KSIĘGA POLITYK I ZASAD
dla Puławskiego Ośrodka Kultury

„Dom Chemika”

POK „Dom Chemika” zapewnia wszystkich swoich klientów oraz pracowników i osoby współpracujące o zachowaniu pełnej gwarancji bezpieczeństwa i poufności przekazywanych, posiadanych i pozyskiwanych informacji. W celu spełnienia tej deklaracji Administrator Danych wdrożył odpowiednie zasady i procedury, które są zawarte w Księdze Polityk i Zasad, której wyodrębniona część podlega udostępnieniu natomiast całość dokumentu jest przeznaczona tylko do użytku wewnętrznego z uwagi na zawarte w niej zabezpieczenia organizacyjno-techniczne.

Udostępnieniu podlegają następujące informacje:

1. Podstawa prawna

Księga Polityk i Zasad oraz inne dokumenty szczegółowe związane z bezpieczeństwem informacji opierają się na:

1. Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.U. UE L.2016.119.1), zwanym w dalszej części RODO.
2. Ustawie z dnia 10 maja 2018 roku o ochronie danych osobowych, zwanym w dalszej części (Dz.U. 2018 poz. 1000) zwaną w dalszej części ODO.
3. Ustawie z dnia 21 lutego 2019 r. (Dz.U. 2019 poz. 730) o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.
4. Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. 2005 nr 64 poz. 565).
5. Rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2012 poz. 526),
6. Rozporządzeniu Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz.U.2011 nr 14 poz. 67).
7. Ustawie z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. 2016 poz. 1764 z późn.zm.)
8. Ustawie z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz.U. 2003 nr 153, poz. 1503 z późn.zm.).

2. Definicje

Administrator Danych – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych,
Administrator Systemu Informatycznego – osoba zarządzająca systemem informatycznym, w którym przetwarzane są dane w tym dane osobowe.
Analiza ryzyka – proces dążący do określenia charakteru i poziomu ryzyka.
Bezpieczeństwo informacji – zachowanie poufności, integralności i dostępności informacji.

Dane osobowe – 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.
Hasło – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie.
Inspektor Ochrony Danych – osoba, którą wyznaczył Administrator Danych i powiadomił o tym fakcie Prezesa Urzędu Ochrony Danych Osobowych.
Integralność – właściwość polegająca na zapewnieniu dokładności i kompletności.
Integralność danych – właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
Identyfikator użytkownika – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych w systemie informatycznym.
Naruszenie ochrony danych osobowych (incydent ochrony danych) – 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;
Odbiorca – osoba fizyczna lub prawna, organ publiczny, jednostka 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 Europejskiej 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 co celów przetwarzania.
Osoba upoważniona – osoba posiadająca formalne upoważnienie wydane przez Administratora Danych lub osobą przez niego wyznaczoną.
Podatność – słabość aktywu lub zabezpieczenia, która może być wykorzystana przez co najmniej jedno zagrożenie.
Podmiot przetwarzający (procesor) – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane w imieniu Administratora Danych.
Postępowanie z ryzykiem – proces modyfikowania ryzyka.
Poufność danych – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom.
Prawdopodobieństwo – możliwość wystąpienia zdarzenia.
Przetwarzanie – operacja 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.
Pseudonimizacja – 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.
Rozliczalność – właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
Sieć publiczna – sieć telekomunikacyjna niebędąca siecią wewnętrzną, służąca do świadczenia usług telekomunikacyjnych.
Sieć telekomunikacyjna – urządzenia telekomunikacyjne i linie telekomunikacyjne, zestawione i połączone w sposób umożliwiający przekaz sygnałów pomiędzy określonymi zakończeniami sieci za

pomocą przewodów, fal radiowych bądź optycznych lub innych środków wykorzystujących energię elektromagnetyczną.
Strona trzecia – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający, czy osoby, które z upoważnienia administratora lub podmiotu przetwarzającego mogą przetwarzać dane osobowe.
System teleinformatyczny – sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych. System ten tworzy sieć telekomunikacyjną Administratora Danych.
Tajemnica przedsiębiorstwa – zgodnie z ustawą o zwalczaniu nieuczciwej konkurencji rozumie się „nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich w poufności. Dokumenty oraz informacje w nich zawarte, do których Administrator Danych podpisał umowy o zachowaniu ich w poufności.
Teletransmisja – przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej.
Uwierzytelnianie – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.
Użytkownik – osoba upoważniona do przetwarzania danych, której przyznano identyfikator i hasło.
Zabezpieczenie – środek, który modyfikuje ryzyko.
Zagrożenie – potencjalna przyczyna wystąpienia niepożądanego zdarzenia, które może wywołać szkodę w organizacji lub systemie.
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.
Zgoda osoby, której dane dotyczą – 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;
Zarządzanie incydentami związanymi z bezpieczeństwem informacji – procesy wykrywania, raportowania, szacowania, reagowania, podejmowania akcji i wyciągania wniosków z incydentów związanych z bezpieczeństwem informacji.
Zarządzanie ryzykiem – skoordynowane działania dotyczące kierowania i nadzorowania organizacji w odniesieniu do ryzyka.

3. Osoby odpowiedzialne za bezpieczeństwo informacji i przetwarzanie danych osobowych

3.1 Obowiązki Administratora Danych:

a) wdraża odpowiednie środki organizacyjne i techniczne aby przetwarzanie danych odbywało się zgodnie z prawem, z uwzględnieniem charakteru, kontekstu, zakresu i celu przetwarzania a ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia,
b) podejmuje decyzje o celach i środkach przetwarzania danych z uwzględnieniem przede wszystkim zmian w obowiązującym prawie, organizacji i technik zabezpieczania danych,
c) upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym zakresie, odpowiadającym zakresowi jej obowiązków,
d) powołuje Inspektora Ochrony Danych (art. 37 RODO).
e) wyznacza Administratora Systemu Informatycznego oraz określa zakres jego zadań i czynności,

f) prowadzi rejestr czynności przetwarzania i rejestr kategorii czynności przetwarzania zgodnie z art. 30 RODO. Administrator Danych może zlecić prowadzenie przedmiotowego rejestru Inspektorowi Ochrony Danych,
g) dokonuje oceny skutków planowanych operacji przetwarzania danych przed rozpoczęciem ich przetwarzania,
h) zgłasza naruszenia ochrony danych osobowych do organu nadzorczego oraz zawiadamiania o tym osoby, których te dane dotyczą.

3.2 Rola Inspektora Ochrony Danych

Inspektor Ochrony Danych pełni funkcję opiniodawczo-doradczo-weryfikacyjną i jest odpowiedzialny w szczególności za:

a) informowanie Administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy Rozporządzenia o Ochronie Danych Osobowych (RODO) oraz innych przepisów Unii Europejskiej lub państw członkowskich o ochronie danych osobowych i doradzanie im w tej sprawie,
b) monitorowanie przestrzegania RODO, innych aktów unijnych lub państw członkowskich, o ochronie danych osobowych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania danych osobowych oraz powiązane z tym audyty,
c) udzielanie na żądanie zaleceń do oceny skutków dla ochrony danych osobowych oraz monitorowanie jej wykonania,
d) współpracę z organem nadzorczym,
e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem,
f) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z uprzednimi konsultacjami jeżeli ocena skutków dla ochrony danych wskaże, że przetwarzanie powodowałoby wysokie ryzyko naruszenia praw lub wolności osób oraz w stosownych przypadkach prowadzenie konsultacji we wszystkich innych sprawach,
g) pełnienie roli punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy Rozporządzenia o Ochronie Danych Osobowych,
h) prowadzenie rejestru czynności lub kategorii czynności przetwarzania na zlecenie Administratora Danych.

3.3 Obowiązki Administratora Systemu Informatycznego

Administrator Systemu Informatycznego realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym Administratora Danych, szczegółowo określone w tej części dokumentu, która nie podlega udostępnieniu.

4. Podstawy przetwarzania danych osobowych

4.1 Przetwarzanie danych jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim zostanie spełniona co najmniej jedna z poniższych przesłanek:

a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie jej danych osobowych w jednym lub większej liczbie określonych celów,
b) przetwarzanie jest niezbędne do wykonania umowy, gdzie stroną jest osoba, której dane dotyczą lub do podjęcia działań na żądanie osoby, której dane dotyczą przed zawarciem umowy,
c) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej,
d) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze,
e) przetwarzanie jest niezbędne do wykonania zadań realizowanych w interesie publicznym lub do sprawowania władzy publicznej powierzonej Administratorowi,
f) przetwarzanie jest niezbędne do realizacji celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora lub stronę trzecią.

5. Obowiązek informacyjny

5.1 Administrator Danych podczas pozyskiwania danych od osoby, której dane dotyczą jest zobowiązany poinformować tę osobę o:

a) swojej tożsamości i danych kontaktowych,
b) danych kontaktowych Inspektora Ochrony Danych,
c) celu i podstawie prawnej przetwarzania tych danych osobowych,
d) prawnie uzasadnionym interesie realizowanym przez Administratora Danych lub stronę trzecią,
e) odbiorcach danych lub kategorii odbiorców,
f) okresie, przez który te dane będą przechowywane, a gdy nie jest to możliwe, kryteria ustalenia takiego okresu,
g) prawie do żądania od Administratora:
   - ✓ dostępu do danych osobowych osoby, której te dane dotyczą,
   - ✓ do sprostowania jej danych osobowych,
   - ✓ do usunięcia jej danych osobowych,
   - ✓ do ograniczenia przetwarzania jej danych osobowych,
   - ✓ do wniesienia sprzeciwu wobec przetwarzania jej danych osobowych,
   - ✓ do przenoszenia danych;
h) prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem - jeżeli przetwarzanie odbywa się na podstawie zgody,
i) prawie wniesienia skargi do organu nadzorczego,
j) właściwości: czy podanie danych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą jest zobowiązana do ich podania i jakie są ewentualne konsekwencje nie podania tych danych,
k) zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję Europejską odpowiedniego stopnia ochrony lub w przypadku przekazania, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych,
l) zautomatyzowanym podejmowaniu decyzji , w tym profilowaniu – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

W przypadku zbierania danych nie od osoby, której dane dotyczą, osobę tę należy poinformować dodatkowo o kategorii i źródle pochodzenia danych osobowych.

6. Udostępnianie danych osobowych

6.1 Administrator Danych udostępnia przetwarzane dane osobowe tylko osobom lub podmiotom uprawnionym do ich otrzymania na podstawie i w granicach przepisów prawa:

a) na wniosek osoby, której dane dotyczą,
b) za wyraźną zgodą podmiotu, którego dane dotyczą,
c) na wniosek podmiotu uprawnionego do otrzymywania danych osobowych (np.: Policji, Prokuraturze),
d) na podstawie umowy z innym podmiotem, w ramach której istnieje konieczność udostępnienia danych.

7. Upoważnienie do przetwarzania danych osobowych

Do przetwarzania danych osobowych mogą mieć dostęp wyłącznie osoby posiadające pisemne upoważnienie nadane przez Administratora Danych.

8. Rejestr czynności przetwarzania, rejestr kategorii czynności przetwarzania

8.1 Administrator Danych prowadzi rejestr czynności przetwarzania, który zawiera m.in.:

a) imię, nazwisko lub nazwę i dane kontaktowe Administratora oraz Inspektora Ochrony Danych, Współadministratora, Przedstawiciela – jeżeli zostali wyznaczeni,
b) nazwę czynności przetwarzania,
c) cele przetwarzania,
d) opis kategorii osób, których dane dotyczą oraz kategorii danych osobowych,
e) kategorię odbiorców, którym dane osobowe zostały lub zostaną ujawnione,
f) gdy ma to zastosowanie – przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku innych przekazań, o których mowa w (art. 49 ust. 1 akapit drugi RODO), dokumentacja odpowiednich zabezpieczeń,
g) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych,
h) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa

8.2 Rejestr kategorii czynności przetwarzania prowadzony jest przez podmiot przetwarzający lub przedstawiciela podmiotu przetwarzającego, który w imieniu Administratora Danych przetwarza dane osobowe na podstawie zawartej umowy lub innego instrumentu prawnego. W przedmiotowym rejestrze znajdują się m.in.: następujące informację:

a) imię i nazwisko, lub nazwa oraz dane kontaktowe podmiotu przetwarzającego lub podmiotów przetwarzających oraz każdego administratora, w imieniu którego działa podmiot przetwarzający, a gdy ma to zastosowanie – przedstawiciela administratora lub podmiotu przetwarzającego oraz inspektora ochrony danych,
b) kategorię przetwarzań dokonywanych w imieniu każdego z administratorów,

c) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa,
d) gdy ma to zastosowanie – przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej, a w przypadku innych przekazań, o których mowa w (art. 49 ust. 1 akapit drugi RODO), dokumentacja odpowiednich zabezpieczeń,

Rejestry prowadzone są w formie pisemnej oraz elektronicznej

9. Umowy powierzenia przetwarzania danych osobowych

9.1 Zasady wskazane poniżej stosuje się do umów zawieranych z podmiotami trzecimi dotyczących powierzenia przetwarzania danych osobowych. W szczególności dostawcy usług informatycznych, szkoleniowych, serwisowych. Umowy te powinny zawierać w szczególności:

a) przedmiot umowy,
b) czas trwania,
c) charakter i cel przetwarzania,
d) rodzaj danych osobowych,
e) kategorie osób, których dane dotyczą,
f) obowiązki i prawa Administratora,
g) zobowiązanie podmiotu przetwarzającego do przetwarzania danych osobowych wyłącznie na udokumentowane polecenie Administratora Danych,
h) zobowiązanie podmiotu przetwarzającego, aby osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub aby podlegały odpowiedniemu ustawowemu obowiązkowi zachowania w tajemnicy danych do których będą miały dostęp na podstawie zawartej umowy,
i) informacje, że podmiot przetwarzający wdroży wszelkie środki techniczne i organizacyjne, aby zapewnić odpowiedni stopień bezpieczeństwa przed rozpoczęciem przetwarzania,
j) zobowiązanie podmiotu przetwarzającego do korzystania z usług innego podmiotu przetwarzającego tylko po wyrażeniu pisemnej zgody Administratora Danych, zapewniając, że w przypadku wyrażenia zgody przez niego wybrany podmiot przetwarzający spełnia te kryteria, które zostały zawarte w umowie pomiędzy Administratorem a podmiotem przetwarzającym,
k) biorąc pod uwagę charakter przetwarzania, podmiot przetwarzający w miarę możliwości pomaga administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw zgodnie z RODO,
l) uwzględniając charakter przetwarzania oraz dostępne mu informacje, podmiot przetwarzający pomaga administratorowi wywiązać się z obowiązków określonych w art. 32–36 RODO m.in.: pomoc przy informowaniu organu nadzorczego o naruszeniu ochrony danych,
m) po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora, podmiot przetwarzający usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych,
n) udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszym artykule oraz umożliwia Administratorowi

Danych lub audytorowi upoważnionemu przez Administratora Danych przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich,

10. Bezpieczeństwo fizyczne jednostki

10.1 Budynek jednostki podlega całodobowej ochronie pełnionej przez upoważnionych pracowników Administratora.

11. Analiza ryzyka

Administrator danych wykonuje analizę ryzyka w oparciu o operację przetwarzania danych uwzględniając ich charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia.

Analizę wykonuje się w oparciu o metody wybrane przez kierownictwo.

12. Ochrona danych w fazie projektowania (privacy by design)

12.1 Administrator Danych uwzględnia ochronę danych już w fazie tworzenia poszczególnych projektów. W tym celu wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z prawem.

Przy wyborze środków należy uwzględniać czynniki takie jak:

a) stan wiedzy technicznej,
b) koszt wdrażania,
c) charakter, zakres, a także kontekst i cele przetwarzania,
d) ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikającego z przetwarzania.

13. Domyślna ochrona danych (privacy by default).

Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. Administrator korzysta z rozwiązań zapewniających jak najwyższy poziom ochrony danych osobowych i wykorzystuje mechanizmy techniczne i technologiczne chroniące dane w momencie ich przetwarzania.

14. Ocena skutków planowanych operacji

14.1 Administrator danych dokonuje oceny planowanych operacji, jeżeli operacje przetwarzania wiążą się z wysokim ryzykiem naruszenia praw lub wolności osób, których dotyczą. Oceny skutków operacji przetwarzania dokonuje się także w przypadku przyjęcia przez organ nadzorczy wykazu takich operacji, które podlegają przedmiotowej ocenie, jeżeli operacje przedstawione w tym wykazie są wykonywane przez Administratora Danych.

Ocena zawiera co najmniej:

a) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora,
b) ocenę, czy operację przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów,
c) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą
d) środki planowane w celu zaradzeniu ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie niniejszego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą i innych osób, których sprawa dotyczy.

15. Prawa osoby, której dane dotyczą

Osoba, której dane dotyczą ma prawo:

a) żądania od Administratora dostępu do swoich danych,
b) do sprostowania swoich danych,
c) do usunięcia swoich danych,
d) do ograniczenia przetwarzania swoich danych,
e) do wniesienia sprzeciwu do przetwarzania swoich danych.

Każda osoba, której dane dotyczą ma prawo skorzystać z niniejszych praw poprzez złożenie stosownego wniosku do Administratora.