POLITYKA OCHRONY DANYCH OSOBOWYCH

w Fundacji TryIT z siedzibą w Krakowie przy al. A. Mickiewicza 30, 30-059 Kraków wpisanej do Rejestru Przedsiębiorców Krajowego Rejestru Sądowego oraz do Rejestru Stowarzyszeń, innych organizacji społecznych i zawodowych, fundacji oraz samodzielnych publicznych zakładów opieki zdrowotnej Krajowego Rejestru Sądowego nr KRS 0000859303, NIP 6772456275, REGON 387052706

§ 1. Cele Polityki ochrony danych

Podstawowym zadaniem Polityki ochrony danych osobowych jest oznaczenie zasad przetwarzania, ochrony i udostępniania danych osobowych, gromadzonych i przetwarzanych w Fundacji TryIT z siedzibą w Krakowie, przy al. A. Mickiewicza 30, 30-059 Kraków, wpisanej do Rejestru Przedsiębiorców Krajowego Rejestru Sądowego oraz do Rejestru Stowarzyszeń, innych organizacji społecznych i zawodowych, fundacji oraz samodzielnych publicznych zakładów opieki zdrowotnej Krajowego Rejestru Sądowego nr KRS 0000859303, NIP 6772456275, REGON 387052706 (dalej „Try IT" lub „Fundacja") oraz nadzoru nad procesem przetwarzania tych danych.

§ 2. Zakres podmiotowy obowiązywania

Polityka ochrony danych osobowych w ustalona w Try IT obowiązuje wszystkie osoby realizujące jakiekolwiek zadania w Try IT lub na zlecenie Try IT, niezależnie od podstawy wykonywania tych czynności.

§ 3. Zakres przedmiotowy obowiązywania

1. Polityka ochrony obejmuje wszystkie przypadki przetwarzania danych osobowych, dokonywane przez Try IT we wszelkiego rodzaju kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych, a także w systemach informatycznych będących w dyspozycji Try IT.
2. Wykaz budynków i pomieszczeń, tworzących przestrzeń, w której przetwarzane są dane osobowe (obszar przetwarzania danych osobowych), stanowi **Załącznik nr 1 do Polityki**.
3. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów komputerowych zastosowanych do przetwarzania danych (w przypadku zbiorów danych prowadzonych w wersji elektronicznej), stanowi **Załącznik nr 2 do Polityki.**
4. Dane osobowe przetwarzane w systemach informatycznych przechowywane są na serwerach zlokalizowanych w Polsce w budynku przy ul. Kawiory 21 lok. 4.8, 30-055 Kraków.

§ 4. Podstawa prawna

Podstawą prawną dla opracowania niniejszej Polityki ochrony są przepisy:

1) 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 (dalej „RODO").
2) Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018 poz. 1000 z poz. zm.).

§ 5. Obszar obowiązywania

1. Niezależnie od praw i obowiązków, określonych w RODO, niniejszej Polityce ochrony, przetwarzanie danych osobowych w Try IT odbywa się w zakresie i zasadach określonych w szczególności w:
   1) dokumentach statutowych Try IT,
   2) przepisach ogólnych oraz szczególnych, w tym:
      a) dotyczących ubezpieczeń społecznych oraz świadczeń pieniężnych z ubezpieczenia społecznego w razie choroby i macierzyństwa,

b) w kodeksie pracy,
c) ordynacji podatkowej oraz ustawie o podatku dochodowym od osób fizycznych.

2. Przepisy, o których mowa w ust. 1, wskazują w szczególności:
   1) podstawę przetwarzania danych osobowych,
   2) zakres gromadzonych i przetwarzanych danych osobowych,
   3) formę przetwarzania danych osobowych,
   4) podstawę i zakres udostępniania danych osobowych posiadanych przez Try IT oraz podmiot uprawniony do dostępu do tych danych osobowych,
   5) okres przetwarzania (przechowywania) tych danych osobowych.

§ 6. Definicje pojęć

Użyte w niniejszej Polityce ochrony określenia oznaczają:

1) **Administrator danych** – Try IT,
2) **Polityka bezpieczeństwa** – niniejszy dokument opisujący stosowane w Try IT zasady ochrony danych osobowych,
3) **Ustawa** – ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018 poz. 1000 z poz. zm.).

§ 7. Instrukcja zarządzania systemem informatycznym

1. W przypadku przetwarzania danych osobowych w systemie informatycznym dane informatyczne są zabezpieczone za pomocą pełnych kopii zapasowych, co polega na kopiowaniu danych przynajmniej jeden raz na trzy miesiące lub przed aktualizacją programu na pamięć zewnętrzną.
2. Nośnik zewnętrznych danych zawierających kopię zapasową zabezpieczony jest hasłem dostępu oraz jest przechowywany poza obszarem przetwarzania danych wskazanym w Załączniku nr 1 do polityki bezpieczeństwa.
3. Wszystkie komputery w Try IT zabezpieczone są hasłami dostępu oraz licencjonowanym oprogramowaniem antywirusowym oraz programem do usuwania złośliwego oprogramowania.
4. Hasła dostępu do komputera zmieniane są raz na pół roku.
5. Po każdej naprawie i konserwacji komputera sprzęt jest sprawdzany pod kątem występowania wirusów i konieczności zainstalowania nowego oprogramowania antywirusowego.
6. Szczegółowa instrukcja zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, stanowi **Załącznik nr 3 do Polityki**.

§ 8. Czynności wdrożeniowe podjęte przez Administratora

W związku z obowiązkiem ochrony danych osobowych w Try IT zrealizowano postulaty, o których mowa w RODO, a w szczególności:

1) dokonano oceny skutków dla ochrony danych,
2) przeprowadzono czynności mające na celu analizę ryzyka w odniesieniu do zasobów biorących udział w poszczególnych procesach,
3) do czynności przetwarzania danych osobowych zostały dopuszczone wyłącznie osoby upoważnione przez Administratora,

4) zawarto umowy powierzenia przetwarzania danych z podmiotami zewnętrznymi,
5) została opracowana i wdrożona niniejsza polityka bezpieczeństwa oraz inne dokumenty określone przepisami prawa.

§ 9. Obowiązki Administratora danych

1. Administrator danych wdraża środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, stosowne do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnianiem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem prawa oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
2. Administrator danych zobligowany jest do zapewnienia, aby dane osobowe były:
   1) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość"),
   2) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami („ograniczenie celu"),
   3) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych"),
   4) prawidłowe i w razie potrzeby uaktualniane. Należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość"),
   5) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane („ograniczenie przechowywania"),
   6) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność").
3. Administrator danych na podstawie art. 37 ust. 1 RODO nie jest zobowiązany do wyznaczenia IOD.
4. Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez Administratora danych, zgodnie z **Załącznikiem nr 4 do Polityki**. Osoby te są zobowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczania.
5. Administrator danych jest obowiązany zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.

§10. Zadania Administratora danych

1. Administrator danych jest odpowiedzialny za bezpieczeństwo systemu informatycznego, w którym przetwarzane są dane osobowe.
2. Do podstawowych obowiązków Administratora danych należy:
   1) realizowanie zadań określonych w RODO,
   2) realizacja oraz nadzór nad przestrzeganiem Polityki ochrony i Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
   3) nadzór i kontrola systemów informatycznych służących do przetwarzania danych

osobowych,

4) kontrola właściwego zabezpieczenia sprzętu oraz pomieszczeń, w których przetwarzane są dane osobowe,
5) nadzór nad wykorzystanym w Try IT oprogramowaniem oraz jego legalnością,
6) przeciwdziałanie dostępowi osób nieupoważnionych i niepowołanych do systemu, w którym przetwarzane są dane osobowe,
7) podejmowanie stosownych czynności w celu właściwego zabezpieczania danych,
8) badanie i monitorowanie ewentualnych naruszeń w systemie zabezpieczeń danych osobowych,
9) podejmowanie decyzji o instalowaniu nowych urządzeń oraz oprogramowania wykorzystanego do przetwarzania danych osobowych,
10) nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, zawierających dane osobowe,
11) zdefiniowanie haseł dostępu,
12) aktualizowanie oprogramowania antywirusowego i innego chyba, że aktualizacje te wykonywane są automatycznie,
13) wykonywanie kopii zapasowych, ich przechowywanie oraz okresowe sprawdzanie pod kątem ich dalszej przydatności,
14) sporządzanie raportów z naruszenia bezpieczeństwa systemu informatycznego oraz systemu przechowywania i zabezpieczenia danych osobowych zgromadzonych i utrwalonych w innej formie, niż elektroniczna,
15) zapewnienie ochrony i bezpieczeństwa danych osobowych znajdujących się w systemie informatycznym Try IT oraz w tradycyjnych zbiorach danych,
16) podejmowanie, zgodnie z Polityką ochrony, stosownych działań w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych znajdujących się w systemie informatycznym oraz danych osobowych zgromadzonych i utrwalonych w innej formie, niż elektroniczna,
17) zapewnienie fizycznego bezpieczeństwa systemu informatycznego oraz systemu przechowywania i zabezpieczenia danych osobowych zgromadzonych i utrwalonych w innej formie, niż elektroniczna,
18) zapewnienie bezpieczeństwa funkcjonowania wszystkich urządzeń pracujących w systemie,
19) zapewnienie dostępu do systemu wyłącznie dla osób uprawnionych,
20) kontrola, aby monitory komputerów, na których przetwarzane są dane osobowe były ustawione tak, żeby osoby postronne nie miały wglądu w przetwarzane dane osobowe,
21) przeprowadzenie analizy ryzyka każdorazowo w przypadku zamiaru rozpoczęcia przetwarzania danych osobowych w ramach nowego procesu,
22) uwzględnienie praw osób, których dane dotyczą, w każdym przypadku tworzenia i wdrażania nowego produktu lub usług.

3. Administrator danych prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych, która zawiera:
   1) imię i nazwisko osoby upoważnionej,
   2) rodzaj stosunku prawnego,

3) rodzaj zbioru,
4) datę nadania i ustania upoważnienia,
5) podpis osoby upoważnionej, potwierdzający zapoznanie się ze wszystkimi dokumentami regulującymi bezpieczeństwo przetwarzania danych osobowych w Try IT.

4. Administrator zobowiązany jest zapewnić przeprowadzenie analizy ryzyka dla zasobów przetwarzanych danych. W tym celu każdorazowy właściciel procesu wskazany przez Administratora lub sam Administrator danych samodzielnie przeprowadza analizę ryzyka.
5. Analiza ryzyka jest przeprowadzana nie rzadziej niż raz w roku i stanowi podstawę do aktualizacji sposobu postępowania z ryzykiem.
6. W oparciu o wyniki przeprowadzonej analizy ryzyka, wskazani przez Administratora danych właściciele procesów lub administrator danych samodzielnie wdrażają sposoby postępowania z ryzykiem.
7. Każdorazowo po wykonaniu analizy ryzyka Administrator wybiera sposób postępowania z ryzykiem i określa, które ryzyka i w jakiej kolejności będą uwzględniane w pierwszej kolejności.

§ 11. Obowiązki pracowników i współpracowników

1. Pracownicy, współpracownicy Try IT oraz osoby określone w §2 (dalej „Pracownicy") mają obowiązek przestrzegać postanowień zawartych w niniejszej Polityce ochrony i Instrukcji zarządzania systemem informatycznym oraz pozostałych dokumentach obejmujących regulację ochrony danych obowiązującą w Try IT.
2. Przed przystąpieniem do podjęcia czynności związanych z przetwarzaniem danych osobowych, każdy Pracownik ma obowiązek odbycia szkolenia oraz zapoznania się z przepisami dotyczącymi ochrony danych osobowych, w tym z niniejszą Polityką, Instrukcją zarządzania systemem oraz pozostałymi dokumentami wskazanymi w ust. 1 powyżej. Fakt zapoznania się zostaje potwierdzony osobiście podpisanym oświadczeniem. Oświadczenie podlega włączeniu do akt pracownika lub dokumentów związanych z inną podstawą świadczenia usług w Try IT zgodnie z **Załącznikiem nr 5 do Polityki.**
3. Pracownicy są zobowiązani dbać o bezpieczeństwo powierzonych im do przetwarzania, archiwizowania lub przechowywania danych zgodnie z obowiązującą w placówce Polityką ochrony, w tym w szczególności:
   1) chronić dane przed dostępem osób nieupoważnionych,
   2) chronić dane przed przypadkowym zniszczeniem, utratą lub modyfikacją,
   3) chronić wszelkie nośniki zawierające dane osobowe, w tym nośniki magnetyczne, optyczne, nośniki pamięci półprzewodnikowej oraz wszelkiego rodzaju druki i wydruki, przed dostępem osób nieupoważnionych oraz przed przypadkowym zniszczeniem,
   4) utrzymywać w tajemnicy wszelkie informacje odnośnie danych osobowych oraz sposobu środków ich ochrony,
   5) utrzymywać w tajemnicy hasła, częstotliwość ich zmiany oraz szczegóły technologiczne, także po ustaniu zatrudnienia w Try IT.
4. Pracownikom stanowczo zabrania się:
   1) ujawniać danych, w tym danych osobowych zawartych w obsługiwanych systemach,
   2) kopiować i przenosić baz danych lub ich części bez wyraźnego upoważnienia,
   3) przetwarzać dane w sposób inny, niż wynikający z obowiązujących przepisów prawa oraz

niniejszej Polityki.

5. Przypadki zaniechania przez Pracownika obowiązków wynikających z niniejszej Polityki, Instrukcji zarządzania systemem informatycznym oraz pozostałych dokumentów obejmujących regulacje ochrony danych obowiązującą w Try IT mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych lub rażące nienależyte wykonanie zobowiązania, w szczególności przez osobę, która wobec naruszenia nie powiadomiła o tej okoliczności Administratora.

§12. Procedura współpracy z podmiotami zewnętrznymi

1. Administrator odpowiada za poprawną realizację współpracy z podmiotami zewnętrznymi. Każdorazowe skorzystanie z usług podmiotu zewnętrznego (przetwarzającego) musi zostać poprzedzone zawarciem umowy powierzenia przetwarzania danych osobowych zgodnie z **Załącznikiem nr 6 do Polityki**.
2. Administrator zobowiązany jest do weryfikacji funkcjonowania pod względem zgodności z RODO wszystkich podmiotów zewnętrznych (przetwarzających), z których usług korzysta lub ma zamiar skorzystać z wykorzystaniem listy kontrolnej, nie rzadziej niż raz w roku oraz każdorazowo przed zawarciem umowy powierzenia przetwarzania danych.

§ 13. Zabezpieczenie danych osobowych

1. Jednym z podstawowych sposobów zabezpieczenia danych osobowych przetwarzanych w formie tradycyjnej, tj. na papierowych nośnikach danych, jest ograniczenie dostępu do niej za pomocą elementów zabezpieczeń fizycznych na przykład przez ograniczenie dostępu do pomieszczeń i szaf lub innego wyposażenia biurowego, w których przechowywane są te dokumenty oraz organizacyjnych, takich jak nadawanie, weryfikowanie i kontrolowanie dostępu do tych danych przez upoważnionych pracowników określone w §11 i 12 Polityki.
2. W Try IT w celu ochrony danych osobowych stosuje się następujące środki ochrony fizycznej danych:
   1) zbiory danych osobowych przechowywane są w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi), wejście do lokalu zabezpieczone jest alarmem oraz systemem ograniczonego dostępu (zamek domofonowy), wejście do budynku, w którym znajduje się lokal Try IT podlega całodobowemu monitoringowi oraz ochronie,
   2) zbiory danych osobowych w formie papierowej przechowywane są w zamkniętej niemetalowej szafie,
   3) kopie zapasowe/archiwalne zbiorów danych osobowych przechowywane są także w zamkniętej niemetalowej szafie,
   4) pomieszczenia, w których przetwarzane są zbiory danych osobowych, zabezpieczone są przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy.
3. Podstawowym sposobem zabezpieczenia danych przetwarzanych w systemie informatycznym i dostępu do nich jest system definiowania loginów lub/i haseł osób upoważnionych do przetwarzania danych osobowych. Są to zabezpieczenia programowe zainstalowane w eksploatowanych w Try IT systemach, uniemożliwiające dostęp do systemu osobom nieupoważnionym.

4. W celu właściwej ochrony danych w Try IT:
   1) zalogowanie się do systemu informatycznego wymaga podania loginu lub/i hasła. Administrator danych ustala i zmienia hasło systemowe,
   2) hasła systemowe są zmieniane nie rzadziej, niż co pół roku,
   3) na każdym komputerze pracującym w systemie, który posiada dostęp do Internetu, jest zainstalowany odpowiedni program antywirusowy oraz program do usuwania złośliwego oprogramowania.
   4) wydruki zawierające dane osobowe powinny znajdują się w miejscu, które uniemożliwia dostęp osobom postronnym.
   5) Administrator danych lub Pracownik może zakończyć pracę dopiero po wylogowaniu się z systemu. Obowiązek ten istnieje także w przypadku czasowego opuszczenia stanowiska pracy, chyba że wylogowanie następuje automatyczne.
5. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do ich przetwarzania.
6. Za wykonywanie kopii zapasowych, umożliwiających odtworzenie sprawności systemu, odpowiada Administrator danych. Są one przechowywane na nośnikach zewnętrznych. Nośniki zewnętrzne Try IT przechowuje poza obszarem przetwarzania danych, o którym mowa w **Załączniku nr 1 do Polityki**.
7. Z nośników magnetycznych kopie zapasowe usuwa się niezwłocznie po ustaniu ich użyteczności w taki sposób, aby nie można było odtworzyć ich zawartości.

§ 14. Kontrola obiektu, sprzętu i systemu

1. Administrator danych kontroluje, czy stan obiektu, urządzeń oraz systemu pozwala na należytą realizację obowiązków z zakresu ochrony danych.
2. W ramach kontroli obiektu i sprzętu sprawdzane jest, w szczególności, czy pomieszczenia, komputery i urządzenia służące do przechowywania danych, w tym na papierowych nośnikach, nie wskazują na zagrożenie naruszenia danych osobowych (losowe zewnętrzne, wewnętrzne i zamierzone).
3. Monitoring systemu przeprowadza się przede wszystkim poprzez następujące działania:
   1) okresowe sprawdzanie kopii zapasowych pod względem przydatności do odtworzenia danych,
   2) kontrola ewidencji nośników zewnętrznych.
4. Administrator danych raz na rok dokonuje analizy zagrożeń dla danych osobowych zgromadzonych przez Try IT.

§ 15. Bezpieczeństwo nośników danych

1. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
   1) likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,
   2) przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie,
   3) naprawy – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich

odzyskanie, albo naprawia się je pod nadzorem osoby upoważnionej przez Administratora danych lub w inny sposób gwarantujący zachowanie poufności tych danych.

2. Wydruki zawierające dane osobowe po ich wykorzystaniu są niszczone w sposób uniemożliwiający odczytanie znajdujących się na nich danych.

§ 16. Naruszenia bezpieczeństwa danych

1. Zdarzenia naruszające bezpieczeństwo danych osobowych lub grożące takim naruszeniem dzielą się na:
   1) zagrożenia losowe zewnętrzne (np. pożar, powódź, brak zasilania itp.), które mogą prowadzić do utraty integralności danych, zniszczenia i uszkodzenia infrastruktury technicznej systemu oraz zakłócenia ciągłości jego pracy,
   2) zagrożenia losowe wewnętrzne (np. pomyłki, awarie sprzętowe, błędy oprogramowania itp.), które mogą prowadzić do zniszczenia danych, zakłócić ciągłość pracy systemu, powodować naruszenie poufności danych, integralności danych oraz ich prawidłowości,
   3) zagrożenia zamierzone, świadome i celowe, które polegać mogą na nieuprawnionym dostępie do systemu z jego wnętrza, nieuprawnionym przekazie danych, pogorszeniu jakości sprzętu i oprogramowania, bezpośrednim zagrożeniu materialnych składników systemu.
2. Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia ochrony danych osobowych, w tym zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe, to w szczególności:
   1) sytuacje losowe, nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu (np. pożar, zalanie pomieszczeń, katastrofa budowlana, itp.),
   2) rażące naruszenie dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji, w tym danych osobowych (np. prace na danych osobowych w celach prywatnych, nie zamknięcie pomieszczenia, w którym znajduje się komputer lub urządzenie albo element wyposażenia do przechowywania danych osobowych, itp.),
   3) niewłaściwe parametry środowiska, w którym pracuje sprzęt komputerowy (np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych itp.),
   4) awaria sprzętu lub oprogramowania albo urządzenia lub elementu wyposażenia do przechowywania danych osobowych, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia zabezpieczeń lub ochrony danych, a także niewłaściwe działanie serwisu,
   5) jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
   6) naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,
   7) próba modyfikacji lub modyfikacja danych albo zmiana w strukturze danych bez odpowiedniego upoważnienia,
   8) niedopuszczalna manipulacja danymi osobowymi w systemie,
   9) ujawnienie osobom nieupoważnionym danych osobowych lub procedury przetwarzania albo innych strzeżonych elementów systemu zabezpieczeń,
   10) odstępstwa od założonego rytmu pracy wskazujące na złamanie lub zaniechanie ochrony

danych osobowych, w tym praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywych nieautoryzowanych próbach logowania, itp.

3. Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc i urządzeń (szaf, regałów) służących do przechowywania danych osobowych na papierowych nośnikach, wydrukach, lub innych elektronicznych nośnikach zewnętrznych tych danych.
4. W każdym z przypadków naruszenia ochrony danych osobowych Administrator weryfikuje, czy naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób, których dane dotyczą.
5. Administrator w przypadku stwierdzenia, że naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, zawiadamia niezwłocznie organ nadzorczy, jednak nie później niż w ciągu 72 godzin od chwili identyfikacji naruszenia. Wzór Zgłoszenia naruszenia stanowi **Załącznik nr 7 do Polityki.**
6. W przypadku wystąpienia naruszeń wobec osób, których dane dotyczą, skutkujących ryzykiem naruszenia ich praw lub wolności, Administrator jest zobowiązany je o tym fakcie zawiadomić, chyba że zastosował środki eliminujące prawdopodobieństwo wysokiego ryzyka wystąpienia wyżej wskazanego naruszenia.
7. Administrator dokumentuje naruszenia, które skutkują naruszeniem praw i wolności osób fizycznych - Rejestr naruszeń - zgodnie ze wzorem stanowiącym **Załącznik nr 8 do Polityki.**

§ 17. Obowiązek poinformowania o naruszeniu

1. Każda osoba wykonująca jakiekolwiek zadania w Try IT, która stwierdzi lub podejrzewa naruszenie zabezpieczenia ochrony danych osobowych, zobowiązana jest niezwłocznie informować o tym Administratora danych.
2. Obowiązek, o którym mowa w ust. 1, dotyczy także sytuacji, gdy stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci (w odniesieniu do elektronicznych zbiorów danych) mogą wskazywać na naruszenie zabezpieczeń tych danych.
3. Osoba wykonująca jakiekolwiek zadania przy przetwarzaniu danych osobowych, która uzyskała informację lub sama stwierdziła naruszenie zabezpieczenia bazy danych osobowych w systemie informatycznym lub naruszenie zabezpieczenia zbioru danych przetwarzanych na papierowych nośnikach, zobowiązana jest niezwłocznie powiadomić o tym Administratora danych.
4. Administrator danych w pierwszej kolejności powinien podjąć czynności polegające na:
   1) ustaleniu wszelkich okoliczności związanych z tym zdarzeniem, w szczególności dokładny czas uzyskania informacji o naruszeniu zabezpieczenia danych osobowych i czas samodzielnego wykrycia tego faktu,
   2) niezwłocznym wygenerowaniu i wydrukowaniu (jeżeli zasoby systemu na to pozwalają) wszystkich możliwych dokumentów i raportów, które mogą pomóc w ustaleniu okoliczności zdarzenia, opatrzyć je datą i podpisem, przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, a zwłaszcza do określenia skali naruszeń i metody dostępu do danych osobowych nieuprawnionej osoby.
5. Po wykonaniu ww. czynności, należy niezwłocznie podjąć dalsze odpowiednie kroki w celu powstrzymania lub ograniczania dostępu do danych osoby nieuprawnionej, zminimalizowania

szkód i zabezpieczenia przed usunięciem śladów jej ingerencji, w szczególności przez:

1) fizyczne odłączenie urządzeń i sieci, które mogły umożliwić dostęp do bazy danych osobie nieuprawnionej, w szczególności poprzez dostęp z zewnątrz,
2) przejściowe ograniczenie dostępu dla niektórych osób do danych osobowych przetwarzanych na papierowych nośnikach oraz dokonanie weryfikacji uprawnień do przetwarzania takich danych osobowych, jak również sprawdzenia i weryfikacji ustalonych zasad obiegu dokumentów, zawierających dane osobowe,
3) zmianę hasła do konta, poprzez które uzyskano nielegalny dostęp w celu uniknięcia ponownej próby włamania.

6. Po wyeliminowaniu bezpośredniego zagrożenia Administrator powinien przeprowadzić wstępną analizę stanu systemu informatycznego, w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych.
7. W tym celu Administrator powinien sprawdzić w szczególności:
   1) stan urządzeń wykorzystywanych do przetwarzania danych osobowych,
   2) zawartość zbioru danych osobowych,
   3) sposób działania programu,
   4) jakość komunikacji w sieci,
   5) możliwość obecności wirusów komputerowych.
8. Po dokonaniu czynności, o których mowa powyżej, Administrator danych powinien przeprowadzić szczegółową analizę stanu systemu informatycznego obejmującego identyfikację:
   1) rodzaju zaistniałego zdarzenia,
   2) metody dostępu do danych osoby nieuprawnionej,
   3) skali zniszczeń.
9. Po przywróceniu normalnego stanu działania systemu przetwarzania danych osobowych, jeżeli nastąpiło uszkodzenie bazy danych lub zbioru tradycyjnego, niezbędne jest odtworzenie jej z dostępnych źródeł, w tym z ostatniej kopii zapasowej, z zachowaniem wszelkich środków ostrożności, mających na celu uniknięcie ponownego dostępu tą samą drogą przez osobę nieuprawnioną.
10. Po przywróceniu właściwego stanu bazy danych osobowych, należy przeprowadzić szczegółową analizę przyczyny naruszenia ochrony danych osobowych oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości. Jeśli przyczyną był:
    1) błąd osoby wykonującej jakiekolwiek zadania przy przetwarzaniu danych osobowych w systemie informatycznym, należy przeprowadzić szkolenie osób biorących udział przy przetwarzaniu danych,
    2) uaktywnienie wirusa, należy ustalić źródło jego pochodzenia oraz zainstalować zabezpieczenia antywirusowe lub sprawdzić stan istniejących zabezpieczeń,
    3) zaniedbanie ze strony osoby wykonującej jakiekolwiek zadania przy przetwarzaniu danych osobowych, należy wyciągnąć odpowiednie konsekwencje,
    4) włamanie w celu uzyskania bazy danych osobowych, należy dokonać szczegółowej analizy wdrożonych środków zabezpieczających w celu zapewnienia skutecznej ochrony danych osobowych,
    5) zły stan urządzenia, w tym urządzenia do przechowywania danych utrwalonych na

papierowych nośnikach, lub sposób działania programu, należy niezwłocznie przeprowadzić kontrolne czynności serwisowe.

11. Administrator danych zobowiązany jest przygotować szczegółowy raport o przyczynach, przebiegu i wnioskach ze zdarzenia i podjąć czynności zmierzające do usunięcia jego skutków.

§ 18. Rejestr czynności przetwarzania

1. Administrator prowadzi rejestr czynności przetwarzania danych osobowych, o którym mowa w art. 30 ust. 1 RODO. Rejestr stanowi **Załącznik nr 9 do Polityki**.
2. Rejestr, o którym mowa w ust. 1, ma formę pisemną oraz formę elektroniczną.

§ 19. Postępowanie w przypadku realizacji praw osób których dane dotyczą

1. Administrator danych odpowiada za prawidłowość procedury realizacji praw osób, których dane dotyczą. Każdy przypadek zgłoszenia woli skorzystania z praw przewidzianych w RODO przez taką osobę, Administrator danych rozpatruje indywidualnie.
2. Administrator zobowiązany jest bez zbędnej zwłoki zrealizować prawa osób, których dane dotyczą, w zakresie:
   1) prawa dostępu do danych,
   2) prawa do sprostowania danych,
   3) prawa do usunięcia danych,
   4) prawa do przenoszenia danych,
   5) prawa do sprzeciwu wobec przetwarzania danych,
   6) prawa do niepodlegania decyzjom oparty wyłącznie na profilowaniu.
3. W przypadku realizacji prawa do sprostowania, usunięcia i ograniczenia przetwarzania danych Administrator niezwłocznie informuje odbiorców danych, którym udostępnił on przedmiotowe dane, chyba że jest to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.
4. Administrator odmawia realizacji praw osób, których dane dotyczą, jeżeli możliwość taka wynika z RODO, jednak każda odmowa realizacji praw osób, których dane dotyczą, wymaga uzasadnienia z podaniem podstawy prawnej wynikającej z RODO.
5. W każdym przypadku pobierania danych bezpośrednio od osoby, której dane dotyczą, Administrator informuje osobę, której dane dotyczą, o zakresie i sposobie w jaki przetwarza dane.
6. W każdym przypadku pobierania danych z innych źródeł niż osoba, której dane dotyczą, Administrator informuje osobę, której dane dotyczą, niezwłocznie, jednak nie później niż przy pierwszym kontakcie z osobą, której dane dotyczą.

§20. Postanowienia końcowe

1. Wszelkie zasady opisane w niniejszym dokumencie są przestrzegane przez osoby upoważnione do przetwarzania danych osobowych ze szczególnym uwzględnieniem dobra osób, których dane te dotyczą.
2. Dokument niniejszy obowiązuje od dnia jego zatwierdzenia przez Administratora danych.