Sylwia Czub-Kiełczewska

RODO i bezpieczeństwo danych osobowych

Prowadząca

Sylwia Czub-Kiełczewska

» ekspertka ds. ochrony danych osobowych
» audytor wewnętrzny PN-ISO/IEC 27001
» wykładowca akademicki
» autorka komentarzy i książek o RODO
» czołowa ekspertka LEX ODO
» od 11 lat w branży
» praktyk

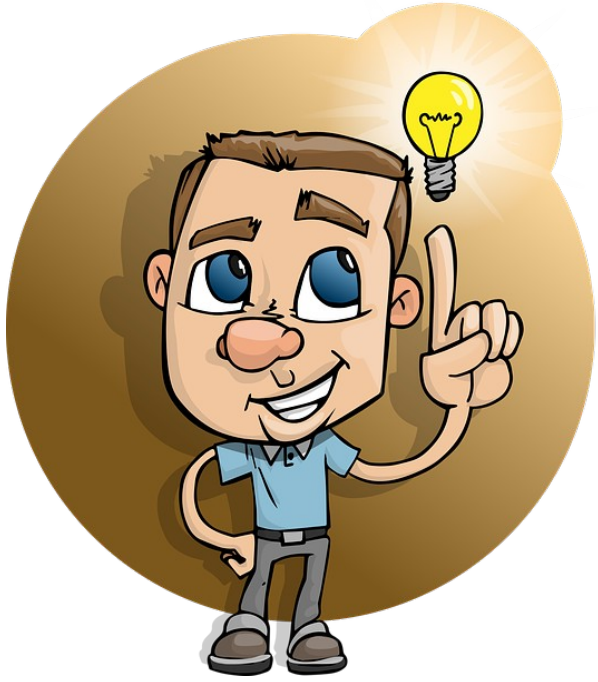
Agenda

1) Przetwarzanie danych w ramach FinxS - omówienie krok po kroku
2) Umowa powierzenia danych - najważniejsze fakty
3) Ankiety bezpieczeństwa - omówienie na przykładzie
4) Obowiązki związane z przetwarzaniem danych
5) Naruszenia ochrony danych - jak postępować

Przetwarzanie danych w ramach FinxS

Dane osobowe

Każda informacja, która umożliwia identyfikację osoby fizycznej. Nie ma znaczenia, czy identyfikacja jest bezpośrednia, czy pośrednia (wymaga podjęcia działania)



Dane osobowe w FinxS

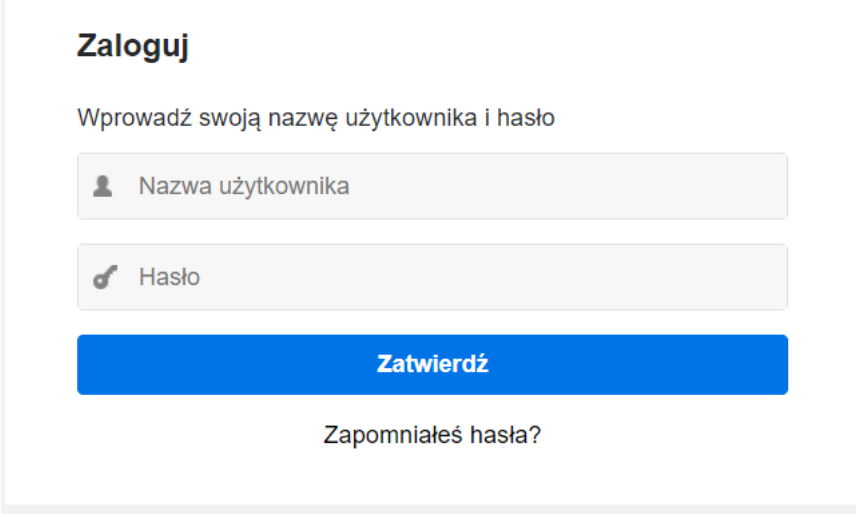
W systemie FinxS są przetwarzane dwie kategorie danych:

- dane użytkowników systemu
- dane respondentów.

Dane użytkowników

Dane są wprowadzane przez administratora na podstawie listy przekazanej przez klienta (pracodawcę).

Pracodawca nie prosi pracowników o zgodę na ich wprowadzenie do FinxS, gdyż jest to związane z ich obowiązkami służbowymi.



Dane respondentów

Respondenci wprowadzają swoje dane samodzielnie, poprzez formularz i ankiety z pytaniami.

Niezależnie od relacji łączącej ich z klientem (umowa o pracę, rekrutacja, współpraca) klient musi uzyskać zgodę na przetwarzanie ich danych osobowych w celu przeprowadzenia badania.

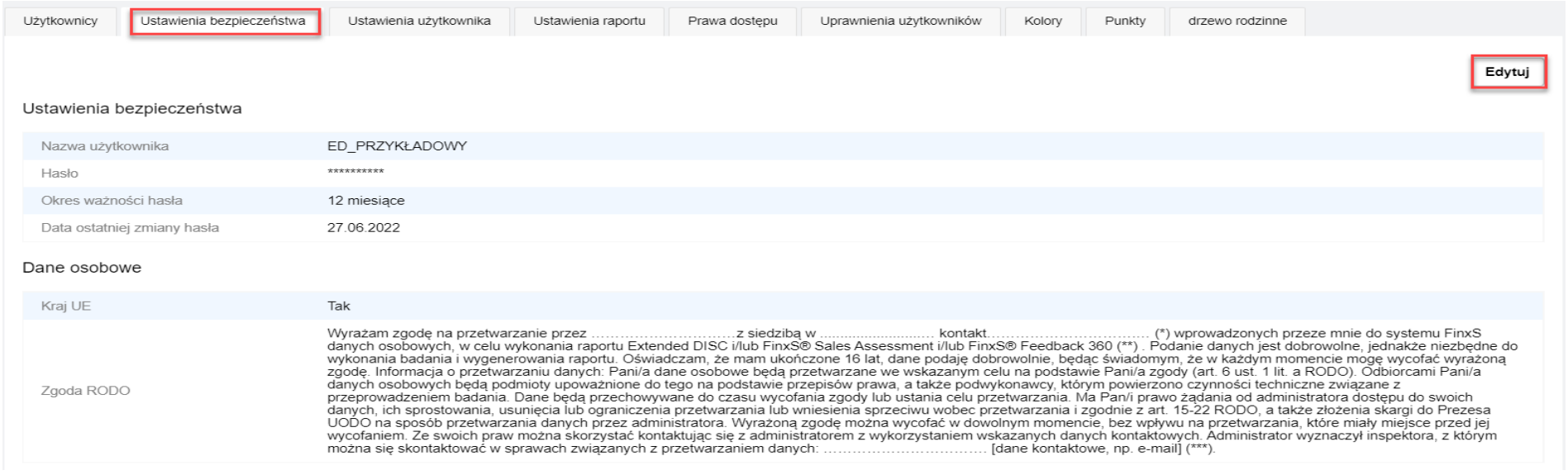
Zgoda respondenta

Klient może uzyskać zgodę samodzielnie, np. przekazując respondentom przed badaniem odpowiednie oświadczenie zgody.

System FinxS ułatwia uzyskanie zgody umożliwiając pozyskanie jej bezpośrednio w formularzu wprowadzania danych.

Zgoda respondenta

Klient, jako administrator danych osobowych, decyduje o treści zgody oraz klauzuli informacyjnej zbieranej w FinxS.



Dlaczego to klient jest administratorem danych?

Zgodnie z art. 4 RODO administratorem jest podmiot, który decyduje o celach i sposobach przetwarzania danych osobowych.

Klient zleca badanie, decyduje kto bierze w nim udział oraz o sposobie postępowania z wynikami – ma zatem status administratora danych.

Dlaczego należy uzyskać zgodę respondenta?

Badanie przeprowadzane z wykorzystaniem FinxS nie jest niezbędne do świadczenia pracy, zawarcia umowy, czy wywiązania się z obowiązku prawnego administratora. Nie można zmusić respondenta do wzięcia udziału.

W związku z tym zastosowanie ma art. 6 ust. 1 lit. a RODO, tzn. należy uzyskać zgodę na przetwarzanie.

Umowa powierzenia – najważniejsze fakty

Powierzenie danych

Przetwarzanie danych w imieniu administratora w związku z przeprowadzeniem badania, czy szkoleniami, wymaga zawarcia umowy powierzenia.

Wynika to z art. 28 RODO.

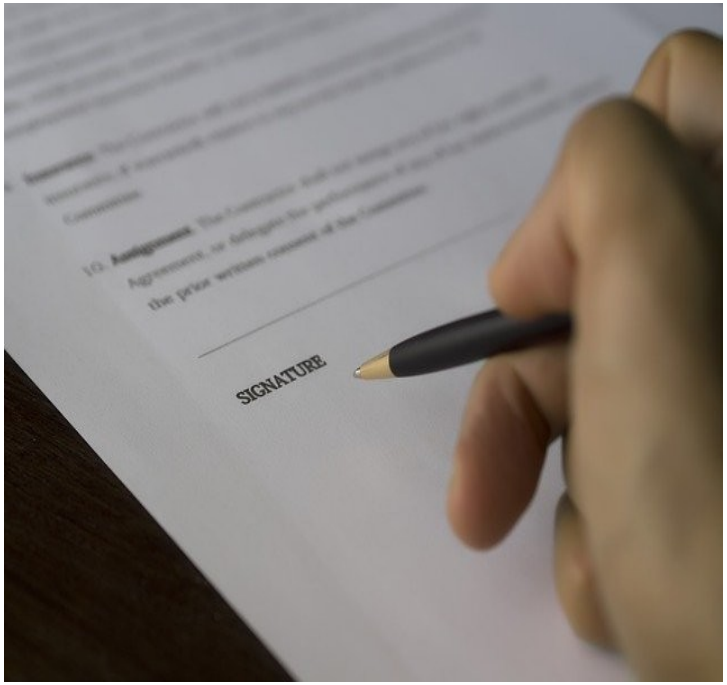
Powierzenie a umowa na usługi

Art. 28 RODO określa konkretne elementy, które musi zawierać umowa, aby powierzenie było zgodne z RODO.

Standardowa umowa na świadczenie usług nie zawiera tych zapisów.

Umowy dostarczane przez Extended Tools Polska zawierają umowę powierzenia.

Wzór umowy od klienta

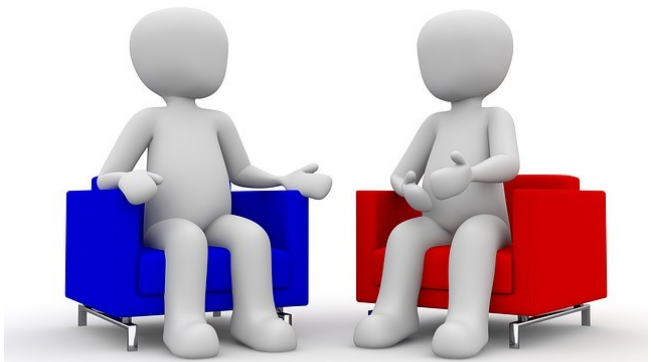


Umowa powierzenia dostarczona przez klienta może zawierać zapisy niekorzystne dla wykonawcy, jak kary umowne, czy warunki techniczne lub organizacyjne, których spełnienie oznacza poniesienie dodatkowych kosztów.

Dalsze podmioty przetwarzające

Korzystanie z FinxS wymaga dalszego powierzenia danych do Extended Tools Polska oraz jego Partnera Technologicznego.

Partnerem technologicznym jest FinxS OY Ltd z siedzibą w Finlandii korzystający z usług hostingu od Amazon.com.



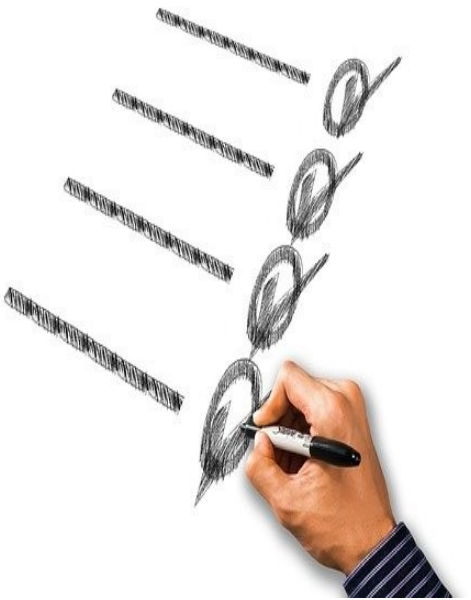
Dalsze podmioty przetwarzające

Przedstawicielem Amazon.com w Europejskim Obszarze Gospodarczym jest Amazon Web Services z siedzibą w Luksemburgu.

Centra danych są zlokalizowane na terenie EOG i dane nie są transferowane poza EOG.

Ankiety bezpieczeństwa - omówienie na przykładzie

Kontrola podmiotu przetwarzającego



Zgodnie z art. 28 ust. 3 RODO, klient jako administrator danych jest uprawniony do kontroli podmiotów przetwarzających dane.

Najczęściej jest to realizowane poprzez ankiety bezpieczeństwa (omówmy na przykładzie).

Obowiązki związane z przetwarzaniem danych

Klauzule informacyjne

Przepisy art. 13 RODO wymagają przekazywania przez administratora osobom, których dane dotyczą klauzuli na przetwarzanie danych (pracownicy, zleceniobiorcy, uczestnicy szkoleń).

Nie dotyczy osób, dla których administratorem jest inny podmiot.

Obligowanie do poufności i upoważnianie

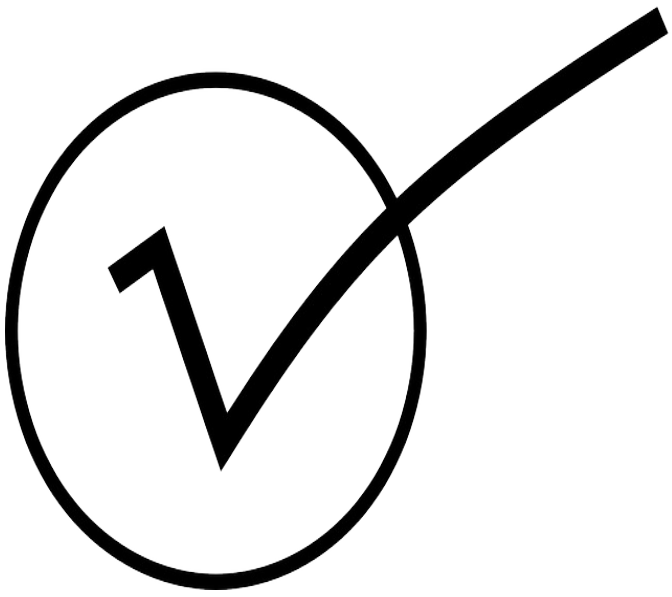
Administrator ma obowiązek zapewnić, aby dostęp do danych osobowych miały tylko osoby, które zostały wcześniej upoważnione i zobligowane od poufności.

Powinny zostać także przeszkolone z zasad ochrony danych osobowych.

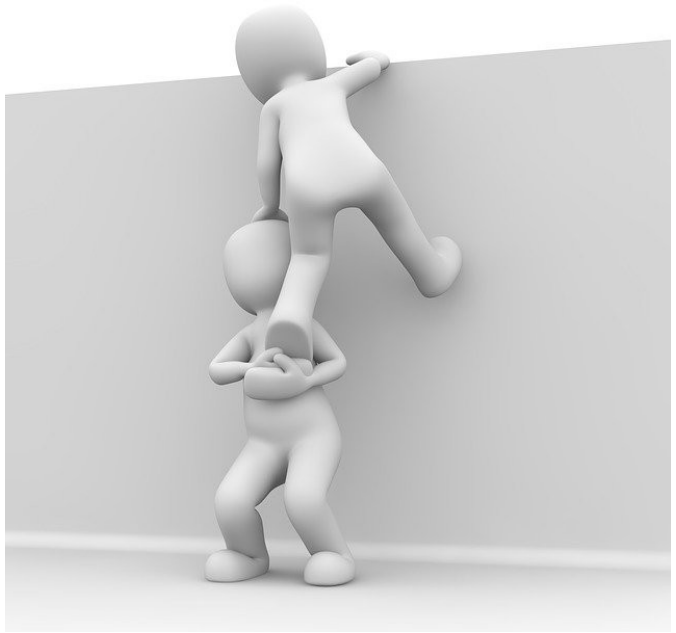
Polityka ochrony danych

Przepisy art. 32 RODO wymagają wdrożenia zasad ochrony danych osobowych, które odpowiadają ryzykom i zagrożeniom dla ochrony danych.

Osoby upoważnione muszą zostać zobligowane do ich przestrzegania.



Realizowanie praw osób



Każda osoba może złożyć żądanie:

- potwierdzenia, czy administrator przetwarza dane oraz uzyskania ich kopii,

- ograniczenia, usunięcia lub sprzeciwu,

- przeniesienia danych,

- wycofania zgody,

- niepodlegania profilowaniu.

Administrator powinien mieć na tę okoliczność procedurę.

Naruszenia ochrony danych - jak postępować

Procedura na okoliczność naruszenia

Naruszenie to zdarzenie, które może nieść negatywne skutki dla osoby, której dane dotyczą.

Stwierdzenie, czy doszło do naruszenia ochrony danych wymaga oceny ryzyka naruszenia.

Zgłoszenie naruszenia ochrony danych

Administrator ma 72 godziny na zgłoszenia naruszenia do Prezesa UODO.

Podmiot przetwarzający musi zgłosić w terminie wskazanym w umowie powierzenia (nie później niż 72 godziny od stwierdzenia) do administratora.

Zgłoszenie naruszenia

Naruszenie jest czynnością techniczną, która nie skutkuje automatyczną karą lub kontrolą.

Nie wymagają zgłoszenia jedynie naruszenia, dla których jest bardzo mało prawdopodobne, aby niosły negatywne skutki dla osoby, której dane dotyczą.

Zgłoszenie naruszenia

W jaki sposób powiadomić Prezesa UODO o naruszeniu?

Organem właściwym do zgłaszania naruszeń ochrony danych osobowych jest Prezes Urzędu Ochrony Danych Osobowych (Prezes UODO).

Zgłoszenia można dokonać na 4 sposoby:

1. Elektronicznie poprzez wypełnienie **dedykowanego formularza elektronicznego** dostępnego bezpośrednio na platformie biznes.gov.pl będącego odwzorowaniem formularza dostępnego w załączniku.
2. Elektronicznie poprzez wysłanie wypełnionego formularza na elektroniczną skrzynkę podawczą ePUAP: **/UODO/SkrytkaESP**
3. Elektronicznie poprzez wysłanie wypełnionego formularza (dostępnego poniżej w załączniku) za pomocą **pisma ogólnego dostępnego na platformie biznes.gov.pl** (Jak znaleźć Urząd w formularzu pisma ogólnego?) lub **platformie epuap.gov.pl**
4. Tradycyjną pocztą wysyłając wypełniony formularz na adres Urzędu.

Dziękuję za uwagę!

Zapraszam do kontaktu mailowego: kontakt@sylwiaczub.pl

W prezentacji zostały wykorzystane darmowe grafiki

dostępne w serwisie