Whistleblowing - dyrektywa 2019/1937 Rady UE i PE w sprawie ochrony osób zgłaszających naruszenia prawa Unii

intencje – logika – realia

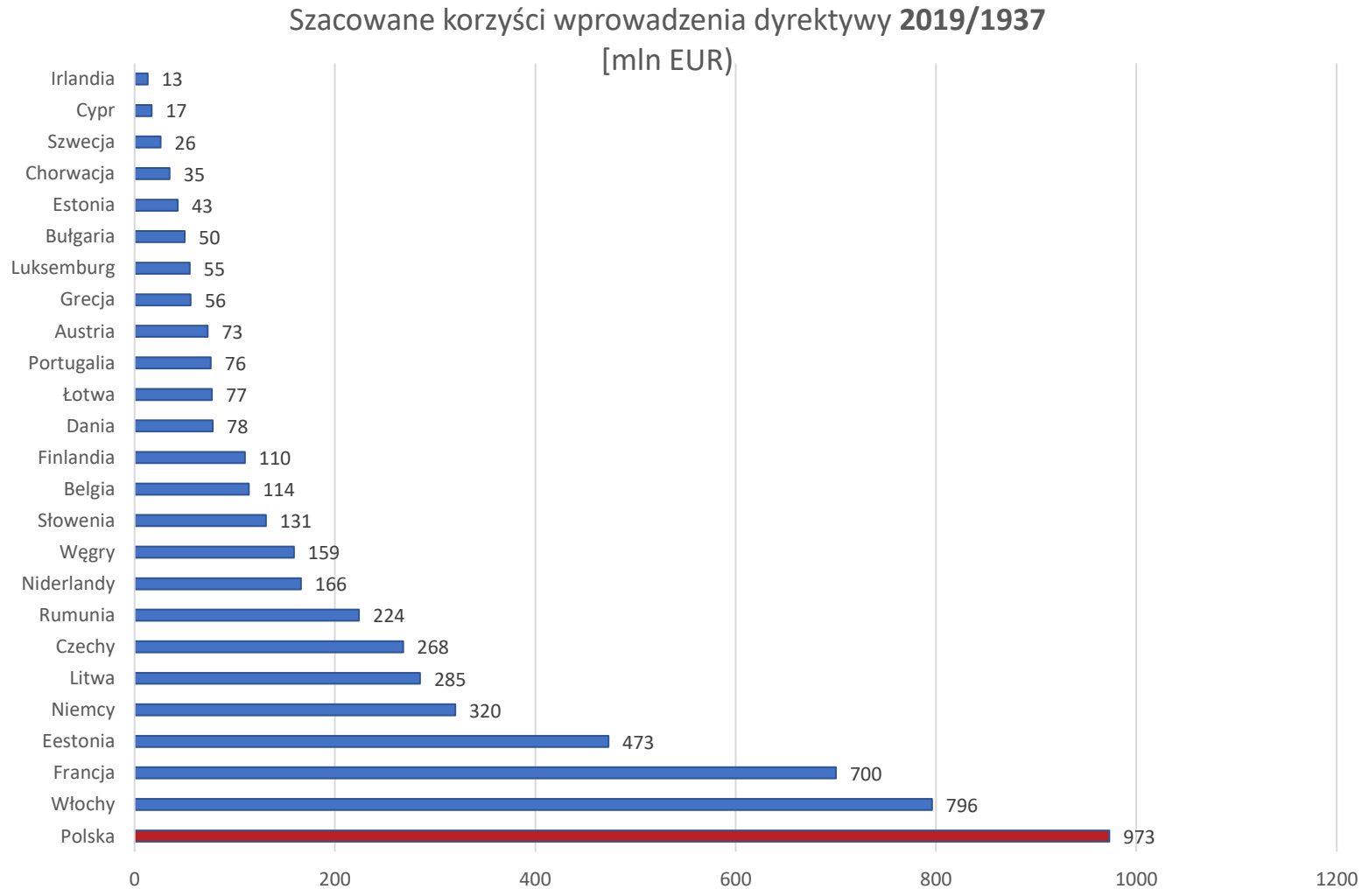
Tadeusz Reczyński

FCR
fast certified reliable

Intencje wprowadzenia nowej regulacji prawnej

- naruszanie prawa Unii zarówno przez organizacje publiczne jak i prywatne niejednokrotnie powoduje wymierne szkody dla interesu publicznego;
- szczególnie szkodliwe są naruszenia prawa Unii w dziedzinie zamówień publicznych;
- w niektórych dziedzinach polityki przypadki naruszenia prawa Unii mogą wyrządzić poważną szkodę interesowi publicznemu;
- osoby zatrudnione w takich organizacjach zwykle jako pierwsze dowiadują się o zagrożeniach dla interesu publicznego, do jakiego może dojść w tym zakresie;
- osoby te często jednak rezygnują ze zgłaszania swoich zastrzeżeń lub podejrzeń z obawy przed działaniami odwetowymi;
- doświadczenia wielu krajów członkowskich wskazują, że zapewnienie tym osobom szczególnej ochrony przed represjami spowoduje obniżenie bariery obaw i w konsekwencji będzie sprzyjało ograniczaniu szkód dla interesu publicznego;
- dyrektywa wprowadza ujednolicenie zasad ochrony osób zgłaszających naruszenie prawa Unii, ustala normy minimalne zapewniające im skuteczną i zrównoważoną ochronę;
- w dyrektywie stwierdza się, że działalność sygnalistów jest istotnym elementem kontroli oddolnej, i jako taka wzmacnia systemy demokratyczne.

Szacowane korzyści wprowadzenia dyrektywy 2019/2037 [mln EUR]



Obszary stosowania i wyłączenia stosowania dyrektywy

Zastosowania

- zamówienia publiczne,
- usługi, produkty i rynki finansowe,
- zapobieganie praniu pieniędzy i finansowaniu terroryzmu,
- bezpieczeństwo produktów i ich zgodność z wymogami,
- bezpieczeństwo transportu w sektorze kolejowym, drogowym, morskim i żeglugi śródlądowej,
- ochrona środowiska, począwszy od gospodarowania odpadami aż po chemikalia,
- ochrona radiologiczna i bezpieczeństwo jądrowe,
- bezpieczeństwo żywności i pasz,
- zdrowie i dobrostan zwierząt,
- zdrowie publiczne, w tym prawa pacjentów i kontrola wyrobów tytoniowych,
- ochrona konsumentów,
- ochrona prywatności i danych osobowych,
- bezpieczeństwo sieci i systemów teleinformatycznych
- naruszenia mające wpływ na interesy finansowe Unii
- naruszenia unijnych zasad konkurencji i pomocy państwa,

Wyłączenia

- w zakresie zamówień publicznych w dziedzinach obronności i bezpieczeństwa,
- ochrony informacji niejawnych,
- tajemnicy związanej z wykonywaniem zawodu,
- tajemnicy narady sędziowskiej,
- postępowania karnego,
- naruszenie prawa godzi wyłącznie w prawa zgłaszającego lub zgłoszenie naruszenia prawa następuje wyłącznie w indywidualnym interesie zgłaszającego
- Sprawa została zgłoszona na postawie przepisów odrębnych, w szczególności jako skarga lub zawiadomienie o możliwości popełnienia przestępstwa,

Uprawnienia przedmiotowe

- Dyrektywa odnosi się do osoby fizycznej, która ujawnia informację o naruszeniu prawa uzyskaną w kontekście związanym z pracą, tzn.:
- pracownika, także w przypadku, gdy stosunek pracy już ustał,
- osoby ubiegającej się o zatrudnienie, która uzyskała informację o naruszeniu prawa w procesie rekrutacji lub negocjacji poprzedzających zawarcie umowy,
- osoby świadczącej pracę na innej podstawie niż stosunek pracy, w tym na podstawie umowy cywilnoprawnej,
- przedsiębiorcy,
- akcjonariusza lub wspólnika,
- członka organu osoby prawnej,
- osoby świadczącej pracę pod nadzorem i kierownictwem wykonawcy, podwykonawcy lub dostawcy, w tym na podstawie umowy cywilnoprawnej,
- stażysty,
- wolontariusza.

Rodzaje zgłoszeń

- zgłoszenie wewnętrzne
  - obowiązek stworzenia możliwości przyjmowania zgłoszeń obciąża pracodawców spełniających wymogi ustawowe,
  - pozostali pracodawcy mogą stosować ustawę fakultatywnie,
- zgłoszenie zewnętrzne,
  - może być realizowane z pominięciem pracodawcy,
  - zgłoszenia zewnętrzne przyjmują:
    - wskazane w ustawie urzędy centralne – w polskim projekcie świadomie wskazuje się jeden urząd RPO
    - wskazane urzędy publiczne
      - wskazano wprost jeden organ publiczny: Prezes Urzędu Ochrony Konkurencji i Konsumentów. w zakresie zasad konkurencji i ochrony konsumentów,
      - ustawa nieprecyzyjnie określa, że: organem publicznym mogą być inne instytucje publiczne przyjmujące zgłoszenia w dziedzinach należących do ich zakresu działania,
  - ujawnienie publiczne – głównie media wg wyboru sygnalisty

Ochrona osób zgłaszających naruszenie prawa myślą przewodnią

- w ślad za dyrektywą podąża polski projekt ustawy dostosowującej (projekt wyedytowany pod datą 14 października 2021),
- zapisy dotyczące przeciwdziałaniu represjom i działaniom odwetowym stanowią nie mniej niż 1/3 treści dyrektywy oraz projektowanej polskiej ustawy dostosowującej,
- w projekcie ustawy wpisano długą i bardzo szczegółową listę zakazanych działań uznawanych, w świetle ustawy, za zakazane i karalne,
- logicznie interpretując, działania te, z natury rzeczy, mają sens wyłącznie w przypadku ujawnienia tożsamości sygnalisty,
- maksymalne kary za ujawnienie tożsamości są identyczne w każdym innym przypadku naruszenia zasady zapewnienia poufności - sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3,

Ochrona osób zgłaszających naruszenie prawa myślą przewodnią

- zgłaszający podlega ochronie tylko w zakresie objętym dyrektywą (ustawą)
- osoba dokonująca ujawnienia publicznego podlega ochronie tylko wówczas, jeżeli wcześniej dokonała przynajmniej zgłoszenia zewnętrznego
- zgłaszający podlega ochronie, pod warunkiem że miał w momencie dokonywania zgłoszenia lub ujawnienia publicznego uzasadnione podstawy sądzić, że będąca przedmiotem zgłoszenia lub ujawnienia publicznego informacja o naruszeniu prawa jest prawdziwa w momencie dokonywania zgłoszenia lub ujawnienia publicznego i że informacja taka stanowi informację o naruszeniu prawa,
- ustawa nieprecyzyjnie określa, że: organem publicznym mogą być inne instytucje publiczne przyjmujące zgłoszenia w dziedzinach należących do ich zakresu działania,
- przepisy ustawy stosuje się do zgłoszenia informacji o naruszeniu prawa anonimowo, wyłącznie w przypadkach gdy możliwość zgłoszenia informacji o naruszeniu prawa anonimowo przewiduje:
  - regulamin zgłoszeń wewnętrznych, stosowany przez pracodawcę, określający wewnętrzną procedurę zgłaszania naruszeń prawa lub
  - procedura zgłaszania naruszeń prawa organowi publicznemu.
- obecnie jedynie policja i prokuratura stosują procedury anonimowego zgłaszania,

Realia

- osoba zgłaszająca przypadek naruszenia prawa UE podlega ochronie wyłącznie w zakresie i na zasadach zdefiniowanych przez dyrektywę (ustawę),
- świadomie i właściwe przeprowadzenie procedury zgłoszenia tak, by nie utracić prawa do ochrony wymaga nieoczywistej wiedzy,
- można oczekiwać, że najczęściej będą podejmowaliby zgłoszenia anonimowe,
- pracodawca może, ale nie jest zobowiązany, przyjmować zgłoszenia anonimowe,
- obecnie, jedynymi instytucjami publicznym przyjmującymi zgłoszenia anonimowe są policja i prokuratura,
- udowodnienie, że zgłoszenie dokonane było w dobrej wierze, w sytuacjach kontrowersyjnych nie jest łatwe,
- sygnalista musi mieć możność zapisania na swoim własnym nośniku kopii zgłoszenia z opatrzonym cyfrową pieczęcią potwierdzeniem doręczenia oraz odpowiedzi lub próśb o dodatkowe informacje, również cyfrowo opieczętowanych lub podpisanych

Zapewnienie bezpieczeństwa cyfrowego

- w procesie regulowanym dyrektywą (potencjalnie ustawą) występują trzy zasadnicze kategorie informacji:
  - zawartość zgłoszenia,
  - dane osobowe zgłaszającego,
  - treść odpowiedzi,
- wszystkie ww. kategorie mają charakter danych wysoce wrażliwych,
- duża koncentracja danych wrażliwych w ściśle określonych lokalizacjach zwiększa ryzyko ich ujawnienia,
- wraz z rozwojem technik przetwarzania (wzrost mocy obliczeniowych, wykorzystywanie AI) maleje odporność wielu dotychczas stosowanych rozwiązań,
- być może jest czas na szersze korzystanie z sugerowanej od kilku już lat przez ekspertów techniki określanej mianem: *client-side encryption wzgl. client-side cryptography.*

Client-side encryption – charakterystyka metody

- Dane wrażliwe pozostają zaszyfrowane w całym procesie przesyłania i przechowywania kluczami niedostępnymi dla administratorów, serwisantów itp. personelu pomocniczego – niezależnie od poziomu ich uprawnień w systemach przetwarzania.
- Postać jawna występuje i może być wykorzystywana tylko na stacji roboczej uprawnionego użytkownika.
- Tym samym dostęp do danych mają jedynie osoby którym nadano takie uprawnienia i przydzielono do wyłącznej dyspozycji odpowiednie klucze szyfrowe.
- Dla osób postronnych, w tym także w przypadku skutecznego włamania się do przestrzeni serwerowej, zawartość tak zaszyfrowanych danych pozostaje niedostępna.
- Nawet drastyczne naruszenie zasad postępowania z uszkodzonymi lub zużytymi nośnikami danych niekoniecznie powoduje katastrofę.

Tadeusz Reczyński

+48 509 674 001

tadeusz.reczynski@fcr.net.pl

FCR

fast certified reliable