Polityka Ochrony Danych Osobowych w firmieFHU ITA Izabela Tajstra

1 Wstęp

PolitykaOchrony Danych Osobowych jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez Administratora w celu spełnienia wymagań Rozporządzenia PE i RE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO).

Polityka stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z powyższym Rozporządzeniem.

2 Analiza ryzyka

Procedura opisuje sposób przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń wynikających z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

Przyjęto, że analiza ryzyka przeprowadzana jest dla zbioru lubgrupy zbiorów (kategorii osób) lub dla procesów przetwarzania

2.1 Definicje

1. Aktywa – środki materialne i niematerialne mające wpływ na przetwarzanie danych osobowych
2. Naruszenie (Incydent) ochrony danych osobowych – to 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
3. Zagrożenie – potencjalne naruszenie (potencjalny incydent)
4. Skutki – rezultaty niepożądanego incydentu (straty w wypadku wystąpienia zagrożenia)
5. Ryzyko – prawdopodobieństwo, że określone zagrożenie wystąpi i spowoduje straty lub zniszczenie aktywów

2.2 Rejestr czynności przetwarzania(inwentaryzacja danych osobowych)

Administratorjest zobowiązany zgodnie z art. 30 RODO do prowadzenia rejestru czynności przetwarzania. Rejestr stanowi podstawę do przeprowadzenia analizy ryzyka.

1. Administrator prowadzi rejestr zgodnie z załącznikiem 01a Rejestr czynności przetwarzania (wykaz zbiorów danych osobowych)

2.3 Wyznaczenie zagrożeń

1. Administrator jest odpowiedzialny za określenie listy zagrożeń naruszenia poufności, dostępności i integralności, które mogą wystąpić podczas przetwarzania danych osobowych
2. Zagrożenia powinny być identyfikowane w odniesieniu do uprzednio zinwentaryzowanych zbiorów (kategorii osób), aktywów oraz procesów przetwarzania

2.4 Wyliczenie ryzyka dla zagrożeń

1. Administrator określa Prawdopodobieństwo (**P**) wystąpienia poszczególnych zagrożeń w zbiorze (dla kategorii osób) lub w procesie przetwarzania
2. Proponowaną skalę prawdopodobieństwa prezentuje Tabela A
3. Administrator określa Skutki (**S**) wystąpienia incydentów (materializacji zagrożeń), uwzględniając straty finansowe, utratę reputacji, sankcje/skutki karne
4. Proponowaną Skalę skutków prezentuje Tabela B

5. Administrator wylicza Ryzyka (R) dla wszystkich zagrożeń i ich skutków w/g formuły: **R = P * S**

Tabela A PRAWDOPODOBIEŃSTWO WYSTĄPIENIA ZAGROŻENIA	**SKALA (WAGA)**

zagrożenie niskie	1
zagrożenie średnie	2
zagrożenie wysokie	3

Tabela B SKUTKI WYSTĄPIENIA ZAGROŻENIA	**SKALA (WAGA)**
małe (do 10000 PLN, incydent prasowy lokalny)	1
średnie (10000-100000 PLN, incydent prasowy ogólnopolski)	2
duże (od 100000 PLN, naruszenie prawa)	3

2.4.1 Porównanie wyliczonych ryzyk ze skalą i określenie dalszego postępowania z ryzykiem

1. Administrator porównuje wyliczone ryzyka ze skalą i podejmuje decyzje dotyczące dalszego postępowania z ryzykiem
2. Proponowaną skalę Ryzyka prezentuje Tabela C

Tabela C POZIOM RYZYKA	**WARTOŚĆ [R = P*S]**
ryzyko pomijalne i akceptowalne (akceptujemy)	1-2
ryzyko jest opcjonalne (akceptujemy albo obniżamy)	3-6
ryzyko jest nieakceptowalne (musimy obniżyć)	9

2.4.2 Reakcja na wartość ryzyka

1. Akceptacja ryzyka – zabezpieczenia są właściwe – brak potrzeby stosowania dodatkowych zabezpieczeń
2. Działania obniżające ryzyko, które może zastosować Administrator:
    1. Przeniesienie –przerzucenie ryzyka (outsourcing, ubezpieczenie)
    2. Unikanie – eliminacja działań powodujących ryzyko
3. Redukcja – zastosowanie zabezpieczeń w celu obniżenia ryzyka

4. Analizę ryzyka przeprowadza się w specjalnym szablonie 02e Arkusz analizy ryzyka RODO

2.4.3 Ponowna analiza ryzyka

Ponowna analiza ryzyka przeprowadzana jest cyklicznie lub po znaczących zmianach w przetwarzaniu danych (np. przetwarzanie nowych zbiorów, nowych procesów przetwarzania, zmiany prawne)

2.5 Plan postępowania z ryzykiem

1. Wszędzie, gdzie Administrator decyduje się obniżyć ryzyko, wyznacza listę zabezpieczeń do wdrożenia, termin realizacji i osoby odpowiedzialne, patrz 02f Plan postępowania z ryzykiem

1. Administrator zobowiązany jest do monitorowania wdrożenia zabezpieczeń

3 Upoważnienia

1. Administratorodpowiada za nadawanie / anulowanie upoważnień do przetwarzania danych w zbiorach (dla kategorii osób) w postaci papierowej oraz w systemach informatycznych
2. Każda osoba upoważniona musi przetwarzać dane wyłącznie na polecenie administratora lub na podstawie przepisu prawa
3. Upoważnienia nadawane są w formie udokumentowanego zakresu obowiązków. Upoważnienia określają zakres operacji na danych, np. tworzenie, usuwanie, wgląd, przekazywanie – patrz załącznik 01d Upoważnienie do przetwarzania danych osobowych .
4. Administrator prowadzi ewidencję osób upoważnionych w celu sprawowania kontroli nad prawidłowym dostępem do danych osób upoważnionych. Ewidencja ma charakter pomocniczy i nie jest wymagana przepisami RODO. Patrz załącznik 01c Ewidencja osób upoważnionych.
5. W przypadku powierzenia przetwarzania danych do Podmiotu przetwarzającego, Administrator jest zobowiązany do sporządzenia z nim umowy powierzenia, stanowiącą podstawę upoważnienia dla osób z Podmiotu przetwarzającego – patrz załącznik 01f Umowa powierzenia uniwersalna

4 Środki techniczne i organizacyjne zabezpieczające dane osobowe

1. Administrator prowadzi wykaz zabezpieczeń, które stosuje w celu ochrony danych osobowych, patrz załącznik Instrukcja zarządzania RODO
2. W instrukcji wskazano stosowane zabezpieczenia proceduralne oraz zabezpieczenia jako środki techniczne i organizacyjne
3. Instrukcja jest aktualizowana, jeśli zajdzie taka potrzeba po przeprowadzeniu analizy ryzyka

5 Regulamin Ochrony Danych Osobowych

Regulamin ma na celu zapewnienie wiedzy osobom przetwarzającym dane osobowe odnośnie bezpiecznych zasad przetwarzania. Patrz załącznik – 04 Regulamin Ochrony Danych Osobowych

Po zapoznaniu się z zasadami ochrony danych osobowych, osoby zobowiązane są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania poprzez podpisanie oświadczenia o poufności zawartego w arkuszu 01c Ewidencja osób upoważnionych

6 Instrukcja postępowania z incydentami

Procedura definiuje katalog podatności i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Jej celem jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa oraz ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadamiania o stwierdzeniu podatności lub wystąpieniu incydentu bezpośredniego przełożonego (lub jeśli jest powołany – Inspektora Ochrony Danych)
2. Do typowych podatności bezpieczeństwa danych osobowych należą:
    1. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów
    2. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych
    3. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek)
3. Do typowych incydentów bezpieczeństwa danych osobowych należą:
    1. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności)
    2. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych)
    3. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania)
4. W przypadku stwierdzenia wystąpienia incydentu, Administrator (lub w przypadku powołania – IOD) prowadzi postępowanie wyjaśniające w toku, którego:
    1. ustala zakres i przyczyny incydentu oraz jego ewentualne skutki
    2. inicjuje ewentualne działania dyscyplinarne
    3. działa na rzecz przywrócenia działań organizacji po wystąpieniu incydentu
    4. rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia
5. Administrator dokumentuje powyższe wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze –patrz załącznik 03 Formularz rejestracji incydentu
6. Zabrania się świadomego lub nieumyślnego wywoływania incydentów przez osoby upoważnione do przetwarzania danych
7. W przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu.

Skrócony Regulamin Ochrony Danych Osobowych

w firmie FHU ITA Izabela Tajstra

Niniejszy regulamin stanowi wykaz podstawowych obowiązków z zakresu przestrzegania zasad ochrony danych osobowych zgodnie z przepisami RODO dla:

- Pracowników
- Współpracowników
- Pracowników podmiotów trzecich, posiadających dostęp do danych osobowych przetwarzanych przez Administratora / Podmiot przetwarzający
- Użytkowników systemów informatycznych z dostępem do danych osobowych przetwarzanych przez Administratora / Podmiot przetwarzający

Każda z w/w osób powinna zapoznać się z poniższym regulaminem oraz zobowiązać się do stosowania zasad w nim zawartych

SPIS TREŚCI

1 Zasady bezpiecznego użytkowania sprzętu IT, dysków, programów

1. Użytkownik odpowiada za zabezpieczenie przed zniszczeniem, uszkodzeniem oraz utratą sprzętu IT (komputerów, urządzeń biurowych, tabletów i smartfonów)
2. Demontaż, instalowanie lub podłączanie dodatkowych urządzeń jest zabronione
3. Użytkownik jest zobowiązany do usuwania tymczasowych plików z nośników/dysków z miejsc, gdzie dostęp do nich miałyby osoby nieupoważnione
4. Użytkownik jest zobowiązany do przekazania informatykowi nośników przeznaczonych do zniszczenia

2 Zarządzanie uprawnieniami – procedura rozpoczęcia, zawieszenia i zakończenia pracy

1. Każdy użytkownik komputerów, programów i systemu operacyjnego zobowiązany jest do pracy na własnym koncie. Zabronione jest udostępnianie konta innemu użytkownikowi
2. Użytkownik nie może zmieniać swoich uprawnień, np. zostać Administratorem na swoim komputerze
3. Użytkownik komputera oraz programów rozpoczyna i kończy pracę logowaniem i wylogowaniem się

1. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. klientom, pracownikom innych działów) wglądu do danych wyświetlanych na monitorach – tzw. **Polityka czystego ekranu**
2. Użytkownik przed tymczasowym odejściem od komputera musi włączyć wygaszacz ekranu (**WINDOWS + L**) lub wylogować się z systemu bądź z programu.

6. Zabrania się uruchamiania jakiejkolwiek aplikacji lub programu na prośbę innej osoby, o ile nie została ona zweryfikowana jako bezpieczna przez administratora. Dotyczy to zwłaszcza programów przesłanych za pomocą poczty elektronicznej lub wskazanych w formie odnośnika internetowego.

1. Po zakończeniu pracy, użytkownik zobowiązany jest wylogować się z systemu informatycznego oraz zabezpieczyć nośniki elektroniczne, magnetyczne i optyczne na których znajdują się dane osobowe

3 Polityka haseł

1. Hasła powinny składać się z min 8 znaków lub min 4 cyfrowego PIN-u.
2. Hasła powinny zawierać duże litery + małe litery + cyfry (lub znaki specjalne)
3. Hasła nie mogą być łatwe do odgadnięcia. Nie powinny być powszechnie używanymi słowami.
4. 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 lub w szufladzie
5. W przypadku ujawnienia hasła – należy natychmiast go zmienić
6. Hasła muszą być zmieniane raz na pół roku.
7. Jeżeli system nie wymusza zmiany haseł, użytkownik zobowiązany jest do samodzielnej zmiany hasła

4 Zabezpieczenie dokumentacji papierowej z danymi osobowymi

1. Pracownicy są zobowiązani do stosowania tzw. „**Polityki czystego biurka**”. Polega ona na zabezpieczaniu (zamykaniu na klucz) dokumentów oraz nośników np. w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób postronnych

2. Pracownicy zobowiązani są do niszczenia dokumentów i wydruków w niszczarkach
3. Zabrania się pozostawiania dokumentów w miejscach dostępnych dla osób postronnych
4. Zabrania się wyrzucania niezniszczonych dokumentów na śmietnik

5 Zasady wynoszenia nośników z danymi poza firmę

1. Użytkownicy nie mogą wynosić na zewnątrz niezaszyfrowanych nośników z danymi osobowymi (np. przenośnych dysków twardych, pendrive, płyt CD, DVD, pamięci typu Flash)
2. Dane osobowe wynoszone poza organizację muszą być zaszyfrowane (szyfrowane dyski przenośne, za hasłowane pliki, zabezpieczone smartfony)
3. Należy zapewnić bezpieczne przewożenie dokumentacji papierowej w plecakach, teczkach w celu zabezpieczenia ich przed zagubieniem i kradzieżą

6 Zasady korzystania z internetu

1. Zabrania się instalowania programów z Internetu bez konsultacji z informatykiem
2. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez takie oprogramowanie
3. Zabrania się wchodzenia na strony z nielegalnym oprogramowaniem do pobrania oraz na hackerskie
4. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł

7 Zasady korzystania z poczty elektronicznej

1. Pliki w danymi osobowymi w Wordzie, Excelu, w Pdf lub spakowane (7zip), przed wysłaniem ich do osób trzecich powinny być za hasłowane a hasło powinno być przesłane do odbiorcy telefonicznie lub SMS
2. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 10 znaków: duże i małe litery i cyfry lub znaki specjalne
3. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu
4. **WAŻNE:**Nie otwierać załączników (.zip, .rar, .xlsm, .pdf, .exe) w mailach!!!!! Są to zwykle „wirusy", które infekują komputer oraz często pozostałe komputery w sieci.
5. **WAŻNE:**Nie wolno „klikać" na hiperlinki w mailach, gdyż mogą to być hiperlinki do stron z „wirusami". Użytkownik „klikając" na taki hiperlink infekuje komputer oraz inne komputery w sieci.
6. Należy zgłaszać informatykowi przypadki podejrzanych e-maili
7. Użytkownicy nie powinni rozsyłać „niezawodowych" e-maili w formie „łańcuszków szczęścia"
8. 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"!
9. Użytkownicy powinni okresowo kasować niepotrzebne maile
10. Zakazuje się wysyłania korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych osób
11. Użytkownik bez zgody Pracodawcy / Zleceniodawcy nie ma prawa wysyłać wiadomości zawierających dane osobowe dotyczące Pracodawcy / Zleceniodawcy, jego pracowników, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej

8 Skrócona instrukcja postępowania w przypadku naruszenia ochrony danych osobowych

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadomienia Pracodawcy / Zleceniodawcy w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych

2. Do sytuacji wymagających powiadomienia, należą:
    1. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów
    2. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych
    3. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek)
3. Do incydentów wymagających powiadomienia, należą:
    1. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności)
    2. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych)
    3. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania)
4. Typowe przykłady incydentów wymagające reakcji:

1.
    1. ślady na drzwiach, oknach i szafach wskazują na próbę włamania
    2. dokumentacja jest niszczona bez użycia niszczarki
    3. fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie
    4. otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe
    5. ustawienie monitorów pozwala na wgląd osób postronnych w dane osobowe
    6. wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz organizacji bez upoważnienia Pracodawcy / Zleceniodawcy
    7. udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej i ustnej
    8. telefoniczne próby wyłudzenia danych osobowych
    9. kradzież, zagubienie komputerów lub CD, twardych dysków, Pendrive z danymi osobowymi
    10. maile zachęcające do ujawnienia identyfikatora i/lub hasła,
    11. pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów
    12. hasła do systemów przyklejone są w pobliżu komputera

9 Obowiązek zachowania poufności i ochrony danych osobowych

1. Każda z osób dopuszczonych do przetwarzania danych osobowych jest zobowiązana do:

    1. przetwarzania danych osobowych wyłącznie w celu i zakresie powierzonych jej zadań
    2. zachowania w tajemnicy danych osobowych do których ma
    3. niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych jej zadań
    4. zachowania w tajemnicy sposobów zabezpieczenia danych osobowych
2. Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym lub osobom których tożsamości nie można zweryfikować lub osobom podszywającym się pod kogoś innego
3. Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać się jasną podstawą prawną do dostępu do takich danych
4. Każda z osób dopuszczonych do przetwarzania danych osobowych jest zobowiązana zabezpieczenia danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem

10 Postępowanie dyscyplinarne

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy
2. Postępowanie sprzeczne z powyższymi zobowiązaniami, może też być uznane przez Pracodawcę / Zleceniodawcę za naruszenie przepisów karnych zawartych w ogólnym Rozporządzeniu o ochronie danych UE z dnia 27 kwietnia 2016 r.