Polityka ochrony danych osobowych

Cel wprowadzenia Polityki, zakres stosowania

Fundacja Instytut Nowej Kultury, z siedzibą w Warszawie, ul. Cypryjska 60, (02-761) Warszawa Numer KRS 0000772319, NIP 5213856785, REGON 38259204200000 w dalszej części dokumentu zwana „Instytut", dąży do przestrzegania obowiązujących przepisów związanych z ochroną danych osobowych. Niniejszy dokument „Polityka ochrony danych osobowych" (dalej jako Polityka) ma za zadanie stanowić określenie mapy wymogów, zasad i regulacji ochrony danych osobowych przetwarzanych w Instytucie osób fizycznych, pracowników, klientów, współpracowników, dostawców, usługobiorców.

Użytkownikami niniejszego dokumentu są wszyscy pracownicy, zatrudnieni na stałe lub tymczasowo oraz wszyscy wykonawcy pracujący na rzecz Instytutu.

Dokumenty referencyjne

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) (Dz. Urz. UE L 119, s. 1),

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r., poz. 1781, z późn. zm.),

Statut Fundacji z dnia 6 listopada 2018 r.

Definicje

Poniższe definicje terminów zastosowanych w niniejszym dokumencie pochodzą z artykułu 4 Ogólnego Rozporządzenia o Ochronie Danych Unii Europejskiej;

"dane osobowe" oznaczają wszelkie 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;

"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;

“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;

„anonimizacja”: nieodwracalne pozbawienie danych osobowych elementów pozwalających na identyfikację, przez co osoba nie może zostać zidentyfikowana przy rozsądnym nakładzie czasu, środków i za pomocą technologii przez administratora lub inną osobę. Zasady przetwarzania danych osobowych nie mają zastosowania do danych zanonimizowanych, ponieważ nie są to w dalszym ciągu dane osobowe,

“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;

“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;

“podmiot przetwarzający” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

“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;

“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;

“główna jednostka organizacyjna” 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;

„główna jednostka organizacyjna” 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;

“organ nadzorczy” oznacza niezależny organ publiczny ustanowiony przez państwo członkowskie zgodnie z art. 51;

“transgraniczne przetwarzanie” oznacza 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 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;

Ochrona danych osobowych w Instytucie – zasady ogólne

W Instytucie przestrzegane są następujące zasady przetwarzania danych osobowych:

zasada zgodności z prawem, rzetelności i przejrzystości

Komunikaty związane z przetwarzaniem danych osobowych są łatwo dostępne i zrozumiałe oraz sformułowane jasnym i prostym językiem. Informacje te są przekazywane w formie elektronicznej za pomocą stron internetowych. Ponadto Instytut w sposób bezpośredni powiadamia osoby, których dane dotyczą, wysyłając do nich bezpośrednio w formie tradycyjnej papierowej lub w formie elektronicznej klauzule informacyjne, w których podaje informacje przewidziane w Rozporządzeniu. Instytut podaje te informacje zarówno w przypadku zbierania danych od osoby, której dane dotyczą, jak i w przypadku zbierania danych w sposób inny niż od osoby, której dane dotyczą.

Instytut informuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania każdego odbiorcę, któremu ujawnił dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Instytut

informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

zasada ograniczenia celu przetwarzania danych

Dane osobowe zbierane są w konkretnych, wyraźnych i prawnie uzasadnionych celach, wynikających z działań statutowych Instytutu i nieprzetwarzane dalej niezgodnie z tymi celami. Osoby, których dane dotyczą, są informowane o celach przetwarzania, zgodnie z zasadami i w sposób określony powyżej (pkt. IV, ppkt.1).

Instytut, w sytuacji gdy planuje przetwarzać dane w innym celu niż zostały zebrane, wysyła przed dalszym przetwarzaniem stosowną informację do osoby, której danej dotyczą i dostarcza jej wszystkich niezbędnych informacji w tym zakresie. Instytut może podjąć decyzję, że dane osobowe będą przetwarzane do celów archiwalnych i statystycznych.

Wskazując ogólną podstawę prawną (zgoda, umowa, obowiązek prawny, żywotne interesy, zadanie publiczne/władza publiczna, uzasadniony cel Instytutu) Instytut dookreśla podstawę w czytelny sposób, gdy jest to potrzebne. Np. dla zgody wskazując na jej zakres, gdy podstawą jest prawo – wskazując na konkretny przepis i inne dokumenty, np. umowę, żywotne interesy – wskazując na kategorie zdarzeń, w których się zmaterializują, uzasadniony cel – wskazując na konkretny cel, np. marketing własny, dochodzenie roszczeń.

Instytut wdraża metody zarządzania zgodami umożliwiające rejestrację i weryfikację posiadania zgody Osoby na przetwarzanie jej konkretnych Danych w konkretnym celu, zgody na komunikację na odległość (email, telefon, sms, in.) oraz rejestrację odmowy zgody, cofnięcia zgody lub podobnych czynności (sprzeciw, ograniczenie itp.).

zasada minimalizacji danych

Dane osobowe przetwarzane są w sposób i w czasie niezbędnym do celów, w których są przetwarzane. Celami Instytutu są jego prawnie uzasadnione cele wyrażające się w jego działalności statutowej. Instytut dokonuje okresowo selekcji danych i wybiera tylko taką ilość danych, jaka jest dla niego niezbędna do realizacji celów statutowych.

zasada prawidłowości danych

Instytut zapewnia prawidłowość i aktualność danych. Każda osoba, której dane dotyczą, może zgłosić Instytutowi prośbę o poprawienie, uaktualnienie, sprostowanie danych a także usunięcie danych, które są nieprawidłowe. Po zgłoszeniu pracownicy Instytutu do tego upoważnieni dokonują poprawienia, aktualizacji, sprostowania lub usunięcia nieprawidłowych danych w zbiorze danych.

zasada ograniczenia przechowania danych

Dane osobowe są adekwatne, stosowne i ograniczone do tego, co niezbędne do celów, dla których są one przetwarzane. Celem Instytutu jest realizacja prawnie uzasadnionego celu, tj. jego celów statutowych. Działalność Instytutu jest nieograniczona w czasie. Dlatego też Instytut nie określa czasu przechowania danych. Wdraża natomiast procedurę okresowego przeglądu danych i wybiera tylko taką ilość danych, jaka jest dla niego niezbędna do realizacji celów statutowych.

zasada integralności i poufności danych

Dane osobowe są przetwarzane w sposób zapewniający im odpowiednie bezpieczeństwo i odpowiednią poufność, w tym ochronę przed nieuprawnionym dostępem do nich i do sprzętu służącego ich przetwarzaniu oraz przed nieuprawnionym korzystaniem z tych danych i z tego sprzętu. Służą temu rozwiązania organizacyjne i techniczne stosowane przez Instytut, a opisane w pkt. 5 niniejszej Polityki.

zasada rozliczalności

Instytut wykazuje przestrzeganie zasad przetwarzania danych osobowych poprzez:

informacje dla osób, których dane są przetwarzane na stronach internetowych,

informacje dla osób, których dane są przetwarzane przekazywane w sposób bezpośredni w formie elektronicznej lub papierowej w formie klauzul informacyjnych,

możliwość uzyskania przez każdą osobę w powszechnie używanym formacie jej danych osobowych,

możliwość uzyskania informacji dotyczących danych osobowych na specjalnie przeznaczonej do tego skrzynce pocztowej: projekty.terlikowski@gmail.com

dokumentowanie obsługi obowiązków informacyjnych, zawiadomień i żądań osób, których dane dotyczą,

wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe (obszar przetwarzania danych osobowych),

rejestr czynności przetwarzania danych dokumentujący podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania,

upoważnienia do przetwarzania danych osobowych,

umowy z podmiotami, którym powierzono przetwarzanie danych,

ewidencja osób upoważnionych do przetwarzania danych osobowych.

prawo do przenoszenia danych

Instytut zapewnia osobie, której dane dotyczą, otrzymanie w powszechnie używanym formacie danych osobowych jej dotyczących. Osoba, której dane dotyczą, ma prawo

przesłać te dane osobowe innemu administratorowi. Żądanie przesłania danych osobowych może być zgłoszone drogą elektroniczną na adres: instytutnowejkultury@gmail.com lub drogą poczty tradycyjnej. Przesłanie danych odbywa się drogą elektroniczną na podany przez osobę, której dane dotyczą, adres e-mail lub drogą poczty tradycyjnej.

Zakres stosowania Polityki

Niniejsza Polityka dotyczy przetwarzania wszystkich danych osobowych administrowanych przez Instytut: w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych a także w systemach informatycznych będących w dyspozycji Instytutu i zawiera następujące informacje:

wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe (obszar przetwarzania danych osobowych)

Przetwarzanie danych osobowych w Instytucie odbywa się zarówno przy wykorzystaniu systemów informatycznych, jak i poza nimi, tj. w wersji tradycyjnej, „papierowej". Obszar przetwarzania danych osobowych w Instytucie został określony w Załączniku nr 1 do niniejszej Polityki pt.: „Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w których przetwarzane są dane osobowe".

Za obszar przetwarzania danych należy rozumieć obszar, w którym wykonywana jest choćby jedna z czynności przetwarzania danych osobowych, w szczególności stanowią go wszystkie komputery przenośne oraz inne nośniki danych znajdujące się poza obszarami wskazanym w Załączniku nr 1 do niniejszej Polityki.

rejestr czynności przetwarzania danych osobowych

Instytut opracowuje, prowadzi i utrzymuje Rejestr Czynności Danych Osobowych, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe. Rejestr jest jednym z podstawowych narzędzi rozliczania zgodności z ochroną danych w Instytucie. Rejestr jest przede wszystkim dokumentem wewnętrznym, którego zadaniem, oprócz wskazywania metod i powodów przetwarzania danych osobowych, jest wskazanie Organowi Nadzorczemu w przypadku postępowania wyjaśniającego, że Instytut jest świadomy operacji na danych oraz sprawuje nad nimi kontrolę.

Zarząd Instytutu jest odpowiedzialny za prowadzenie ewidencji czynności przetwarzania prowadzonych przez Instytut w formie rejestru czynności przetwarzania.

Rodzaj rejestru będzie zależał od tego czy Instytut działa w charakterze Administratora Danych czy Podmiotu Przetwarzającego Dane.

Dla każdej czynności przetwarzania danych, którą Instytut uznał za odrębną dla potrzeb Rejestru, odnotowuje co najmniej:

imię i nazwisko oraz dane kontaktowe osoby odpowiedzialnej za ochronę danych,

nazwę czynności,

cel przetwarzania,

kategoria osób,

kategoria danych,

podstawę prawną przetwarzania, wraz z wyszczególnieniem kategorii uzasadnionego interesu administratora, jeśli podstawą jest prawnie uzasadniony interes,

sposób zbierania danych,

kategoria odbiorców danych (w tym przetwarzających),

informację o przekazaniu poza EOG

ogólny opis technicznych i organizacyjnych środków ochrony danych.

Jeśli Instytut działa w charakterze podmiotu przetwarzającego, musi prowadzić rejestr czynności przetwarzania wszystkich kategorii czynności przetwarzania wykonywanych w imieniu administratora, który będzie zawierał przynajmniej poniższe informacje:

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,

kategoria czynności przetwarzania wykonywanych w imieniu każdego administratora,

ogólny opis technicznych i organizacyjnych środków ochrony danych.

Wzór Rejestru stanowi Załącznik nr 2 do Polityki – „Wzór Rejestru Czynności Przetwarzania Danych”.

analiza ryzyka i ocena skutków dla ochrony danych

Instytut zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych przez Instytut.

Instytut przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych. W tym celu Instytut:

zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania − wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych,

kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają,

przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. Instytut analizuje możliwe sytuacje i scenariusze naruszenia ochrony danych osobowych uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.

Instytut dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych tam, gdzie zgodnie z analizą ryzyka ryzyko naruszenia praw i wolności osób jest wysokie. Wzór analizy ryzyka i oceny skutków stanowi Załącznik nr 3 do Polityki – „Wzór analizy ryzyka”

środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

Instytut ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania. Do elementów zabezpieczenia danych osobowych w instytucie zalicza się: metody ochrony pomieszczeń, w których przetwarzane są dane osobowe, zabezpieczenia danych (zabezpieczenie organizacyjne), odpowiednie środki zabezpieczenia danych w systemach informatycznych.

zabezpieczenia fizyczne obejmują: wydzielenie obszaru przetwarzania danych, samodzielny dostęp do pomieszczeń w Instytucie jest możliwy wyłącznie dla osób upoważnionych (wzór upoważnienia stanowi załącznik nr 4 do Polityki), wstęp osób postronnych jest możliwy jedynie podczas obecności pracowników Instytutu, przechowywanie akt w wersji papierowej w specjalnie do tego celu przeznaczonych pomieszczeniach, w zamykanych na klucz szafach, budynki, w których odbywa się przetwarzanie danych osobowych dodatkowo są zabezpieczone przez system alarmowy;

zabezpieczenia organizacyjne obejmują: osobą odpowiedzialną za bezpieczeństwo danych osobowych w Instytucie jest Prezes Zarządu, który będzie aktualizował niniejszą Politykę wraz z załącznikami do niej oraz Instrukcję zarządzania systemami informatycznym służącymi do przetwarzania danych osobowych; pracownicy Instytutu, którzy na bieżąco kontrolują pracę systemu informatycznego z należytą starannością, zgodnie z aktualnie obowiązującą w tym zakresie wiedzą, o zaobserwowanych nieprawidłowościach informują Prezesa Zarządu; pracownicy mający dostęp do danych osobowych, które są w dyspozycji Instytutu zobowiązani są do utrzymywania w tajemnicy danych osobowych i sposobów ich zabezpieczenia, również po odwołaniu z określonego stanowiska a także po ustaniu zatrudnienia; w tym celu pracownicy mający dostęp do danych osobowych podpisują oświadczenie o utrzymywaniu w tajemnicy danych osobowych i sposobów ich zabezpieczenia (wzór oświadczenia o zachowaniu w poufności stanowi załącznik nr 5 do Polityki); przetwarzanie danych osobowych może być wykonywane wyłącznie przez osoby,

które zostały upoważnione do przetwarzania danych osobowych; osoby przetwarzające dane osobowe zostały upoważnione do przetwarzania danych osobowych poprzez wpisanie określonych kompetencji do zakresu obowiązków na danym stanowisku. Określone stanowiska wraz z przypisanym zakresem upoważnienia znajdują się w ewidencji osób upoważnionych do przetwarzania danych osobowych, stanowiącej załącznik 6 do niniejszej Polityki;

zabezpieczenia techniczne obejmują: mechanizmy kontroli dostępu do systemów informatycznych i ich zasobów; uprawnienia są różne dla różnych grup użytkowników, zastosowanie odpowiednich i regularnych aktualizacji narzędzi ochronnych (Eset, system antywirusowy); system informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych i logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem; tworzone są regularnie kopie zapasowe zbiorów danych przetwarzanych w systemach informatycznych (raz w miesiącu) oraz testowanie kopii zapasowych raz na 6 miesięcy; systemy informatyczne zastosowane do przetwarzania danych osobowych spełniają wymagania określone w Rozporządzeniu.

W ramach zabezpieczenia danych osobowych ochronie podlegają: sprzęt komputerowy –komputery osobiste (w tym laptopy) i inne urządzenia zewnętrzne, oprogramowanie, dane osobowe zapisane na informatycznych nośnikach danych oraz dane przetwarzane w systemach informatycznych, hasła użytkowników, bazy danych i kopie zapasowe, wydruki, związana z przetwarzaniem danych dokumentacja papierowa.

Prezes Zarządu będzie w miarę potrzeb analizowali zagrożenia i ryzyko w celu weryfikacji środków zabezpieczających. W szczególności taka analiza będzie dokonywana w każdym przypadku istotnych zmian działania lub struktury Instytutu.

Oprócz tego Prezes Zarządu w miarę potrzeb będzie dokonywać inwentaryzacji systemów informatycznych i czynności przetwarzania danych osobowych w celu zapewnienia aktualności opisu zawartego w punkcie V niniejszej Polityki oraz Załączniku nr 1 do niniejszej Polityki pt. „Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w których przetwarzane są dane osobowe u ADO” i Załączniku nr 2 do niniejszej Polityki pt. „Rejestr Czynności Przetwarzania Danych”.

powierzenie przetwarzania danych osobowych

Instytut może powierzyć przetwarzanie danych osobowych innemu podmiotowi wyłącznie w drodze umowy zawartej w formie pisemnej, zgodnie z wymogami wskazanymi dla takich umów w art. 28 RODO. Instytut przyjął minimalne wymagania co do umowy powierzenia przetwarzania danych stanowiące Załącznik nr 7 do niniejszej Polityki – „Wzór umowy powierzenia przetwarzania danych”.

W celu zapewnienia, aby przetwarzający dawali wystarczające gwarancje wdrożenia odpowiednich środków organizacyjnych i technicznych dla zapewnienia bezpieczeństwa, realizacji praw jednostki i innych obowiązków ochrony danych spoczywających na Instytucie, przed powierzeniem przetwarzania danych osobowych Instytut w miarę możliwości uzyskuje informacje o dotychczasowych praktykach procesora dotyczących zabezpieczenia danych osobowych.

zasady przekazywania danych osobowych do państwa trzeciego

Instytut rejestruje w Rejestrze przypadki przekazywania danych poza Europejski Obszar Gospodarczy. W przypadku korzystania z rozwiązań informatycznych opartych na usługach świadczonych w chmurze obliczeniowej lub serwisowanych poza Europejskim Obszarem Gospodarczym Instytut zapewnia mechanizm, który zgodnie z prawem Unii Europejskiej legalizuje transfer danych osobowych i zapewnia odpowiednie gwarancje ich ochrony.

projektowanie prywatności

Instytut zarządza zmianą mającą wpływ na prywatność w taki sposób, aby umożliwić zapewnienie odpowiedniego bezpieczeństwa danych osobowych oraz minimalizacji ich przetwarzania. W tym celu zasady prowadzenia projektów i zadań przez Instytut odwołują się do zasad bezpieczeństwa danych osobowych i minimalizacji, wymagając oceny wpływu na prywatność i ochronę danych, uwzględnienia i zaprojektowana bezpieczeństwa i minimalizacji przetwarzania danych od początku projektu lub zadania.

naruszenia zasad ochrony danych osobowych,

W przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych, należy niezwłocznie powiadomić Prezesa Zarządu. Typowe sytuacje, gdy użytkownik powinien powiadomić Prezesa Zarządu:

ślady na drzwiach, oknach i szafach wskazują na próbę włamania;

dokumentacja jest niszczona bez użycia niszczarki;

fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się

podejrzanie;

otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe;

ustawienie monitorów pozwala na wgląd osób postronnych w dane osobowe;

wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz firmy bez upoważnienia Prezesa Zarządu;

udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej i ustnej;

telefoniczne próby wyłudzenia danych osobowych;

kradzież komputerów lub CD, twardych dysków, pendrive z danymi osobowymi;

maile zachęcające do ujawnienia identyfikatora lub hasła;

pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów;

hasła do systemów przechowywane są w pobliżu komputera.

W razie niemożliwości zawiadomienia Prezesa Zarządu lub osoby przez niego upoważnionej, należy powiadomić bezpośredniego przełożonego.

Do czasu przybycia na miejsce naruszenia ochrony danych osobowych Prezesa Zarządu lub upoważnionej przez niego osoby, należy: niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców; rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia; zaniechać – o ile to możliwe – dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę; podjąć inne działania przewidziane i określone w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu; podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej; zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku; nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Prezesa Zarządu lub osoby upoważnionej.

Po przybyciu na miejsce Prezes Zarządu lub osoba go zastępująca: zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania, mając na uwadze ewentualne zagrożenia dla prawidłowości pracy; może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem; nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, z zewnętrznymi specjalistami.

Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu Prezes Zarządu zasięga niezbędnych opinii i proponuje postępowanie naprawcze, a w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.

Prezes Zarządu dokumentuje zaistniały przypadek naruszenia oraz sporządza raport, który powinien zawierać w szczególności: wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem, określenie czasu i miejsca naruszenia i powiadomienia, określenie

okoliczności towarzyszących i rodzaju naruszenia, kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie, wyszczególnienie wziętych pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania, wstępną ocenę przyczyn wystąpienia naruszenia, opis możliwe konsekwencje naruszenia ochrony danych osobowych, ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego, w szczególności opis zastosowanych lub proponowanych środków w celu zaradzenia naruszeniu ochrony danych osobowych lub zminimalizowania jego ewentualnych negatywnych skutków.

Wzór raportu z naruszenia ochrony danych załącznik nr 8 do niniejszej Polityki.

Wzór rejestru naruszeń ochrony danych stanowi załącznik nr 9 do niniejszej Polityki.

W przypadku naruszenia ochrony danych osobowych Prezes Zarządu bez zbędnej zwłoki – w miarę możliwości nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia. Zgłoszenie, o którym mowa powyżej, musi co najmniej: opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości, wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie; zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych; opisywać możliwe konsekwencje naruszenia ochrony danych osobowych; opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Jeżeli zgłoszenia do organu nadzoru nie da się udzielić jednorazowo, należy go udzielać sukcesywnie bez zbędnej zwłoki. Jeśli zdarzenie ma charakter przestępstwa, sprawa kierowana jest do organów ścigania.

Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator danych bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu, chyba że: wdrożono odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych; zastosowano następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą; wymagałoby ono niewspółmiernie dużego wysiłku; w takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za

pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób. Zawiadomienie, o którym powyżej, powinno jasnym i prostym językiem opisywać charakter naruszenia ochrony danych osobowych oraz zawierać przynajmniej następujące informacje: imię i nazwisko oraz dane kontaktowe Prezesa Zarządu, opis możliwych konsekwencji naruszenia ochrony danych osobowych, opis środków zastosowane lub proponowane przez Administratora danych w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków. Zaistniałe naruszenie może stać się przedmiotem szczegółowej, zespołowej analizy prowadzonej przez Administratora Danych oraz osób wyznaczonych przez Administratora danych. Analiza powinna zawierać wszechstronną ocenę zaistniałego naruszenia, wskazanie odpowiedzialnych, wnioski co do ewentualnych przedsięwzięć proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

Prezes Zarządu dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.

VI. Postanowienia końcowe

Za niedopełnienie obowiązków wynikających z niniejszego dokumentu pracownik ponosi odpowiedzialność na podstawie Kodeksu pracy, przepisów o ochronie danych osobowych.

Niniejsza polityka obowiązuje od 01.05.2019 r