczeniowi, muszą pochylić się nad przepisami rozporządzenia RODO, a konkretnie nad dokumentacją w której należy dokonać obowiązkowych zmian.

Zwracam uwagę, że w przypadku podmiotów obowiązanych nie ma zastosowania 50-osobowy próg zatrudnienia. To również jest jednoosobowa działalność jakkolwiek to absurdalnie brzmi.

Przepisy RODO w kontekście sygnalistów to proces nierozerwalny. Unijny prawodawca już w motywie 83 dyrektywy o ochronie sygnalistów poczynił zastrzeżenie, że przetwarzanie danych osobowych musi być dokonywane zgodnie z zapisami art. 5 i 25 RODO. Zgodność z RODO i najwyższe standardy bezpieczeństwa to priorytet każdej organizacji. Myśląc o sygnalistach, należy mieć na uwadze szeroki zakres osób jakimi należy się zaopiekować, a dokładnie ich danymi osobowymi.

Czyje dane? Przede wszystkim sygnalistów, ale również osób pomagających w zgłoszeniu, świadków, osób których dotyczy zgłoszenie, osób pokrzywdzonych czy członków komisji prowadzącej postępowania wyjaśniające. To nie koniec, bo mogą to być też dane osobowe zabezpieczone w materiałach dowodowych np. korespondencji e mail, czy z logów w systemach informatycznych.

Przetwarzanie danych ma miejsce we wszystkich etapach systemu whistleblowing od przyjęcia zgłoszenia o nieprawidłowości, prowadzenia postępowania wyjaśniającego, komunikacji z sygnalistą do momentu archiwizacji informacji.

Obowiązkowe zmiany w dokumentacji RODO

1. **aktualizacja RCP**
    - ustalenie celu przetwarzania, a więc wybór właściwej podstawy prawnej -*art. 6 ust.1 RODO*
    - ustalenie rodzaju i zakresu danych oraz kategorii osób, których dane są przetwarzane,
    - ustalenie prawidłowych okresów retencji**.**
2. **spełnienie obowiązku informacyjnego - *art.13, 14 RODO,***
3. **przekazanie okresowych upoważnień i oświadczeń do przetwarzania danych,**
4. **weryfikacja umowy powierzenia, w przypadku realizacji obsługi zgłoszeń przez podmiot zewnętrzny lub przez aplikacji zewnętrzną,**
5. **przestrzeganie zasad: Privacy by designe, Privacy by default,**

6. **stosowanie zasady minimalizacji,**
7. **ewentualne włączenie nowych zadań do obowiązków IOD lub KODO.**
8. **wykonanie analizy ryzyka – *art. 32 RODO***
9. **wykonanie DPIA - Oceny skutków dla ochrony danych osobowych – *art. 35***

Podmioty prowadzące **RCP** muszą w nim uwzględnić nowe czynności przetwarzania danych osobowych związane z obsługą zgłoszeń sygnalistów i określić: cel i podstawę prawną przetwarzania, kategorie danych i osób, których dane dotyczą, opis zastosowanych środków technicznych i organizacyjnych oraz okres retencji czyli planowany termin usunięcia danych. Okres przechowywania tych danych osobowych to 3 lata.

Realizacja obowiązku informacyjnego wymaga: ustalenie statusu osób występujących w zgłoszeniu: sygnalista, świadek, osoba której dotyczy zgłoszenie, eksperci wewnątrz organizacji itd.) i dostosowania zakresu informacji do konkretnej osoby. Z uwagi na bezwzględną ochronę tożsamości osób uczestniczących w całym procesie nie podajemy informacji o źródle danych tzn. następuje wyłączenie stosowania ***art.14 ust.2 lit .f; art.15 ust.1 lit. g RODO.*** Należy również ustalić jakim kanałem będzie realizowany obowiązek informacyjny oraz poinformować o możliwości dokonywania przez sygnalistów zgłoszeń zewnętrznych i ujawnień publicznych.

Osoby obsługujące proces zgłoszeń muszą otrzymać odpowiednie **upoważnienia** oraz podpisać **oświadczenie** że zapoznały się z **Procedurą zgłaszania naruszeń i podejmowania działań następczych oraz zasad ochrony sygnalistów** w firmie

Analogicznie jak w przypadku stosowania przepisów RODO należy uwzględnić ochronę danych osobowych i prywatności na etapie tworzenia założeń projektu nowego produktu lub usługi **(privacy by designe)** i wprowadzania domyślnych ustawień zapewniających maksymalny, stały stopień prywatności **(privacy by default).**

Mamy obowiązek stosować **zasadę minimalizacji,** co oznacza wyraźne, ustawowe ograniczenie zakresu przetwarzania danych osobowych *(art.8 pkt.4 u.o.s.)* Przetwarzamy dane osobowe tylko w zakresie niezbędnym do przyjęcia zgłoszenia lub ewentualnego podjęcia działania następczego. Natomiast dane osobowe, które nie mają znaczenia dla rozpatrywania zgłoszenia powinny być zbierane, a w razie przypadkowego zebrania są niezwłocznie usuwane – 14 dni.

Musimy się zastanowić, czy **nowe obowiązki mogą zostać powierzone IOD/KODO?** Nie ma zakazów prawnych, bo Prezes UODO nie zabrania aby Inspektor czy Koordynator uczestniczył w tym procesie. Ważne tylko w jakim zakresie, bo przecież ma on swoje obowiązki określone art. 39 RODO więc jego wolny czas jest ograniczony. Poza tym jest jeszcze kwestia zakresu kompetencji, bo można spodziewać się że zapewni poufność danych, ale czy będzie w stanie przeprowadzić działania następcze z zakresu np. prania pieniędzy, bezpieczeństwa produktu czy transportu? Z drugiej strony nie możemy eliminować go z tego procesu. Musi w nim uczestniczy, ale może nie jako główny podmiot.

Przeprowadzenie **analizy ryzyka** to najważniejszy obowiązek jakie nakłada rozporządzenie RODO. Wadliwie przeprowadzona, nieaktualizowana często bywa wskazywana przez Prezesa UODO, jako jeden z elementów, które przyczyniły się do nałożenia administracyjnej kary pieniężnej. Każda realizowana przez ADO czynność powinna być poprzedzona wykonaniem analizy ryzyka, która pozwoli na dobranie odpowiednich środków technicznych i organizacyjnych zapewniających odpowiedni poziom bezpieczeństwa danych osobowych.

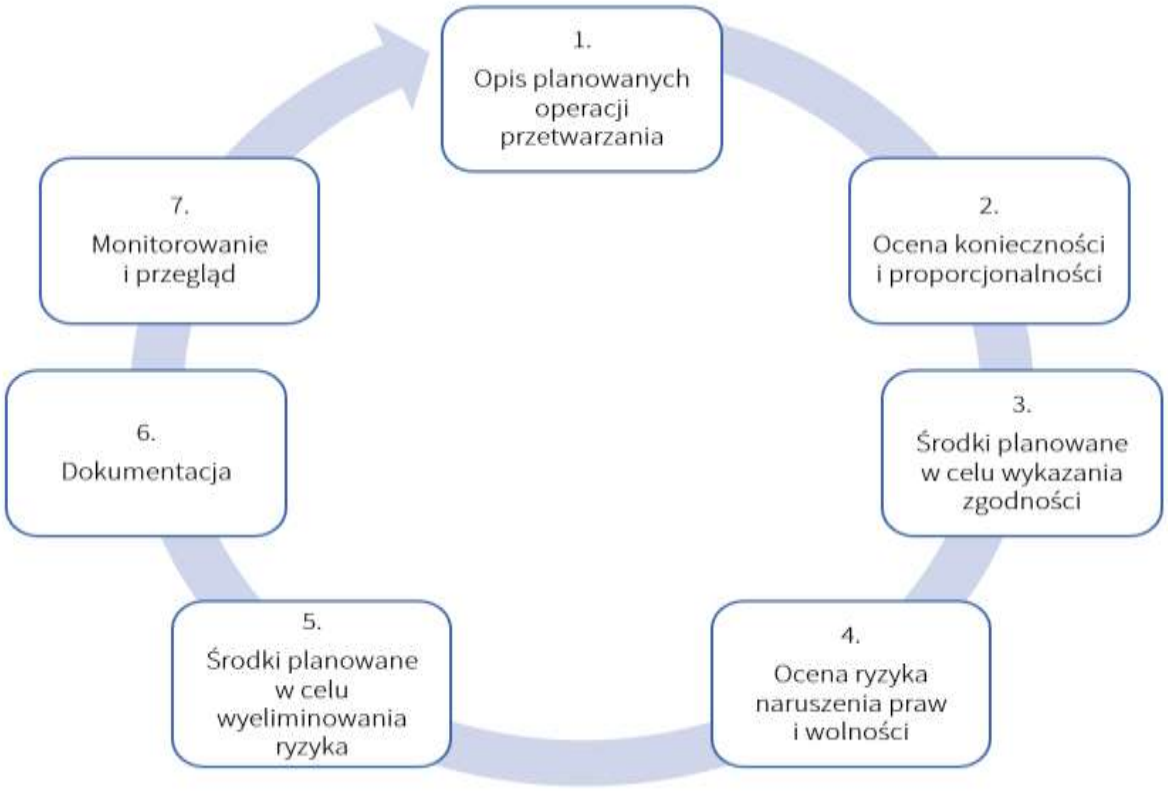
W procesie **analizy ryzyka** na gruncie przepisów o ochronie sygnalistów należy uwzględnić: wybór kanału zgłoszeń (ustne/pisemne) sposób realizacji oraz wybór narzędzi obsługi zgłoszeń (aplikacja, strona www.)

DPIA (Data Protection Impact Assessment) - Ocena skutków dla ochrony danych to nowy obowiązek, którego wymaga wprowadzony system whistleblowing. Komunikat Prezesa Urzędu Ochrony Danych Osobowych z 17.06.2019r ***(MP 8.07.2019 poz. 666)*** określa wykaz rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony - ***pkt 9. Serwisy służące do zgłaszania nieprawidłowości (whistleblowing)***

DPIA to proces oceny ryzyka, który obejmuje analizę metod przetwarzania danych, ocenę potencjalnych zagrożeń oraz wdrożenie odpowiednich środków ochronnych, a jej przeprowadzenie jest obowiązkowe.

Dokonując **DPIA** stawiamy się na miejscu osoby, której dane dotyczą i analizujemy, co złego może się stać w wyniku nieprawidłowego przetwarzania danych.

Schemat wykonania **DPIA**



Źródło: Wytyczne Grupy Roboczej Art. 29. dotyczące oceny skutków dla ochrony danych (WP 248)

1. Opis planowanych operacji przetwarzania
to przede wszystkim odpowiedzi na pytania, w jakim celu, zakresie i czasie będą przetwarzane dane osobowe. Jeśli dla analizowanego procesu prowadzisz już **rejestr czynności przetwarzania**, znasz odpowiedzi na te pytania.

2. Ocena konieczności i proporcjonalności
to odpowiedź na pytanie, czy zakres przetwarzanych danych, zakres osób, których dane przetwarzamy, a także zakres odbiorców którym te dane udostępniamy, jest niezbędny z punktu widzenia celów i podstaw prawnych przetwarzania.

3. Środki planowane w celu wykazania zgodności
opisujemy przez wskazanie zabezpieczeń organizacyjnych i technicznych, a także rekomendacji dotyczących usunięcia wykrytych niezgodności.

4. Ocena ryzyka naruszenia praw i wolności osób, których dane dotyczy

- jakie naruszenie może wystąpić?
- z czego wynika możliwość wystąpienia zagrożenia (jakie są podatności),
- jakie są możliwe skutki,
- jaka jest waga zagrożenia,

- jakie jest prawdopodobieństwo naruszenia,
- jaki jest poziom ryzyka (jest to wynik mnożenia wagi i prawdopodobieństwa),
- jakie są rekomendacje (jak zminimalizować ryzyko).

5. Środki planowane w celu wyeliminowania ryzyka
ustala się na podstawie rekomendacji wydanych w poprzednim kroku. Realizując je, najczęściej niwelujemy podatności, z których wynika możliwość wystąpienia zagrożenia.

6. Dokumentacja
DPIA obejmuje zapis czynności podejmowanych w ramach DPIA, jak również dowody audytowe, czyli np. kopie dokumentów potwierdzających prawdziwość ustaleń.

7. Monitorowanie i przegląd
DPIA należy dokonywać zawsze, gdy występuje możliwość zmiany ryzyka naruszenia praw lub wolności osób fizycznych. W ramach dobrych praktyk, oceny skutków dla ochrony danych należy dokonywać raz w roku.Ryzyka, które musimy uwzględnić w **DPIA** to**:** nieautoryzowane ujawnienie tożsamości sygnalisty, dostęp osób nieuprawnionych do treści zgłoszenia, manipulacja danymi czy zagrożenia technologiczne.

Podsumowując

Przedstawiłam katalog zadań, jakie ma administrator w zakresie prawidłowej ochrony danych osobowych w procesie przyjmowania i realizacji zgłoszenia od sygnalisty. Dla podmiotów, które mają prawidłowo wdrożone procedury RODO, to zadanie nie będzie mega trudne, bo będzie polegało na dokonaniu pewnych uzupełnień czy zmian w już posiadanej dokumentacji oraz przeprowadzenia dodatkowej analizy ryzyka z uwagi na inne aspekty. Oczywiście największym wyzwaniem będzie przeprowadzenie **DPIA,** która jest procesem budowania i pokazywania zgodności z zapisami RODO. Najważniejsza zasada to patrzeć na ten proces jak na całość. Ochrona sygnalistów to nie tylko wymóg prawny, ale przede wszystkim element budowania silnej i etycznej organizacji.

Jeżeli ktoś będzie zainteresowany WZOREM DPIA lub praktycznym przykładem DPIA zapraszam do kontaktu.

Teresa Grabowska

TG-Doradztwo i Zarządzanie