GDPR
RISK TRACKER

GDPR Risk Tracker jako narzędzie do zapewnienia rozliczalności pracy IOD wobec Prezesa UODO

27 pytań Prezesa UODO do ADO - zakres

- Pytania statutowe – podstawowe obowiązki formalne
- Sposób realizacji funkcji i podstawy decyzji ADO
- Wsparcie ze strony ADO
- Umożliwienie sprawowanie aktywnej rola IOD
- Zapewnienie niezależności
- Gwarancje i skuteczność wykonywania funkcji IOD / konflikt interesów
- Zadania IOD

Inspektor ochrony danych

Obligatoryjne powołanie inspektora ochrony danych (IOD), gdy:

- przetwarzania dokonuje organ lub podmiot publiczny (z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości)
- główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą na dużą skalę
- główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę danych osobowych szczególnych kategorii, a także danych o wyrokach skazujących i o przestępstwach.

Inspektor ochrony danych

Pozostali ADO

- fakultatywność powołania IOD

Grupa przedsiębiorstw

- możliwość wyznaczenia jednego inspektora ochrony danych dla grupy, pod warunkiem, że będzie można nawiązać z nim kontakt z każdej jednostki

Organy lub podmioty publiczne

- możliwość wyznaczenia jednego inspektora ochrony danych dla kilku takich organów lub podmiotów, z uwzględnieniem ich struktury organizacyjnej i wielkości

Inspektor ochrony danych

Wymogi kwalifikacyjne

- Kwalifikacje zawodowe
- Wiedza fachowa na temat prawa i praktyk w dziedzinie ochrony danych
- Umiejętność wykonywania powierzonych mu zadań

IOD może, ale nie musi być członkiem personelu ADO

ADO ma obowiązek publikacji danych IOD oraz zawiadomienia o nim organu nadzorczego

Gwarancje

Terminowe włączanie IOD we wszystkie sprawy w zakresu ODO

Wspieranie w wykonaniu zadań przez ADO

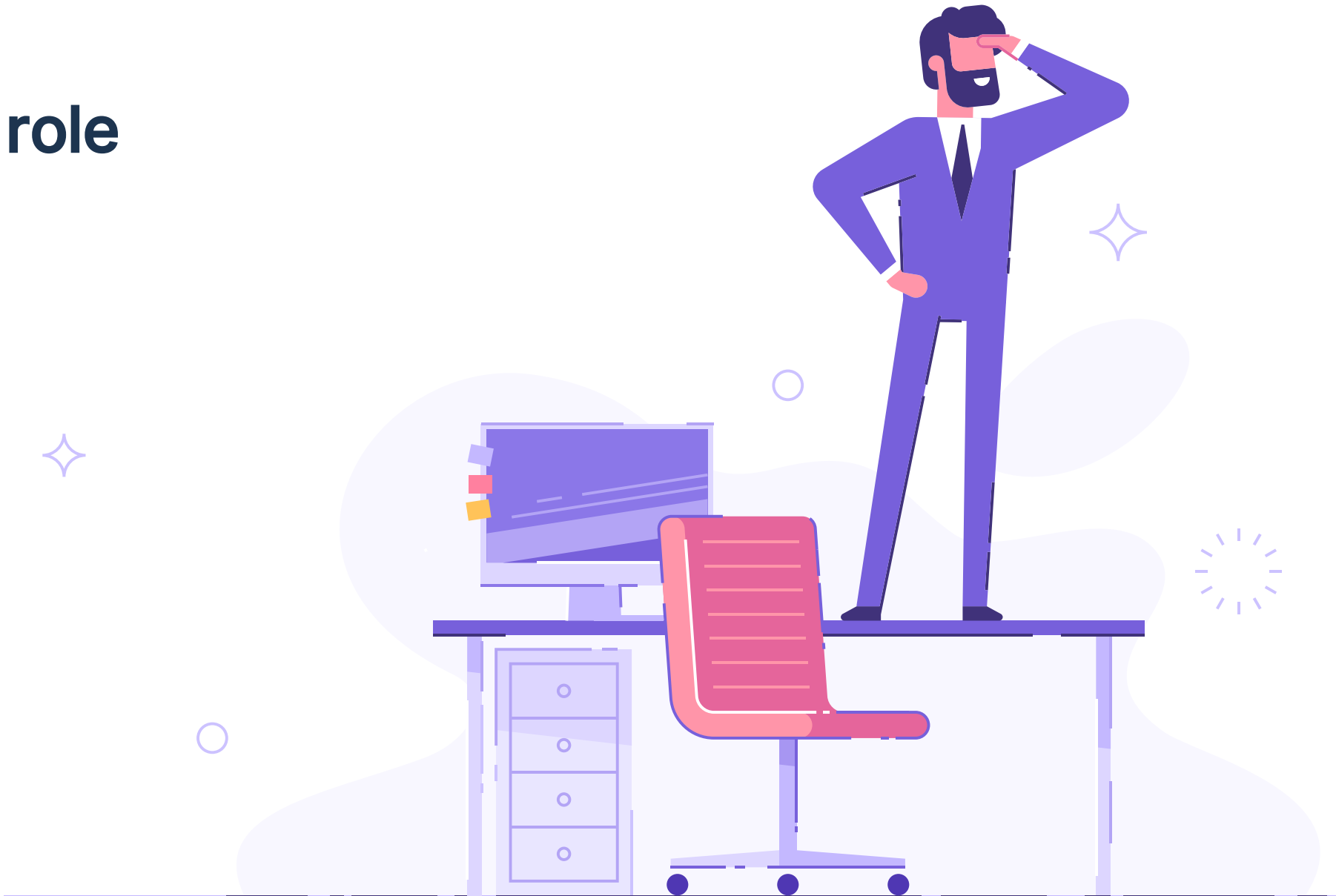
- W tym zapewnienie zasobów niezbędnych do wykonania zadań

Zakaz przekazywania poleceń dotyczących wykonywania zadań

Podleganie bezpośrednio najwyższemu kierownictwu

Zadania IOD - role

- Konsultacyjna
- Doradcza
- Kontrolna
- Uświadamiająca



Zadania inspektora ochrony danych – art. 39

- informowanie ADO lub podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO i doradzanie im w tej sprawie;
- monitorowanie przestrzegania RODO oraz strategii ADO lub podmiotu przetwarzającego w dziedzinie ODO;
- udzielanie porad na żądanie co do oceny skutków pod kątem ochrony danych oraz monitorowanie jej wykonania ;
- współpraca z organem nadzorczym;
- pełnienie funkcji punktu kontaktowego wobec organu nadzorczego;
- Pełnienie funkcji punktu kontaktowego dla podmiotów danych

Cechy regulacji wpływające na IOD

- Technologiczna neutralność i podejście oparte na ryzyku
- Podejście holistyczne
- Ogólnikowość
- Adekwatność i konieczność jej zapewnienia
- Uwzględnienie wpływu przetwarzania na prawa i wolności osoby, której dane dotyczą
- Domniemanie winy?

Etapy analizy zgodności


Opis planowanych operacji przetwarzania
Ocena konieczności i proporcjonalności
Środki planowane w celu wykazania zgodności
Ocena ryzyka naruszenia praw i wolności
Środki planowane w celu wyeliminowania ryzyka
Dokumentacja
Monitorowanie i przegląd

Informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie

Niewątpliwie prawidłowe wykonywanie powyższego zadania przez IOD bezpośrednio przekłada się na podejmowanie przez administratorów i podmioty przetwarzające świadomych i trafnych decyzji.

Aby kompetentnie edukować i doradzać innym IOD musi być do tego dobrze przygotowany merytorycznie, musi sam bardzo dobrze znać obowiązki administratorów i podmiotów przetwarzających oraz powiązane z nimi uprawnienia podmiotów danych. Dbanie o edukację osób podejmujących działania i decyzje w zakresie ochrony danych osobowych jest działaniem ciągłym i powtarzalnym, wymagającym umiejętności interpersonalnych i dydaktycznych

Monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty

Aktywność inspektora ochrony danych w tym zakresie nie powinna mieć charakteru jednorazowego, a charakter ciągły i długofalowy. Zgodnie z Wytycznymi Grupy Roboczej art. 29 dotyczącymi inspektorów ochrony danych monitorowanie to:

- zbieranie informacji w celu identyfikacji procesów przetwarzania;
- analizowanie i sprawdzanie zgodności przetwarzania;
- informowanie, doradzanie i rekomendowanie określonych działań.

Wykonując ten obowiązek inspektor ochrony danych powinien dostosować sposób i rodzaj przekazywanych informacji do grupy docelowej, tak aby zadanie to było realizowane w sposób efektywny i skuteczny.

GDPR
RISK TRACKER

Udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35

Zgodnie z art. 35 ust. 2 RODO administrator dokonując oceny skutków konsultuje się z IOD, jeżeli został wyznaczony, w celu wydania przez niego zaleceń.

Zgodnie z Wytyczny Grupy Roboczej Art. 29, administrator dokonując DPIA powinien konsultować się z IOD w następujących kwestiach:

- czy należy przeprowadzić ocenę skutków dla ochrony danych;
- metodologii przeprowadzenia oceny skutków dla ochrony danych;
- czy należy przeprowadzić wewnętrzną ocenę czy też zlecić ją podmiotowi zewnętrznemu;
- zabezpieczeń (w tym środków technicznych i organizacyjnych) stosowanych do łagodzenia wszelkich zagrożeń praw i interesów osób, których dane dotyczą;
- prawidłowości przeprowadzonej oceny skutków dla ochrony danych i zgodności jej wyników z RODO (czy należy kontynuować przetwarzanie, czy też nie oraz jakie zabezpieczenia należy zastosować).

Jeśli administrator nie zgadza się z zaleceniami IOD w wyżej wymienionych przypadkach, dokumentacja oceny skutków dla ochrony danych powinna zawierać pisemne uzasadnienie nieuwzględnienia zaleceń IOD.

PODMIOT UKARANY	Szkoła Główna Gospodarstwa Wiejskiego w Warszawie
NARUSZENIE	Brak wdrożenia odpowiednich środków organizacyjnych i technicznych, które pozwalają na zapewnienie bezpieczeństwa przetwarzania danych osobowych, brak należytego przeprowadzenia analizy ryzyka art. 5 ust. 1 lit. e, art. 5 ust. 1 lit. f, art. 5 ust. 2, art. 25 ust. 1, art. 32 ust. 1 lit. b, art. 32 ust. 1 lit. d, art. 32 ust. 2, art. 38 ust. 1, brak należytego wypełniania obowiązków przez IOD - art. 39 ust. 1 lit. b i art. 39 ust. 2, naruszenie zasady rozliczalności i aktualności dokumentacji – art. 5 ust. 2 oraz art. 30 ust. 1 lit. d
ZASTRZEŻENIA ORGANU	Naruszenie art. 38 ust. 1 poprzez **brak włączania IOD** w sprawy ochrony danych osobowych w zakresie przyjmowanych rozwiązań technicznych Art. 39 ust. 2 wymaga by, inspektor ochrony danych wypełniał swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania. Przepis ten wymaga od inspektora **ustalania priorytetów w swojej pracy,** które powinny polegać na **indywidualnym i samodzielnym określaniu środków oraz metod działania i dostosowywania ich do specyfiki konkretnego administratora**. Problemem był **też brak kontynuacji zadań poprzednich IOD w zakresie analizy ryzyka**. **Administrator ponosi odpowiedzialność za działania inspektora ochrony danych**, gdyż to na nim ciąży obowiązek jego wyznaczenia 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. Odpowiedzialność ADO **za niewłaściwy nadzór nad przestrzeganiem bezpieczeństwa danych.**
WYSOKOŚĆ KARY	11.200 EUR (50.000 PLN)

Na czym polega wykonywanie zadań przez IOD z należytym uwzględnieniem ryzyka?

Przepis dotyczący zadań inspektora ochrony danych (art. 39 ust. 2 RODO) wyraźnie wskazuje na konieczność dostosowania trybu i metod pracy do specyfiki przetwarzania danych oraz związanego z tym przetwarzaniem ryzyka. Inspektor ma wypełniać swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

Wypełnianie zadań „z należytym uwzględnieniem ryzyka" wymaga od IOD ustalania priorytetów w swojej pracy i koncentrowania się na aspektach pociągających za sobą większe ryzyko.

Zdaniem Grupy Roboczej Art. 29, takie podejście powinno ułatwić IOD doradzenie administratorowi, m.in.:

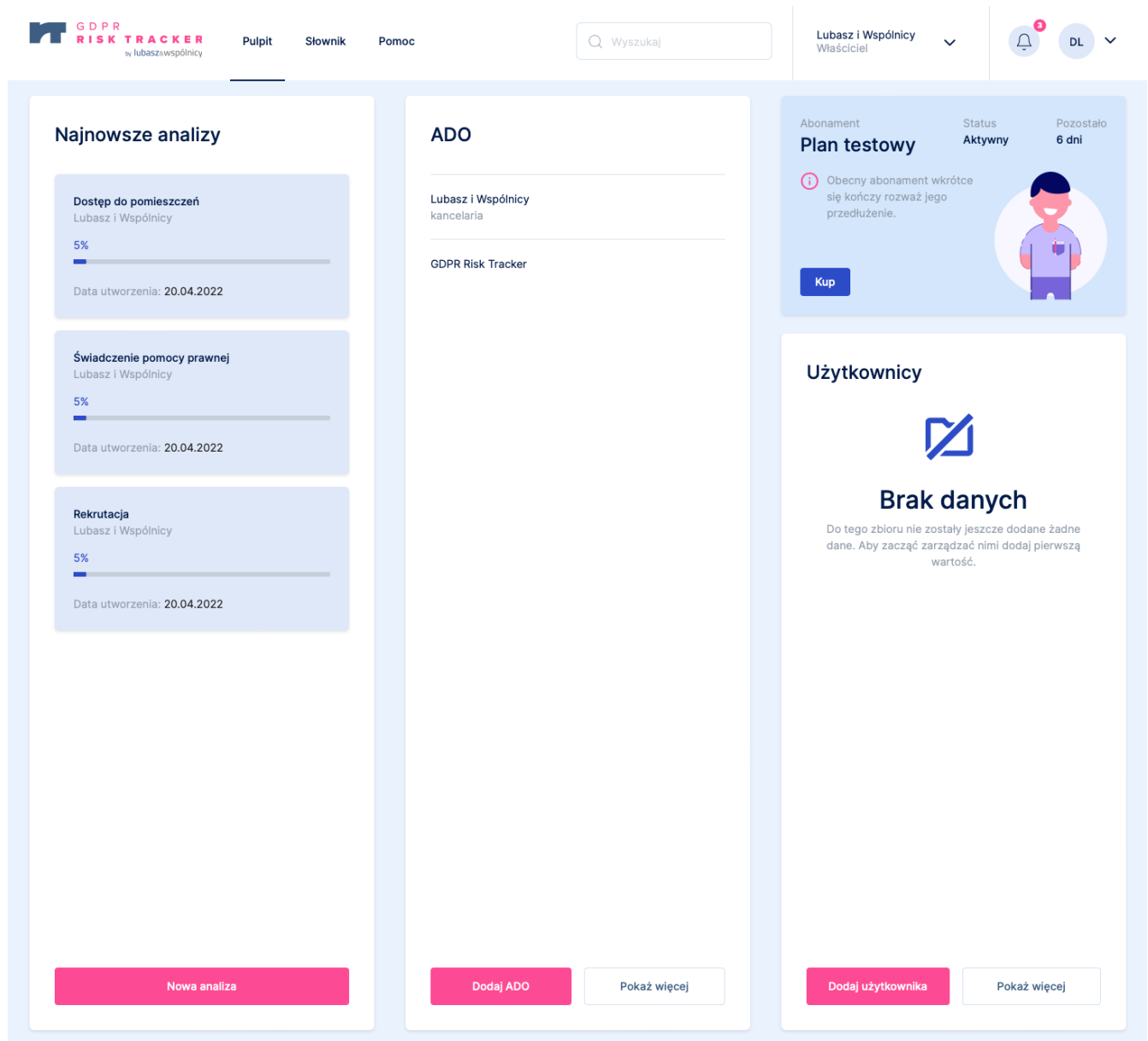
- które obszary powinny zostać poddane wewnętrznemu albo zewnętrznemu audytowi,
- jakie szkolenia dla pracowników lub kierowników odpowiedzialnych za przetwarzanie danych należy przeprowadzić,
- na które operacje przetwarzania należy przeznaczyć więcej czasu i zasobów.

Kto powinien opracować wewnętrzną politykę ochrony danych osobowych? Administrator czy IOD?

- Zgodnie z art. 24 RODO administrator, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane. Treść powyższego artykułu wskazuje jednoznacznie, że wdrożenie odpowiednich środków technicznych i organizacyjnych (które mogą obejmować również wdrożenie przez administratora odpowiednich polityk ochrony danych) należy do obowiązków administratora (osób przez niego wyznaczonych).
- Rolą IOD jest natomiast dokonywanie oceny przyjętych przez administratora środków (w tym wewnętrznych polityk) pod kątem ich zgodności z przepisami prawa i skuteczności. Do zadań inspektora ochrony danych należy też monitorowanie przestrzegania przyjętej w dziedzinie ochrony danych osobowych polityki przez osoby upoważnione do przetwarzania danych (art. 39 ust 1 lit. b RODO).
- W trakcie tworzenia polityk dotyczących ochrony danych wskazane jest, aby administrator zasięgał opinii i wskazówek u swojego inspektora ochrony danych (IOD), który posiada fachową wiedzę na temat prawa i praktyk w dziedzinie ochrony danych, zgodnie z treścią art. 39 ust 1 lit. a RODO

Czy prowadzenie rejestru czynności powinno być zaliczane do zadań IOD?

- Zgodnie z art. 30 ust. 1 i 2 RODO, do administratora należy obowiązek prowadzenia rejestru czynności przetwarzania danych osobowych, za które odpowiada, a do podmiotu przetwarzającego - prowadzenie rejestru kategorii czynności przetwarzania dokonywanych w imieniu administratora. To te podmioty są odpowiedzialne za efektywne wykonanie tego obowiązku i pozostawanie w gotowości do wykazania tego na żądanie organów ochrony danych. Tym samym są one zobowiązane określić, kto konkretnie w danej organizacji ma wykonywać określone czynności składające się na spełnienie wymogów określonych w art. 30 RODO, uwzględniając konkretne okoliczności, m.in. takie jak wielkość i struktura organizacyjna danego podmiotu oraz skala przetwarzania danych. Zgodnie z jedną z najważniejszych zasad, na których oparta jest nowa regulacja – zasadą rozliczalności, odpowiedni dobór rozwiązań zapewniających zgodność z przepisami o ochronie danych osobowych należy do administratorów danych i podmiotów przetwarzających.
- Ze względu na swoją zawartość i cele, rejestry czynności oraz rejestry kategorii czynności mogą być również przydatnym instrumentem monitorowania zgodności dla inspektorów ochrony danych. Wprawdzie z art. 30 rozporządzenia ogólnego bezsprzecznie wynika, że obowiązek prowadzenia rejestrów należy do administratorów i podmiotów przetwarzających, nie zaś do inspektora ochrony danych, niemniej trudno sobie wyobrazić, że inspektor ochrony danych - jako osoba dysponująca odpowiednią wiedzą i umiejętnościami w dziedzinie ochrony danych osobowych - nie będzie angażowała się w tworzenie i prowadzenie rejestrów, a następnie wykorzystywała ich w swojej pracy.
- Inspektor ochrony danych jako fachowiec może wspomagać administratora w tworzeniu i prowadzeniu rejestrów na przykład poprzez doradzanie mu w kwestiach związanych z wykonaniem tego obowiązku.


GDPR
RISK TRACKER
by lubaszwspólnicy
Pulpit
Słownik
Pomoc
Wyszukaj
Lubasz i Wspólnicy
Właściciel
3
DL
Najnowsze analizy
Dostęp do pomieszczeń
Lubasz i Wspólnicy
5%
Data utworzenia: 20.04.2022
Świadczenie pomocy prawnej
Lubasz i Wspólnicy
5%
Data utworzenia: 20.04.2022
Rekrutacja
Lubasz i Wspólnicy
5%
Data utworzenia: 20.04.2022
Nowa analiza
ADO
Lubasz i Wspólnicy
kancelaria
GDPR Risk Tracker
Dodaj ADO
Pokaż więcej
Abonament
Plan testowy
Status
Aktywny
Pozostało
6 dni
Obecny abonament wkrótce się kończy rozważ jego przedłużenie.
Kup
Użytkownicy
Brak danych
Do tego zbioru nie zostały jeszcze dodane żadne dane. Aby zacząć zarządzać nimi dodaj pierwszą wartość.
Dodaj użytkownika
Pokaż więcej

Dziękujemy i zapraszamy!

„Przeszłość, teraźniejszość i przyszłość RODO”

konferencja online

25 maja 2022

- Najlepsi eksperci z dziedziny ochrony danych osobowych przybliżą funkcjonowanie RODO w praktyce z trzech różnych perspektyw.

- **Premiera GDPR Risk Tracker 2.0**