POLITYKA OCHRONY DANYCH OSOBOWYCH

ENGLISH SCHOOL Magdalena Swół

SPIS TREŚCI

- **Administratorem danych osobowych jest ENGLISH SCHOOL Magdalena Swół,** zwany dalej „firmą”, „Administratorem”.

KIEDY firma JEST ADMINISTRATOREM DANYCH OSOBOWYCH?

W sytuacji gdy decyduje o celach i sposobach przetwarzania danych osobowych, czyli **decyduje o tym: jakie dane zbiera** (np. imię, nazwisko, adres zamieszkania), **w jakim celu** (np. cel – realizacja umowy), **jak je będzie przetwarzać i jak zabezpieczać.**

- **Celem Polityki jest zapewnienie właściwej ochrony przetwarzanych danych osobowych.**

CZYM SĄ DANE OSOBOWE?

Są to wszelkie informacje o osobie, które ją identyfikują wprost lub umożliwią jej zidentyfikowanie, np. imię i nazwisko, PESEL, NIP, numer telefonu, adres e-mail, adres zamieszkania/zameldowania/siedziby, dane udostępniane w ramach profilu na portalu społecznościowych, wizerunek, numer Klienta, dane o lokalizacji, identyfikator internetowy, pseudonim, inne dane określające fizyczną, fizjologiczną, psychiczną, ekonomiczną, kulturową, społeczną tożsamość danej osoby.

RODO wyróżnia dane zwykłe i dane szczególnej kategorii (tzw. dane wrażliwe).
CZYM SĄ DANE WRAŻLIWE?
Dane ujawniające pochodzenie rasowe, etniczne, poglądy polityczne, przekonania religijne/ światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby, oraz dane dot. zdrowia, seksualności, orientacji seksualnej.

- Wprowadzenie Polityki zostało poprzedzone dokonaniem ogólnej oceny ryzyka w zakresie przetwarzania danych osobowych oraz przeprowadzeniem wewnętrznego audytu oraz weryfikacją tego czy potrzebny jest Inspektor Ochrony Danych Osobowych.

I. NAJWAŻNIENIE ZASADY DOT. OCHRONY DANYCH OSOBOWYCH

PODSUMOWANIE:

- **Firma nie zbiera danych „na wszelkich wypadek" lub „bo może kiedyś się przydadzą do innego celu".** Należy dbać o to, żeby dane były zbierane **w niezbędnej ilości** i **w zakresie** a także **przez czas niezbędny do realizacji celu i gdy mamy do tego podstawę prawną.**

  Przykład: jeśli do wykonywania danej pracy, wizerunek nie jest istotną cechą, nie możemy w ogłoszeniu rekrutacyjnym wymagać od kandydatów „wysyłania CV ze zdjęciem". Ponadto, po przeprowadzeniu rekrutacji, przesłane CV powinny być co do zasady niezwłocznie usunięte, chyba że planowana jest kolejna rekrutacja a kandydaci wyrazili zgodę na udział w kolejnych rekrutacjach.

- **Firma chroni dane przy użyciu odpowiednich środków bezpieczeństwa**.
  Przykład:
  1) stosujemy odpowiednie oprogramowanie antywirusowe/firewall, itp.
  2) nie zostawiamy danych w miejscu, do którego inni mają swobodny dostęp
  3) stosujemy silne hasła lub inne zabezpieczenia do komputera/laptopa/dysku lub korzystamy z managera haseł, itp.

- **Firma stosuje się do zaleceń wskazanych w dokumencie**: „**Zasady pracy zgodnie z RODO"** (załącznik nr 1)

- **Firma informuje osoby o zasadach przetwarzania ich danych osobowych** *(np. poprzez umieszczenie odpowiednich informacji w Polityce prywatności, stopce maila, poprzez przekazywanie ww. informacji przy okazji zawierania umów).*

- **Firma odpowiada na prośby/ pytania/ wnioski osób, których dane posiada/zbiera; Wdrożono w tym zakresie „Procedurę dot**. **obsługi żądać ww. osób"** (załącznik nr 2)

- **W przypadku gdy podmiot trzeci (poza Administratorem) ma mieć dostęp do danych osobowych należy wydać mu upoważnienie lub zawrzeć umowę powierzenia,** chyba że zachodzi inna sytuacja wynikająca m.in. z przepisów prawa.

1. **ZASADY DOT. PRZETWARZANIA DANYCH**

Firma zapewnia przetwarzanie danych osobowych zgodnie z RODO, tj.

1) w oparciu o podstawę prawną i zgodnie z prawem (legalizm);
2) rzetelnie i uczciwie (rzetelność);
3) w konkretnych celach, nie „na zapas" (minimalizacja);
4) nie więcej niż potrzeba (adekwatność);
5) z dbałością o prawidłowość danych (prawidłowość)
6) nie dłużej niż potrzeba (czasowość);
7) zapewniając odpowiednie bezpieczeństwo danych i wprowadzając odpowiednie środki techniczne i organizacyjne (bezpieczeństwo), m.in. poprzez wprowadzenie *Zasad pracy zgodnych z RODO – załącznik do Polityki;* (w tym w zakresie systemów informatycznych i Polityki czystego biurka)
8) spełniając obowiązki informacyjne względem osób, których dane przetwarza,
9) umożliwiając osobom, których dane dotyczą wykonywanie swoich praw; wprowadzono *Procedurę obsługi żądań ww. osób - załącznik do Polityki;*
10) zapewniając rozliczalność, w celu wykazania zgodności wypełniania obowiązków RODO.

2. **PODSTAWA PRZETWARZANIA DANYCH**

Przetwarzanie przez firmę jest zgodne z prawem m.in. gdy:

1) osoba, której dane dotyczą **wyraziła zgodę** na przetwarzanie danych (np. do celów przyszłych rekrutacji lub zgodę na przetwarzanie danych wrażliwych, np. dot. zdrowia);
2) przetwarzanie jest **niezbędne do wykonania umowy** (np. realizacji zamówienia, realizację umowy zlecenia, umowy o pracę) lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy (np. do przygotowania oferty, do przeprowadzenia prezentacji produktu);
3) przetwarzanie jest niezbędne do **wypełnienia obowiązków prawnych** nałożonych na Administratora (m.in. do celów archiwizacyjnych, podatkowych np. przechowywanie faktury czy dokumentacji pracowniczej);
4) wynika to z **prawnie uzasadnionych interesów** realizowanych przez Administratora (np. dochodzenie i obrona przed roszczeniami, marketing bezpośredni);
5) wynika to z innej podstawy prawnej przewidzianej przepisami RODO.

3. **ŚRODKI TECHNICZNE I ORGANIZACYJNE**

Dane osobowe są chronione przy zastosowaniu zabezpieczeń niezbędnych dla zapewnienia poufności, integralności, dostępności i rozliczalności danych osobowych. **Firma przeprowadza m.in.:**

1) audyt oraz **analizę ryzyka** dla czynności przetwarzania danych/kategorii;
2) wprowadza **niezbędne procedury i regulacje** (m.in. wprowadza niniejszą Politykę, procedurę zgłaszania naruszeń, upoważnienia);
3) zarządza zmianami mającymi wpływ na prywatność. Administrator stosuje politykę *privacy by design i privacy by default - załącznik do Polityki;*
4) wykonuje inne obowiązki wynikające z przepisów obowiązującego prawa.

4. W przypadku gdy podmiot trzeci ma dostęp do danych powinno zostać wydane *upoważnienie do przetwarzania danych* (załącznik do Polityki) lub powinna zostać zawarta *umowa powierzenia* (więcej w pkt III Polityki ochrony danych)
5. Administrator umożliwia osobom, których dane dotyczą zapoznanie się z informacjami dot. przetwarzania ich danych osobowych. Procedura dot. realizacji obowiązków informacyjnych określona została w dokumencie *Zalecenia dot. realizacji obowiązków informacyjnych* i stanowi załącznik do niniejszej Polityki.

Załączniki do Polityki ochrony danych, o których mowa w rozdziale:

- Zasady pracy zgodnych z RODO
- Procedurę obsługi żądań ww. osób
- Polityka privacy by design i privacy by default
- Upoważnienie do przetwarzania danych
- Umowa powierzenia
- Zalecenia dot. realizacji obowiązków informacyjnych

II. REJESTR CZYNNOŚCI PRZETWARZANIA – PODSTAWOWY DOKUMENT OPISUJĄCY JAKIE DANE FIRMA PRZETWARZA

PODSUMOWANIE:

- **W Rejestrze czynności przetwarzania wskazano procesy w firmie, w których dochodzi m.in. do zbierania (przetwarzania) danych osobowych** (np. proces związany z obsługą potencjalnych Klientów, proces związany z obsługą Klientów (tj. umów/zamówień), proces związany z zarządzaniem portalami społecznościowymi).
- **W przypadku gdy po dniu stworzenia rejestru czynności pojawi się nowy proces**, np. związany z zatrudnieniem pracowników – **należy ten Rejestr uzupełnić o nowy proces.**

1. Firma prowadzi Rejestr czynności przetwarzania, w którym opisuje procesy, jakie zachodzą w firmie, w ramach których dochodzi do zbierania i innego przetwarzania danych.
2. Rejestr stanowi formę dokumentowania czynności przetwarzania danych, pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację zasady rozliczalności.
3. Rejestr należy systematycznie weryfikować i ewentualnie aktualizować.

Załączniki do Polityki ochrony danych, o których mowa w rozdziale:

- Rejestr czynności przetwarzania

III. UMOWA POWIERZENIA – JAKO DOKUMENT UPOWAŻNIAJĄCY PRZEKAZANIE DANYCH FIRMIE ZEWNĘTRZNEJ (PODMIOTOWI TRZECIEMU)

PODSUMOWANIE:

- **Jeżeli innej firmie przekazywane są dane, które co do zasady Firma „sama zbiera”** (np. dane Klientów, dane subskrybentów newslettera, potencjalnych Klientów) **należy zawrzeć umowę powierzenia z firmą zewnętrzną.**
- **W praktyce umowa powierzenia stanowi często np. załącznik do Regulaminu świadczenia usług, np. usług hostingowych.**
- **Jeżeli Firma otrzymuje od innego podmiotu dane – należy zadbać o to, żeby firma przekazująca dane przedstawiła umowę powierzenia.** W takim przypadku należy także **uzupełnić informację w dokumencie Rejestr kategorii przetwarzań.**
- **Umowę można sporządzić w oparciu o wzór umowy** powierzenia oraz zgodnie z instrukcją stanowiące załącznik do Polityki ochrony danych;
- **Przykłady podmiotów, z którymi należy zawrzeć umowę powierzenia**: księgowa, firma hostingowa, wirtualna asystentka, podmiot obsługujący newsletter, firma prowadząca monitoring, podmioty, które współpracującą przy realizacji zleceń i otrzymują dane osobowe.
- **Ważne**! Przekazanie danych firmie specjalistycznej nie zwalnia Administratora, tj. firmy z odpowiedzialności w przypadku gdy dojdzie do naruszenia ochrony przekazanych danych. Warto więc wybierać firmy do współpracy, które dbają o ochronę danych.

UMOWA POWIERZENIA

1. Umowa powierzenia reguluje współpracę między firmą a Procesorem (Podmiotem przetwarzającym), tj. innym podmiotem, któremu firma przekazuje dane osobowe do przetwarzania (np. księgowa, firma hostingowa) - (lub odwrotnie). Wzór umowy – załącznik do Polityki.
2. W umowie opisano zasady, w oparciu o które podmiot otrzymujący dane może działać, tj. m.in. zasady korzystania z danych, zabezpieczania danych, dalszego przekazywania itp.
3. Przed podpisaniem umowy powierzenia, firma m.in. weryfikuje czy:
   1) podmiot przetwarzający zapewnia gwarancję należytego przetwarzania powierzonych danych, tj. czy dba o dane osobowe zgodnie z RODO,
   2) umowa powierzenia zawiera wszystkie elementy przewidziane art. 28 RODO (jeżeli nie została stworzona w oparciu o wzór stanowiący załącznik do Polityki),
   3) nie zachodzi konieczność dodatkowych zabezpieczeń umowy.

REJESTR KATEGORII PRZETWARZANIA (dot. sytuacji gdy firma otrzymuje dane od innego podmiotu trzeciego)

1. W przypadku gdy to firma otrzymuje dane osobowe do przetwarzania od podmiotu trzeciego – zawiera z nimi umowę powierzenia. Umowa powinna być dostarczona przez podmiot trzeci, ale jeśli to nie nastąpi, firma powinna zadbać o to, żeby uregulować współpracę umową powierzenia.
2. Przekazanie danych od innych podmiotów należy wskazać w Rejestrze Kategorii przetwarzań.

Załączniki do Polityki ochrony danych, o których mowa w rozdziale:

- Umowa powierzenia wraz z instrukcją
- Rejestr kategorii przetwarzań

IV. UDOSTĘPNIANIE DANYCH BEZ KONIECZNOŚCI ZAWIERANIA UMOWY POWIERZENIA

1. Otrzymując od organu państwowego (ZUS, US, sądy itp.) wniosek o udostępnienie danych należy sprawdzić czy istnieje podstawa prawna takiego wniosku i czy została w takim wniosku wskazana.
2. Dane bez umowy powierzenia udostępniane są także innym podmiotom, które są do tego uprawnione, jak np. Poczta Polska, banki.
3. W przypadku gdy brak jest takiej podstawy, należy wezwać do wskazania takiej podstawy prawnej, a jeśli nie zostanie wskazana - odmówić udostępnienia danych
4. Inne przypadku udostępnienia danych muszą być każdorazowo weryfikowane co do podstaw prawnych takiego udostępnienia.

V. ZGŁASZANIE NARUSZEŃ OCHRONY DANYCH OSOBOWYCH

PODSUMOWANIE:

W przypadku wystąpienia incydentu/ naruszenia ochrony danych należy zastosować Procedurę zgłaszania naruszeń opisaną w załączniku do Polityki.

1. Firma stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie naruszenia ochrony danych Urzędowi Ochrony Danych w terminie 72 godzin od stwierdzenia naruszenia zgodnie z załącznikiem do niniejszej Polityki.
2. Administrator prowadzi Rejestr naruszeń, w którym opisuje wszystkie naruszenia ochrony danych, jakie wystąpiły.

Załączniki do Polityki ochrony danych, o których mowa w rozdziale:

- Procedura zgłaszania naruszeń wraz z Rejestrem naruszeń

VI. MONITOROWANIE

1. Firma dba o to, żeby zasady ochrony danych były przestrzegane w toku jej działalności. Zaleca się, aby audyt dot. właściwej ochrony danych był przeprowadzany przynajmniej raz na rok lub w razie potrzeby – częściej. Przykładowy wzór audytu – załącznik do Polityki.

Załączniki do Polityki ochrony danych, o których mowa w rozdziale:

- Wzór raportu z audytu

VII. PRZEKAZYWANIE DANYCH DO PAŃSTW TRZECICH

W przypadku gdy zachodzi przekazanie danych do państw trzecich poza UE/EOG, Administrator dokonuje przekazania bądź do podmiotów w ramach tzw. Tarczy Prywatności bądź też w oparciu o standardowe klauzule umowne lub bez ww. zabezpieczeń w oparciu o zgodę osoby, której dane dotyczącą lub też w oparciu o inne przesłanki przewidziane w RODO (m.in. niezbędność do zawarcia/realizacji umowy).

VIII. WSPÓŁADMINISTROWANIE o ile dotyczy

1. W przypadku gdy zachodzi współadministrowanie, tzn. poza firmą również inny podmiot decyduje o celach przetwarzania danych i środkach ich zabezpieczania (np. dwie firmy razem są współorganizatorami jakiegoś przedsięwzięcia), informacja o współadministrowaniu wskazywana jest w:
   1) klauzulach informacyjnych,
   2) rejestrze czynności przetwarzania.

2. W związku ze współadministrowaniem zawierana jest także umowa o współadministrowanie.

IX. OBOWIĄZKI OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH (NP. PRACOWNIKÓW)

1. Dane osobowe mogą być przetwarzane wyłącznie w oparciu o upoważnienie do przetwarzania wydane przez Administratora. Wzór upoważnienia i oświadczenia stanowi załącznik do Polityki.

2. Każda osoba, która uzyskała upoważnienie do przetwarzania danych osobowych zobowiązana jest do:

   1) przetwarzania ich co do zasady wyłącznie na polecenia Administratora;

   2) ochrony danych w sposób zgodny z przepisami prawa i wewnętrznymi zaleceniami;

   3) zachowania w tajemnicy danych osobowych i sposobów ich zabezpieczania.

3. Podczas przetwarzania danych trzeba zachować szczególną ostrożność i podjąć wszelkie możliwe środki umożliwiające zabezpieczenie oraz ochronę danych przed nieuprawnionym dostępem, modyfikacją, utratą, zniszczeniem lub ujawnieniem.

4. Administrator prowadzi ewidencję upoważnień. Wzór – załącznik do Polityki

---

Załączniki do Polityki ochrony danych osobowych, o których mowa w rozdziale:

- Upoważnienie wraz z oświadczeniem
- Ewidencja upoważnień

X. POSTANOWIENIA KOŃCOWE

1. Dokumentacja przetwarzania danych osobowych stanowi wewnętrzną regulację firmy i obowiązuje wszystkich pracowników i współpracowników Administratora oraz inne osoby przetwarzające dane osobowe przetwarzane przez Administratora.
2. Dokumentacja przetwarzania danych osobowych obowiązuje od dnia jej wprowadzenia w życie w sposób przyjęty u Administratora.
3. W sprawach nieuregulowanych mają zastosowanie przepisy powszechnie obowiązującego prawa, w tym w szczególności przepisy ustawy i Rozporządzenia Ogólnego.

XI. NAJWAŻNIEJSZE POJĘCIA

1. **Dane osobowe** oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej ("osobie, której dane dotyczą");
2. **Integralność i poufność** oznacza przetwarzanie w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych;
3. **Naruszenie ochrony danych osobowych** oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
4. **Podmiot przetwarzający** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora;
5. **Przetwarzanie** oznacza operację lub zestaw operacji wykonywanych na danych osobowych takich jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
6. **RODO** oznacza Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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)
7. **Ustawa** oznacza ustawę o ochronie danych osobowych z dnia 10 maja 2018r.

8. **Zbiór danych** oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
9. **Zgoda osoby, której dane dotyczą** oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;

XII. ZAŁĄCZNIKI

- Zasady pracy zgodnych z RODO
- Procedura obsługi żądań ww. osób
- Polityka privacy by design i privacy by default
- Zalecenia dot. realizacji obowiązków informacyjnych
- Rejestr czynności przetwarzania
- Umowa powierzenia wraz z instrukcją
- Rejestr kategorii przetwarzań
- Procedura zgłaszania naruszeń wraz z Rejestrem
- Wzór raportu z audytu
- Upoważnienie wraz z oświadczeniem
- Ewidencja upoważnień

ZASADY PRACY ZGODNIE Z RODO

I. Polityka czystego biurka

1. Pracując z danymi osobowymi w formie papierowej należy zabezpieczać je przed kradzieżą lub wglądem osób nieupoważnionych.
2. Nie należy pozostawiać dokumentów zawierających dane osobowe (a także inne istotne dla firmy dane i informacje) na biurku podczas nieobecności, w szczególności gdy w obszarze przetwarzania danych osobowych pojawia się osoba nieupoważniona (np. klienci, kurier itp.).
3. Zabrania się pozostawiania dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami, np. w korytarzach, na kserokopiarkach, drukarkach.
4. Kończąc pracę należy w miarę możliwości schować całą dokumentację papierową zawierającą dane osobowe (a także tą, która zawiera inne istotne dla organizacji dane i informacje) do zamykanych szaf i szuflad, stosując w ten sposób techniczne środki zabezpieczenia przetwarzania danych osobowych.
5. Dokumenty z danymi/ wydruki z danymi osobowymi, które nie są już potrzebne należy niszczyć w niszczarce.
6. Powyższe zapisy mają także zastosowanie odpowiednio do przenośnych fizycznych nośników danych.

II. Polityka czystego ekranu

1. Monitor komputera wyposażony jest we włączający się samoczynnie wygaszacze ekranu. Wznowienie wyświetlenia następuje dopiero po wprowadzeniu odpowiedniego hasła.

2. Ekran laptopa powinien być, w miarę możliwości, ustawiony tak by w momencie pojawienia się osób nieupoważnionych w pomieszczeniu, osoby te nie mogły widzieć treści wyświetlanych na ekranach.

III. Zasady użytkowania sprzętu informatycznego

Zalecenia:

1. Skonfiguruj hasło administracyjne do BIOS-u,
2. Szyfruj dane na dysku, w tym dyskach przenośnych
3. Wyposaż sprzęt mobilny w oprogramowanie umożliwiające jego nadzór, blokowanie dostępu, czyszczenie zawartości,
4. Aktualizuj oprogramowanie systemów i aplikacji, urządzeń sieciowych i innych (systemy operacyjne/ przeglądarki www / CMS (Wordpress, Drupal, Joomla) / Dedykowany CMS / Adobe / Flash / Java / inne). Aktualizacja dokonywana jest zgodnie z zaleceniami producentów oraz opinią rynkową co do bezpieczeństwa i stabilności nowych wersji (np. aktualizacje, service pack-i, łatki)
5. Wprowadza się zakaz korzystania z nośników danych pochodzących od podmiotów zewnętrznych (np. podłączenie znalezionego pendrive do laptopa) z zastrzeżeniem wyjątkowych sytuacji.

Szyfrowanie jest metodą zapewnienia bezpieczeństwa danych.

6. Stosuje się szyfrowanie poczty wychodzącej (SSL) a także szyfrowanie połączeń internetowych z użyciem protokołu SSL.
7. Stosuje się szyfrowanie dysku oraz nośników zewnętrznych w celu ochrony danych na wypadek np. kradzieży czy innej utraty nośnika.

Naprawa sprzętu

8. W przypadku napraw dokonywanych na zewnątrz (z komputerów należy uprzednio wymontować dyski i wszelkie nośniki, z urządzeń mobilnych karty pamięci, usunąć dane z nośnika z użyciem specjalistycznego oprogramowania).
9. Rekomendowane jest korzystanie z serwisu, który dokonuje napraw u klienta.
10. Czynności konserwacyjne i naprawcze wykonywane przez osoby nieposiadające upoważnień do przetwarzania danych (np. specjalistów z firm zewnętrznych) muszą być wykonywane pod nadzorem osób upoważnionych.
11. Wszelkie prace konserwacyjne i naprawcze sprzętu komputerowego oraz uaktualnienia systemu informatycznego wykonywane przez podmiot zewnętrzny, powinny odbywać się

na zasadach określonych w szczegółowej umowie z uwzględnieniem klauzuli dotyczącej ochrony danych.

12. W przypadku napraw dokonywanych na zewnątrz (z komputerów należy uprzednio wymontować dyski i wszelkie nośniki, z urządzeń mobilnych karty pamięci, usunąć dane z nośnika z użyciem specjalistycznego oprogramowania, a jeśli to nie jest możliwe- rekomendowane jest przekazywanie do naprawy uszkodzonego sprzętu z danymi zaszyfrowanymi na dysku / karcie pamięci. Sprzęt przekazywany jest do serwisu bez podania hasła).

IV. Procedura korzystania z telefonów

1. Należy unikać prowadzenia rozmów telefonicznych w miejscach publicznych, w czasie których wypowiada się informacje dot. danych osobowych, mogących w jakikolwiek sposób zidentyfikować osobę, o której się mówi.
2. Podczas korzystania z poczty e-mail za pośrednictwem telefonu/komputera należy wyłączyć opcję autozapamiętywania hasła do tej poczty.
3. Nie należy korzystać z otwartych sieci wi-fi, w szczególności w celu logowania się z hotspot na pocztę e-mail czy do chmury lub do innych miejsc, w których znajduje się dane osobowe objęte ochroną.
4. Telefon powinien zostać zabezpieczony silnym kodem, tj. np. nie będącym ciągiem cyfr/datą urodzenia, nie przyjmujący znaku w postaci kwadratu, prostokąta, trójkąta czy też liter C, M, W, U. Telefon powinien być zabezpieczony przy użyciu metody/znaku/hasł, która utrudni użycie telefonu przez nieupoważnione osoby.
5. Telefon powinien być zaszyfrowany.
6. Telefon powinien mieć zainstalowane oprogramowanie antywirusowe .
7. Instalując aplikacje na telefonie należy sprawdzać czy pochodzą z wiarygodnego źródła oraz jaki zakres informacji chcą uzyskać (Informacja ta wyświetla się przy instalowaniu; instalowanie najczęściej nie rozpoczyna się zanim nie wyrazi się zgody na dostęp do ww. informacji) .

V. Polityka haseł

Hasło to podstawowa bariera chroniąca zarówno dane osobowe we wszelkiego rodzaju programach, systemach, aplikacjach.

1. Dostęp do systemu/ konta/aplikacji powinien być możliwy wyłącznie co najmniej po wprowadzeniu właściwego identyfikatora i właściwego hasła.
2. Nie można używać w serwisach internetowych takich samych lub podobnych haseł jak w systemie komputerowym firmy. Do każdej aplikacji/ konta/ systemu powinno być stworzone inne hasło.

3. Hasła nie mogą być łatwe do odgadnięcia.

4. Nie twórz haseł, które:

   - będą odnosiły się do właściciela konta, tzn. będą zawierały w sobie np. imię, nazwisko, daty urodzenia, inne ważne daty, PESEL, imiona dzieci, nazwę firmy, numerów rejestracyjnych auta itp.

   - będą składały się z prostego ciągu znaków typu QWERTY (ciąg znaków z klawiatury), 12345 czy 11111 lub odnosiły się do innych popularnych haseł typu STARWARS, ADMIN itp.,

   - nie twórz haseł w oparciu o jeden, nawet skomplikowany wzór. W ten sposób „wykradniecie" jednego hasła i wygenerowanie kolejnych przez inne osoby nadal będzie prostym zadaniem. Przykład błędnego tworzenia haseł: E089$09080KIRFT543 i kolejne hasła powstające w oparciu o poprzednie wzbogacone o kilka cyfr typu E089$09080KIRFT543123

5. Zaleca się korzystanie z Managera haseł, dzięki któremu możliwe jest bezpieczne generowanie, przechowywanie i wprowadzanie haseł na stronach www, do poszczególnych kont itp.

6. Należy zachowywać hasła w poufności, nawet po utracie przez nie ważności lub zmianie.

7. Zmiana hasła powinna następować nie rzadziej niż co 90 dni;

8. Należy zmieniać hasło zawsze gdy zachodzi podejrzenie, że ktoś mógł uzyskać informacje o haśle.

9. Użytkownicy są odpowiedzialni za zachowanie poufności swoich haseł. Hasła nie powinny być ujawnianie innym osobom. Nie należy zapisywać haseł na kartkach i w notesach, nie naklejać na monitorze komputera, nie trzymać pod klawiaturą, itp.

10. W systemach umożliwiających zapamiętanie nazwy użytkownika lub jego hasła nie należy korzystać z tego ułatwienia.

Dwukrotne uwierzytelnianie

11. Do miejsc ważnych z punktu widzenia prowadzenia działalności, a także do miejsc takich jak prywatna skrzynka e-mailowa, na której znajduje się istotne informacje powinno stosować się co najmniej dwukrotne uwierzytelnianie.

VI. Ochrona antywirusowa

1. Podstawowym sposobem zabezpieczenia przed ww. oprogramowanie jest zastosowanie, na wszystkich stacjach roboczych, serwerach, komputerach przenośnych oprogramowania antywirusowego. Stosowany jest firewall programowy.
2. Oprogramowanie antywirusowe jest cykliczne i automatycznie aktualizowane. Zaleca się okresowe monitorowanie czy aktualizacja ta przebiega bez zakłóceń.

3. Oprogramowanie, o którym mowa w pkt 2, sprawuje ciągły nadzór (ciągła praca w tle) nad pracą systemu i jego zasobami oraz serwerami i stacjami roboczymi.

VII. Zasady korzystania z poczty elektronicznej

1. W przypadku przesyłania danych osobowych poza organizację należy ocenić czy zasadne byłoby w określonym przypadku wysłanie pliku zaszyfrowanego/ spakowanego (np. programem 7 zip, winzipem, winrarem) i zahasłowane, gdzie hasło powinno być przesłane do odbiorcy telefonicznie SMS, lub kolejną wiadomością e-mail.
2. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy.
3. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW". Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości"
4. Użytkownicy powinni okresowo kasować niepotrzebne maile.

VIII. Kopie zapasowe

Tworzenie kopii zapasowych to jeden ze środków technicznych pozwalających na zapewnienie dostępności danych osobowych w celu ochrony danych np. przed ich utratą.

1. Kopie zapasowe tworzy się co najmniej co 2 tygodnie.
2. W szczególności należy wykonywać następujące kopie bezpieczeństwa:
   1) przed dokonaniem zmian w konfiguracji systemów lub oprogramowania,
   2) przed dokonaniem zmian w programach (np. zmiana wersji).
4. Zasady dot. tworzenia kopii zapasowych.
   Zaleca się stosowanie metody 3-2-1 rekomendowanej przez US-CERT[1]
   1) 3 egzemplarze, tzn. 1 oryginał + 2 kopie danych zapisanych na różnych nośnikach
   2) 2 różne formaty - np. jeśli dane pierwotne są przechowywane w formie papierowej, warto je np. zeskanować i przechowywać w formie elektronicznej np. w chmurze, na skrzynce pocztowej, nośnikach zewnętrznych.
      UWAGA! W przypadku zapisywania kopii zapasowych na nośnikach zewnętrznych należy pamiętać o ich zaszyfrowaniu.
   3) 1 kopia poza firmą (w tym m.in. w chmurze): zmniejsza ryzyko utraty danych na wypadek zdarzeń związanych bezpośrednio z firmą.

[1] United States Computer Emergency Readiness Team

5. W celu zapewnienia poprawności wykonywanych kopii bezpieczeństwa należy co najmniej raz na kwartał poddać testowi cyklicznie wybraną kopię. Próba polega na odtworzeniu danych w warunkach testowych i sprawdzeniu, czy jest możliwość odczytania danych.
6. Nośniki zawierające nieaktualne kopie danych, likwiduje się. W przypadku nośników jednorazowych, takich jak płyty CD-R, DVD-R, likwidacja polega na ich fizycznym zniszczeniu w taki sposób, by nie można było odczytać ich zawartości. Nośniki wielorazowego użytku, takie jak dyski twarde, pendrive, płyty CD-RW, DVD-RW, można wykorzystać ponownie do celów przechowywania kopii bezpieczeństwa po uprzednim usunięciu ich zawartości.
7. Nośniki wielorazowego użytku nienadające się do ponownego użycia należy zniszczyć fizycznie.

PROCEDURA ZGŁASZANIA NARUSZEŃ OCHRONY DANYCH OSOBOWYCH

I. STWIERDZENIE NARUSZENIA I ZGŁOSZENIE DO ORGANU

Należy wszcząć niniejszą procedurę, jeśli doszło do naruszenia ochrony danych osobowych lub pojawi się podejrzenie, że mogło dojść do takiego zdarzenia.

Typowe sytuacje, które mogą budzić podejrzenie, że mogło dojść do naruszenia:
Zniszczenie dokumentacji zawierającej dane osobowe bez użycia niszczarki
Fizyczna obecność w budynku lub pomieszczenia osób podejrzanie się zachowujących
Udostępnianie danych osobowych osobom nieupoważnionych
Telefoniczne próby wyłudzenia danych osobowych
E-maile zachęcające do ujawnienia identyfikatora i/lub hasła
Przechowywanie haseł do systemów w pobliżu komputera
Pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów
Typowe naruszenia ochrony danych osobowych
Kradzież danych (np. m.in. kradzież zarówno w formie elektronicznej jaki i kradzież dokumentów papierowych, czy też fizycznych nośników danych)
Błąd ludzki (np. pozostawienie danych – w formie dokumentu lub nośnika fizycznego – poza obszarem przetwarzania bez możliwości kontroli osób, które mają dostęp do tak pozostawionych danych osobowych, omyłkowe przesłanie korespondencji zawierającej dane osobowe do podmiotu nieuprawnionego)
Incydent spowodowany zaniedbaniem (np. pracownik pozostawia niezabezpieczone dokumenty zawierające dane osobowe w miejscu, do którego mają dostęp osoby nieuprawnione do przetwarzania danych osobowych – efektem takiego działania jest utrata poufności danych)
Incydent spowodowany zaniechaniem (np. m.in. pracownik, pomimo tego, że dysponuje odpowiednimi środkami technicznymi np. zamykanymi szafkami, nie korzysta z nich w celu zabezpieczenia danych osobowych – efektem takiego działania jest kradzież danych)
Incydent spowodowany włamaniem do sieci lub do kont użytkowników stacji roboczych (np. m.in. pracownik używa hasła do stacji roboczej, które składa się z jego imienia i nazwiska)

Utrata kopii zapasowych (np. m.in. kradzież niezabezpieczonej kopii zapasowej)

2. W przypadku gdy Administrator współpracuje z innymi osobami (pracownicy, zleceniobiorcy), osoby te są zobowiązane niezwłocznie powiadomić **Administratora**, jeśli doszło do naruszenia ochrony danych osobowych lub pojawi się podejrzenie, że mogło dojść do takiego zdarzenia

CO ZROBIĆ gdy stwierdzono naruszenie lub prawdopodobieństwo naruszenia ochrony danych?

KROK 1: ZMNIEJSZENIE SKUTKÓW

1. **Należy podjąć niezwłocznie czynności niezbędne dla powstrzymania niepożądanych skutków** zaistniałego zdarzenia uwzględniając także potrzebę ustalenia jego przyczyn lub sprawców.

KROK 2: USTALENIE RODZAJU NARUSZENIA

2. Należy określić:
    1) Jaka jest waga naruszenia
    2) Czy zdarzenie prowadzi lub skutkuje ryzykiem naruszenia prawa lub wolności osoby fizycznej
    3) czy zaistniałe naruszenie podlega obowiązkowi zgłoszenia organowi nadzorczemu,
    4) czy zaistniałe naruszenie podlega obowiązkowi powiadomienia osoby, której dane dotyczą.

KROK 3: WPISAĆ NARUSZENIE DO REJESTRU NARUSZEŃ

3. Administrator prowadzi rejestr naruszeń. Wzór rejestru znajduje się w załączniku do Procedury zgłoszenia naruszeń.

KROK 4: GDY ZACHODZI RYZYKO, ŻE NARUSZENIE BĘDZIE SKUTKOWAŁO RYZYKIEM

NARUSZENIA PRAW LUB WOLNOŚCI OSÓB FIZYCZNYCH

4. Administrator bez zbędnej zwłoki – w miarę możliwości, **nie później niż w terminie 72 godzin po stwierdzeniu** naruszenia – **zgłasza się je organowi nadzorczemu**.
5. Zgłoszenie dokonuje się przy wykorzystaniu formularza udostępnionego przez Urząd. Informacje o tym, jak zgłosić naruszenie znajdują się na stronie Urzędu Ochrony Danych Osobowych - uodo.gov.pl. [https://uodo.gov.pl/pl/134/233].
6. Jeżeli naruszenie zgłosi się po 72 godzinach, do takiego zgłoszenia należy załączyć wyjaśnienia ze wskazaniem powodu opóźnienia.
7. **Zgłoszenie do organu nadzorczego** zawiera:
    1) charakter naruszenia ochrony danych osobowych wraz ze wskazaniem kategorii i przybliżonej liczby osób, których dane dotyczą oraz przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,
    2) imię i nazwisko oraz dane kontaktowe osoby, która posiada szczegółowe informacje odnośnie naruszenia, a organizacja wyznaczyła ją do załatwiania spraw związanych z ochroną danych osobowych,
    3) opis możliwych konsekwencji naruszenia danych osobowych,
    4) opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu, w tym w stosownych przypadkach opis środków możliwych do podjęcia w celu minimalizacji skutków naruszenia.

KROK 5: GDY ZACHODZI <u>WYSOKIE</u> RYZYKO, ŻE NARUSZENIE BĘDZIE SKUTKOWAŁO

RYZYKIEM NARUSZENIA PRAW LUB WOLNOŚCI OSÓB FIZYCZNYCH

8. Administrator **bez zbędnej zwłoki** zawiadamia osoby, których dane dotyczą, o takim naruszeniu.
9. Zawiadomienie powinno być sformułowane jasnym i prostym językiem i zawierać:
    1) imię i nazwisko oraz dane kontaktowe osoby, która posiada szczegółowe informacje odnośnie incydentu, a organizacja wyznaczyła ją do załatwiania spraw związanych z ochroną danych osobowych,
    2) opis możliwych konsekwencji naruszenia danych osobowych,
    3) opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu, w tym w stosownych przypadkach opis środków możliwych do podjęcia w celu minimalizacji skutków naruszenia.
10. Przyjmuje się, że **zawiadomienie nie będzie wymagane gdy**:
    1) Administrator zastosował odpowiednie techniczne i organizacyjne środki ochrony i

środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, tj. w szczególności środki takie jak szyfrowanie uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych,

2) Administrator zastosował środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,

3) wymagałoby to niewspółmiernie dużego wysiłku – wówczas Administrator wyda publiczny komunikat lub zastosowany zostanie podobny środek, za pomocą osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

4. Zawiadomienie może być wysłane drogą elektroniczną, tj. email lub pocztą

Załącznik do Procedury zgłaszania naruszeń – Rejestr naruszeń

REJESTR NARUSZEŃ DLA ADMINISTRATORA

L.p.	**Data naruszenia**	**Rodzaj naruszenia**	**Okoliczność naruszenia**	**Skutki naruszenia**	**Przyjęte działania zaradcze**
1.	**Przykładowe naruszenie:* *29.06.2020*	*Kradzież laptopa*	*Pozostawienie laptopa w bagażniku i jego kradzież przez nieznanego sprawcę*	*Utrata danych na dysku C – możliwy dostęp osób nieuprawnionych do danych, w konsekwencji możliwość powstania szkody majątkowej, poprzez utratę kontroli nad własnymi danymi, kradzież tożsamości*	*Szyfrowanie dysków twardych komputerów przenośnych*
2.					

***** przy każdym kolejnym naruszeniu należy skopiować tabelę i ją uzupełnić

PROCEDURA OBSŁUGI WNIOSKÓW I ŻĄDAŃ OSÓB, KTÓRYCH DANE DOTYCZĄ

SPIS TREŚCI

- **PROCEDURA POWINNA BYĆ STOSOWANA W PRZYPADKU GDY DO ADMINISTRATORA WPŁYWIE WNIOSEK, w ramach którego osoba chce skorzystać z prawa dot. danych osobowych**

Cel procedury: zapewnienie osobie, której dane dotyczą:

1) **prawa dostępu (art. 15 RODO),**
2) **prawa do sprostowania danych (art. 16 RODO),**
3) **prawa do bycia zapomnianym (art. 17 RODO),**
4) **prawa do ograniczenia przetwarzania (art. 18 RODO),**
5) **powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania (art. 19 RODO),**
6) **prawa do przenoszenia danych (art. 20 RODO),**
7) **prawa do sprzeciwu (art. 21 RODO).**

I. ZASADY DOTYCZĄCE PRAW OSÓB, KTÓRYCH DANE DOTYCZĄ

NAJWAŻNIEJSZE INFORMACJE:

I. ZBIERAJĄC DANE OSOBOWE **INFORMUJ OSOBY, KTÓRYCH DANE DOTYCZĄ O ZASADACH DOTYCZĄCYCH PRZETWARZANIA DANYCH OSOBOWYCH**

- **KIEDY NALEŻY INFORMOWAĆ O ZASADACH PRZETWARZANIA DANYCH OSOBOWYCH?**

Przy pozyskiwaniu danych od tej osoby lub gdy otrzymaliśmy informacje o osobie X od osoby Y, osobę X musimy poinformować nie później niż w terminie miesiąca o zasadach dot. przetwarzania jej danych osobowych.

- **JAK NALEŻY INFORMOWAĆ?**

PRZYKŁAD: Polityka prywatności na stronie/fanpage, Link do Polityki prywatności w stopce e-maila, odwołania do Polityki prywatności w serwisach ogłoszeniowych, okazując klauzule informacyjne przy zawieraniu umów, itp

II. **DZIAŁAJ ZGODNIE Z PROCEDURĄ** W PRZYPADKU GDY WPŁYNIE WNIOSEK NP. O UDOSTĘPNIENIE DANYCH, USUNIĘCIE ITP**.**

Najważniejsze zasady:

- **O CZYM PAMIĘTAĆ PRZED UDZIELENIEM ODPOWIEDZI?**

Przed udzieleniem odpowiedzi, jeżeli jest to możliwe, a wniesione zapytanie pozostawia wątpliwości co do tożsamości osoby, **należy podjąć próbę dokładniejszego zidentyfikowania** osoby, która wnosi o realizację prawa lub żądania.

- **JAK UDZIELAĆ ODPOWIEDZI NA WNIOSKI/ŻĄDANIA OSÓB DOT. ICH DANYCH OSOBOWYCH?**

Jeżeli żądanie/wniosek osoba składa na piśmie, i konieczne jest udzielenie odpowiedzi, **odpowiedzi udziela się na piśmie.**

- **KIEDY i JAK NALEŻY UDZIELAĆ ODPOWIEDZI?**

Odpowiedzi należy udzielić **bez zbędnej zwłoki, lecz w terminie nie dłuższym niż miesiąc** od dnia otrzymania żądania.

Jeżeli czynności potrzebne do udzielenia odpowiedzi mają skomplikowany charakter, termin **można wydłużyć o kolejne dwa miesiące**. Jednak w terminie miesiąca należy poinformować osobę, której dane dotyczą o przedłużeniu terminu.

W przypadku gdy wniosek/żądanie złożone jest drogą mailową, odpowiedzi udziela się drogą mailową, chyba że osoba, której dane dotyczą zażąda konkretnej formy udzielenia odpowiedzi. Realizowanie zgłoszonego żądania lub zapytania od osoby, której dane dotyczą nie może naruszać praw innych osób.

W przypadku zrealizowania prawa do sprostowania danych, prawa do usunięcia danych oraz prawa do ograniczenia danych, Administrator **informuje o zrealizowanych czynnościach każdego odbiorcę**, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Ponadto administrator informuje osobę, której dane dotyczą, o odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

III.	**UDOKUMENTUJ obsługę wniosków/żądań**, tzn. wskaż w rejestrze (wzór poniżej)

REJESTR DOT. OBSŁUGI WNIOSKÓW OSÓB, KTÓRYCH DANE DOTYCZĄ

Dokumentuj w poniższym rejestrze wnioski/żądania osób, które zostały skierowane do firmy w zakresie dostępu do danych/usunięcia danych/ ograniczenia przetwarzania/przeniesienia/ sprostowania/ sprzeciwu.

Lp	Rodzaj wniosku i data wniosku	Kogo dotyczy wniosek	Odpowiedź Administratora (uwzględniono wniosek/ nieuwzględniono wniosek i dlaczego) data odpowiedzi	Inne uwagi
1				
2				
3				

II. PRAWO DOSTĘPU DO DANYCH OSOBOWYCH

STUDIUM PRZYPADKU:

Do Administratora Danych wpłynął wniosek od Jana Kowalskiego – pracownika zwolnionego 5 lat temu o następującej treści: „Proszę o udzielenie informacji odnośnie tego, jakie dane Państwo przetwarzają i na jakiej podstawie".

SUGEROWANE ROZWIĄZANIE:

Pracownik odbierający zapytanie przekazuje je Administratorowi Danych. Administrator, w celu uwierzytelnienia, prosi osobę zgłaszającą żądanie o precyzyjne określenie np. okresu zatrudnienia/ zajmowanego stanowiska/podania przyczyny rozwiązania stosunku pracy. Po otrzymaniu prawidłowej odpowiedzi, Administrator realizuje żądanie, wysyłając wiadomość, której treść zawiera m.in. informacje o tym jakie dane są przetwarzane z informacją, że są one przetwarzane tylko w celach archiwalnych, z uwagi na to, że okres przetwarzania jest uzależniony od przepisów Kodeksu pracy.

Co powinien zrobić Administrator danych osobowych (dalej zwany ADO)?

- ADO powinien udzielić wszelkich informacji odnoszących się do przetwarzanych przez ADO danych osobowych osoby, która o to prosi.

Jakich informacji może żądać Jan Kowalski?

- Osoba, której dane dotyczą, zgodnie z treścią art. 15 RODO, jest upoważniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, osoba ta jest uprawniona do uzyskania dostępu do nich oraz następujących informacji takich jak:
  1) cel przetwarzania,
  2) kategorie odnośnych danych osobowych,
  3) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lu organizacjach międzynarodowych,
  4) planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu,
  5) informacje o prawie żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą oraz do wniesienia sprzeciwu wobec takiego przetwarzania,
  6) informacje o prawie wniesienia skargi do organu nadzorczego,
  7) wszelkie dostępne informacje o źródle danych osobowych (w przypadku danych osobowych, które nie zostały zebrane od osoby, której dane dotyczą),

8) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu (jeżeli ma zastosowanie),

9) informacje o podjętych zabezpieczeniach, o których mowa w art. 46 RODO, w przypadku przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej.

W jaki sposób należy udzielić informacji?

- Informacja powinna być udzielona na piśmie lub w inny sposób, także elektronicznie. Elektronicznie powinno się udzielić informacje, jeśli osoba, złożyła wniosek w tej formie. Ustnie można udzielić informacji po uprzednim zweryfikowaniu tożsamości, która o to prosi, aczkolwiek dla celów rozliczalności zaleca się rezygnację z ww. formy. Sposób weryfikacji tożsamości należy odnotować na wypadek kontroli organu nadzoru, żeby móc wykazać wykonanie tej czynności.

Jaki jest termin na udzielenie informacji?

- Informacji należy udzielić bez zbędnej zwłoki, nie później jednak niż w terminie miesiąca od otrzymania prośby.

Czy 1-miesięczny termin można wydłużyć?

- **W razie potrzeby** termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań**. W terminie miesiąca od otrzymania żądania administrator informuje osobę, której dane dotyczą o takim przedłużeniu terminu, z podaniem przyczyn** opóźnienia.

Co należy zrobić w sytuacji gdy ADO nie podejmuje żadnych działań w celu przekazania informacji?

- ADO musi niezwłocznie - najpóźniej w terminie miesiąca od otrzymania prośby poinformować osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

Czy można pobrać opłatę za udzielenie informacji?

- Informacje są wolne od opłat, chyba że żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter. W takim przypadku administrator może pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań; albo odmówić podjęcia działań w związku z żądaniem.

Kto ma wykazać, że żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter?

- Administrator będzie musiał wykazać, że mógł nie wykonać obowiązku udzielenia informacji.

- W przypadku uznania, że żądanie ma charakter ewidentnie nieuzasadniony lub nadmierny zaleca się sporządzenie uzasadnienia na potrzeby ewentualnej kontroli przez organ nadzorczy.

Czy można przed udzieleniem odpowiedzi, zażądać dodatkowych informacji w celu potwierdzenia tożsamości osoby, której dane dotyczą?

- Tak. Jeśli Administrator ma uzasadnione wątpliwości co do tożsamości osoby zgłaszającej żądanie.

Czy ADO musi przekazać kopię danych osobowych?

- Tak, przy czym pierwsza kopia danych podlegających przetwarzaniu jest wolna od opłat. Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, administrator może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się drogą elektroniczną.

III. SPROSTOWANIE DANYCH

Do Administratora Danych wpłynął wniosek od pracownika Anny Kowalskiej o następującej treści: „Proszę o sprostowanie moich danych osobowych z uwagi na zmianę nazwiska. ”

Kiedy i kto ma tego dokonać?

- Osoba, której dane dotyczą, zgodnie z treścią art. 16 RODO, ma prawo żądać by administrator dokonał niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Nadto, z uwzględnieniem celu przetwarzania, osoba, której dane dotyczą, ma prawo do żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.
- Osoba, której dane dotyczą musi wykazać zasadność swojego żądania w przedmiocie zrealizowania uprawnień korekcyjnych
- Administrator musi niezwłocznie sprostować dane na żądanie osoby, której dotyczą. Osoba ta może żądać uzupełnienia niekompletnych danych.
- Administrator informuje o sprostowaniu danych każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

IV. PRAWO DO BYCIA ZAPOMNIANYM/PRAWO DO USUNIĘCIA

Jak Kowalski chce skorzystać z prawa do bycia zapomnianym. Jak wygląda procedura przeprowadzana przez Administratora?

Czy zawsze Jan Kowalski może prawo do bycia zapomnianym realizować?

- Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a **administrator ma obowiązek <u>bez zbędnej zwłoki</u> usunąć dane osobowe**, jeżeli zachodzi jedna z następujących okoliczności:

a) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;

b) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania;

c) osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania;

d) dane osobowe były przetwarzane niezgodnie z prawem;

e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator;

f) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego.

W przypadku upublicznienia danych osobowych osoby zgłaszającej żądanie, administrator, biorąc pod uwagę dostępną technologię i koszt realizacji – podejmie rozsądne działania, w tym środki techniczne, by poinformować administratorów tych danych osobowych, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych lub ich replikacje.

Zapisy ww. ustępów nie mają zastosowania gdy przetwarzanie jest niezbędne do:

a) do korzystania z prawa wolności do wypowiedzi i informacji,

b) do wywiązywania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator,

c) do ustalenia dochodzenia lub roszczeń.

Co należy rozumieć pod pojęciem usunąć?

- Administrator musi usunąć dane ze wszystkich miejsc, w których dane te mogą się znajdować, tj. np: z serwera, z poczty elektronicznej, z dokumentów typu Excel, Work, z dysków zewnętrznych i przenośnych, jak również papierowych kopii, a także kopii zapasowych. .

Jakie dodatkowe obowiązki ciążą na administratorze?

- Jeżeli administrator upublicznił dane osobowe, ma obowiązek usunąć te dane osobowe. Podejmuje rozsądne działania, w tym środki techniczne, by poinformować administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje.
- Administrator informuje o usunięciu danych każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

INNE

- W przypadku realizowania prawa do bycia zapomnianym należy sporządzić swojego rodzaju protokół z usunięcia danych, w którym odnotuje się usunięcie danych osobowych osoby, która zgłasza żądanie ze wszystkich zbiorów danych osobowych, w których takie dane mogły być przetwarzane. Po wykonaniu czynności protokół należy zanonimizować, przyporządkowując mu indywidualny numer.

- W przypadku konieczności przewrócenia systemu lub jego elementów za pomocą kopii zapasowej, Administrator korzysta z ww. protokołów, by w ten sposób uniknąć sytuacji, w której przywróci się do przetwarzania dane, które np. zostały poprawione lub usunięte.

PRZYKŁADOWE WZORY DOKUMENTÓW DO WYKORZYSTANIA

- Wzór odpowiedzi do wykorzystania gdy wniosek o usunięcie danych zostanie uwzględniony

REALIZACJA WNIOSKU O USUNIĘCIE DANYCH OSOBOWYCH

(na podstawie art. 17 RODO)

Imię i nazwisko osoby, która wnioskuje	

Odpowiadając na Pani / Pana wniosek o usunięcie danych osobowych ze zbioru ..... firmy, informujemy, iż Pani / Pana wniosek **został uwzględniony** i wskazane dane nie będą dłużej przetwarzane.

Usuniecie danych z kopii zapasowych będzie możliwe po okresie ……..…. przez który przechowywane są te kopie.

Pani/Pana dane zostały udostępnione podmiotom: ……,

Podmioty te zostały one powiadomione w dniu …… o obowiązku usunięcia Pani/Pana danych w związku z otrzymanym żądaniem.

…… ……

Data Administrator

- Wzór odpowiedzi do wykorzystania gdy wniosek o usunięcie danych nie zostanie uwzględniony

REALIZACJA WNIOSKU O USUNIĘCIE DANYCH OSOBOWYCH

(na podstawie art. 17 RODO)

Imię i nazwisko osoby, która wystąpiła z wnioskiem	

Odpowiadając na Pani / Pana wniosek o usunięcie danych osobowych ze zbioru ..... firmy ..... (dane firmy) informuję, iż na podstawie art. 17 ust. 3 Ogólnego Rozporządzenia O Ochronie Danych Osobowych z dnia 27 kwietnia 2016 roku 2016/679 (RODO), Pani / Pana wniosek **nie został uwzględniony** w związku z tym, że ich dalsze przetwarzanie przez administratora jest niezbędne[wybrać odpowiednią przyczynę nieuwzględnienia wniosku]:

- € do korzystania z prawa do wolności wypowiedzi i informacji;
- € do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
- € z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego zgodnie z art. 9 ust. 2 lit. h) oraz i) i art. 9 ust. 3;
- € do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, o ile prawdopodobne jest, że prawo, o którym mowa w ust. 1, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania; lub
- € do ustalenia, dochodzenia lub obrony roszczeń,
- € dane osobowe nadal konieczne do celów, w których zostały zebrane;

Przysługuje Pani / Panu prawo wniesienia skargi do organu nadzorczego .

…… …….

Data Podpis Administratora

STUDIUM PRZYPADKU:

- były Klient będący osobą fizyczną (współpraca zakończona na rok przed zgłoszeniem) zwrócił się z wnioskiem o usunięcie jego danych. Po zweryfikowaniu tożsamości Administrator dochodzi do wniosku, że nie może zrealizować żądania osoby, której dane dotyczą. Usunięcie danych osobowych nie może nastąpić z tego względu, że dane muszą być przechowane dla celów rachunkowych, jak też w celu zabezpieczenia i dochodzenia dalszych roszczeń. O podjętych krokach administrator informuje osobę, której dane dotyczął

- kiedy np. Jan Kowalski chce usunięcia danych, które zostały zebrane w związku z Usługą płatnego dostępu, która nadal jest świadczona.

- kiedy np. Jan Kowalski chce usunięcia danych, które Pracodawca uzyskał w związku z jego zatrudnieniem. Pomimo żądania Jana Kowalskiego, Pracodawca – Administrator nie może usunąć danych osobowych swojego byłego pracownika, bo ciąży na nim obowiązek przechowywania dokumentacji pracowniczej przez okres 50 lat lub 10 lat (w zależności od tego kiedy pracownik był zatrudniony i czy firma spełniła wymogi umożliwiające mu skrócenie okresu przechowywania do 10 lat)

V. PRAWO DO OGRANICZENIA PRZETWARZANIA DANYCH

Jan Kowalski chce skorzystać z prawa do ograniczenia przetwarzania.

Czy zawsze może to prawo realizować? Jak wygląda procedura przeprowadzana przez Administratora?

- Osoba, której dane dotyczą ma prawo żądać od administratora ograniczenia przetwarzania w następujących przypadkach:
  1) osoba, której dane dotyczą kwestionuje prawidłowość danych osobowych – ograniczenia przetwarzania powinno nastąpić na okres pozwalający ustalić administratorowi prawidłowość tych danych,
  2) przetwarzanie danych osobowych jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,
  3) administrator nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą do ustalenia dochodzenia lub obrony roszczeń,
  4) osoba, której dane dotyczą, wniosła sprzeciw wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

- Jeżeli administrator zdecyduje się ograniczyć przetwarzanie, może przetwarzać objęte żądaniem dane osobowe, z wyjątkiem przechowania, wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony prawnej innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego.

- W przypadku uchylenia ograniczenia przetwarzania administrator informuje o tym osobę, której dane dotyczą i która to osoba żądała ograniczenia, o którym mowa w niniejszym paragrafie.

Co można robić z danymi osobowymi w przypadku gdy ograniczono przetwarzanie danych?

- Jeżeli przetwarzanie zostało ograniczone, takie dane osobowe można przetwarzać, z wyjątkiem przechowywania, wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego.

VI. SPRZECIW WZGLĘDEM PRZETWARZANIA DANYCH OSOBOWYCH

Czy Jan Kowalski może wnieść sprzeciw względem przetwarzania jego danych osobowych? Czego sprzeciw dotyczy?

Na czym polega prawo do wniesienia sprzeciwu i kiedy przysługuje?

- Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw - z przyczyn związanych z jej szczególną sytuacją - wobec przetwarzania dotyczących jej danych osobowych opartego na art. 6 ust. 1 lit. e) lub f) Rozporządzenia, w tym profilowania na podstawie tych przepisów.
- Administratorowi nie wolno już przetwarzać tych danych osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.
- Jeżeli dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby takiego marketingu, w tym profilowania, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim.
- Jeżeli osoba, której dane dotyczą, wniesie sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, **danych osobowych nie wolno już przetwarzać do takich celów.**

VII. PRAWO DO PRZENOSZENIA DANYCH

Administrator otrzymał od Jana Kowalskiego – kandydata do pracy pismo: „Chcę przenieść swoje dane do innej firmy celem uczestnictwa w innym procesie rekrutacji".

Czego Jan Kowalski może oczekiwać od Administratora? Na czym polega prawo do przeniesienia danych?

- Jan Kowalski:

1) ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dotyczące go dane osobowe, a które to dane dostarczył administratorowi (np. plik WORD), oraz

2) ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe.

Kiedy prawo do przenoszenia danych może być wykonywane?

- Prawo to powinno mieć zastosowanie w przypadkach, gdy osoba, której dane dotyczą, dostarczyła danych osobowych za własną zgodą (art. 6 ust. 1 lit. a lub 9 ust. 2 lit. a Rozporządzenia) lub gdy przetwarzanie jest niezbędne do wykonania umowy (art. 6 ust. 1 lit. b Rozporządzenia). Nie powinno mieć zastosowania, jeżeli przetwarzanie opiera się na innej podstawie prawnej niż zgoda lub umowa. Prawa tego – z uwagi na jego charakter – nie powinno się wykonywać w stosunku do administratorów przetwarzających dane osobowe w ramach wykonywania obowiązków publicznych. Dlatego nie powinno ono mieć zastosowania w

przypadkach, gdy przetwarzanie danych osobowych jest niezbędne do wywiązania się z obowiązku prawnego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

Jeżeli określony zestaw danych osobowych odnosi się do więcej niż jednej osoby, której dane dotyczą, prawo do otrzymania danych osobowych nie powinno powodować uszczerbku dla praw i wolności innych osób, których dane dotyczą, na podstawie niniejszego rozporządzenia. Prawo to powinno ponadto pozostawać bez uszczerbku dla prawa osoby, której dane dotyczą, do spowodowania, by dane osobowe zostały usunięte, oraz bez uszczerbku dla ograniczeń tego prawa określonych w niniejszym rozporządzeniu i nie powinno w szczególności skutkować usunięciem danych osobowych dotyczących osoby, której dane dotyczą, których osoba ta dostarczyła do wykonania umowy, o ile i w takim zakresie, w jakim te dane osobowe są niezbędne do wykonania tej umowy.

Czy Jan Kowalski może żądać by dane osobowe zostały przesłane przez Administratora bezpośrednio innemu administratorowi?

- Tak, o ile jest to technicznie możliwe.

Jaki jest termin na udzielenie informacji?

- Informacji należy udzielić bez zbędnej zwłoki, nie później jednak niż w terminie miesiąca od otrzymania prośby.

Czy 1-miesięczny termin można wydłużyć?

- **W razie potrzeby** termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań**. W terminie miesiąca od otrzymania żądania administrator informuje osobę, której dane dotyczą o takim przedłużeniu terminu, z podaniem przyczyn** opóźnienia.

Co należy zrobić w sytuacji gdy ADO nie podejmuje żadnych działań w celu przekazania informacji?

- ADO musi niezwłocznie - najpóźniej w terminie miesiąca od otrzymania prośby poinformować osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

Czy można pobrać opłatę za udzielenie informacji?

- Informacje są wolne od opłat, chyba że żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter. W takim przypadku administrator może pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań; albo odmówić podjęcia działań w związku z żądaniem.

Kto ma wykazać, że żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter?

- Administrator będzie musiał wykazać, że mógł nie wykonać obowiązku udzielenia informacji.

PROCEDURA DOT. OCHRONY DANYCH W WERSJI BETA (tzw. PRIVACY BY DESIGN I PRIVACY BY DEFAULT)

Podsumowanie:
Wprowadzając na rynek nowy produkt/wprowadzając w firmie nową aplikację/nowy system/nowy sposób kontaktu z Klientem należy zadbać o to, żeby prywatność była chroniona już na etapie projektowania ww. systemu/aplikacji (czyli już w wersji Beta powinno się zadbać o prywatność i minimalną ilość zbierania danych)

1. Administrator w momencie planowania procesu zbierania i przetwarzania danych osobowych będzie stosował zasady wskazane w Polityce ochronie danych osobowych. Ponadto będzie:
   1) przewidywał i przeciwdziałał możliwym problemom zakresie ochrony danych,
   2) dbał o to by prywatność nie mogła powodować utraty funkcjonalności,
   3) dbał o bezpieczeństwo całego procesu przetwarzania danych,
   4) podejmował transparentne i czytelne rozwiązania,
   5) chronił użytkownika i jego prywatność.
2. Privacy by Design wymaga zapewnienia ochrony danych osobowych już w fazie projektowania, co będzie skutkować koniecznością uprzedniego (przed przystąpieniem do przetwarzania) przeprowadzenia analizy ryzyka oraz położenia nacisku na działania prewencyjne (wykluczając lub ograniczając zachowania oparte na późniejszym – po wykryciu naruszenia – „naprawianiu" braków). Administrator ujmuje ramy ochrony danych szeroko, obejmując nimi zarówno system informatyczny, rodzaje operacji, przesłankę legalności, minimalizacji, obowiązek informacyjny i wszystkie inne obowiązki jakie wiążą się z prawidłowym zabezpieczeniem danych osobowych.
3. Administrator w momencie planowania procesu zbierania i przetwarzania danych osobowych będzie dbał o to by prywatność była „ustawieniem domyślnym" a nie dodatkową funkcją. Przykładowo, użytkownik nie powinien podejmować działań dodatkowych po to by jego prywatność była chroniona, gdyż ustawienia fabryczne mają mu to zapewnić.
4. Administrator w momencie planowania procesu zbierania i przetwarzania danych osobowych będzie dbał o to by:
   1) ilość zbieranych danych była ograniczona do niezbędnego minimum;

2) dane i zależności między nimi nie były widoczne dla osób mających do nich dostęp (dodatkowe działanie w celu dostępu do danych)
3) dochodziło do przetwarzania danych z możliwością ich zakwalifikowania do odrębnych zbiorów
4) o ile to możliwe, aby nie następowały jego dalsze przekazywanie.