OCHRONA DANYCH OSOBOWYCH.

Prezentację opracował: Mariusz Słowikowski - Inspektor Ochrony Danych.

ARKADIA SP. Z O.O.
ul. Bydgoska 17, 89-520 Gostycyn
NIP:5611598816 , REGON:341243187, BDO: 000153915
Tel. +48 52 3341339
+48 690600284
E-mail: sekretariat@arkadia-choco.pl
www.arkadia-choco.pl

Podstawa prawna.

Podstawowymi aktami prawnymi odnoszącymi się do zagadnienia ochrony danych są:

- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych,
- 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 (ogólne rozporządzenie o ochronie danych, zwane potocznie ROZPORZĄDZENIEM RODO).

Polityka ochrony danych osobowych.

W ARKADIA Sp. z o.o. z siedzibą w Gostycynie przy ul. Bydgoskiej 17, woj. kujawsko-pomorskie, została wprowadzona „Polityka ochrony danych osobowych”

Polityka ochrony danych osobowych określa zasady przetwarzania oraz zabezpieczenia danych osobowych w ARADIA SP.Z O.O. w celu zapewnienia zgodności przetwarzania z wymaganiami RODO, przepisami obowiązujących przepisów, norm prawnych w zakresie przetwarzania danych osobowych.

Informacje o ochronie danych osobowych.

Producent wyrobów cukierniczych Arkadia sp. z o.o. zamieściło na stronie internetowej klauzulę informacyjną dotyczącą przetwarzania danych osobowych.

Administrator wyznaczył Inspektora Danych Osobowych w osobie Pana Mariusza Słowikowskiego, z którym można się kontaktować za pośrednictwem poczty elektronicznej iod@arkadia-choco.pl

Cennym źródłem informacji i interpretacji przepisów o ochronie danych osobowych jest strona internetowa Urzędu Ochrony Danych Osobowych https://uodo.gov.pl/ z której pracownicy czerpią zweryfikowane treści odnoszące się do prezentowanego zagadnienia.

Dane osobowe – definicja.

Przez dane osobowe należy rozumieć wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Oznacza to, że dana informacja jest daną osobową, jeśli na jej podstawie można, bezpośrednio lub pośrednio, ustalić tożsamość konkretnej osoby.

Są to zatem wszelkie informacje o osobie, której tożsamość jest oczywista, a jej identyfikacja nie wymaga wielkiego nakładu czasu.*

Dane osobowe dzielimy na:

- zwykłe,
- szczególnej kategorii.

**Definicja prawna została zawarta w art. 4 tzw. Rozporządzenia RODO.*

Podział danych osobowych.

Dane osobowe zwykłe (Art. 6 RODO):	Dane osobowe szczególnej kategorii (Art. 9 RODO):
- imię i nazwisko, **- Zawód, wykształcenie, płeć,** **- adres zamieszkania,** **- nr PESEL, NIP, nr telefonu,** **- adres mailowy np. jan.nowak@zakład.com** **- nr dowodu potwierdzającego tożsamość,** **- dane o lokalizacji, współrzędne GPS,** **- adres IP, identyfikator internetowy,**	- ujawniające pochodzenie rasowe, etniczne, - poglądy polityczne, - przekonania religijne, światopogląd, - przynależność do organizacji związkowych (związki zawodowe), - dane genetyczne, - dane biometryczne*, - dane dotyczące zdrowia, seksualności, orientacji seksualnej, - orzeczenia wydane w postępowaniu sądowym, administracyjnym (Art. 10 RODO). **Dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych bądź behawioralnych osoby fizycznej oraz umożliwiają, lub potwierdzają jednoznaczną identyfikację tej osoby: takie jak wizerunek twarzy lub dane daktyloskopijne (linie papilarne).*

Danymi osobowymi nie są:

- Numer KRS.
- Mailowy adres firmowy jak np. sekretariat@arkadia-choco.pl
- Dane zanonimizowane osób w taki sposób, że osób, które dotyczą, nie da się zidentyfikować. Proces anonimizacji musi być nieodwracalny.

Wskazane w podstawie prawnej (slajd nr 2) ustawa i rozporządzenie mają zastosowanie wyłącznie do osób fizycznych. Przepisy te nie dotyczą osób prawnych. Co ważne osoba fizyczna, to osoba żyjąca. Przepisy przywołanych regulacji prawnych nie mają zastosowania do osób zmarłych.

Dane szczególnej kategorii.

Ważne!

Istnieje 10 warunków, które pozwalają nam na przetwarzanie powyższych danych:

- posiadamy zgodę osoby, której dane maja być przetwarzane (pisemną),
- przetwarzanie wynika z przepisów prawa (szczególnej innej ustawy niż Ustawy o ochronie danych osobowych),
- w celu ochrony żywotnych interesów osoby,
- w celu dochodzenia roszczeń (realizacja obowiązku wynikającego z orzeczeń sądowych, decyzji administracyjnych),
- z uwagi na ważny interes publiczny,
- w celach zdrowotnych (do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy),
- z uwagi na interes publiczny w dziedzinie zdrowia publicznego,
- z uwagi na interes publiczny w odniesieniu do celu jakim są badania naukowe, historyczne, statystyczne.

Przetwarzanie danych – co to znaczy?

Przez przetwarzanie danych należy rozumieć dokonywanie operacji w formie elektronicznej, papierowej w sposób zautomatyzowany i niezautomatyzowany poprzez :

zbieranie	**przeglądanie**
utrwalanie	wykorzystywanie
organizowanie	ujawnianie lub przesyłanie
porządkowanie	udostępnianie
przechowywanie	dopasowywanie lub łączenie
adaptowanie lub modyfikowanie	ograniczanie
pobieranie	usuwanie lub niszczenie

Zasady przetwarzania danych.

Rozporządzenie RODO zawiera katalog zamknięty warunków, w jakich przetwarzanie danych można uznać za zgodny z obowiązującym prawem. Każdy proces przetwarzania musi opierać się na co najmniej jednej podstawie prawnej wskazanej w Rozporządzeniu RODO. Są to następujące sytuacje:

- osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub w większej liczbie określonych celów,
- przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy,
- przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze,
- przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi danych osobowych,
- przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów maja interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą jest dzieckiem.

Administrator danych osobowych.

Zgodnie z definicją zawartą w RODO, administratorem danych osobowych (ADO) jest osoba fizyczna lub prawna, organ, jednostka organizacyjna, podmiot bądź też osoba decydująca samodzielnie lub wspólnie z innymi o celach i środkach przetwarzania danych osobowych (art.4 pkt.7 RODO).

Administrator danych osobowych c.d.

Praktycznie rzecz ujmując, każdy podmiot, który przetwarza dane osobowe do realizacji własnego celu, jest administratorem danych osobowych. Celem tym może być m.in. przeprowadzenie rekrutacji, nawiązanie stosunku pracy czy np. pozyskanie klienta.

W tym miejscu warto podkreślić, że dany podmiot może być zarówno administratorem danych osobowych, jak i podmiotem przetwarzającym (nazywamy go wówczas procesorem). Przykładowo:

Biuro rachunkowe „X” Sp. z o.o. wobec swoich pracowników jest administratorem danych osobowych, a wobec swoich klientów, którzy powierzają im dane osobowe, jest już podmiotem przetwarzającym.

Obowiązki administratora danych osobowych.

Prawo nakłada szereg obowiązków na administratorów danych osobowych, które można podzielić na trzy grupy:

I. Obowiązki wobec osób, których dane dotyczą.

II. Obowiązki w zakresie zapewnienia bezpieczeństwa danych.

III. Obowiązki wykonywane w ramach organu nadzorczego.

I. Obowiązki wobec osób których dane dotyczą.

- Spełnić obowiązek informacyjny osób, wobec których dane przetwarza w tym zrealizowanie prawa dostępu do danych osobowych (art. 13 i 14 RODO).
- Uwzględnienie żądanie usunięcia danych (zgodnie z obowiązującymi przepisami) – (zrealizowanie prawa do bycia zapomnianym).
- Uwzględnienia sprzeciwu wobec przetwarzania danych, dla których został wniesiony.
- Obowiązek przenoszenia danych, jeżeli osoba, której dane dotyczą, zażądała tego.
- Uwzględnienie cofnięcia zgody, która została wyrażona.
- Obowiązek niezwłocznego zawiadomienia osoby, której dane dotyczą o naruszeniu ochrony danych.

II. Obowiązki w zakresie zapewnienia bezpieczeństwa danych.

Zgodnie z Rozporządzeniem RODO, biorąc pod uwagę charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych, administrator ma obowiązek wdrażania w ramach swojej organizacji odpowiednich środków technicznych i organizacyjnych, które będą w stanie zapewnić zgodność z przepisami prawa, ale także wykazanie tego, czyli:

- przygotować właściwą dokumentację zapewniającą ochronę danych, bezpieczeństwo ich przetwarzania,

- nadać upoważnienia do przetwarzania danych oraz odebrać stosowne zobowiązania do zachowania poufności (w formie pisemnej),

- podpisać umowy powierzenia, gdy dane osobowe są przekazywane podmiotom zewnętrznym w celu realizacji zadań zleconych (np. podmiotom odpowiedzialnym za stronę internetową zakładu, dostawcom oprogramowania (…)).

- umożliwić dostęp do szkoleń dla osób, które mają dostęp do danych, uświadamiać ich w zakresie bezpieczeństwa danych.

Środki mające na celu zapewnienie bezpieczeństwa zawarte w art. 32 RODO:

- Pseudonimizację i szyfrowanie danych osobowych.
- Zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania.
- Zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.
- Regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

W celu ustalenia, czy stopień bezpieczeństwa przetwarzania danych jest poprawny, niezbędnym jest przeprowadzenie analizy ryzyka.

III. Obowiązki wykonywane w ramach organu nadzorczego.

Organem nadzorczym sprawującym nadzór nad ochroną danych osobowych zgodnie z Ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych jest Prezes Urzędu Ochrony Danych Osobowych (PUODO). Tym zastąpił on Generalnego Inspektora Ochrony Danych Osobowych (GIODO).

Administratorzy mają obowiązek zgłaszania naruszeń ochrony danych osobowych do organu nadzorczego, BEZ ZBĘDNEJ ZWŁOKI, nie później niż w terminie 72 godzin od stwierdzenia naruszenia danych. Dodatkowo w ramach swojej organizacji są zobowiązani do prowadzenia rejestru / dokumentowania wszelkich naruszeń ochrony danych.

Zgłaszania do Prezesa Urzędu Ochrony Danych Osobowych informacji o powołaniu Inspektora Ochrony Danych (w ciągu 14 dni od powołania) i opublikowanie jego danych wraz nr telefonu lub adresem mailowym do kontaktu (jeżeli dany podmiot zgodnie z przepisami ma obowiązek powołania takiej osoby).

Inne obowiązki administratora danych osobowych.

- Dokonywać oceny skutków planowanych operacji przetwarzania danych osobowych przed rozpoczęciem tego procesu.
- Prowadzić rejestr czynności przetwarzania danych osobowych.
- Prowadzić rejestr kategorii czynności przetwarzania.
- Przetwarzać dane zgodnie z zasadami z Rozporządzenia RODO, w tym m.in. minimalizować ilość zbieranych danych oraz ograniczyć ich przechowywanie.

Nie należy gromadzić zbędnych danych. Nadmiarowość jest elementem niepożądanym.

Najczęściej polega na gromadzeniu danych i ich przetwarzaniu, które nie są niezbędne do realizacji określonych celów.

Administrator systemów informatycznych (ASI).

Na gruncie przepisów dotyczących ochrony danych osobowych nie mamy obowiązku powoływania osoby na stanowisko ASI. Najczęściej obowiązki ASI spoczywają na informatykach. W Arkadia sp. z o.o. usługa z zakresu obsługi sieci komputerowej, wdrażanie i aktualizację oprogramowania, usuwanie awarii, zabezpieczanie danych, programowanie czy rozwiązywanie problemów technicznych spoczywa na podmiocie zewnętrznym z którym spółka posiada podpisaną umowę o powierzeniu danych osobowych.

Administrator systemów informatycznych (ASI).

Jednym z głównych celów administratora danych osobowych jest zapewnienie bezpieczeństwa danych osobowych. Współcześnie coraz częściej przetwarzamy dane osobowe z wykorzystaniem systemów informatycznych. Wiedzę z zakresu bezpieczeństwa systemów posiadają informatycy, kierownicy działów IT. Administrator danych ma w powyższych osobach fachowców zapewniających wsparcie w realizacji obowiązków wynikających z Rozporządzenia RODO. ASI, a w razie jego niewyznaczenia, informatyk/informatycy, maja obowiązek współpracować z Inspektorem Ochrony Danych, zapewniając gwarancję odpowiedniego zabezpieczenia systemów IT. To właśnie **ASI/Informatyk** potrafi prawidłowo zarządzać systemami informatycznymi, również tymi wykorzystywanymi do przetwarzania danych osobowych.

Administrator systemów informatycznych (ASI).

Administrator Systemów Informatycznych/PODMIOT ŚWIADCZĄCY USŁUGI Z ZAKRESU INFORMATYKI wspiera w ARKADIA SP.O.O. bezpieczeństwo danych osobowych w takich obszarach jak:

- zabezpieczenia teleinformatyczne,

- identyfikacja potencjalnych zagrożeń i podatności dla systemów informatycznych,

- wykrywanie nieautoryzowanego dostępu do systemu, użytkowaniu niezatwierdzonego oprogramowania,

- administrowanie serwerami służącymi przetwarzaniu danych (dbałość o stan techniczny i prawidłowe wykorzystywanie pomieszczeń serwerowni),

- zachowanie ciągłości funkcjonowania systemów służących przetwarzaniu danych osobowych,

- poprawnym konfigurowaniu kont użytkowników (dostęp do oprogramowania, poczty elektronicznej).

Administrator systemów informatycznych (ASI).

WAŻNE!

Na gruncie RODO administrator danych osobowych ma obowiązek zapewnienia bezpieczeństwa przetwarzanych danych za pomocą właściwych środków organizacyjnych i technicznych (art. 32 RODO).

Dobór tych środków technicznych wymaga wiedzy i doświadczenia w zarządzaniu bezpieczeństwem systemów IT, którą zapewnia ASI/PODMIOT ŚWIADCZĄCY USŁUGI Z ZAKRESU IT.

Środki te są w razie potrzeby poddawane przeglądom i uaktualniane (art. 24 RODO).

Administrator systemów informatycznych (ASI).

Niektóre organizacje, podmioty łączą funkcję IOD-a z funkcją Administratora Systemów Informatycznych. Jest to podejście niebezpieczne dla organizacji, jest ono jednocześnie niezgodne z wymaganiami RODO. Ze stanowiska Urzędu Ochrony Danych Osobowych w tym temacie jasno wynika, że UODO nie zaleca takich powiązań. IOD nie może podlegać jakimkolwiek innym osobom niż najwyższe kierownictwo (art. 38 ust. 3 RODO), co ma mu gwarantować niezależne, prawidłowe i skuteczne wykonywanie funkcji.

Administrator Systemów Informatycznych będący często, informatykiem, podlega nadzorowi i poleceniom różnych osób. Dodatkowo ASI/PODMIOT ŚWIADCZĄCY USŁUGI Z ZAKRESU IT często odpowiada za bieżące przetwarzanie danych osobowych w systemach informatycznych oraz ich bezpieczeństwo.

Sprawując funkcję IOD-a sprawowałby jednocześnie nadzór nad samym sobą co stoi w sprzeczności i jest niedopuszczalne.

Inspektor Ochrony Danych (IOD).

Inspektorem może być osoba która:

- posiada fachową wiedzę na temat prawa i praktyk w dziedzinie ochrony danych. Może to być zarówno pracownik zatrudniony przy innych obowiązkach w firmie (za wyjątkiem osób zarządczych i ASI), jak i podmiot zewnętrzny.

WAŻNE!

Osoba powołana na to stanowisko musi mieć pełne wsparcie Zarządu, Najwyższego Kierownictwa (Prezes, Dyrektor Zarządzający).

Może ona dokonywać niezapowiedzianych kontroli wewnątrz organizacji, a pracownicy nie mogą odmówić współpracy, czy zwodzić go argumentami o pilnych obowiązkach do wykonania czy brakiem czasu.

Inspektor Ochrony Danych Osobowych nie potrzebuje specjalnego upoważnienia wydanego przez Zarząd (lub przedstawiciela zarządu) do dokonania kontroli w DZIALE KADR, MARKETINGU, ZAOPATRZENIU, LOGISTYCE (…)

Zadania IOD (Art. 39 RODO).

- 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,
- 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,
- udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35,
- współpraca z organem nadzorczym,
- pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

Kadry a RODO.

Minimalizacja danych jest kluczowa. Oznacza to, że KADRY powinny zbierać tylko te dane osobowe, które są niezbędne do osiągnięcia określonego celu. W kontekście rekrutacji oznacza to, że pracodawcy powinni ograniczyć ilość zbieranych informacji do tych, które są naprawdę potrzebne:

- imię i nazwisko,

- data urodzenia,

- dane kontaktowe,

- wykształcenie,

- kwalifikacje zawodowe,

- poprzedni przebieg zatrudnienia.

Ważne jest, aby wszystkie dane pozyskiwane w procesie rekrutacji były dostępne jedynie dla osób biorących udział w procesie rekrutacji, np. pracownika działu KADR czy dyrektora/kierownika.

Kadry a RODO.

Dokumenty, których można żądać od zatrudnionego wg Kodeksu pracy.

Kategorie danych	Sposób postępowania
• imię (imiona) i nazwisko; • datę urodzenia; • dane kontaktowe wskazane przez taką osobę.	Pracodawca żąda (wymaga podania)
• wykształcenie; • kwalifikacje zawodowe; • przebieg dotychczasowego zatrudnienia	Pracodawca wymaga podania wyłącznie, gdy jest to niezbędne do wykonywania pracy określonego rodzaju lub na określonym stanowisku. Udokumentowana ocena w tym przypadku następuje w oparciu o załącznik nr 1 do procedury (formularz rekrutacyjny).
• Inne niż wskazane powyżej (np. o stanie zdrowia, karalność)	Pracodawca wymaga podania, gdy zidentyfikuje się wyraźną ku temu podstawę w przepisach prawa (stan zdrowia, karalność, etc.).

Monitoring wizyjny i poczty elektronicznej.

Pracownicy Arkadia Sp. z o.o. są poinformowani o zainstalowanych kamerach na terenie spółki. Dokument potwierdzający ich zapoznanie znajduje się w aktach osobowych. Nadto w widocznych miejscach jest informacja o obszarze objętym zapisem z informacją, że dane te są zapisywane na nośnikach na okres 21dni.

Każdy z pracowników, któremu przydzielono dostęp do poczty elektronicznej został poinformowany, że podlega ona kontroli. Dokument w wersji papierowej potwierdzający zapoznanie się z informacją o monitoringu poczty elektronicznej znajduje się w teczkach osobowych pracowników.

Zasada czystego biurka.

Zgodnie z tą zasadą na biurku powinny znajdować się jedynie dokumenty aktualnie wykorzystywane przez pracownika. Wszystkie pozostałe wydruki muszą zostać umieszczone w przeznaczonym do tego miejscu – takim, do którego nie mają dostępu osoby nieupoważnione. Po zakończeniu wykonywania obowiązków służbowych należy schować wszystkie dokumenty do szuflady lub szafy zamykanej na klucz – nawet jeśli następnego dnia rano będziemy z nich korzystać. Warto pamiętać o tym, by usunąć z biurka wszelkie notatki zawierające informacje o klientach firmy.

Nawet wychodząc z biura do toalety zadbaj o zabezpieczenie dokumentów przed osobami postronnymi.

Zasada czystego ekranu.

Ekran monitora – w miarę możliwości - powinien być ustawiony w taki sposób, by osoby nieupoważnione nie mogły zobaczyć np. treści dokumentów elektronicznych zawierających dane klienta. Pracownik, który odchodzi od komputera na dłuższy czas, powinien wylogować się z systemu, żeby podczas jego nieobecności nikt nie miał dostępu do poufnych informacji, w tym do poczty elektronicznej. Warto również ustawić automatyczny wygaszacz ekranu w taki sposób, by użytkownik musiał wprowadzić hasło dostępu, zanim na nowo rozpocznie pracę.

Odchodząc od monitora upewnij się czy osoby postronne w biurze nie mają możliwości odczytania treści wyświetlanej na monitorze.

Zasada czystego wydruku.

Jeżeli drukujemy, kopiujemy lub skanujemy dokumenty, powinniśmy jak najszybciej zabierać je z wykorzystywanego przez nas urządzenia. W innym przypadku istnieje ryzyko, że wydruk zobaczą osoby do tego nieupoważnione.

Aby dbać o bezpieczeństwo poufnych informacji, należy wyrobić w sobie nawyk pozbywania się zbędnych dokumentów. Jeżeli część wydruków przeznaczona jest do wyrzucenia, warto jak najszybciej umieszczać je w niszczarce. Dokumenty zawierające dane osobowe powinno się niszczyć w taki sposób, by nie można było ponownie odczytać znajdujących się na nich informacji.

W celu zwiększenia bezpieczeństwa danych warto zamykać pomieszczenie służbowe, kiedy nie znajduje się w nim żaden upoważniony do tego pracownik. Klucz należy przekazać do sekretariatu lub zabrać ze sobą, jeżeli przemieszczamy się na terenie zakładu bez jego opuszczania.

Zasada czystego kosza.

Pamiętaj by do kosza nie wrzucać dokumentów, notatek zawierających dane osobowe.

Dokumenty powinny być niszczone w sposób uniemożliwiający ich ponowne odczytanie np. w niszczarce, umieszczane w specjalnie przeznaczonych do tego celu pojemnikach, spalone, itp.

Pod żadnym pozorem nie wolno zawartości kosza zabierać poza organizację.

Szyfrowanie wiadomości.

Stosowanie przez administratora danych (pracodawcę) szyfrowania przesyłanych wiadomości elektronicznych, które zawierają dane osobowe pracownika jest jak najbardziej prawidłowe.

Stosowanie tego typu zabezpieczeń wynika z art. 32 ust. 1 RODO.

Rozsyłając wiadomości na zewnątrz tej samej treści pamiętaj, by użyć funkcji UDW, która powoli zachować w tajemnicy inne adresy mailowe do których przesłaliśmy wiadomość.

Warto, by dane szyfrować w taki sposób, że nadawca chcący zapoznać się z jej treścią będzie musiał użyć hasła.

Hasło powinno być udostępnione inną drogą np. za pomocą sms. Jeżeli wysyłasz maila hasło ślesz wyłącznie na telefon.

Elektroniczne nośniki zapisu.

Pendrive, przenośne dyski pamięci, tablety, laptopy, koniecznie powinny być zabezpieczone hasłem. Nadto zaleca się by np. pendrive były szyfrowane poprzez np. programy VeraCrypt.

VeraCrypt to otwarto-źródłowe narzędzie używane do szyfrowania danych. Pozwala na szyfrowanie całych dysków, partycji, przenośnych dysków USB oraz na tworzenie wirtualnych zaszyfrowanych dysków o określonej pojemności.

Program zapewnia wiarygodne zaprzeczenie, co oznacza, że możliwe jest stworzenie ukrytego wolumenu, którego istnienie jest trudne do udowodnienia.

Porty USB w komputerach powinny być poblokowane, uniemożliwiając podłączenie prywatnego sprzętu USB do kopiowania danych.

Dział IT powinien poblokować porty z jednoczesnym zainstalowaniem oprogramowania wykrywającym próby podłączenia prywatnych, niezabezpieczonych nośników do służbowego sprzętu.

Co zrobić w razie naruszenia danych osobowych.

W razie stwierdzenia naruszenia danych osobowych należy bezwzględnie zgłosić ten fakt pracodawcy, wyznaczonemu w zakładzie IOD jak i pracownikowi działu IT.

Zgłoszenia o naruszeniu ochrony danych osobowych do UODO dokonuje:

- administrator – przedsiębiorca lub jednostka publiczna przetwarzająca dane osobowe,

- pełnomocnik administratora, IDO.

Przykłady naruszenia danych osobowych:

- poufności – np. gdy twój pracownik wyśle przypadkowo bazę danych osobowych klientów do osoby postronnej lub niewłaściwego działu firmy,

- dostępności – np. gdy zaginie pendrive z bazą danych klientów,

- integralności – np. gdy pracownik umyślnie lub nieumyślnie zmieni nazwiska klientów.

Poczta elektroniczna – DO ZAPAMIĘTANIA!

- **Nie używaj prywatnych kont** poczty elektronicznej i komunikatorów do korespondencji służbowej,

- **Nie używaj prywatnych komputerów** i telefonów do spraw służbowych,

- **Nie używaj służbowych komputerów** i telefonów do spraw prywatnych (w szczególności do czytania prywatnej poczty elektronicznej), nie udostępniaj ich członkom rodziny,

- Logując się na konto zawsze sprawdź czy **domena danego portalu jest prawidłowa**. Domena to nazwa zawierająca się między https://, a pierwszym kolejnym znakiem /

- **Ignoruj wszystkie inne prośby o podanie swojego hasła**, nawet jeżeli komunikat wygląda oficjalnie, wymaga natychmiastowej reakcji i grozi deaktywacją konta.

- Wszystkie podejrzane wiadomości na skrzynce służbowej zgłaszaj administratorom w swojej organizacji, POD ŻADNYM POZOREM ICH NIE OTWIERAJ! Może to spowodować, że „wpuścisz" wirusa, który będzie penetrował sprzęt, oprogramowanie w taki sposób, że nawet nie wzbudzi to u Ciebie podejrzeń, że wirus gromadzi dane, które po pewnym czasie wykorzystane zostaną np. do zablokowania systemu.

- O wszystkie podejrzane wiadomości na prywatnej skrzynce możesz zapytać CERT Polska (https://incydent.cert.pl / cert@cert.pl)

Poczta elektroniczna – DO ZAPAMIĘTANIA!

Szczególnie podejrzane są wiadomości:

– Zawierające załączniki, a zwłaszcza archiwa i dokumenty Office z hasłem podanym w treści wiadomości.

Wiadomości zmuszające do podjęcia natychmiastowej reakcji.

-Stosuj długie hasła (powyżej 14 znaków).

Dobrą metodą na długie hasło jest wymyślenie całej frazy, składającej się z kilku słów, np. Zieloy12#owoc! Wykorzystuj znaki specjalne w haśle. Unikaj haseł, które łatwo powiązać z publicznymi informacjami na temat Twojej osoby np. zawierających nazwisko, datę urodzenia, nr PESEL, itp.

- Hasło zmieniamy wtedy, gdy mamy podejrzenie, że mogła poznać je inna osoba. Dobrą praktyką jest zmiana hasła raz na 6 miesięcy. Nigdy nie zostawiaj na kartce zapisanych haseł i pod żadnym pozorem nie pozostawiaj ich np. na kartce pod klawiaturą.

- Nie używaj tego samego hasła więcej niż raz (w szczególności do konta email, banku i innych wrażliwych kont).

- Włącz uwierzytelnianie dwuskładnikowe (tzw. 2FA) tam gdzie jest to możliwe.

Poczta elektroniczna – DO ZAPAMIĘTANIA!

- Zweryfikuj wszystkie dane kontaktowe w ustawieniach profilu poczty elektronicznej i mediów społecznościowych; dobra alternatywna metoda kontaktu ułatwi odzyskanie utraconego konta.

- Jeżeli podejrzewasz, że ktoś mógł włamać się na twoje konto, zmień hasło, sprawdź dostępną w profilu historię logowania i zakończ wszystkie aktywne sesje.

- Nie zaniedbuj aktualizacji systemu operacyjnego i programów na używanym komputerze.

- Posiadaj aktualny program antywirusowy.

- Używaj opcji automatycznego kasowania wiadomości po upływie określonego czasu – nie da się ukraść czegoś, czego już nie ma.

Ochrona pomieszczeń, polityka kluczy.

Należy zapewnić ochronę pomieszczeń w których przetwarzane są dane osobowe.

Podstawowe zasady ochrony to:

Upoważnienia do pobierania kluczy do określonych pomieszczeń.

Ochrona zewnętrzna budynków lub w ramach pracowników sprawujących dozór na portierni.

Systemy alarmowe, przeciwwłamaniowe, przeciwpożarowe.

Okresowe przeglądy techniczne pomieszczeń.

Niepozostawianie otwartych pomieszczeń bez nadzoru osób upoważnionych do przetwarzania danych osobowych.

Zabezpieczenie dokumentacji w szafach i szufladach z odpowiednimi zabezpieczeniami.

URZĄD OCHRONY DANYCH OSOBOWYCH.

Organ do spraw ochrony danych osobowych, jakim jest UODO, to stosunkowo młoda instytucja – powołano ją do życia 25 maja 2018 roku na mocy ustawy o ochronie danych osobowych. Wcześniej zadaniami w tym zakresie zajmował się Generalny Inspektor Ochrony Danych Osobowych (GIODO). Przyjęcie nowych przepisów oznaczało przekazanie jego dotychczasowych kompetencji Prezesowi UODO, który dodatkowo stał się organem nadzorującym przestrzeganie ogólnego rozporządzenia o ochronie danych osobowych (RODO).

Zadania UODO.

Treść zaczerpnięta z oficjalnej strony UODO:
https://uodo.gov.pl/pl/79/140
Dostęp z dnia 23 lipca 2025 r.

- monitorowanie i egzekwowanie stosowania przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (zwanego dalej "rozporządzeniem") przez instytucje lub organy Unii, z wyjątkiem przetwarzania danych osobowych przez Trybunał Sprawiedliwości działający jako władza sądownicza,

- upowszechnianie w społeczeństwie wiedzy o ryzyku, przepisach, zabezpieczeniach i prawach związanych z przetwarzaniem oraz rozumienie tych zjawisk,

- upowszechnianie wśród administratorów i podmiotów przetwarzających wiedzy o obowiązkach spoczywających na nich na mocy rozporządzenia,

- udzielanie osobie, której dane dotyczą, na jej żądanie informacji o wykonywaniu praw przysługujących jej na mocy rozporządzenia, a w stosownym przypadku współpracowanie w tym celu z krajowymi organami nadzorczymi,

Zadania UODO.

Treść zaczerpnięta z oficjalnej strony UODO:
https://uodo.gov.pl/pl/79/140
Dostęp z dnia 23 lipca 2025 r.

- rozpatrywanie skarg wniesionych przez osobę, której dane dotyczą lub przez podmiot, organizację lub zrzeszenie zgodnie z art. 67 rozporządzenia, w odpowiednim zakresie prowadzenie postępowania dotyczącego tych skarg i w rozsądnym terminie informowanie skarżącego o postępach i wynikach tych postępowań, w szczególności jeżeli niezbędne jest dalsze postępowanie lub koordynacja działań z innym organem nadzorczym,

- prowadzenie postępowania w sprawie rozporządzenia, w tym na podstawie informacji otrzymanych od innego organu nadzorczego lub innego organu publicznego,

- doradzanie, z własnej inicjatywy lub na wniosek, wszystkim instytucjom i organom Unii w sprawie prawnych i administracyjnych środków ochrony praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych,

- monitorowanie zmiany w stosownych dziedzinach, o ile zmiany te mają wpływ na ochronę danych osobowych, w szczególności monitorowanie rozwoju technologii informacyjno-komunikacyjnych,

- przyjmowanie standardowych klauzul umownych, o których mowa w art. 29 ust. 8 i w art. 48 ust. 2 lit. c) rozporządzenia,

- ustanawianie i prowadzenie wykazów związanych z wymogiem dokonania oceny skutków dla ochrony danych na mocy art. 39 ust. 4 rozporządzenia,

Zadania UODO.

Treść zaczerpnięta z oficjalnej strony UODO:
https://uodo.gov.pl/pl/79/140
Dostęp z dnia 23 lipca 2025 r.

- uczestniczenie w działaniach Europejskiej Rady Ochrony Danych,

- zapewnienie obsługi sekretariatu na potrzeby Europejskiej Rady Ochrony Danych zgodnie z art. 75 rozporządzenia (UE) 2016/679,

- wydawanie zaleceń, o których mowa w art. 40 ust. 2 rozporządzenia, dotyczące przetwarzania,

- zatwierdzanie klauzul umownych i przepisów, o których mowa w art. 48 ust. 3 rozporządzenia,

- prowadzenie wewnętrznych rejestrów naruszeń rozporządzenia i działań podjętych zgodnie z art. 58 ust. 2 rozporządzenia,

- wypełnianie innych zadań związanych z ochroną danych osobowych,

- uchwalanie swojego regulaminu wewnętrznego.

Sankcje i kary administracyjne.

Przepisy RODO przewidują dwie kategorie kar finansowych, które zależne są od rodzaju przewinienia. **UODO może nałożyć karę w wysokości**:

- do 10 lub 20 mln euro,
- do 2 lub 4% całkowitego rocznego obrotu firmy z poprzedniego roku.

Prezes UODO może również zdecydować, iż kara nie będzie miała charakteru finansowego.

W Polsce uprawnionym organem do nakładania kar przewidzianych w RODO jest Prezes Urzędu Ochrony Danych Osobowych. Kary nakładane są w wyniku przeprowadzonego postępowania w drodze decyzji administracyjnej.

Sankcje i kary administracyjne.

Wysokość kary zależna jest od takich czynników jak:

- charakter i waga czynu,
- czas trwania naruszenia,
- liczba poszkodowanych osób i rozmiar poniesionej przez nich szkody,
- kategorie danych osobowych, których dotyczyło naruszenie przepisów RODO,
- rodzaj działań podjętych w celu zminimalizowania szkody,
- stopień odpowiedzialności administratora danych lub podmiotu przetwarzającego dane (z uwzględnieniem wdrożonych przez nich środków technicznych i organizacyjnych),
- stopień współpracy z organem nadzorczym,
- sposób, w jaki organ nadzorczy dowiedział się o naruszeniu, a w szczególności czy i w jakim zakresie administrator lub podmiot przetwarzający zgłosił naruszenie.

Do zapamiętania.

- Każdy pracujący z danymi osobowymi powinien przestrzegać zasad zgodności z prawem przetwarzania danych osobowych.

- Zgromadzone dane osobowe nie mogą być wykorzystywane dla swoich osobistych celów.

- Pracownicy nie powinni wykorzystywać sprzętu służbowego do osobistego użytku.

- Pracownicy nie mogą dzielić się danymi osobowymi dostępnymi w ramach wykonywanych obowiązków z osobami trzecimi.

Do zapamiętania.

Przed podpisaniem umowy z podmiotami, które będą miały dostęp do danych osobowych pracowników administratora należy zadbać, by w umowie znalazła się informacja o powierzeniu danych i zasadach ich przetwarzania.

Zawieranie umów z pominięciem w/w zapisów jest niedozwolone.

Obowiązki pracowników.

- Zachowania w poufności danych osobowych przetwarzanych w Arkadia sp. z o.o. oraz informacji o sposobach ich zabezpieczenia.

- Ochrony danych osobowych przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem.

- Informowania o każdym przypadku bądź podejrzeniu naruszenia zasad lub środków ochrony danych.

- Przechowywania dokumentów lub nośników informacji zawierających dane osobowe w miejscu niedostępnym dla osób spoza grona podmiotów i osób upoważnionych do ich przetwarzania.

- Niepozostawiania informacji zawierających dane osobowe przy urządzeniach służących do wydruku, do których mogą mieć dostęp osoby nieupoważnione tj. przy kopiarkach, drukarkach czy faksach.

Obowiązki pracowników.

- Pracy w systemach informatycznych służących do przetwarzania danych jedynie na przypisanych kontach oraz zachowania poufności udostępnionych mu haseł oraz kodów dostępu.

- Odpowiedniego zabezpieczenia pomieszczenia obejmującego obszar przetwarzania jeżeli nie pozostaje w nim inna osoba upoważniona, zarówno w godzinach pracy, jak i po jej zakończeniu.

- Niepozostawiania bez nadzoru jakichkolwiek dokumentów zawierających dane osobowe.

- Niszczenia nadmiarowych dokumentów zawierających dane osobowe w sposób uniemożliwiający ich ponowne odczytanie.

COKOLWIEK USŁYSZAŁEŚ/USŁYSZAŁAŚ W ZAKŁADZIE PRACY, NIGDY NIE DZIEL SIĘ TĄ INFORMACJĄ Z RODZINĄ I ZNAJOMYMI. POZYSKUJĄC POUFNE DANE JESTEŚ ZOBOWIĄZANY DO ZACHOWANIA TAJEMNICY SŁUŻBOWEJ.

Dziękuję za uwagę.

Powyższą prezentację opracowano na podstawie:

- wewnętrznych regulacji Arkadia sp. z o.o. z siedzibą przy ul. Bydgoskiej 17, 89-520 Gostycyn („Polityka ochrony danych osobowych”, Regulamin ochrony danych osobowych”.

- Aktualnych przepisach prawnych:

https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001000/U/D20181000Lj.pdf

https://publications.europa.eu/resource/cellar/3e485e15-11bd-11e6-ba9a-01aa75ed71a1.0018.03/DOC_1

Podczas tworzenia prezentacji posiłkowano się bibliografią:

Wójcik G.P., Obowiązki przedsiębiorców wynikające z RODO, Wydanie II, Warszawa 2024.

Mariusz Słowikowski – Inspektor Ochrony Danych,

ARKADIA SP. Z O.O.

ul. Bydgoska 17, 89-520 Gostycyn

NIP:5611598816 , REGON: 341243187, BDO: 000153915

Tel. +48 52 3341339 +48 690600284

E-mail: sekretariat@arkadia-choco.pl

www.arkadia-choco.pl