Polityka Ochrony Danych Osobowych

Niniejszy dokument opisuje metody ochrony danych osobowych przetwarzanych przez administratora danych w ramach prowadzonej działalności zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady UE (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)

Opracował: Grzegorz Nowak
OchronaDanych.it

Spis Treści

Definicje

Zgodnie z definicjami zawartymi w treści rozporządzenia Parlamentu Europejskiego i Rady Europy UE 2016/679 w niniejszej polityce stosuje się poniższe definicje:

1. „dane osobowe” oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
2. „przetwarzanie” oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką 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;
3. „ograniczenie przetwarzania” oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
4. „profilowanie” oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
5. „pseudonimizacja” oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
6. „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;
7. „administrator” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;
8. „podmiot przetwarzający” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
9. „odbiorca” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;
10. „strona trzecia” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy

osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe;

11. „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;
12. „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;
13. „dane genetyczne” oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej;
14. „dane biometryczne” oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;
15. „dane dotyczące zdrowia” oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia;
16. „główna jednostka organizacyjna” oznacza:
    a. jeżeli chodzi o administratora posiadającego jednostki organizacyjne w więcej niż jednym państwie członkowskim – miejsce, w którym znajduje się jego centralna administracja w Unii, a jeżeli decyzje co do celów i sposobów przetwarzania danych osobowych zapadają w innej jednostce organizacyjnej tego administratora w Unii i ta jednostka organizacyjna ma prawo nakazać wykonanie takich decyzji, to za główną jednostkę organizacyjną uznaje się jednostkę organizacyjną, w której zapadają takie decyzje;
    b. jeżeli chodzi o podmiot przetwarzający posiadający jednostki organizacyjne w więcej niż jednym państwie członkowskim – miejsce, w którym znajduje się jego centralna administracja w Unii lub, w przypadku gdy podmiot przetwarzający nie ma centralnej administracji w Unii – jednostkę organizacyjną podmiotu przetwarzającego w Unii, w której odbywają się główne czynności przetwarzania w ramach działalności jednostki organizacyjnej podmiotu przetwarzającego, w zakresie w jakim podmiot przetwarzający podlega szczególnym obowiązkom na mocy niniejszego rozporządzenia;
17. „przedstawiciel” oznacza osobę fizyczną lub prawną mającą miejsce zamieszkania lub siedzibę w Unii, która została wyznaczona na piśmie przez administratora lub podmiot przetwarzający na mocy art. 27 do reprezentowania administratora lub podmiotu przetwarzającego w zakresie ich obowiązków wynikających z niniejszego rozporządzenia;
18. „przedsiębiorca” oznacza osobę fizyczną lub prawną prowadzącą działalność gospodarczą, niezależnie od formy prawnej, w tym spółki osobowe lub zrzeszenia prowadzące regularną działalność gospodarczą;
19. „grupa przedsiębiorstw” oznacza przedsiębiorstwo sprawujące kontrolę oraz przedsiębiorstwa przez nie kontrolowane;
20. „wiążące reguły korporacyjne” oznaczają polityki ochrony danych osobowych stosowane przez administratora lub podmiot przetwarzający, którzy posiadają jednostkę organizacyjną na terytorium państwa członkowskiego, przy jednorazowym lub wielokrotnym przekazaniu

danych osobowych administratorowi lub podmiotowi przetwarzającemu w co najmniej jednym państwie trzecim w ramach grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą;

21. „organ nadzorczy” oznacza niezależny organ publiczny ustanowiony przez państwo członkowskie zgodnie z art. 51;
22. „organ nadzorczy, którego sprawa dotyczy” oznacza organ nadzorczy, którego dotyczy przetwarzanie danych osobowych, ponieważ:
    a. administrator lub podmiot przetwarzający posiadają jednostkę organizacyjną na terytorium państwa członkowskiego tego organu nadzorczego;
    b. przetwarzanie znacznie wpływa lub może znacznie wpłynąć na osoby, których dane dotyczą, mające miejsce zamieszkania w państwie członkowskim tego organu nadzorczego; lub
    c. wniesiono do niego skargę;
23. „transgraniczne przetwarzanie” oznacza:
    a. przetwarzanie danych osobowych, które odbywa się w Unii w ramach działalności jednostek organizacyjnych w więcej, niż jednym państwie członkowskim administratora lub podmiotu przetwarzającego w Unii posiadającego jednostki organizacyjne w więcej niż jednym państwie członkowskim; albo
    b. przetwarzanie danych osobowych, które odbywa się w Unii w ramach działalności pojedynczej jednostki organizacyjnej administratora lub podmiotu przetwarzającego w Unii, ale które znacznie wpływa lub może znacznie wpłynąć na osoby, których dane dotyczą, w więcej niż jednym państwie członkowskim;
24. „mający znaczenie dla sprawy i uzasadniony sprzeciw” oznacza sprzeciw wobec projektu decyzji dotyczącej tego, czy doszło do naruszenia niniejszego rozporządzenia lub czy planowane działanie wobec administratora lub podmiotu przetwarzającego jest zgodne z niniejszym rozporządzeniem, który to sprzeciw musi jasno wskazywać wagę wynikającego z projektu decyzji ryzyka naruszenia podstawowych praw lub wolności osób, których dane dotyczą, oraz gdy ma to zastosowanie – wagę ryzyka zakłócenia swobodnego przepływu danych osobowych w Unii;
25. „usługa społeczeństwa informacyjnego” oznacza usługę w rozumieniu art. 1 ust. 1 lit. b) dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/1535 (1);
26. „organizacja międzynarodowa” oznacza organizację i organy jej podlegające działające na podstawie prawa międzynarodowego publicznego lub inny organ powołany w drodze umowy między co najmniej dwoma państwami lub na podstawie takiej umowy.

Obowiązki Administratora Danych Osobowych

Administrator

Administratorem Danych Osobowych jest Szkoła Podstawowa nr 2 im. Kadm. Włodzimierza Steyera , ul. 1000-lecia PP 2, 84-120 Władysławowo. Administrator przetwarza dane osobowe zgodnie z artykułem 6 RODO, ustęp 1, litera c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze, oraz litera e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

Charakter przetwarzania

Przetwarzanie danych osobowych osób fizycznych jest niezbędne do realizacji statutowych celów administratora danych osobowych. Charakter przetwarzania nie jest sporadyczny i powiązany jest ściśle ze szczególnymi przepisami prawa.

Zakres przetwarzania

Administrator przetwarza dane osobowe w zakresie przewidzianym w przepisach szczególnych, a także na podstawie zgód udzielonych przez osoby fizyczne. Kontekst przetwarzania

Cele przetwarzania

Szczególne cele przetwarzania danych osobowych osób fizycznych opisane są w rejestrze zbiorów danych osobowych oraz rejestr czynności przetwarzania. Dla każdego zbioru danych przetwarzanego na podstawie szczególnych przepisów prawa cele są indywidualne i opisane w załączniku.

Ryzyko naruszenia praw lub wolności osób fizycznych

Administrator danych osobowych zgodnie z zapisami artykułu 32 RODO dokonał analizy ryzyka naruszenia praw lub wolności osób których dane dotyczą, a wyniki analizy zamieszczone zostały w rejestrze ryzyk dla każdego ze zbiorów indywidualnie.

Obowiązek informacyjny

Administrator danych osobowych zgodnie z wymogami wynikającymi z artykułu 12 i 13 oraz 14 rozporządzenia wywiązuje się z obowiązku informacyjnego wobec osób których dane dotyczą poprzez:

1. Opublikowanie informacji wymaganych w artykule 13 oraz 14 na tablicach ogłoszeń oraz przy wejściu do strefy przetwarzania.
2. Opublikowanie informacji wymaganych w artykule 13 oraz 14 na stronie internetowej administratora danych.
3. Opublikowanie informacji wymaganych w artykule 13 oraz 14 na biuletynie informacji publicznej administratora danych.
4. Informowanie o przetwarzaniu danych osobowych przed rozpoczęciem ich przetwarzania wobec każdej osoby fizycznej indywidualnie.

Informacje o których mowa powyżej mają charakter zwięzły, pisany jasnym i prostym językiem zgodnie z wymogami artykułu 12 rozporządzenia.

Kodeksy postępowań.

Z uwagi na brak w jakichkolwiek kodeksów postępowań wydrążonych przez podmiot prowadzący w dniu wejścia w życie niniejszej polityki ochrony danych osobowych, administrator odstąpił od stosowania wyżej wymienionych kodeksów postępowań, tym samym nie ma zastosowania artykuł 40 rozporządzenia.

Certyfikacja.

Z uwagi na fakt że administrator jest podmiotem publicznym, finansowanym ze środków publicznych systemy certyfikacji omawiane w artykule 43 nie ma zastosowania, zatem administrator odstąpił od stosowania procedur certyfikacji opisanych w rozporządzeniu.

Analiza zasobów zbiorów danych osobowych

Aby zdefiniować zakres i cele przetwarzania dokonuje się analizy przetwarzanych danych osobowych na podstawie inwentaryzacji przetwarzanych zbiorów. W wyniku inwentaryzacji ustala się:

- miejsce przetwarzania
- cel przetwarzania
- zakres danych przetwarzanych
- sposób ich zabezpieczenia
- metody przetwarzania.

Zakres przetwarzanych danych obrazuje:

1. Rejestr zbiorów danych osobowych
2. Rejestr czynności przetwarzania
3. Rejestr pomieszczeń przetwarzania

Zarządzanie ryzykiem

Opierając się na opisanych w normie ISO 27005: 2014 metodach zarządzania ryzykiem wprowadza się cykl polegający na:

1. szacowaniu ryzyka,
2. postępowaniu z ryzykiem,
3. akceptowaniu ryzyka,
4. monitorowaniu ryzyka,
5. informowaniu o ryzyku

Na potrzeby niniejszego rozdziału wprowadza się dodatkowo następujące definicje:

Definicje

1. akceptacja ryzyka - decyzja uprawnionej osoby o zaniechaniu działań mających na celu zmianę poziomu ryzyka
2. analiza ryzyka - systematyczne podejście mające na celu zidentyfikowanie w systemie źródeł ryzyka i przypisanie zidentyfikowanym ryzykom wartości
3. estymacja ryzyka - proces przypisywania wartości poziomowi ryzyka
4. dostępność informacji - właściwość polegającą na tym, że informacja jest możliwa do wykorzystania przez uprawniony podmiot na jego żądanie, w założonym czasie
5. identyfikowanie ryzyka - proces znajdowania, zestawiania i charakteryzowania przyczyn ryzyka w systemie
6. incydent - pojedyncze niepożądane lub niespodziewane zdarzenie związane z bezpieczeństwem informacji lub seria takich zdarzeń, które stwarzają znaczne

prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji
7. informowanie o ryzyku - wymiana lub dzielenie się informacjami o ryzyku między interesariuszami systemu
8. integralność informacji - właściwość polegającą na tym, że informacja nie została zmodyfikowana w sposób nieuprawniony
9. interesariusz - osoba lub organizacja, która może wpływać, na którą można wpływać lub która postrzega siebie jako zależną od podejmowanych decyzji lub działań
10. końcowy poziom ryzyka - poziom ryzyka pozostający po procesie postępowania z ryzykiem
11. materializacja zagrożenia - stan, w którym zagrożenie oddziałuje na system
12. ocena ryzyka - proces porównywania wartości ryzyka z określonymi kryteriami w celu określenia znaczenia ryzyka
13. podatność - słabość aktywu (zasobu) lub zabezpieczenia, która może być wykorzystana przez co najmniej jedno zagrożenie
14. postępowanie z ryzykiem - proces wyboru i wdrażania środków sterowania ryzykiem mających na celu zmianę wartości poziomu ryzyka
15. poziom ryzyka - produkt operacji na wartości przypisanej skutkowi i wartości związanej z prawdopodobieństwem zaistnienia zdarzenia powodującego skutek
16. poufność informacji - właściwość polegająca na tym, że informacja nie jest udostępniana ani ujawniana nieautoryzowanym osobom, podmiotom lub procesom
17. ryzyko - skutek niepewności w odniesieniu do ustalonego celu
18. ryzyko szczątkowe - ryzyko, którego poziom nie przekracza akceptowanej wartości
19. skutek - negatywna zmiana w odniesieniu do zaplanowanego poziomu miernika celu w wyniku oddziaływania zagrożenia
20. szacowanie ryzyka - całościowy proces analizy i oceny ryzyka
21. właściciel ryzyka - osoba odpowiedzialna za zarządzanie danym ryzykiem w systemie
22. zagrożenie - potencjalna przyczyna niepożądanego oddziaływania na system
23. zarządzanie ryzykiem - skoordynowane działania mające na celu kierowanie i sterowanie ryzykiem w systemie
24. zdarzenie - wystąpienie lub zmiana konkretnego zestawu okoliczności

Identyfikacja i analiza ryzyk

1. Proces identyfikacji ryzyka rozpoczyna się od etapu analizy zasobów przeprowadzonej przez inspektora ochrony danych lub administratora, oraz pracowników merytorycznych.
2. Następnie lista zasobów przekazywana jest w celu analizy ryzyka inspektorowi ochrony danych bądź wyznaczonej przez administratora osobie posiadającej kompetencje w zakresie wykonania analizy ryzyka.
3. Na analizę ryzyka składa się:
    a. szacowanie następstw
    b. szacowanie prawdopodobieństwa
    c. określenie poziomu ryzyka
4. Osoba dokonująca analizy ryzyka sporządza wykaz podatności. Wykaz podatności poddawany jest okresowym przeglądom.
5. Wykaz podatności jest integralną częścią dokumentu zawierającą analiza ryzyka.

Szacowanie prawdopodobieństwa

W wyniku szacowania prawdopodobieństwa osoba dokonująca analizy ryzyka bierze pod uwagę częstotliwość występowanie podobnych ryzyk w podobnej branży w jakiej dokonywana jest analiza ryzyka dla podobnych podatności. Do prawidłowego oszacowania prawdopodobieństwa wystąpienia ryzyka należy także wziąć pod uwagę:

1. doświadczenie osoby dokonującej szacowania prawdopodobieństwa
2. położenie geograficzne siedziby administratora w której przetwarzane są dane
3. istniejące zabezpieczenia
4. dla ryzyka zależnych od czynnika ludzkiego atrakcyjność zasobu

Szacowanie następstw

W wyniku szacowania następstw osoba dokonująca analizy ryzyka sporządza wykaz skutków jakie nieść może materializacja zagrożeń z uwzględnieniem prawdopodobieństwa ich wystąpienia oraz podatności.

Określenie poziomu ryzyka

Osoba dokonująca analizy ryzyka określa poziom ryzyka na podstawie przypisanie wartości następującym parametrom:

1. dostępność systemu lub informacji,
2. integralność systemu lub informacji,
3. poufność informacji przetwarzanej w systemie,

Poziom ryzyka wyznacza się według następującego wzoru:

$$Rp = P \times (Sd + Si + Sp)$$

gdzie:
Rp – pierwotny poziom ryzyka,
P – wartość przypisana prawdopodobieństwu materializacji zagrożenia,
Sd – wartość przypisana skutkowi dla dostępności informacji,
Si – wartość przypisana skutkowi dla integralności informacji,
Sp – wartość przypisana skutkowi dla poufności informacji,

P∈{0,1,2,3,4} gdzie:
0 – zdarzenie nieprawdopodobne (zagrożenie nie występuje),
1 – zdarzenie prawie nieprawdopodobne,
2 – zdarzenie mało prawdopodobne,
3 – zdarzenie wysoce prawdopodobne,
4 – zdarzenie niemal pewne.

(Sd, Si, Sp)∈{0,1,2,3,4} gdzie:
0 – zdarzenie nie powoduje skutku (brak podatności),
1 – zdarzenie wywołuje niewielki skutek,
2 – zdarzenie wywołuje znaczący skutek,
3 – zdarzenie wywołuje bardzo znaczący skutek,
4 – zdarzenie wywołuje skutek katastrofalny.

Ocena ryzyka

W końcowej części należy ocenić ryzyka porównując wyznaczony poziom ryzyka z ustalonymi wstępnie kryteriami akceptowania ryzyka. Kryteria akceptacji ustala administrator danych osobowych. Ryzyka w których wartość pierwotnego poziomu jest niższa lub równa 20% poziom maksymalnego poznaje się z ryzyka szczątkowy i nie poddaję się w procedurze postępowania z ryzykiem.

Postępowanie z ryzykiem

Postępowanie z ryzykiem polega na:

1. sterowaniu ryzykiem,
2. unikaniu ryzyka,
3. przeniesieniu ryzyka,
4. akceptacji ryzyka mimo, że jego poziom przekracza poziom ryzyka szczątkowego

Sterowanie ryzykiem

Jednym ze środków sterowanie ryzykiem jest wprowadzenie odpowiedniego zabezpieczenia w celu minimalizacji ryzyka. po wprowadzeniu zabezpieczenia dokonuje się ponownej analizy ryzyka według poniższego wzoru:

$$Rk = Px\left(\frac{Sd}{Cd} + \frac{Si}{C1} + \frac{Sp}{Cp}\right)$$

gdzie:
Rk – końcowy poziom ryzyka,
P, Sd, Si, Sp zdefiniowane uprzednio
C – skuteczność zabezpieczenia,
(Cd,Ci,Cp)∈ {1,2,3,4}
gdzie:
1 – brak zabezpieczenia,
2 – zabezpieczenie ogranicza poziom ryzyka,
3 – zabezpieczenie w istotny sposób ogranicza poziom ryzyka,
4 – zabezpieczenie w bardzo istotny sposób ogranicza poziom ryzyka.

Zastosowanie zabezpieczenia musi uwzględniać wpływ zastosowania zabezpieczenia na pozostałe atrybuty bezpieczeństwa i samo w sobie może stanowić czynnik ryzyka. Przykładowo: zastosowanie zabezpieczenia ograniczającego ryzyko utraty poufności może spowodować podniesienie ryzyka utraty dostępności. W takim przypadku należy powrócić do estymacji początkowego poziomu ryzyka z uwzględnieniem zastosowanego zabezpieczenia.

Unikanie ryzyka

W przypadku realizacji zadań publicznych unikanie ryzyka, co do zasady, nie ma zastosowania.

Przeniesienie ryzyka

W przypadku realizacji zadań publicznych przeniesienie ryzyka, co do zasady, nie ma zastosowania. Niemniej przeniesienie ryzyka może być zasadne w postaci ubezpieczenia składników majątkowych systemu.

Akceptacja ryzyka

W wyniku przeliczenia poziomów ryzyk uzyskuje się wartość końcową poziomu ryzyka. Ryzyka, dla których końcowy poziom ryzyka jest niższy lub równy 20% poziomu maksymalnego (Rk ≤ 9,6) podlegają automatycznej akceptacji, ale pozostają pod nadzorem właściciela ryzyka w celu ich monitorowania. Ryzyka dla których poziom zawiera się w przedziale 9,6 < Rk ≤ 38,4 podlegają akceptacji według zasad ustalonych w podmiocie lub dokonywana jest ich ponowna analiza. Ryzyka dla których poziom ryzyka jest większy od 80% poziomu maksymalnego (Rk > 38,4), przedstawiane są do akceptacji administratorowi danych osobowych

Informowanie o ryzyku

Ryzyka których administrator nie będzie w stanie zniwelować poprzez Zarządzanie ryzykiem Lecz nadal wykazuje wody przetwarzania danych zobowiązany jest zgłosić prezesowi urzędu ochrony danych osobowych w drodze konsultacji poprzez inspektora ochrony danych bądź osobiście.

Dokumentacja szacowania poszczególnych ryzyk zawarta jest dokumencie Rejestr Ryzyk stanowiącym załącznik niniejszej polityki ochrony danych osobowych.

Środki ochrony

Administrator danych osobowych w celu dostosowania ochrony do wymogów rozporządzenia stosuje następujące techniczne oraz organizacyjne środki ochrony:

Organizacyjne środki ochrony

Zgodnie z treścią rozporządzenia administrator w celu ochrony danych osobowych zapewnia następujące organizacyjne środki ochrony danych.

1. Każda osoba będąca pracownikiem Administratora przetwarzająca dane osobowe zostaje do tego pisemnie upoważniona przez Administratora.
2. Administrator wydaje upoważnienie do przetwarzania na podstawie Wzoru upoważnienia do przetwarzania danych
3. Pracownik po uzyskaniu upoważnienia podpisuje oświadczenie zgodnie ze Wzorem oświadczenia osoby upoważnionej o zachowaniu poufności
4. Administrator prowadzi Rejestr upoważnień do Przetwarzania, w którym zawarte są informacje wskazujące zakres zbiorów oraz zakres czynności przetwarzania realizowanych przez upoważnioną osobę.
5. Upoważnieni pracownicy wpisani do Rejestru Upoważnień objęci są cyklicznymi szkoleniami z zakresu Ochrony Danych Osobowych. Inspektor Ochrony Danych weryfikuje wiedzę przeszkolonych pracowników.
6. Administrator powierzając przetwarzanie danych zewnętrznemu podmiotowi przetwarzającemu, niebędącemu pracownikiem Administratora, powierza przetwarzanie na podstawie wzoru umowy o powierzenie przetwarzania danych.
7. Administrator prowadzi Rejestr umów powierzenia przetwarzania

Techniczne środki ochrony

Administrator ze względu na rodzaj zastosowanych środków technicznych dzieli je na techniczne zabezpieczenia fizyczne oraz techniczne zabezpieczenia teleinformatyczne.

Techniczne zabezpieczenia fizyczne

1. Dokumenty zawierające dane osobowe poza godzinami pracy osób upoważnionych do przetwarzania danych zamykane są na klucz w szafkach w pomieszczeniach przetwarzania.
2. Pomieszczenia przetwarzania danych podczas nieobecności osób upoważnionych do przetwarzania danych a także poza godzinami pracy tych osób, zamykane są na klucz, a klucze przechowywane są w pomieszczeniu dozorowanym.
3. Strefa przetwarzania dozorowana jest całodobowo.

Techniczne zabezpieczenia teleinformatyczne.

1. Dane osobowe przetwarzane w informatycznych systemach dziedzinowych zabezpieczone są unikalnym loginem oraz hasłem dla każdego z użytkowników, certyfikatem lub zabezpieczeniem biometrycznym w którym dane biometryczne przechowywane są przez osobę przetwarzającą o której mowa. Powyższe pozwala spełnić wymogi rozliczalności i poufności przetwarzania danych osobowych.
2. Dane osobowe przetwarzane poza systemami dziedzinowymi w systemach teleinformatycznych sporządzane i przechowywane są w formie dokumentów elektronicznych pod kontrolą systemu operacyjnego posiadającego wsparcie producenta, w kontekście użytkownika systemu posiadającego indywidualny login oraz hasło. Powyższe pozwala spełnić wymogi rozliczalności i poufności przetwarzania danych osobowych,
3. Każde z urządzeń teleinformatycznych dla których dokonywane jest przetwarzanie danych osobowych zabezpieczone jest aktualnym systemem antywirusowym oraz zaporą sieciową. Powyższe pozwala na spełnienie zasady integralności danych.
4. Punkt styku sieci komputerowej z siecią internet zabezpieczony jest urządzeniem klasy UTM wyposażonym w procedury IPS, zaporę sieciową oraz opcjonalnie antywirusowym. Powyższe pozwala na spełnieniu zasady integralności oraz odporności, a także dostępności danych osobowych.
5. Dyski twarde oraz inne nośniki na których zachodzi przetwarzanie danych osobowych, wykorzystywane poza strefą przetwarzania zabezpieczone są poprzez szyfrowanie całości nośników metodą bitlocker lub równoważną.
6. Administrator nakłada na pracownika odpowiedzialnego za kwestie informatyczne obowiązek okresowych i cyklicznych przeglądów:
    a. wymienionych powyżej zabezpieczeń,
    b. dzienników zdarzeń systemów operacyjnych,
    c. dzienników zdarzeń systemów antywirusowych,
    d. dzienników zdarzeń zapory sieciowej
7. Wszystkie wykryte ślady incydentów oraz podatności pracownik odpowiedzialny za kwestie informatyczne bezzwłocznie zgłasza Administratorowi.

Ocena skutków przetwarzania danych

Administrator danych osobowych stwierdza iż ocena skutków przetwarzania danych konieczna jest jedynie dla zbioru monitoringu wizyjnego miejsc publicznych. Oceny skutków przetwarzania danych dokonano metodą PIA. Raport oceny skutków przetwarzania danych zawarty jest w załączniku.

Przeglądy

Na mocy artykułu 39 RODO Administrator upoważnia Inspektora Ochrony Danych do monitorowania, audytowania oraz dostosowania niniejszej polityki oraz procedur ochrony danych do bieżących zagrożeń ochrony danych osobowych

Załączniki

Integralną częścią niniejszego dokumentu jest poniższy zestaw załączników:

1. Rejestr zbiorów danych osobowych
2. Rejestr czynności przetwarzania
3. Rejestr pomieszczeń przetwarzania
4. Rejestr upoważnień do przetwarzania
5. Rejestr umów powierzenia przetwarzania
6. Rejestr ryzyk przetwarzania
7. Rejestr naruszeń ochrony danych osobowych
8. Wzór klauzuli informacyjnej
9. Wzór zgody na przetwarzanie
10. Wzór upoważnienia do przetwarzania danych
11. Wzór oświadczenia osoby upoważnionej o zachowaniu poufności
12. Wzór umowy o powierzenie przetwarzania danych
13. Raport oceny skutków przetwarzania danych

Dokumentację załączników prowadzi się w wersji elektronicznej.

Rejestr zmian dokumentu

Data	Wersja	Zakres zmian	Autor zmian
2018-05-21	1.0	wersja pierwotna	Grzegorz Nowak

Przedkładam (data i podpis sporządzającego dokument)	Zatwierdzam: (data i podpis Administratora Danych Osobowych)
Grzegorz Nowak Inspektor Ochrony Danych Signature Not Verified Dokument podpisany przez Grzegorz Nowak Data: 2018.05.24 23:54:07 CEST	