OCHRONA DANYCH OSOBOWYCH

W ramach realizacji Lokalnych Strategii Rozwoju

szkolenie dedykowane przedstawicielom: Rybackich Lokalnych Grup Działania i Instytucji Pośredniczących

iSecure

Agenda szkolenia

- Zagadnienia wstępne: podstawowe informacje i definicje
- Kategorie danych osobowych przetwarzanych przez Rybackie Lokalne Grupy Działania i Instytucje Pośredniczące (Samorządy Województw)
- Legalność przetwarzania danych osobowych
- Adekwatność danych osobowych
- Obowiązki informacyjne
- Powierzenie przetwarzania danych osobowych
- Zabezpieczenie danych osobowych
- Dokumentacja przetwarzania danych
- Odpowiedzialność

Zagadnienia wstępne – obowiązujące akty prawne

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych i akty wykonawcze

Stosowane od 25 maja 2018 r. – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO)

Przepisy szczególne, w tym: ustawa z dnia 10 lipca 2015 r. **o wspieraniu zrównoważonego rozwoju sektora rybackiego z udziałem Europejskiego Funduszu Morskiego i Rybackiego,** ustawa z dnia 20 lutego 2015 r**. o rozwoju lokalnym z udziałem lokalnej społeczności**

Zagadnienia wstępne – kluczowe pojęcia (definicje)

- Dane osobowe [UODO] - **wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej**. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne
- Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań

Zagadnienia wstępne – kluczowe pojęcia (definicje)

- Dane osobowe [Rozporządzenie UE] - oznaczają **informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej**; możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej

Zagadnienia wstępne – kluczowe pojęcia (definicje)

Zagadnienia wstępne – kluczowe pojęcia (definicje)

Dane „**wrażliwe**” – art. 27 ust. 1 UODO: ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym

Dane „**zwykłe**” – nienależące do katalogu wyżej wskazanego

Dane „**służbowe**” – imię, nazwisko, stanowisko/funkcja, nazwa zakładu pracy, służbowy nr telefonu, służbowy adres e-mail (Wyrok Sądu Najwyższego z dnia 19 listopada 2003 r. - sygn. I PK 590/02)

Zagadnienia wstępne – kluczowe pojęcia (definicje)

Stosowanie UODO i RODO do danych osobowych przedsiębiorców:

- Do jawnych danych i informacji udostępnianych przez CEIDG nie stosuje się przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2016 r. poz. 922 ze zm.), z wyjątkiem przepisów art. 14-19a *[uprawnienia kontrolne GIODO]* i art. 21-22a *[możliwość odwołania się od decyzji GIODO]* oraz rozdziału 5 *[zabezpieczenia danych]* tej ustawy – art. 39b ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej (nowelizacja z maja 2016 r.)
- Dane osób fizycznych reprezentujących przedsiębiorców i dane kontaktowe – od wejścia w życie UODO były to dane osobowe

Zagadnienia wstępne – kluczowe pojęcia (definicje)

- **Przetwarzanie danych** - jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych
- Powyższe wyliczenie ma charakter przykładowy
- Przykłady przetwarzania danych: zbieranie danych we wnioskach o dofinansowanie, przekazywanie danych pomiędzy RLGD i SW oraz ARiMR, opracowywanie danych z wniosków o płatność, archiwizacja dokumentacji

Zagadnienia wstępne – kluczowe pojęcia (definicje)

Administrator Bezpieczeństwa Informacji [UODO] - osoba fizyczna, do której zadań należy:

- zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:

- sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych
- nadzorowanie opracowania i aktualizowania dokumentacji (polityka, instrukcja) oraz przestrzegania zasad w niej określonych
- zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych

- prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych (uwaga na wyjątki)

Zagadnienia wstępne – kluczowe pojęcia (definicje)

Administrator Bezpieczeństwa Informacji [UODO] →
Inspektor Ochrony Danych [RODO]

Dziś [UODO] – powołanie ABI możliwością

Po 25 maja 2018 r. [RODO] – powołanie IOD obowiązkiem organów lub podmiotów publicznych

Zagadnienia wstępne – kluczowe pojęcia (definicje)

- **Administrator danych (ADO)** – organ, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych osobowych

- ADO, to np.:

a) RLGD (w szczególności w zakresie naboru wniosków o dofinansowanie),

b) SW (jako Instytucje Pośredniczące realizujące przypisane im zadania w zakresie priorytetu IV)

Kategorie przetwarzanych danych

Lokalne Grupy Rybackie, jako ADO przetwarzają:

- dane wnioskujących o dofinansowanie, w celu przyjęcia wniosków
- dane osób reprezentujących ww. wnioskujących

Samorządy Województw, jako ADO przetwarzają:

- dane stron umowy o dofinansowanie lub ich reprezentantów, w celu realizacji umowy
- dane wnioskujących o dofinansowanie lub ich reprezentantów, w celu przyjęcia wniosków i udzielenia dofinansowania

ARiMR, jako ADO w priorytecie 4? (pomoc techniczna PO RYBY 2014-2020)

Zakres obowiązków ADO

- Podstawy prawne – obowiązek legalności
- Zasada adekwatności danych
- Obowiązek informacyjny
- Obowiązki związane z powierzeniem przetwarzania danych
- Obowiązki zabezpieczenia danych
- Obowiązek prowadzenia dokumentacji opisującej sposób przetwarzania danych osobowych

Obowiązek legalności

- Przetwarzanie danych „zwykłych” jest dopuszczalne tylko wtedy, gdy:

- osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych,

- jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa,

- jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą,

- jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego,

- jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą

Obowiązek legalności

Przykłady wyjątków umożliwiających przetwarzanie danych wrażliwych:

- osoba, której dane dotyczą, wyrazi na to zgodę na piśmie, chyba że chodzi o usunięcie dotyczących jej danych
- przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony,
- przetwarzanie jest niezbędne do wykonania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych jest określony w ustawie
- przetwarzanie danych jest prowadzone przez stronę w celu realizacji praw i obowiązków wynikających z orzeczenia wydanego w postępowaniu sądowym lub administracyjnym

Obowiązek legalności

ZGODA nie zawsze jest wymagana, lecz gdy po nią sięgamy…

- musi być wyraźna i konkretna
- musi być wyrażona w określonym celu
- musi być wyrażona dobrowolnie

Przykłady:

„Zgadzam się na przetwarzanie moich danych osobowych podanych w formularzu przez LGD w … w celu …”

„Wyrażam zgodę na przetwarzanie moich danych osobowych zgodnie z ustawą z dn. 29 sierpnia 1997 r. o ochronie danych osobowych”

Zasada adekwatności [UODO]

Minimalizacja danych [RODO]

Zbieranie danych w minimalnym, niezbędnym zakresie.

W przypadku pozyskania danych innych, niż niezbędne do osiągnięcia zakładanego celu, wyrażenie zgody tego nie zalegalizuje

W praktyce dochodzi do naruszeń w przypadku kopiowania dokumentów tożsamości czy całych treści umów

Obowiązek informacyjny

Obowiązek informacyjny w przypadku zbierania danych osobowych bezpośrednio od osoby, której one dotyczą – wymagane informacje [**UODO**]:

- adres siedziby ADO i jego pełna nazwa
- cel zbierania danych, a w szczególności informacja o znanych ADO w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych
- prawo dostępu do treści swoich danych oraz ich poprawiania
- dobrowolność albo obowiązek podania danych, a jeżeli taki obowiązek istnieje, wskazanie jego podstawy prawnej

Obowiązek informacyjny

RODO wymagać będzie podania dodatkowo m. in.:

- Okresu przechowywania danych lub kryterium jego ustalenia
- Wskazania podstawy prawnej przetwarzania danych
- Podania informacji o możliwości wniesienia skargi do GIODO
- Podania danych kontaktowych Inspektora Ochrony Danych

Przykład? Wniosek o dofinansowanie

Przyjmuję do wiadomości, iż zebrane dane osobowe będą przechowywane i przetwarzane przez LGD, która dokonuje wyboru operacji do finansowania, Samorząd Województwa właściwy ze względu na siedzibę ww. LGD oraz Agencję Restrukturyzacji i Modernizacji Rolnictwa z siedzibą: 00-175 Warszawa Al. Jana Pawła II 70, zgodnie z przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922) w celu przyznania pomocy finansowej i płatności w ramach działania "Realizacja lokalnych strategii rozwoju kierowanych przez społeczność" objętego Priorytetem 4. Zwiększenie zatrudnienia i spójnosci terytorialnej, zawartym w Programie Operacyjnym Rybactwo i Morze oraz przysługuje mi prawo wglądu do moich danych osobowych jak również prawo do ich poprawiania. Przyjmuję również do wiadomości, że moje dane osobowe mogą być przetwarzane przez organy audytowe i dochodzeniowe Unii Europejskie i państw członkowskich dla zabezpieczenia interesów finansowych Unii.

Powierzenie przetwarzania danych

UODO i RODO

- Procesor (podmiot przetwarzający) – podmiot zewnętrzny w stosunku do ADO, któremu ADO powierza dane do przetwarzania. Procesor wykonuje czynności na danych osobowych ADO tylko i wyłącznie w jego imieniu i na jego rzecz
- Powierzenie następuje na podstawie **umowy** pomiędzy ADO i procesorem
- Przykład procesora: firma informatyczna serwisująca oprogramowanie (jeżeli serwisowanie wiąże się z dostępem do danych osobowych), firma organizująca szkolenie (zbiera dane, rezerwuje miejsca w hotelu etc.), wsparcie techniczne (ARiMR w PO RYBY 2014-2020?)

Powierzenie przetwarzania danych

UODO

Nie wymaga zawarcia umowy między administratorem a podmiotem przetwarzającym dane w imieniu i na rzecz ADO, powierzenie przetwarzania danych, w tym przekazywanie danych, jeżeli ma miejsce między podmiotami będącymi organami państwowymi, organami samorządu terytorialnego oraz państwowymi i komunalnymi jednostkami organizacyjnymi [art. 31 ust. 2a UODO, nowelizacja z 1.04.2016 r.]

Powierzenie przetwarzania danych

UODO

Umowa powierzenia przetwarzania danych – wymogi formalne (obligatoryjne):

- umowa sporządzona na piśmie
- określenie celu powierzenia (np. hosting bazy danych)
- określenie zakresu powierzenia (np. imię, nazwisko, adres)
- podjęcie środków zabezpieczających powierzane dane (środki organizacyjne i techniczne)

Powierzenie przetwarzania danych

UODO

Umowa powierzenia przetwarzania danych – zapisy opcjonalne (fakultatywne):

- określenie środków przetwarzania danych
- forma przekazania danych osobowych (np. na jakim nośniku)
- informacje na temat zwrotu powierzonych danych
- kwestie płatności
- możliwość dalszego powierzenia danych osobowych (subprocesor)
- odpowiedzialność procesora np. kary umowne
- uprawnienia kontrolne
- możliwość przeprowadzenia audytu

Powierzenie przetwarzania danych

RODO

Znacznie rozbudowuje wymagania dla umowy powierzenia. Oprócz celu i zakresu przetwarzania konieczne będzie m. in.:

- zapewnienie kontroli
- potwierdzenie wymogów zabezpieczenia danych
- uczulenie procesora dot. pomocy w wywiązywaniu się z obowiązków nakładanych przez RODO
- warunki dotyczące dalszego powierzenia
- ustalenie kwestii zwrotu lub usunięcia danych

Zabezpieczenie danych - organizacyjne

- możliwość powołania ABI, innych osób funkcyjnych
- nadawanie upoważnień do przetwarzania danych, prowadzenie ewidencji osób upoważnionych
- szkolenia i instruktaże dla pracowników
- szyfrowanie plików zawierających dane osobowe przesyłanych pocztą elektroniczną z wykorzystaniem sieci publicznej (8 znaków, małe, wielkie litery, cyfry oraz znaki specjalne)
- wykorzystywanie zasobów komputerowych oraz sieciowych wyłącznie w celach służbowych
- dbanie o bezpieczeństwo stanowiska pracy, w tym blokowanie komputera lub włączanie wygaszacza ekranu chronionego hasłem lub wylogowanie z systemu operacyjnego podczas opuszczania stanowiska pracy

Zabezpieczenie danych - organizacyjne

- ustawienie ekranu monitora tak, aby uniemożliwić wgląd w przetwarzane dane osobowe osób nieuprawnionych
- nie wysyła się wiadomości na prywatnego e-maila ani też nie nagrywa się na prywatne nośniki danych osobowych przetwarzanych w ramach obowiązków służbowych
- zasada „czystego biurka”. Na biurku znajdują się dokumenty potrzebne do wykonania konkretnej pracy, niepozostawianie wydruków w miejscu ogólnodostępnym
- niepozostawianie bez osoby upoważnionej osób nieupoważnionych w pomieszczeniach, w których przetwarzane są dane osobowe
- zachowanie w tajemnicy danych osobowych i sposobów ich zabezpieczenia

Zabezpieczenie danych - fizyczne

- pomieszczenia zabezpieczone zamykanymi drzwiami, zabezpieczenia okien (kraty, rolety)
- zamykane sejfy, szafy, szuflady. Dostęp do kluczy mają osoby uprawnione do przetwarzania danych
- system alarmowy przeciwwłamaniowy
- system monitoringu oraz ochrona fizyczna
- system przeciwpożarowy, wolnostojące gaśnice
- niszczarki dokumentów
- kopie bezpieczeństwa są w innym pomieszczeniu niż serwerownia
- zabezpieczenie serwerowni (jak np. brak okien, klimatyzacja, czujki przeciwpożarowe, drzwi o wzmocnionej odporności, czytniki kart magnetycznych)

Zabezpieczenie danych - techniczne

- urządzenia typu UPS – ochrona przed skutkami awarii zasilania
- mechanizmy uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła
- systemowe mechanizmy wymuszające okresową zmianę haseł
- system rejestracji dostępu do systemu informatycznego
- środki ochrony przed szkodliwym oprogramowaniem takim jak np. robaki, wirusy, konie trojańskie, rootkity
- system Firewall do ochrony dostępu do sieci komputerowej
- wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe
- mechanizm automatycznej blokady dostępu do systemu informatycznego w przypadku dłuższej nieaktywności pracy użytkownika

Dokumentacja przetwarzania danych osobowych

Polityka bezpieczeństwa - Elementy wymagane:

- Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar w którym przetwarzane są dane osobowe
- Wykaz zbiorów danych osobowych wraz ze wskazaniem programów służących do przetwarzania tych danych
- Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi
- Sposób przepływu danych między poszczególnymi systemami
- Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przy przetwarzaniu danych

Dokumentacja przetwarzania danych osobowych

Co jeszcze może zawierać Polityka Bezpieczeństwa?

- Zasady zabezpieczenia danych osobowych
- Kompetencje i zakres odpowiedzialności osób funkcyjnych
- Zasady udostępniania danych osobowych
- Zasady powierzania przetwarzania danych

Dokumentacja przetwarzania danych osobowych

Instrukcja zarządzania systemem informatycznym - Elementy wymagane:

- Procedury nadawania uprawnień do przetwarzania danych i rejestrowania uprawnień do przetwarzania danych w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności
- Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem
- Procedury rozpoczęcia, zawieszenia i zakończenia pracy
- Procedury tworzenia kopii zapasowych zbiorów danych
- Sposób, miejsce i okres przechowywania nośników zawierających dane osobowe oraz kopii zapasowych

Dokumentacja przetwarzania danych osobowych

Instrukcja zarządzania systemem informatycznym - Elementy wymagane:

- Sposób zabezpieczenia systemu informatycznego przed działalnością szkodliwego oprogramowania
- Sposób realizacji wymogu odnotowania informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia
- Procedury wykonywania przeglądów i konserwacji systemów i nośników informacji służących do przetwarzania danych osobowych

Odpowiedzialność

- Odpowiedzialność **administracyjna** (np. usunięcie uchybień, usunięcie danych osobowych, nałożenie tzw. kary grzywny w celu przymuszenia wykonania decyzji w wysokości do 200 000 zł)
- Administracyjna kara pieniężna według RODO wzrośnie do 20 000 000 €
- Odpowiedzialność **cywilnoprawna** (dane osobowe jako dobro osobiste, roszczenia o zapłatę zadośćuczynienia pieniężnego, żądanie naprawienia szkody na zasadach ogólnych, kara umowna z tytułu niewykonywania czy nienależytego wykonywania umowy)
- RODO daje możliwość złożenia wniosku o odszkodowanie
- Odpowiedzialność **dyscyplinarna** według prawa pracy
- Odpowiedzialność **karna**

Odpowiedzialność karna

Nieuprawnione przetwarzanie danych osobowych (art. 49)

1. Kto przetwarza w zbiorze dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do których przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

2. Jeżeli czyn określony w ust. 1 dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.

Odpowiedzialność karna

Udostępnianie danych osobom nieupoważnionym (art. 51)

1. Kto administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

2. Jeżeli sprawca działa nieumyślnie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Naruszenie obowiązku zabezpieczenia danych (art. 52)

Kto administrując danymi narusza choćby nieumyślnie obowiązek zabezpieczenia ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Odpowiedzialność karna

Niedopełnienie obowiązku informacyjnego (art. 54)

Kto administrując zbiorem danych nie dopełnia obowiązku poinformowania osoby, której dane dotyczą, o jej prawach lub przekazania tej osobie informacji umożliwiających korzystanie z praw przyznanych jej w niniejszej ustawie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Utrudnianie kontroli (art. 54a)

Kto inspektorowi udaremnia lub utrudnia wykonanie czynności kontrolnej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

Zapraszam do zadawania pytań

Dziękuję za uwagę
Katarzyna Ułasiuk

iSecure

iSecure Sp. z o.o.
ul. Narbutta 22 lok. 23
02-541 Warszawa

tel. +48 22 126 58 54
fax. +48 22 378 26 34
kontakt@isecure.pl