POLITYKA OCHRONY DANYCH OSOBOWYCH

Środki techniczne i organizacyjne Ochrony Danych Osobowych

infraTEAM

Wioletta Curyło

ul. Plebiscytowa 1

44-100 GLIWICE

Zawartość

Wstęp

Realizując postanowienia Rozporządzenia 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.U. UE L 119, s. 1) w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informacyjne służące do przetwarzania danych osobowych **wprowadza się** zestaw reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji danych osobowych, w tym danych szczególnych kategorii (wrażliwych) pozwalający na zapewnienie właściwego stopnia ich ochrony, zwany dalej Polityką Ochrony Danych Osobowych (w skrócie **Polityka**).

Celem **Polityki** jest zapewnienie ochrony danych osobowych przetwarzanych przez **infraTEAM ul. Plebiscytowa 1, 44-100 Gliwice,** zwaną dalej **infraTEAM** w celach określonych w art. 6 i art. 9 Rozporządzenia 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.U. UE L 119, s. 1) zwanego dalej **RODO** przed wszelkiego rodzaju zagrożeniami, tak wewnętrznymi jak i zewnętrznymi, świadomymi lub nieświadomymi.

Polityka obowiązuje wszystkich pracowników **infraTEAM**, w tym również stażystów, wolontariuszy, praktykantów oraz dostawców, podmioty współpracujące na podstawie umów cywilnoprawnych, mające jakikolwiek kontakt z danymi osobowymi objętymi ochroną.

Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:

Legalność – **infraTEAM** dba o ochronę prywatności i przetwarza dane zgodnie z prawem.

Bezpieczeństwo – **infraTEAM** zapewnia odpowiedni poziom bezpieczeństwa danych podejmując stale działania w tym zakresie.

Prawa jednostki – **infraTEAM** umożliwia osobom, których dane przetwarza, realizowanie swoich praw i prawa te respektuje.

Poufność – **infraTEAM** zapewnia, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom,

Integralność – **infraTEAM** zapewnia, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany,

Rozliczalność – **infraTEAM** dokumentuje to, w jaki sposób spełnia obowiązki wynikające z RODO, aby w każdej chwili móc wykazać zgodność przetwarzania danych osobowych z RODO przez prowadzenie rejestru czynności przetwarzania danych – **załącznik nr 7** i rejestru kategorii czynności – **załącznik nr 8,**

Autentyczność – **infraTEAM** zapewnia, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana (autentyczność dotyczy danych, użytkowników, procesów, systemów i informacji),

Niezaprzeczalność – **infraTEAM** zapewnia, że nie wyprze się swego uczestnictwa w całości lub w części wymiany danych z innym podmiotem,

Przetwarzanie danych osobowych w **infraTEAM** odbywa się w wersji papierowej i za pomocą systemów informatycznych.

Prawne determinanty przetwarzania danych osobowych:

1. Konstytucja RP (art. 47, art. 51).
2. 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.U. UE L 119, s. 1) zwane dalej RODO.
3. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych.
4. Ustawa z dnia 7 listopada 2014 r. o ułatwieniu wykonywania działalności gospodarczej.
5. Kodeks pracy.
6. Kodeks cywilny.

Rozdział I Postanowienia ogólne

1. **Administrator Danych Osobowych (ADO),** - należy przez to rozumieć: **Wioletta Curyło.**
2. **Inspektor Ochrony Danych (IOD)** – powołany - **nie dotyczy.**
3. **Administrator Systemu Informatycznego (ASI)** - należy przez to rozumieć osobę odpowiedzialną za funkcjonowanie systemu informatycznego, wyznaczoną przez ADO, **- Mikołaj Salamak.**
4. **Polityka Ochrony Danych Osobowych** – rozumie się przez to zestaw technicznych i organizacyjnych środków ochrony danych osobowych wprowadzonych, wdrożonych i stosowanych w **infraTEAM** niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych opisanych w niniejszym dokumencie**.**
5. **RODO** - Rozporządzenia 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.U. UE L 119, s. 1) - **załącznik nr 28.**
6. **Dane osobowe (dane)** - art. 4 ust. 1 RODO – 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, jeden bądź kilka szczególnych czynników określających: fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
7. **Dane szczególnych kategorii (wrażliwe)** – dane zawierające informacje takie jak: pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane o stanie zdrowia, dane dotyczące seksualności lub orientacji seksualnej, dane biometryczne, kod genetyczny.
8. **Usuwanie danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą (anonimizacja danych).
9. **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;

10. **Ograniczenie przetwarzania** - oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
11. **Zgoda osoby, której dane dotyczą** – rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.
12. **Baza danych osobowych** - zbiór uporządkowanych powiązanych ze sobą tematycznie danych zapisanych np. w pamięci wewnętrznej czy zewnętrznej komputera. Baza danych jest złożona z elementów o określonej strukturze - rekordów lub obiektów, w których są zapisane dane osobowe.
13. **Przetwarzanie danych** - 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, modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
14. **Obszar przetwarzania** - należy przez to rozumieć pomieszczenia biurowe, w których pracownicy **infraTEAM** przetwarzają dane osobowe. Wykaz budynków i pomieszczeń stanowiących obszar przetwarzania danych osobowych wraz z ilustracja graficzną znajduje się w **załączniku nr 23.**
15. **Zbiór danych osobowych** - należy przez to rozumieć każdy posiadający strukturę zestaw danych o charakterze osobowym dostępnych według określonych kryteriów niezależnie od jego rozproszenia czy podziału.
16. **System informatyczny, system teleinformatyczny, system** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
17. **Rejestr czynności przetwarzania** - należy przez to rozumieć dokument, który ma pokazywać w szczególności w jakich procesach w **infraTEAM** są przetwarzane dane osobowe, w jakim celu, kogo dotyczą oraz jak są zabezpieczane. Dokument ten będzie musiał zostać udostępniony na każde wezwanie PUODO - **załącznik nr 7.**
18. **Procedury bezpieczeństwa** - należy przez to rozumieć procedury mające na celu zabezpieczenie przetwarzanych danych osobowych.
19. **Pseudonimizacja** – oznacza przetworzenie danych osobowych w taki sposób, by nie można było ich przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych

informacji, pod warunkiem, że informacje są przechowywane osobno i objęte są środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej osobie. Pseudonimizacja danych osobowych oznacza więc pozbawienie informacji cech danych osobowych, a zatem możliwości identyfikacji na ich podstawie osoby fizycznej.

Ochrona danych w infraTEAM

Zasady ogólne

Zasady ochrony danych:

infraTEAM przetwarza dane osobowe z poszanowaniem następujących zasad:

a. w oparciu o podstawę prawną i zgodnie z prawem (legalizm);
b. rzetelnie i uczciwie (rzetelność);
c. w sposób przejrzysty dla osoby, której dane dotyczą (transparentność);
d. w konkretnych celach i nie „na zapas" (minimalizacja);
e. nie więcej niż potrzeba (adekwatność);
f. z dbałością o prawidłowość danych (prawidłowość);
g. nie dłużej niż potrzeba (czasowość);
h. zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo).

System ochrony danych osobowych w **infraTEAM** składa się z następujących elementów:

1. Inwentaryzacja danych. **infraTEAM** dokonuje identyfikacji zasobów danych osobowych, klas danych, zależności między zasobami danych, identyfikacji sposobów wykorzystania danych i na podstawie tej inwentaryzacji prowadzi rejestr czynności przetwarzania danych- **załącznik nr 7,** w tym:
   a) przypadków przetwarzania danych szczególnych kategorii i danych „kryminalnych" (wyroki skazujące, naruszenia prawa) - identyfikuje się przypadki, w których przetwarza się lub może dojść do przetwarzania danych szczególnych kategorii (wrażliwe i dane karne) oraz utrzymuje dedykowane mechanizmy zapewnienia zgodności z prawem przetwarzania szczególnych kategorii danych - **załącznik nr 7**.
   b) przypadków przetwarzania danych osób, których **infraTEAM** nie identyfikuje (dane niezidentyfikowane/UFO) - ADO identyfikuje przypadki, w których przetwarza lub może przetwarzać dane niezidentyfikowane i utrzymuje mechanizmy ułatwiające realizację praw osób, których dotyczą dane niezidentyfikowane - **załącznik nr 7**.
   c) przypadków przetwarzania danych dzieci - **załącznik nr 7**;
   d) profilowania; ADO identyfikuje przypadki, w których dokonuje profilowania przetwarzanych

danych i utrzymuje mechanizmy zapewniające zgodność tego procesu z prawem. W przypadku zidentyfikowania przypadków profilowania i zautomatyzowanego podejmowania decyzji, ADO postępuje zgodnie z przyjętymi zasadami w tym zakresie - **załącznik nr 7**.

e) współadministrowania danymi; ADO identyfikuje przypadki współadministrowania danymi i postępuje w tym zakresie zgodnie z przyjętymi zasadami - **załącznik nr 7**.

2. **infraTEAM** opracował, prowadzi, utrzymuje i aktualizuje Rejestr Czynności Przetwarzania Danych Osobowych (RCPD). Rejestr jest narzędziem rozliczania zgodności z ochroną danych w **infraTEAM**.
   a) RCPD stanowi formę dokumentowania czynności przetwarzania danych, pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności.
   b) ADO prowadzi Rejestr Czynności Przetwarzania Danych (**załącznik nr 7)**, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe.
   c) Rejestr jest jednym z podstawowych narzędzi umożliwiających ADO rozliczanie większości obowiązków ochrony danych.
   d) W Rejestrze, dla każdej czynności przetwarzania danych, którą ADO uznała za odrębną dla potrzeb Rejestru, ADO odnotowuje co najmniej:
      - nazwę czynności,
      - cel przetwarzania,
      - opis kategorii osób,
      - opis kategorii danych,
      - podstawę prawną przetwarzania, wraz z wyszczególnieniem kategorii uzasadnionego interesu ADO, jeśli podstawą jest uzasadniony interes,
      - sposób zbierania danych,
      - opis kategorii odbiorców danych (w tym przetwarzających),
      - informację o przekazaniu poza EU/EOG;
      - ogólny opis technicznych i organizacyjnych środków ochrony danych.
   e) Rejestr stanowi **Załącznik nr 7** do Polityki. Rejestr zawiera także kolumny nieobowiązkowe. W kolumnach nieobowiązkowych ADO rejestruje informacje w miarę potrzeb i możliwości, z uwzględnieniem tego, że pełniejsza treść Rejestru ułatwia zarządzanie zgodnością ochrony danych i rozliczenie się z niej.

f) **infraTEAM** prowadzi rejestr kategorii czynności, w którym dokumentuje kategorie przetwarzań danych osobowe powierzone przez administratorów danych na podstawie umów powierzenia – **załącznik nr 8**. Rejestr ten odnotowuje następujące dane:
   - kategorie przetwarzań,
   - ogólny opis technicznych i organizacyjnych środków bezpieczeństwa,
   - nazwa i dane kontaktowe administratora,
   - nazwa i dane kontaktowe przedstawiciela administratora (jeśli wyznaczono),
   - Inspektor ochrony danych administratora (jeśli powołano),
   - nazwy państw trzecich lub organizacji międzynarodowych, do których dane są przekazywane,
   - dokumentacja odpowiednich zabezpieczeń danych osobowych przekazywanych na podstawie art. 49 ust. 1 akapit drugi,
   - ewentualne inne dane które w uznaniu ADO mogą dodatkowo pomóc w dokumentowaniu zasady rozliczalności danych.

g) **infraTEAM** dokonuje oceny skutków dla ochrony danych (ang. Data Protection Impact Assessment, DPIA) – **załącznik nr 10**, w przypadku wysokiego ryzyka naruszenia praw lub wolności osób fizycznych.

   Ryzyko dla ochrony danych osobowych może wynikać z:
   - charakteru,
   - zakresu,
   - kontekstu,
   - celów przetwarzania.

   Operacje przetwarzania, które wiążą się z wysokim ryzykiem naruszenia praw lub wolności osób fizycznych, obejmują w szczególności operacje, które:
   - wiążą się z użyciem nowych technologii;
   - są nowe i nie zostały jeszcze poddane przez administratora ocenie skutków dla ochrony danych;
   - stały się niezbędne z uwagi na upływ czasu od pierwotnego przetwarzania.

   Wysokie ryzyko naruszenia praw lub wolności osób fizycznych zachodzi w szczególności w przypadku:
   - systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu i jest podstawą decyzji wywołujących skutki wobec osoby fizycznej;

- przetwarzania na dużą skalę danych wrażliwych, genetycznych, biometrycznych, lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa;
- systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.

3. Podstawy prawne. **infraTEAM** zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania danych i rejestruje je w Rejestrze (RCPD), w tym:
   a) zarządza zgodami na przetwarzanie danych i komunikację na odległość,
   b) inwentaryzuje i uszczegóławia uzasadnienie przypadków, gdy przetwarza dane na podstawie prawnie uzasadnionego interesu – **załącznik nr 7**.
   c) ADO dokumentuje w Rejestrze podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania,
   d) wskazując ogólną podstawę prawną (zgoda, umowa, obowiązek prawny, żywotne interesy, zadanie publiczne/władza publiczna, uzasadniony cel ADO) **infraTEAM** 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, porozumienie administracyjne, żywotne interesy – wskazując na kategorie zdarzeń, w których się zmaterializują, uzasadniony cel – wskazując na konkretny cel, np. marketing własny, dochodzenie roszczeń,
   e) ADO zarządza zgodami **(załącznik 5)** weryfikuje 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 i podobnych czynności (sprzeciw, ograniczenie itp.) **załącznik 5b**.
4. Obsługa praw jednostki. **infraTEAM** spełnia obowiązki informacyjne względem osób, których dane przetwarza, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:
   a) obowiązki informacyjne; **infraTEAM** przekazuje osobom prawem wymagane informacje przy zbieraniu danych i w innych sytuacjach oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków – informacje te dostępne są w siedzibie **infraTEAM**, na w postaci klauzul na zgodach na przetwarzanie danych, klauzula na stronie internetowej.
   b) **infraTEAM** weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu zgodnego z prawem żądania dotyczącego danych osobowych osoby fizycznej przez siebie i swoich przetwarzających.
   c) **infraTEAM** zapewnia odpowiednie nakłady i procedury, aby żądania osób były realizowane

w terminach i w sposób wymagany przez RODO i dokumentowane.

d) **infraTEAM** ocenia skutek naruszenia ochrony danych na prawa i wolności osoby fizycznej pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.

Sposób obsługi praw jednostki i obowiązków informacyjnych:

a) ADO dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza.

b) ADO ułatwia osobom korzystanie z ich praw poprzez różne działania, w tym: zamieszczenie na stronie internetowej ADO informacji lub odwołań (linków) do informacji o prawach osób, sposobie skorzystania z nich w **infraTEAM,** w tym wymaganiach dotyczących identyfikacji, metodach kontaktu z ADO w tym celu, ewentualnym cenniku żądań „dodatkowych" – **załącznik nr 30**, itp.

c) ADO dba o dotrzymywanie prawnych terminów realizacji obowiązków względem osób.

d) **infraTEAM** identyfikuje i uwierzytelniania osoby dla potrzeb realizacji praw jednostki i obowiązków informacyjnych.

5. Minimalizacja. **infraTEAM** przestrzega zasad i metod zarządzania minimalizacją, a w tym:
   a) dba o adekwatnością danych;
   b) przestrzega reglamentacji i zarządzania dostępem do danych;
   c) przestrzega okresów przechowywania danych i weryfikuje ich dalszą przydatność;
6. Bezpieczeństwo. **infraTEAM** zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:
   a) przeprowadza analizy ryzyka dla czynności przetwarzania danych lub ich kategorii;
   b) przeprowadza oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie;
   c) dostosowuje środki ochrony danych do ustalonego ryzyka;
   d) posiada system zarządzania bezpieczeństwem informacji w postaci odpowiedniej polityki;
   e) **infraTEAM** identyfikuje, ocenia i zgłasza zidentyfikowane naruszenia ochrony danych Urzędowi Ochrony Danych − zarządza incydentami.
7. Przetwarzający. **infraTEAM** przestrzega zasady doboru przetwarzających dane na jego rzecz, wymogów co do warunków przetwarzania (umowa powierzenia), weryfikuje wykonywanie umów powierzenia.
8. Eksport danych. **infraTEAM** weryfikuje, czy nie przekazuje danych do państw trzecich (czyli poza UE, Norwegię, Lichtenstein, Islandię) lub do organizacji międzynarodowych oraz zapewnienia zgodne z prawem warunki takiego przekazywania, jeśli ma ono miejsce.
9. Privacy by design. **infraTEAM** zarządza zmianami mającymi wpływ na prywatność. W tym celu

procedury uruchamiania nowych projektów i inwestycji uwzględniają konieczność oceny wpływu zmiany na ochronę danych, zapewnienie prywatności (a w tym zgodności celów przetwarzania, bezpieczeństwa danych i minimalizacji) już w fazie projektowania zmiany, inwestycji czy na początku nowego projektu.

10. Obowiązki informacyjne
    a) ADO określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych – wywieszki z klauzulą obowiązku informacyjnego, klauzule na zgodach i stronie internetowej.
    b) ADO informuje osobę o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie żądania tej osoby.
    c) ADO informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby.
    d) ADO informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych o tej osobie niebezpośrednio od niej.
    e) ADO określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych, tam gdzie to jest możliwe (np. tabliczka o objęciu obszaru monitoringiem wizyjnym).
    f) ADO informuje osobę o planowanej zmianie celu przetwarzania danych.
    g) ADO informuje osobę przed uchyleniem ograniczenia przetwarzania.
    h) ADO informuje odbiorców danych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych (chyba że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe).
    i) ADO informuje osobę o prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą.
    j) ADO bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.
11. Żądania osób:
    a) Prawa osób trzecich. Realizując prawa osób, których dane dotyczą, **infraTEAM** wprowadza gwarancje ochrony praw i wolności osób trzecich. W szczególności w przypadku powzięcia wiarygodnej wiadomości o tym, że wykonanie żądania osoby o wydanie kopii danych lub prawa do przeniesienia danych może niekorzystnie wpłynąć na prawa i wolności innych osób (np. prawa związane z ochroną danych innych osób, prawa własności intelektualnej, tajemnicę handlową, dobra osobiste itp.), **infraTEAM** może zwrócić się do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu.
    b) Nieprzetwarzanie. **infraTEAM** informuje osobę o tym, że nie przetwarza danych jej

dotyczących, jeśli taka osoba zgłosiła żądanie dotyczące jej praw.

c) Odmowa. **infraTEAM** informuje osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych.

d) Dostęp do danych. Na żądanie osoby dotyczące dostępu do jej danych, **infraTEAM** informuje osobę, czy przetwarza jej dane oraz informuje osobę o szczegółach przetwarzania, zgodnie z art. 15 RODO (zakres odpowiada obowiązkowi informacyjnemu przy zbieraniu danych), a także udziela osobie dostępu do danych jej dotyczących. Dostęp do danych może być zrealizowany przez wydanie odpłatnych kopii danych, z zastrzeżeniem, że kopię danych wydaną dla wykonania prawa dostępu do danych **infraTEAM** nie uzna za pierwszą nieodpłatną kopię.

e) Kopie danych. Na żądanie **infraTEAM** wydaje osobie kopię danych jej dotyczących **infraTEAM** wprowadza i utrzymuje cennik kopii danych, zgodnie z którym pobiera opłaty za kolejne kopie danych. Cena kopii danych skalkulowana jest w oparciu o oszacowany jednostkowy koszt obsługi żądania wydania kopii danych – **załącznik nr 30.**

f) Sprostowanie danych. **infraTEAM** dokonuje sprostowania nieprawidłowych danych na żądanie osoby. **infraTEAM** ma prawo odmówić sprostowania danych, chyba że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga. W przypadku sprostowania danych **infraTEAM** informuje osobę o odbiorcach danych, na żądanie tej osoby.

g) Uzupełnienie danych. **infraTEAM** uzupełnia i aktualizuje dane na żądanie osoby. **infraTEAM** ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych (np. **infraTEAM** nie musi przetwarzać danych, które są mu zbędne). **infraTEAM** może polegać na oświadczeniu osoby, co do uzupełnianych danych, chyba że będzie to niewystarczające w świetle prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.

h) Usunięcie danych. Na żądanie osoby, **infraTEAM** usuwa dane, gdy:
   - dane nie są niezbędne do celów, w których zostały zebrane ani przetwarzane w innych celach,
   - zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania,
   - osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,
   - dane były przetwarzane niezgodnie z prawem,
   - konieczność usunięcia wynika z obowiązku prawnego,

- żądanie dotyczy danych dziecka zebranych na podstawie zgody w celu świadczenia usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku.

ADO określa sposób obsługi prawa do usunięcia danych w taki sposób, aby zapewnić efektywną realizację tego prawa przy poszanowaniu wszystkich zasad ochrony danych, w tym bezpieczeństwa, a także weryfikację, czy nie zachodzą wyjątki, o których mowa w art. 17. ust. 3 RODO.

Jeżeli dane podlegające usunięciu zostały upublicznione przez ADO, podejmuje on rozsądne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane osobowe, o potrzebie usunięcia danych i dostępu do nich.

W przypadku usunięcia danych ADO informuje osobę o odbiorcach danych, na żądanie tej osoby.

i) Ograniczenie przetwarzania. ADO dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:
   - osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość,
   - przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,
   - ADO nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,
   - osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, czy po stronie ADO zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.

   W trakcie ograniczenia przetwarzania ADO przechowuje dane, natomiast nie przetwarza ich (nie wykorzystuje, nie przekazuje), bez zgody osoby, której dane dotyczą, chyba że w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego.

   ADO informuje osobę przed uchyleniem ograniczenia przetwarzania.

   W przypadku ograniczenia przetwarzania danych ADO informuje osobę o odbiorcach danych, na żądanie tej osoby.

j) Przenoszenie danych. Na żądanie osoby ADO wydaje w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego lub przekazuje innemu podmiotowi, jeśli jest to możliwe, dane dotyczące tej osoby, które dostarczyła ona ADO, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy

z nią zawartej, w systemach informatycznych ADO.

k) Sprzeciw w szczególnej sytuacji. Jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, a dane przetwarzane są przez **infraTEAM** w oparciu o uzasadniony interes ADO lub o powierzone **infraTEAM** zadanie w interesie publicznym, ADO uwzględni sprzeciw, o ile nie zachodzą po jego stronie ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.

l) Sprzeciw przy badaniach naukowych, historycznych lub celach statystycznych. Jeżeli ADO prowadzi badania naukowe, historyczne lub przetwarza dane w celach statystycznych, osoba może wnieść umotywowany jej szczególną sytuacją sprzeciw względem takiego przetwarzania. ADO uwzględni taki sprzeciw, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

m) Sprzeciw względem marketingu bezpośredniego. Jeżeli osoba zgłosi sprzeciw względem przetwarzania jej danych przez ADO na potrzeby marketingu bezpośredniego (w tym ewentualnie profilowania), ADO uwzględni sprzeciw i zaprzestanie takiego przetwarzania.

n) Prawo do ludzkiej interwencji przy automatycznym przetwarzaniu. Jeżeli ADO przetwarza dane w sposób automatyczny, w tym w szczególności profiluje osoby, i w konsekwencji podejmuje względem osoby decyzje wywołujące skutki prawne lub inaczej istotnie wpływające na osobę, ADO zapewnia możliwość odwołania się do interwencji i decyzji człowieka po stronie ADO, chyba że taka automatyczna decyzja:

- jest niezbędna do zawarcia lub wykonania umowy między odwołującą się osobą a ADO; lub:
- jest wprost dozwolona przepisami prawa; lub:
- opiera się na wyraźnej zgodzie odwołującej osoby.

12. Minimalizacja:

ADO dba o minimalizację przetwarzania danych pod kątem:

- adekwatności danych do celów (ilości danych i zakresu przetwarzania),
- dostępu do danych,
- czasu przechowywania danych.

a) Minimalizacja zakresu

ADO zweryfikował zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania w ramach

wdrożenia RODO.

ADO dokonuje okresowego przeglądu ilości przetwarzanych danych i zakresu ich przetwarzania nie rzadziej niż raz na rok.

ADO corocznie przeprowadza weryfikację zmian co do ilości i zakresu przetwarzania danych.

b) Minimalizacja dostępu

ADO stosuje ograniczenia dostępu do danych osobowych: prawne (zobowiązania do poufności, zakresy upoważnień), fizyczne (strefy dostępu, zamykanie pomieszczeń) i logiczne (ograniczenia uprawnień do systemów przetwarzających dane osobowe i zasobów sieciowych, w których rezydują dane osobowe).

ADO stosuje kontrolę dostępu fizycznego.

ADO dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób, oraz zmianach podmiotów przetwarzających.

ADO dokonuje okresowego przeglądu ustanowionych użytkowników systemów i aktualizuje ich nie rzadziej niż raz na rok.

Szczegółowe zasady kontroli dostępu fizycznego i logicznego zawarte są w procedurach bezpieczeństwa informacji niniejszej polityki **infraTEAM**.

c) Minimalizacja czasu

ADO wdraża mechanizmy kontroli cyklu życia danych osobowych w **infraTEAM**, w tym weryfikacji dalszej przydatności danych względem terminów i punktów kontrolnych wskazanych w Rejestrze.

Dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu są usuwane z systemów **infraTEAM**, jak też z akt podręcznych i głównych. Dane takie mogą być archiwizowane oraz znajdować się na kopiach zapasowych systemów i informacji przetwarzanych przez ADO. Procedury archiwizacji i korzystania z archiwów, tworzenia i wykorzystania kopii zapasowych uwzględniają wymagania kontroli nad cyklem życia danych, a w tym wymogi usuwania danych. Okres przechowywania danych opisuje **załącznik nr 7.**

13. Bezpieczeństwo:

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

a) Analizy ryzyka i adekwatności środków bezpieczeństwa

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

1) ADO zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji,

cyberbezpieczeństwie i ciągłości działania − wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych.

2) ADO kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają – **załącznik nr 6**.
3) ADO przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. ADO 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 - **załącznik nr 6**.
4) ADO ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa. W tym ADO ustala przydatność i stosuje takie środki i podejście jak:
   - pseudonimizacja,
   - szyfrowanie danych osobowych,
   - inne środki cyberbezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
   - środki zapewnienia ciągłości działania i zapobiegania skutkom katastrof, czyli zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego – np. polityka kopii zapasowych.

b) Oceny skutków dla ochrony danych

ADO dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych tam, gdzie zgodnie z analizą ryzyka ryzyko naruszenia praw i wolności osób jest wysokie.

c) Środki bezpieczeństwa

ADO stosuje środki bezpieczeństwa ustalone w ramach analiz ryzyka i adekwatności środków bezpieczeństwa oraz ocen skutków dla ochrony danych.

Środki bezpieczeństwa danych osobowych stanowią element środków bezpieczeństwa informacji i zapewnienia cyberbezpieczeństwa w **infraTEAM** i są bliżej opisane w procedurach przyjętych przez ADO dla tych obszarów (Instrukcja Bezpieczeństwa przetwarzania danych osobowych).

d) Zgłaszanie naruszeń

ADO identyfikuje, ocenia i zgłasza zidentyfikowane naruszenia ochrony danych Urzędowi Ochrony Danych w terminie **72 godzin** od ustalenia naruszenia, informuje Administratorów Danych w przypadku powierzenia danych o zaistniałym incydencie w ciągu 24 godzin od

ustalenia naruszenia.

14. Przetwarzający

ADO dobiera i weryfikuje przetwarzających dane na rzecz **infraTEAM** 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 **infraTEAM**.

ADO przyjął minimalne wymagania co do umowy powierzenia przetwarzania danych stanowiące **załącznik nr 20** do Polityki – umowa powierzenia przetwarzania danych.

ADO rozlicza przetwarzających z wykorzystania podprzetwarzających, jak też z innych wymagań wynikających z zasad powierzenia danych osobowych.

15. Eksport danych

ADO rejestruje w Rejestrze przypadki eksportu danych, czyli przekazywania danych poza Europejski Obszar Gospodarczy (EOG w 2017 r. = Unia Europejska, Islandia, Lichtenstein i Norwegia) – **załącznik 14a.**

16. Projektowanie prywatności

ADO 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 inwestycji przez **infraTEAM** 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 inwestycji.

Rozdział II Administrator Danych Osobowych, Inspektor Ochrony Danych

Obowiązki i zadania Administratora Danych Osobowych

Podmiotem odpowiedzialnym za przetwarzanie danych jest administrator i to on deleguje obowiązki inspektorowi ochrony danych (jeśli został powołany) oraz swoim pracownikom. Na administratorze ciąży odpowiedzialność prawna za wywiązanie się ze swoich obowiązków w związku z przetwarzaniem danych osobowych przez niego samego lub w jego imieniu. Podstawowym obowiązkiem administratora jest dbanie o to aby przetwarzanie odbywało się zgodnie z rozporządzeniem RODO i aby móc to wykazać. W tym celu, ma on wdrażać odpowiednie i skuteczne środki techniczne i organizacyjne:

1) mają one zapewniać najwyższy znany i możliwy w chwili przetwarzania danych, poziom ochrony;
2) nie może być to czynność jednorazowa, środki te są w razie potrzeby poddawane przeglądom i uaktualniane;
3) dokonuje on tego, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia;
4) środki te obejmują wdrożenie przez administratora polityki ochrony danych.

Ryzyko naruszenia praw lub wolności osób o różnym prawdopodobieństwie i wadze zagrożeń:

1) może wynikać z przetwarzania danych osobowych mogącego prowadzić do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych, jeżeli przetwarzanie:
   a) dotyczy danych wielkoskalowych (dużej ilości danych osobowych);
   b) wpływa na dużą liczbę osób, których dane dotyczą, w szczególności:

      jeżeli przetwarzanie może poskutkować dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą zawodową, nieuprawnionym odwróceniem pseudonimizacji lub wszelką inną znaczną szkodą gospodarczą lub społeczną; jeżeli osoby, których dane dotyczą, mogą zostać pozbawione przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi; jeżeli przetwarzane są dane osobowe zawierające informacje takie jak: pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane o stanie zdrowia, dane dotyczące seksualności lub orientacji seksualnej, dane biometryczne, kod genetyczny;

jeżeli oceniane są czynniki osobowe, w szczególności analizowane lub prognozowane aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się – w celu tworzenia lub wykorzystywania profili osobistych; lub jeżeli przetwarzane są dane osobowe osób wymagających szczególnej opieki, w szczególności dzieci; jeżeli przetwarzanie dotyczy dużej ilości danych osobowych i wpływa na dużą liczbę osób, których dane dotyczą,

2) ADO szacuje ryzyko na podstawie obiektywnej oceny, w ramach której stwierdza się, czy z operacjami przetwarzania danych wiąże się ryzyko lub wysokie ryzyko.

Odnośnie obowiązku informacyjnego, administrator danych:

1) prowadzi komunikację z podmiotami danych (osobami fizycznymi) i przekazuje im informacje w sposób zwięzły, przejrzysty, zrozumiały i łatwo dostępny,
2) ułatwia podmiotom danych wykonywanie ich praw,
3) nieodpłatnie udziela podmiotom danych informacji, również na ich żądanie, czas na udzielenie informacji przez ADO to maksymalnie miesiąc; w sytuacjach skomplikowanych okres ten może zostać wydłużony do dwóch miesięcy,
4) weryfikuje tożsamość osób wnoszących żądania udzielenia informacji.

Odnośnie praw osoby, której dane dotyczą:

1) ADO potwierdza czy przetwarzane są dane osobowe dotyczące danej osoby fizycznej, a jeżeli ma to miejsce, udziela wskazanych rozporządzeniem informacji;
2) ułatwia osobie, której dane dotyczą wykonywanie jej praw z art. 15–22;
3) informuje osobę, której dane dotyczą, o działaniach jakie podjął, w związku z jej żądaniami opartymi o art. 15-22;
4) uzasadnienia odrzucenie żądania osoby, której dane dotyczą i poucza ją o prawie skargi;
5) umożliwia dostęp do jej danych osobie, której one dotyczą;
6) dokonuje sprostowania i uzupełniane danych;
7) usuwa dane;
8) ogranicza przetwarzanie danych;
9) powiadamia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu ich przetwarzania;
10) dokonuje przenoszenia danych.

Administrator Danych jest zobowiązany przez RODO do:

1. Wskazania podstawy prawnej do legalnego przetwarzania danych osobowych.
2. Zabezpieczenia przetwarzanych danych osobowych przed ich udostępnieniem osobom nieupoważnionym oraz zabraniem przez osobę nieuprawnioną.
3. Przetwarzania danych zgodnie z wymogami RODO.
4. Chronienia danych przed zmianą, utratą, uszkodzeniem lub zniszczeniem.

Zadania te powinny zostać zrealizowane poprzez:

1. Opracowanie dokumentacji.
2. Prowadzenie ewidencje osób upoważnionych do przetwarzania danych osobowych - **załącznik nr 2,** w tym również stażystów, wolontariuszy, praktykantów, uczniów przetwarzających dane w **infraTEAM.**
3. Monitorowanie czynności wykonywanych na zbiorze danych.
4. Zapewnienie technicznych środków bezpieczeństwa.

Administrator Danych Osobowych w celu zapewnienia ochrony danych osobowych może powołać:

1. Inspektora Ochrony Danych (IOD) - **załącznik nr 12**.
2. Administratora Systemu Informatycznego (ASI) - **załącznik nr 13**.

Obowiązki i zadania IOD (art. 39 ust. 1 RODO)

1. Do obowiązków Inspektora Ochrony Danych należą:
   a. informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy rozporządzenia RODO oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
   b. monitorowanie przestrzegania rozporządzenia RODO, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
   c. udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35;
   d. współpraca z organem nadzorczym;
   e. pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach;

f. 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 niniejszego rozporządzenia.
g. prowadzenie rejestru czynności lub rejestru kategorii czynności.

Prawa Inspektora Ochrony Danych (IOD)

IOD ma prawo do:

a) wyznaczania, rekomendowania i egzekwowania wykonania zadań związanych z ochroną danych osobowych w całej organizacji;
b) wstępu do pomieszczeń w których zlokalizowane są zbiory danych i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z RODO, żądać złożenia pisemnych lub ustnych wyjaśnień w zakresie niezbędnym do ustalenia stanu faktycznego;
c) żądania okazania dokumentów i wszelkich danych mających bezpośredni związek z problematyką kontroli;
d) żądania udostępnienia do kontroli urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych;

Obowiązki i zadania Administratora Systemów Informatycznych (ASI)

1. Administrator Systemów Informatycznych odpowiada za sprawne działanie systemów teleinformatycznych, w tym: stacji roboczych, aplikacji serwerowych, baz danych, poczty email, ich konserwację oraz wdrażanie niezbędnych zabezpieczeń gwarantujących bezpieczeństwo przetwarzania danych osobowych.
2. ASI odpowiada za zaplanowanie, konfigurowanie, aktywowanie specjalistycznego oprogramowania monitorującego wymianę danych na styku sieci lokalnej i sieci rozległej.
3. ASI odpowiada za zaplanowanie i zapewnienie ochrony antywirusowej.
4. Przeglądy i konserwacja systemu informatycznego powinny być wykonywane w terminach określonych przez producentów systemu lub zgodnie z harmonogramem ASI, jednak nie rzadziej, niż raz w roku. Za terminowość przeprowadzenia przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada ASI.
5. ASI odpowiada za optymalizację zasobów dyskowych i serwerowych, wielkości pamięci i dysków.
6. ASI odpowiada za aktualizację oprogramowania zgodnie z zaleceniami producentów oraz opinią rynkową co do bezpieczeństwa i stabilności nowych wersji (np. aktualizacje, service pack-i, łatki).

7. ASI odpowiada za zapewnienie licencjonowanego oprogramowania do przetwarzania danych osobowych.

Rozdział III Środki techniczne i organizacyjne

Zabezpieczenia organizacyjne

W celu ochrony danych osobowych stosuje się następujące zabezpieczenia organizacyjne:

1. Została opracowana i wdrożona **Polityka Ochrony Danych Osobowych oraz Regulamin postępowania z danymi osobowymi.**
2. Przetwarzania danych osobowych zostają dopuszczone wyłącznie osoby posiadające ważne upoważnienia do ich przetwarzania.
3. Prowadzona jest ewidencja osób posiadających upoważnienia do przetwarzania danych osobowych.
4. Osoby posiadające upoważnienia zostały przeszkolone lub zaznajomione w zakresie ochrony danych osobowych i zabezpieczeń systemu informatycznego co zostało odnotowane w **załączniku nr 16**.
5. Osoby posiadające upoważnienia złożyły oświadczenie o zachowaniu poufności przetwarzanych danych osobowych – **załącznik nr 4**.
6. Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy – **załącznik nr 4**.
7. Przetwarzanie danych osobowych odbywa się w warunkach zabezpieczających dane osobowe przed dostępem osób nieupoważnionych.
8. Przebywanie osób nieupoważnionych w obszarze przetwarzania jest możliwe tylko w obecności osób upoważnionych oraz w warunkach zapewniających bezpieczeństwo danych osobowych.
9. Stosuje się pisemne umowy powierzenia przetwarzania danych przy współpracy z podwykonawcami przetwarzającymi dane osobowe.

Zabezpieczenia fizyczne

W celu ochrony danych osobowych stosuje się następujące zabezpieczenia fizyczne:

1. Polityka kluczy i szczegółowy opis postępowania z nimi - opisany w dziale **Polityka Kluczy**.
2. Drzwi do pomieszczeń stanowiących obszar przetwarzania są zamykane na klucz (polityka kluczy).
3. Dane osobowe w wersji papierowej są przechowywane w meblach lub pomieszczeniach zamykanych na klucz (polityka kluczy).
4. W obszarze przetwarzania jest dostępna niszczarka dokumentów klasy co najmniej P4.
5. Klucze, kody dostępu lub inne zabezpieczenia do obszarów przetwarzania są wydane pracownikom przetwarzającym dane w określonym obszarze przetwarzania. Kluczy nie można udostępniać innym pracownikom czy osobom niepowołanym!

6. Szczegółowa lista wydanych kluczy do obszarów przetwarzania i odpowiedzialnych za nie pracowników znajduje się w **załączniku nr 11 i 11a (lista kluczy wydawanych doraźnie).**

Polityka kluczy

1. Ogólne zasady.

Polityka kluczy obejmuje pomieszczenia obszarów przetwarzania danych osobowych użytkowane przez **infraTEAM,** w których przetwarzane są dane osobowe,

a) lista lokalizacji obszarów przetwarzania danych osobowych **infraTEAM** znajduje się w **załączniku nr 23,**
b) harmonogram pracy obszarów przetwarzania danych osobowych **infraTEAM** wyszczególniony jest w **załączniku nr 22,**
c) dostęp do pomieszczeń będących obszarami przetwarzania danych osobowych możliwy jest wyłącznie poprzez drzwi wyznaczone do tego przez **ADO**. Wszystkie pozostałe drzwi umożliwiające dostęp do tych pomieszczeń powinny być trwale zamknięte na klucz. Zabrania się otwierania tych drzwi przez pracowników bez zgody ADO,
d) klucze zapasowe przechowywane są w określonym przez ADO bezpiecznym miejscu.

2. Nadawanie upoważnień.
   a) upoważnienia do pobierania kluczy do pomieszczeń będących obszarami przetwarzania danych mają wyłącznie osoby upoważnione przez ADO. Obejmują one także dostęp do tych pomieszczeń poza godzinami pracy,
   b) udzielenie/anulowanie upoważnienia wymaga wprowadzenia osoby do ewidencji, prowadzonej w postaci **załącznika nr 11** oraz **załącznika 11a (lista kluczy wydawanych doraźnie)**.
3. Wydawanie i zdawanie kluczy w trybie normalnym.
   a) klucze do pomieszczeń będących obszarami przetwarzania danych wydawane zostały wyznaczonym pracownikom, za pobraniem, przez ADO, klucze do tych pomieszczeń pozostają pod osobistym nadzorem osób upoważnionych,
   b) klucze do pomieszczeń będących obszarami przetwarzania danych wydane zostały za pobraniem przez ADO. Klucze do tych pomieszczeń pozostają pod osobistym nadzorem osób upoważnionych,
   c) klucze do pomieszczeń szczególnie chronionych (archiwum), wydawane są za pobraniem u ADO, klucze do pomieszczeń szczególnie chronionych pozostają pod osobistym nadzorem osób upoważnionych, dostęp do tych pomieszczeń osób trzecich odbywa się pod ścisłym nadzorem(!),

d) pracownicy upoważnieni zobowiązani są do odnotowania pobrania i zdania kluczy – **załącznik nr 11** lub **11a.**

4. Wydawanie i zdawanie kluczy w trybie nadzwyczajnym:
   a) wydawanie kluczy zapasowych upoważnionym pracownikom może odbywać się tylko w uzasadnionych sytuacjach oraz przypadkach awaryjnych za zgodą ADO,
   b) klucze zapasowe po ich wykorzystaniu należy niezwłocznie zwrócić do ADO.
5. Bieżące postępowanie w trakcie dnia pracy:
   a) klucze służące do zabezpieczenia biurek i szaf muszą być jednoznacznie opisane,
   b) klucze pozostają pod nadzorem pracowników, którzy ponoszą pełną odpowiedzialność za ich należyte zabezpieczenie,
   c) zabrania się pozostawiania kluczy w biurkach i szafach podczas chwilowej nieobecności osób upoważnionych w pomieszczeniu,
   d) po zakończeniu pracy, klucze służące do zabezpieczenia biurek i szaf muszą być przechowywane we wskazanym przez ADO odpowiednio zabezpieczonym miejscu, klucz zbiorczy jest zabezpieczony w określonym przez ADO bezpiecznym miejscu,
   e) Po zakończeniu pracy, pracownicy są zobowiązani do:
      - wyłączenia i zabezpieczenia urządzeń elektronicznych oraz elektrycznych,
      - wyłączenia oświetlenia,
      - zabezpieczenia i zamknięcia okien i drzwi,
      - opuszczenia rolet,
      - ewentualnie aktywacji alarmu,
      - za przestrzeganie w/w zasad bieżących odpowiadają pracownicy.
6. Naruszenie zasad polityki kluczy może spowodować wyciągnięcie następujących konsekwencji:
   a) poniesienie odpowiedzialności wynikających z art. 52 kodeksu pracy[1],
   b) poniesienie odpowiedzialności wynikających z art. 363 § 1. kodeksu cywilnego[2].

Zabezpieczenia sprzętowe

W celu ochrony danych osobowych stosuje się zabezpieczenia sprzętowe infrastruktury informatycznej i telekomunikacyjnej opisane w dziale **Instrukcja dotycząca sposobu zarządzania**

[1] **Art. 52. § 1**. Pracodawca może rozwiązać umowę o pracę bez wypowiedzenia z winy pracownika w razie:1) ciężkiego naruszenia przez pracownika podstawowych obowiązków pracowniczych, 2) popełnienia przez pracownika w czasie trwania umowy o pracę przestępstwa, które uniemożliwia dalsze zatrudnianie go na zajmowanym stanowisku, jeżeli przestępstwo jest oczywiste lub zostało stwierdzone prawomocnym wyrokiem( )

[2] **Art. 363. § 1.** Naprawienie szkody powinno nastąpić, według wyboru poszkodowanego, bądź przez przywrócenie stanu poprzedniego, bądź przez zapłatę odpowiedniej sumy pieniężnej. dla zobowiązanego nadmierne trudności lub koszty, świadczenia w pieniądzu( )

systemem informatycznym.

Instrukcja zarządzania bezpieczeństwem informacji

Zasady zabezpieczania systemu informatycznego, sprzętu, danych i oprogramowania

Uwzględniając kategorie przetwarzanych danych osobowych, podłączenie sprzętu informatycznego do sieci teleinformatycznej, oraz zagrożenia, wprowadza się w **infraTEAM** wysoki poziom bezpieczeństwa w systemie informatycznym służącym do przetwarzania danych osobowych.

1. Kontroli podlega dostęp do pomieszczeń, w których znajduje się sprzęt komputerowy, w celu zabezpieczenia sprzętu oraz danych osobowych i oprogramowania przed ich wykorzystaniem lub zniszczeniem przez osoby trzecie. Pomieszczenia, w których znajduje się sprzęt komputerowy służący do przetwarzania danych osobowych wyposażone są w solidne zamki. Ostatni z pracowników, który opuszcza pomieszczenie ma obowiązek zamknąć drzwi na klucz! Ponadto prowadzi się pisemną ewidencję wydanych kluczy do pomieszczeń - **załącznik nr 11 i 11a.**
2. Komputery, w których znajdują się dane osobowe muszą być wyposażone w agregaty awaryjne (UPS) na wypadek wahań napięcia w sieci energetycznej w celu prawidłowego zamknięcia wszystkich aplikacji i bezpiecznego wyłączenia komputera, a w przypadku laptopów w sprawne baterie.
3. Kopie przyrostowe danych zawartych w systemie tworzy się raz dziennie, a kopie całościowe raz na miesiąc. Kopia całościowa tworzona jest przez ADO/ASI lub uprawnionego użytkownika, a następnie zabezpieczona przez ADO/ASI w bezpiecznym miejscu.
4. Pracowników **infraTEAM** obowiązuje bezwzględny zakaz wynoszenia płyt lub innych nośników z oprogramowaniem lub innymi danymi poza teren siedziby jednostki i jej komórek organizacyjnych, chyba że zgodę na taką czynność wyrazi ADO.
5. Dopuszcza się, za zgodą ADO, instalowania programów zawierających dane osobowe na komputerach przenośnych. Musi on jednak posiadać zainstalowane mechanizmy ochronne oraz kompleksowe oprogramowanie antywirusowe. Ponadto użytkownik takiego komputera musi zostać zaznajomiony przez ADO/IOD (jeśli został powołany) z wszelkimi zagrożeniami oraz dochować wszelkiej staranności, aby zapobiec kradzieży jego komputera przenośnego – patrz: **Regulamin użytkowania komputerów przenośnych.**
6. Urządzenia, dyski lub inne nośniki informacji przeznaczone do:
   a) likwidacji - pozbawia się danych poprzez formatowanie oraz fizyczne uszkodzenie, uniemożliwiające ich odczytanie,
   b) przekazania - pozbawia się zapisu zawierającego dane osobowe,

c) naprawy - pozbawia się zapisu danych osobowych lub naprawia pod nadzorem ADO/ASI, lub osoby do tego upoważnionej przez ADO.

7. Na stanowiskach pracy, na których przetwarzane są dane osobowe ekrany monitorów powinny być ustawione w sposób uniemożliwiający osobom trzecim wgląd w wyświetlane informacje.
8. W razie przerwania pracy stosuje się "wygaszacz ekranu" zabezpieczony hasłem. Czas aktywacji wygaszacza określony został w Regulaminie.
9. Każdy z komputerów zabezpieczony jest hasłem dostępu do systemu operacyjnego, składającym się z co najmniej ośmiu znaków zawierających wielkie i małe litery, cyfry i znaki specjalne. Każdy z pracowników ma obowiązek comiesięcznej zmiany hasła dostępu do komputera.

Polityka haseł

1. Wszystkie komputery, w tym laptopy i serwer są zabezpieczone hasłem.
2. Każdy uprawniony użytkownik loguje się do systemu za pomocą hasła do swojego konta na poziomie zabezpieczeń określonym przez ADO jako wysoki (hasło zbudowano z ośmiu znaków, w tym duże i małe litery, cyfry, znaki specjalne).

2. Zmiana hasła do systemu następuje nie rzadziej, niż co 30 dni oraz niezwłocznie w przypadku podejrzenia, że hasło mogło zostać ujawnione.

3. Jeżeli zmiany hasła nie wymusza system, wówczas do zmiany hasła zobowiązany jest użytkownik.

4. Użytkownik systemu w trakcie pracy w aplikacji może zmienić swoje hasło.

5. Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów.
6. Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności.

7. Zabronione jest zapisywanie haseł w sposób jawny oraz przekazywanie ich innym osobom.

8. Powyższa polityka haseł obejmuje również stażystów, wolontariuszy, praktykantów, uczniów przetwarzających dane w **infraTEAM.**

Zasady bezpiecznego użytkowania sprzętu stacjonarnego IT

1. Sprzęt IT służący do przetwarzania zbioru danych osobowych składa się z komputerów, laptopów, drukarek.
2. Użytkownik zobowiązany jest korzystać ze sprzętu IT w sposób zgodny z jego przeznaczeniem i chronić go przed jakimkolwiek zniszczeniem lub uszkodzeniem.

3. Użytkownik zobowiązany jest do zabezpieczenia sprzętu IT przed dostępem osób nieupoważnionych, a w szczególności ochronie podlega zawartość ekranów monitorów.
4. Użytkownik ma obowiązek natychmiast zgłosić zagubienie, utratę lub zniszczenie powierzonego mu sprzętu IT.
5. Samowolne otwieranie (demontaż) sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) lub podłączanie jakichkolwiek niezatwierdzonych przez ADO urządzeń do systemu informatycznego jest zabronione.

Zasady korzystania z oprogramowania

1. Użytkownik zobowiązuje się do korzystania wyłącznie z oprogramowania z zachowaniem ochrony praw autorskich.
2. Użytkownik nie ma prawa kopiować oprogramowania zainstalowanego na sprzęcie IT przez ADO na swoje własne potrzeby, ani na potrzeby osób trzecich.
3. Instalowanie jakiegokolwiek oprogramowania na sprzęcie IT może być dokonane wyłącznie przez ADO, lub osobę przez niego upoważnioną.
4. Użytkownicy nie mają prawa bez zgody ADO/ASI do instalowania ani używania oprogramowania innego, niż przekazane lub udostępnione im przez ADO/ASI. Zakaz dotyczy między innymi instalacji oprogramowania z zakupionych płyt CD, programów ściąganych ze stron internetowych, a także odpowiadania na samoczynnie pojawiające się reklamy internetowe.
5. Użytkownicy nie mają prawa do zmiany parametrów systemu, które mogą być zmienione tylko przez ADO/ASI, lub osobę przez ADO upoważnioną.
6. W przypadku naruszenia któregokolwiek z powyższych postanowień ADO ma prawo niezwłocznie i bez uprzedzenia usunąć nielegalne lub niewłaściwie zainstalowane oprogramowanie.

Zasady korzystania z Internetu

1. Użytkownik zobowiązany jest do korzystania z Internetu w celach służbowych.
2. Zabrania się zgrywania na dysk twardy komputera oraz uruchamia jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą ADO/ASI i tylko w uzasadnionych przypadkach.
3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu.
4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo (na większości stron tego typu jest zainstalowane szkodliwe oprogramowanie, infekujące w sposób automatyczny system operacyjny komputera).

5. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.
6. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu WWW rozpoczynającego się frazą ”https:”.
7. Należy zachować szczególną ostrożność w przypadku żądania lub prośby podania kodów, PIN-ów, numerów kart płatniczych przez Internet. Szczególnie tyczy się to żądania podania takich informacji przez rzekomy bank.
8. Użytkownicy nie mogą także korzystać z Internetu dla celów prywatnych, chyba, że za zgodą ADO i powinno być ono ograniczone do niezbędnego minimum.
9. Korzystanie z Internetu dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych, a także na wydajność systemu informatycznego pracodawcy.
10. Przy korzystaniu z Internetu, Użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego.
11. W zakresie dozwolonym przepisami prawa, ADO zastrzega sobie prawo kontrolowania sposobu korzystania przez użytkownika z Internetu pod kątem wyżej opisanych zasad.
12. Ponadto, w uzasadnionym zakresie, ADO zastrzega sobie prawo kontroli czasu spędzanego przez użytkownika w Internecie.
13. Pracodawca może również blokować dostęp do niektórych treści dostępnych przez Internet.

Zasady korzystania z poczty elektronicznej

1. Przesyłanie danych osobowych z użyciem maila może odbywać się tylko przez osoby do tego upoważnione przez ADO.
2. W przypadku przesyłania danych osobowych poza **infraTEAM** należy wykorzystywać mechanizmy kryptograficzne (hasłowanie wysyłanych plików, profil zaufany, certyfikat kwalifikowany).
3. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 8 znaków: duże i małe litery i cyfry lub znaki specjalne a hasło należy przesłać odrębnym mailem lub inną metodą, np. telefonicznie lub SMS-em.
4. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
5. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.

6. Nie należy otwierać załączników (plików) w mailach nadesłanych przez nieznanego nadawcę lub podejrzanych załączników nadanych przez znanego nadawcę.
7. Użytkownicy nie mogą rozsyłać za pośrednictwem maila informacji o zagrożeniach dla systemu informatycznego, „łańcuszków szczęścia", itp.
8. Użytkownicy nie powinni rozsyłać maili zawierających załączniki o dużym rozmiarze.
9. Użytkownicy powinni okresowo kasować niepotrzebne maile w poczcie służbowej.
10. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW" (funkcja poczty elektronicznej umożliwiająca wysyłanie wiadomości do wielu odbiorców tak, by nie widzieli nawzajem swoich adresów).
11. Mail jest przeznaczony do wykonywania obowiązków służbowych.
12. Użytkownicy nie mają prawa korzystać z maila dla celów prywatnych, chyba, że za zgodą ADO, wyłącznie okazjonalnie i powinno być to ograniczone do niezbędnego minimum.
13. Korzystanie z maila dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych.
14. Przy korzystaniu z maila, użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego.
15. Użytkownicy nie mają prawa korzystać z maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.
16. Użytkownik bez zgody ADO nie ma prawa wysyłać wiadomości zawierających dane osobowe dotyczące Pracodawcy, jego pracowników, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej.

Ochrona antywirusowa

Celem procedury jest zabezpieczenie systemów informatycznych przed szkodliwym oprogramowaniem (np. typu robaki, wirusy, konie trojańskie, rootkity) oraz nieautoryzowanym dostępem do systemów przetwarzających dane osobowe.

1. Użytkownicy zobowiązani są do skanowania plików wprowadzanych z zewnętrznych nośników programem antywirusowym.
2. Na komputerach i laptopach zainstalowany został system antywirusowy, a pracownicy zostali przeszkolenie z jego obsługi, **załącznik nr 17.**
3. Zakazane jest wyłączanie systemu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe.

4. System antywirusowy zapewnia ochronę: systemu operacyjnego, przechowywanych plików, poczty wychodzącej i przychodzącej.
5. Aktualizacja definicji wirusów odbywa się automatycznie przez program antywirusowy.

Zabezpieczenie systemu przed nieuprawnionym dostępem

Stosowane zabezpieczenia mają na celu zabezpieczenie systemów informatycznych przed nieautoryzowanym dostępem do sieci lokalnej np. przez programy szpiegujące, hackerów.

1. Za zaplanowanie, konfigurowanie, aktywowanie specjalistycznego oprogramowania monitorującego wymianę danych na styku sieci lokalnej i sieci rozległej odpowiada ADO/ASI.
2. Stosowany jest Firewall.
3. Zastosowano mechanizmy kontroli dostępu do sieci.
4. Sieć bezprzewodową jest odpowiednio zabezpieczona.
5. Dopuszcza się możliwość przyłączenia sieci internetowej do systemu, w którym przetwarzane są dane osobowe pod następującymi warunkami:
   a) na każdym stanowisku komputerowym musi być zainstalowane oprogramowanie antywirusowe,
   b) każdy e-mail wpływający do jednostki musi być sprawdzony pod kątem występowania wirusów,
   c) zabrania się używania nośników niewiadomego pochodzenia bez wcześniejszego sprawdzenia ich programem antywirusowym, którego dokonuje użytkownik zamierzający go użyć,
   d) zabrania się pobierania z Internetu plików niewiadomego pochodzenia oraz odczytywania załączników poczty elektronicznej bez wcześniejszego sprawdzenia ich programem antywirusowym.

1. Każdy użytkownik systemu musi zostać przeszkolony z obsługi programu antywirusowego, co poświadcza stosownym podpisem, zgodnie z **załącznikiem nr 17** do niniejszej polityki bezpieczeństwa.
2. ADO/ASI przeprowadza cykliczne kontrole antywirusowe na wszystkich komputerach systemu.
3. Użytkownicy systemu są odpowiedzialni za nieudostępnianie stanowisk pracy osobom postronnym.

Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych

1. Procedury naprawy sprzętu komputerowego:
   a) naprawa sprzętu komputerowego użytkowanego w systemie może odbywać się w siedzibie **infraTEAM** i dokonywać jej może jedynie wyznaczony pracownik, lub wyspecjalizowana firma

informatyczna. Czynności te muszą być wykonywane w obecności ADO/ASI, lub innego upoważnionego przez ADO użytkownika systemu,

b) naprawa sprzętu komputerowego użytkowanego w systemie poza siedzibą biura musi zostać poprzedzona usunięciem z twardego dysku wszelkich baz danych, rejestrów i zbiorów zawierających dane o charakterze osobowym. ADO/ASI lub wyznaczony pracownik odpowiedzialny jest za stworzenie kopii tej bazy, która jest przechowywana przez ADO/ASI w bezpiecznym miejscu. Po powrocie z serwisu sprzętu komputerowego, bazy danych, rejestry, zbiory są ponownie instalowane.

2. Procedura przeglądu systemu:

a) przeglądu systemu dokonuje ADO/ASI

b) ADO (ASI jeśli został powołany) obsługuje jednostkę pod względem informatycznym,

c) czynności przeglądowe wykonywane przez firmę zewnętrzną muszą odbywać się w obecności ADO, ASI, lub innego upoważnionego przez niego pracownika.

Postępowanie z elektronicznymi nośnikami zawierającymi dane osobowe

1. Elektroniczne nośniki, to: twarde dyski, wymienne twarde dyski, zewnętrzne twarde dyski, pendrive, płyty CD, DVD, pamięci typu Flash.
2. Każdy nośnik powinien zostać opisany w sposób jednoznacznie go identyfikujący. Wykaz elektronicznych nośników znajduje się w **załączniku nr 26**.
3. Użytkownicy nie mogą wynosić na zewnątrz organizacji wymiennych elektronicznych nośników informacji z zapisanymi danymi osobowymi bez zgody ADO.
4. Dane osobowe wynoszone poza organizację muszą być zaszyfrowane.
5. W przypadku uszkodzenia lub zużycia nośnika zawierającego dane osobowe, należy dokonać jego fizycznego zniszczenia lub trwałego usunięcia znajdujących się na nim danych.
6. Przekazywanie nośników z danymi osobowymi powinno być przeprowadzane z uwzględnieniem zasad bezpieczeństwa. Adresat powinien zostać powiadomiony o przesyłce, zaś nadawca powinien sporządzić kopię przesyłanych danych. Adresat powinien powiadomić nadawcę o otrzymaniu przesyłki. Jeżeli nadawca nie otrzymał potwierdzenia, zaś adresat twierdzi, że nie otrzymał przesyłki, użytkownik będący nadawcą powinien poinformować o zaistniałej sytuacji ADO/IOD (jeśli został powołany).

Procedura przechowywania nośników danych osobowych w wersji papierowej i elektronicznej:

1. Nośniki danych osobowych takie jak:

b) Laptop,

c) telefon komórkowy/smartfon,

d) pendrive/karta pamięci,

e) zewnętrzny dysk twardy,

f) płyta CD/DVD/BR,

g) wydruki papierowe

są przechowywane w sposób uniemożliwiający dostęp do nich osób nie upoważnionych jak i zabezpieczający je przed uszkodzeniem spowodowanym np.: zalaniem, spaleniem, stopieniem, etc.

2. Osoby upoważnione są zobowiązane do trwałego niszczenia/kasowania danych osobowych po ustaniu celu ich przetwarzania.
3. Zabrania się wynoszenia danych osobowych poza obszar przetwarzania bez zgody ADO, a w przypadku otrzymania takiej zgody zapewnienia co najmniej takich samych warunków bezpieczeństwa przetwarzania danych osobowych jakie obowiązują w obszarze przetwarzania.
4. Dane osobowe wysyłane drogą elektroniczną poza obszar przetwarzania muszą być zabezpieczone hasłem lub szyfrowane.
5. W sytuacji przekazywania nośników z danymi osobowymi poza obszar organizacji należy stosować następujące zasady bezpieczeństwa:
   a) adresat powinien zostać powiadomiony o przesyłce,
   b) nadawca powinien sporządzić kopię przesyłanych danych,
   c) dane przed wysłaniem powinny zostać zaszyfrowane a hasło podane adresatowi inną drogą,
   d) stosować bezpieczne koperty depozytowe,
   e) adresat powinien powiadomić nadawcę o otrzymaniu przesyłki.
7. Użytkownicy są zobowiązani do niezwłocznego i trwałego usuwania/kasowania danych osobowych z nośników informacji po ustaniu powodu ich przechowywania (chyba, że z powodu odrębnych przepisów należy je zachować na dłużej).
8. Podlegające likwidacji uszkodzone lub przestarzałe nośniki, a w szczególności twarde dyski z danymi osobowymi są komisyjnie niszczone w sposób fizyczny w/g **załącznika nr 27**.
9. Nośniki informacji zamontowane w sprzęcie IT, a w szczególności twarde dyski z danymi osobowymi powinny być wymontowane lub wyczyszczone specjalistycznym oprogramowaniem, zanim zostaną przekazane poza obszar organizacji (np. sprzedaż lub darowizna komputerów stacjonarnych/laptopów).

Zabezpieczenie dokumentów i wydruków

1. Dokumenty i wydruki trwałe z danymi osobowymi przechowuje się w archiwum lub w zabezpieczonych fizycznie pomieszczeniach, biurkach i szafach.

2. Pracownicy są zobowiązani do zabezpieczania dokumentów (np. zamknięcie pomieszczeń, zamykanie dokumentów na klucz w szafach, biurkach) przed dostępem osób nieupoważnionych podczas swojej nieobecności w pomieszczeniach lub po zakończeniu pracy (tzw. polityka czystego biurka).
3. Zabrania się pozostawiania wydruków oraz ksero na drukarkach, skanerach i kserokopiarkach bez nadzoru.
4. Pracownicy są zobowiązani do niszczenia dokumentów i tymczasowych wydruków w niszczarkach niezwłocznie po ustaniu celu ich przetwarzania.
5. Za zapewnienie bezpieczeństwa dokumentów i wydruków odpowiedzialni są wszyscy pracownicy.

Postępowanie z danymi osobowymi w wersji papierowej

1. Za bezpieczeństwo dokumentów i wydruków zawierających dane osobowe odpowiedzialne są osoby upoważnione (użytkownicy).
2. Dokumenty i wydruki zawierające dane osobowe przechowuje się w pomieszczeniach zabezpieczonych fizycznie przed dostępem osób nieupoważnionych.
3. Użytkownicy są zobowiązani do stosowania „polityki czystego biurka". Polega ona na zabezpieczaniu dokumentów np. w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych.
4. Użytkownicy zobowiązani są do przewożenia dokumentów w sposób zapobiegający ich kradzieży, zagubieniu lub utracie.
5. Użytkownicy zobowiązani są do niszczenia dokumentów i tymczasowych wydruków w niszczarkach niezwłocznie po ustaniu celu ich przetwarzania.

Regulamin użytkowania komputerów przenośnych

1. Każdy Użytkownik komputera przenośnego winien zapoznać się z Regulaminem użytkowania komputerów przenośnych.
2. W przypadku przechowywania na komputerze przenośnym danych osobowych lub stanowiących tajemnicę **infraTEAM**, użytkownik zobowiązany jest do ich przechowywania na dysku szyfrowanym, zabezpieczonym co najmniej 8 znakowym hasłem (duże, małe litery, znaki specjalne i cyfry).
3. Na komputerach przenośnych przeznaczonych do zewnętrznych prezentacji multimedialnych nie powinny, o ile jest to możliwe, znajdować się dane osobowe lub stanowiące tajemnicę **infraTEAM.** W przypadku kradzieży lub zgubienia komputera przenośnego, Użytkownik powinien natychmiast powiadomić o tym ADO, zaznaczając jednocześnie, jakiego rodzaju dane były na tym urządzeniu przechowywane.

4. Użytkownik zobowiązany jest do zabezpieczenia komputera przenośnego w czasie transportu, a w szczególności:
   1. zaleca się przenoszenie go w specjalnym futerale,
   2. zabrania się pozostawiania komputera przenośnego w samochodzie podczas postoju w miejscu publicznym bez nadzoru,
   3. podczas jazdy samochodem zaleca się przechowywanie komputera przenośnego pod siedzeniem kierowcy. Zabrania się przewożenia go np. na siedzeniach, co może skutkować kradzieżą na skrzyżowaniach, przejściach dla pieszych lub w korkach.
5. W przypadku, gdy komputer przenośny pozostawiony jest w miejscu dostępnym dla osób nieupoważnionych, Użytkownik jest zobowiązany do stosowania kabla zabezpieczającego. W szczególności dotyczy to zabezpieczenia komputera na stanowisku pracy, podczas konferencji, prezentacji, szkoleń, targów itp.
6. W przypadku pozostawiania komputerów przenośnych w biurze zaleca się umieszczanie ich po zakończeniu pracy w zamykanych szafkach.
7. Użytkownik komputera przenośnego jest zobowiązany do regularnego tworzenia kopii bezpieczeństwa danych na serwerze lub na określonych nośnikach (pendrive, CD, DVD). Nośniki z takimi kopiami powinny być przechowywane w bezpiecznym miejscu, z uwzględnieniem ochrony przed dostępem osób niepowołanych.
8. Pracując na komputerze przenośnym w miejscach publicznych i środkach transportu, Użytkownik zobowiązany jest chronić wyświetlane na monitorze informacje przed wglądem osób nieupoważnionych.

Zasady udostępniania danych

1. Dopuszcza się przekazywanie danych osobowych, o których mowa w art. 6 RODO podmiotom i organom upoważnionym **na podstawie odrębnych przepisów**.
2. Wzór wniosku o udostępnienie danych osobowych, o których mowa w pkt. 1 stanowi **załącznik nr 21**.
3. ADO/IOD (jeśli został powołany) zobowiązany jest do prowadzenia ewidencji udostępniania danych osobowych ze zbiorów zgodnie z **załącznikiem nr 14**.

Procedura postępowania w sytuacji naruszenia polityki bezpieczeństwa.

1. Każda osoba przetwarzająca dane osobowe, w przypadku podejrzenia naruszenia zabezpieczenia danych osobowych, zobowiązana jest niezwłocznie powiadomić o tym ADO i IOD (jeśli został powołany).
2. ADO/IOD (jeśli został powołany) po otrzymaniu powiadomienia:

a) sprawdza stan urządzeń wykorzystywanych do przetwarzania danych osobowych,
b) sprawdza sposób działania programów (w tym obecność wirusów komputerowych),
c) sprawdza jakość komunikacji w sieci telekomunikacyjnej,
d) sprawdza zawartość zbioru danych osobowych,
e) poddaje analizie metody pracy osób upoważnionych do przetwarzania danych osobowych.
f) jeśli incydent może mieć wpływ na naruszenie praw i wolności osoby fizycznej zgłasza fakt zaistnienia incydentu do organu nadzorczego w terminie 72 godzin od powzięcia informacji o incydencie.
g) Jeśli incydent dotyczy danych powierzonych przez innego ADO zgłasza fakt zaistnienia incydentu właściwemu ADO w terminie do 24 godzin.

3. W przypadku stwierdzenia naruszenia zabezpieczeń danych administrator:
   b) podejmuje niezbędne działania mające na celu uniemożliwienie dalszego ich naruszenia (odłączenie wadliwych urządzeń, zablokowanie dostępu do sieci telekomunikacyjnej, programów oraz zbiorów danych itp.),
   c) w celu powstrzymania lub ograniczenia dostępu do danych osoby niepowołanej podejmuje odpowiednie kroki poprzez: fizyczne odłączenie urządzeń i segmentów sieci, które mogłyby umożliwić dostęp do bazy danych osoby nieupoważnionej, wylogowanie użytkownika podejrzewanego o naruszenie zabezpieczenia ochrony danych, zmianę hasła na konto administratora i użytkownika, poprzez które uzyskano nielegalny dostęp w celu uniknięcia ponownej próby włamania,
   d) zabezpiecza, utrwala wszelkie informacje i dokumenty mogące stanowić pomoc przy ustaleniu przyczyn naruszenia,
   e) niezwłocznie przywraca prawidłowy stan działania systemu,
   f) dokonuje analizy stanu zabezpieczeń wraz z oszacowaniem rozmiaru szkód powstałych na skutek naruszenia,
   g) sporządza szczegółowy raport zawierający w szczególności: datę i godzinę otrzymania informacji o naruszeniu, opis jego przebiegu, przyczyny oraz wnioski ze zdarzenia.
3. Raport, wraz z ewentualnymi załącznikami (kopie dowodów dokumentujących naruszenie) ADO dołącza do dokumentacji incydentu.
4. ADO/IOD (jeśli został powołany) podejmują niezbędne działania w celu wyeliminowania naruszeń zabezpieczeń danych w przyszłości, a w szczególności:
   b) jeżeli przyczyną zdarzenia był stan techniczny urządzenia, sposób działania programu, uaktywnienie się wirusa komputerowego lub jakość komunikacji w sieci telekomunikacyjnej, niezwłocznie przeprowadza przeglądy oraz konserwacje urządzeń i programów, ustala źródło

pochodzenia wirusa oraz wdraża skuteczniejsze zabezpieczenia antywirusowe, a w miarę potrzeby kontaktuje się z dostawcą usług telekomunikacyjnych,

c) jeżeli przyczyną zdarzenia były wadliwe metody pracy, błędy i zaniedbania osób zatrudnionych przy przetwarzaniu danych osobowych, przeprowadza się dodatkowe kursy i szkolenia osób biorących udział przy przetwarzaniu danych, a wobec osób winnych zaniedbań wnioskuje do administratora danych osobowych o wyciągnięcie konsekwencji przewidzianych prawem,

d) jeżeli przyczyną zdarzenia jest sprzeczny z prawem czyn lub zachodzi takie podejrzenie, zawiadamia organy ścigania.

Procedura rozpoczęcia, zawieszenia i zakończenia pracy wymagającej przetwarzania danych osobowych:

1. Osoba upoważniona loguje się do systemu oraz programu informatycznego przetwarzającego dane osobowe przy użyciu loginu i hasła.
2. Osoba upoważniona jest zobowiązana do informowania ADO/IOD (jeśli został powołany) o nieautoryzowanych próbach zalogowania do systemu lub programu, jeżeli system lub program takie zjawiska monitoruje.
3. Osoba upoważniona jest zobowiązana do uniemożliwienia wglądu w dane osobowe wyświetlane na ekranie monitora lub w wersji papierowej osobom nieupoważnionym.
4. Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana w trakcie czasowego opuszczenia miejsca pracy do uruchomienia wygaszacza ekranu chronionego hasłem lub wylogowania się z systemu oraz usunięcia wydruków z danymi osobowymi z biurka.
5. Po zakończeniu pracy osoba upoważniona jest zobowiązana do wylogowania się lub wyłączenia komputera oraz usunięcia z biurka wszelkich nośników zawierających dane osobowe jak i zabezpieczenia pomieszczenia przed włamaniem, zalanie, pożarem, etc.

Procedura tworzenia i przechowywania kopii zapasowych

1. Kopie zapasową (przyrostowa, całościowa) tworzy ADO/ASI – jeśli został powołany, lub upoważnieni pracownicy w sposób opisany w pkt. 3 **Zasad zabezpieczania sprzętu informatycznego, danych i oprogramowania** niniejszej instrukcji.
2. Kopie zapasowe danych osobowych w wersji elektronicznej mogą być przechowywane na zewnętrznym nośniku danych zabezpieczonym zgodnie z zabezpieczeniami organizacyjnymi opisanymi w pkt. 3 **Zasad zabezpieczania sprzętu informatycznego, danych i oprogramowania niniejszej instrukcji**.

3. Osoba sporządzająca kopie zapasowe jest zobowiązana do ich oznaczenia oraz sprawdzenia spójności danych i możliwości ich ponownego odtworzenia.
4. Po upływie okresu przechowywania kopie zapasowe są trwale niszczone lub anonimizowane.

Procedura wprowadzania i udostępniania danych osobowych podmiotom zewnętrznym:

1. Każde wprowadzenie i udostępnienie danych osobowych musi być dokonane zarówno zgodnie z RODO jak i niniejszym dokumentem oraz posiadać podstawę prawną.
2. Prowadzi się ewidencje udostępnianych danych, określającą w szczególności:
    a. datę udostępnienia,
    b. nazwisko i imię osoby której dane udostępniono (dokumentacja medyczna)
    c. osoba, podmiot, któremu udostępniono dane,
    d. sposób udostępnienia,
    e. zakres udostępnianych danych osobowych które zostały udostępnione,
    f. imię i nazwisko osoby, której zostały udostępnione dane osobowe, nazwa uprawnionego organu lub podmiotu,
    g. imię i nazwisko pracownika, który dane osobowe udostępnił.

Procedury kontrolne oraz szkolenia pracowników:

1. Corocznie prowadzi się kontrole przestrzegania obowiązujących reguł dotyczących ochrony danych osobowych.
2. Z kontroli sporządza się sprawozdanie, który jest podstawą do dokonania aktualizacji procedur oraz niniejszego dokumentu.
3. Raz do roku przeprowadza się szkolenie aktualizacyjne pracowników w zakresie ochrony danych osobowych.
4. Każdy pracownik przed otrzymaniem upoważnienia musi zostać przeszkolony.
5. Wszelka naprawa lub konserwacja sprzętu komputerowego zawierającego dane osobowe lub pomieszczeń stanowiących obszar przetwarzania może odbywać się tylko pod nadzorem osób upoważnionych.

Postępowanie dyscyplinarne

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie

zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.

2. Kara dyscyplinarna, orzeczona wobec osoby uchylającej się od powiadomienia, nie wyklucza odpowiedzialności karnej tej osoby oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

Instrukcja alarmowa

Instrukcja definiuje katalog zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Celem instrukcji jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa, ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

1. Każdy pracownik **infraTEAM** w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest poinformować o tym fakcie ADO/IOD (jeśli został powołany).
2. Do typowych zagrożeń bezpieczeństwa danych osobowych należą:
   a) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
   b) niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
   c) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek),
3. Do typowych incydentów bezpieczeństwa danych osobowych należą:
   a) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
   b) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/zagubienie danych),
   c) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania),
4. W przypadku stwierdzenia wystąpienia zagrożenia, ADO/IOD (jeśli został powołany) prowadzi postępowanie wyjaśniające w toku którego:
   a) ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki,
   b) dokumentuje prowadzone postępowania,
   c) ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały,

d) zabezpiecza ewentualne dowody,
e) ustala osoby odpowiedzialne za naruszenie,
f) podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody),
g) inicjuje działania dyscyplinarne,
h) wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości,
i) zgłasza fakt naruszenia ochrony danych osobowych organowi nadzorczemu w terminie do 72 godzin od stwierdzenia naruszenia.

Procedura działań korygujących i zapobiegawczych

1. Celem procedury jest uporządkowanie i przedstawienie czynności związanych z inicjowaniem oraz realizacją działań korygujących i zapobiegawczych wynikających z zaistnienia incydentów bezpieczeństwa lub zagrożeń systemu ochrony danych osobowych.
2. Procedura działań korygujących i zapobiegawczych obejmuje wszystkie te procesy, w których incydenty bezpieczeństwa lub zagrożenia mogą wpłynąć na zgodność z wymaganiami RODO, jak również na poprawne funkcjonowanie systemu ochrony danych osobowych.
3. Osobą odpowiedzialną za nadzór nad procedurą jest ADO/IOD (jeśli został powołany).

Definicje

1. **Incydent** - naruszenie bezpieczeństwa informacji ze względu na poufność, dostępność i integralność.
2. **Zagrożenie** – potencjalna możliwość wystąpienia incydentu
3. **Korekcja** – działanie w celu wyeliminowania skutków incydentu.
4. **Działanie korygujące** – jest to działanie przeprowadzane w celu wyeliminowania przyczyny incydentu lub innej niepożądanej sytuacji.
5. **Działanie zapobiegawcze** – jest to działanie, które należy przedsięwziąć, aby wyeliminować przyczyny zagrożenia lub innej potencjalnej sytuacji niepożądanej.
6. **Kontrola** – systematyczna, niezależna i udokumentowana ocena skuteczności systemu ochrony danych osobowych, na podstawie wymagań ustawowych, polityki ochrony danych.

Opis czynności

1. ADO (IOD jeśli został powołany) jest odpowiedzialny za analizę incydentów bezpieczeństwa lub zagrożeń ochrony danych osobowych. Typowymi źródłami informacji o incydentach, zagrożeniach lub słabościach są:
   a) zgłoszenia od pracowników,
   b) wiedza ADO/IOD,

c) wyniki kontroli.

2. W przypadku, gdy ADO (IOD jeśli został powołany) stwierdzi konieczność podjęcia działań korygujących lub zapobiegawczych, określa: źródło powstania incydentu lub zagrożenia, zakres działań korygujących lub zapobiegawczych, termin realizacji, osobę odpowiedzialną.
3. ADO (IOD jeśli został powołany) jest odpowiedzialny za nadzór nad poprawnością i terminowością wdrażanych działań korygujących lub zapobiegawczych.
4. Po przeprowadzeniu działań korygujących lub zapobiegawczych, ADO (IOD jeśli został powołany) jest zobowiązany do oceny efektywności ich zastosowania.
5. Powyższe czynności ADO (IOD jeśli został powołany) rejestruje w pliku **załącznik nr 9**.

Kontrola systemu ochrony danych osobowych

1. Celem procedury jest uporządkowanie i przedstawienie czynności związanych z kontrolą stanu bezpieczeństwa danych osobowych.
2. Procedura obejmuje wszystkie procesy organizacji, gdzie przestrzeganie zasad ochrony danych osobowych jest wymagane.
3. Do kontroli stanu ochrony danych osobowych upoważniony jest ADO (IOD jeśli został powołany).
4. Kontroli podlegają:
   a) systemy informatyczne przetwarzające dane osobowe,
   b) zabezpieczenia fizyczne,
   c) zabezpieczenia organizacyjne,
   d) bezpieczeństwo osobowe oraz zgodność stanu faktycznego z wymaganiami RODO.

e) ADO (IOD jeśli został powołany) przygotowuje plan kontroli uwzględniając zakres oraz potrzebne zasoby fizyczne, czasowe i osobowe. Kontrola powinna odbyć się co najmniej raz na pół roku.

f) Kontrola przeprowadzana jest na podstawie audytu zgodności z RODO - **załącznik nr 1**.

g) Po dokonanej kontroli ADO (IOD jeśli został powołany) sporządza raport pokontrolny, **załącznik nr 19** – na jego podstawie ADO (IOD jeśli został powołany) inicjuje działania korygujące lub zapobiegawcze.

Sprawozdanie roczne stanu systemu ochrony danych osobowych

1. Raz w roku ADO (IOD jeśli został powołany) przygotowuje sprawozdanie roczne stanu funkcjonowania systemu ochrony danych osobowych (audyt).
2. Sprawozdanie przygotowany jest w **załączniku nr 18**.

Szkolenia pracowników

1. Każdy użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej winien być poddany przeszkoleniu lub zapoznany z polityką ochrony danych osobowych.
2. Za przeprowadzenie szkolenia lub zapoznania polityką ochrony danych osobowych odpowiada ADO (IOD jeśli został powołany).
3. Zakres szkolenia powinien obejmować przepisy RODO, dokumentację ochrony danych osobowych (Regulamin) oraz zasady bezpieczeństwa systemu informatycznego obowiązującą u ADO, a także zobowiązanie się do ich przestrzegania. Szczegółowy zakres szkolenia wraz z listą obecności znajduje się w **załączniku nr 16.**
4. Po szkoleniu lub po zapoznaniu się z polityką ochrony danych osobowych, użytkownik zobowiązany jest do podpisania oświadczenia o poufności - **załącznik nr 4.**
5. Dokument ten jest przechowywany w aktach osobowych użytkowników lub w dokumentacji ochrony danych osobowych i stanowi podstawę do podejmowania działań w celu nadania pracownikom uprawnień do korzystania z systemu informatycznego przetwarzającego dane osobowe.

Rozdział IV Procedury zapewniające bezpieczeństwo danych osobowych

Procedura nadawania uprawnień do przetwarzania danych osobowych:

1. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się z następującymi dokumentami:
   a) Rozporządzenia 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.U. UE L 119, s. 1) - **załącznik 28,**
   b) Regulaminem ochrony danych osobowych.
2. Zapoznanie się z powyższymi dokumentami użytkownik systemu potwierdza własnoręcznym podpisem na oświadczeniu, którego wzór stanowi **załącznik nr 16**.
3. Upoważnienia do przetwarzania danych osobowych nadaje ADO.
4. Przetwarzania danych osobowych może dokonywać jedynie użytkownik systemu upoważniony przez ADO. Wzór upoważnienia stanowi **załącznik nr 3**.

5. Przed nadaniem upoważnienia do przetwarzania danych osobowych pracownik zostaje przeszkolony w zakresie ich ochrony oraz zapoznana z zasadami bezpieczeństwa systemu informatycznego.
6. Osoba posiadająca upoważnienie do przetwarzania danych osobowych podpisała oświadczenie o zachowaniu poufności danych osobowych do których ma dostęp - **załącznik nr 4**.
7. Przyznanie uprawnień w zakresie dostępu do systemu informatycznego polega na wprowadzeniu do systemu przez ADO/ASI dla każdego użytkownika systemu unikalnego identyfikatora ze wskazaniem zakresu dostępnych danych i operacji. Hasło jest zmieniane półautomatycznie lub manualnie co 30 dni przez osoby upoważnione.
8. Hasło pierwszego logowania w systemie ustanawia ADO. Każdy użytkownik systemu informatycznego ma obowiązek dokonać jego zmiany na indywidualne, ośmioznakowe hasło zawierające wielkie i małe litery oraz cyfry i znaki specjalne.
9. Osoba upoważniona zobowiązuje się do zachowania w poufności hasła dostępu do danych osobowych oraz jego natychmiastowej zmiany w przypadku ujawnienia.
10. Zabronione jest przechowywanie hasła w sposób jawny lub przekazywania go innym osobom.

Odpowiedzialność.

1. Użytkownik systemu ma prawo do wykonywania tylko tych czynności, do których został upoważniony.
2. Użytkownik systemu ponosi wszelką odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu z wyjątkiem sytuacji, kiedy ADO użyje hasła użytkownika podczas jego nieobecności. ADO ma obowiązek sporządzić z tego zdarzenia protokół, z którym zostaje zapoznany użytkownik systemu, którego hasło zostało użyte. Po zapoznaniu się z protokołem, użytkownik systemu ma obowiązek dokonać natychmiastowej zmiany hasła dostępu i przekazać je ADO.
3. Wszelkie przekroczenia lub jakiekolwiek próby przekroczenia przyznanych uprawnień, traktowane będą jako naruszenie podstawowych obowiązków pracowniczych.
4. ADO może odebrać uprawnienia pracownikowi z podaniem daty oraz przyczyny odebrania uprawnień.
5. Hasło oraz uprawnienia użytkownika systemu, który je utracił, należy niezwłocznie wyrejestrować z systemu informatycznego. Wyrejestrowania z systemu dokonuje ADO/ASI.
6. Użytkownik systemu zatrudniony przy przetwarzaniu danych osobowych zobowiązany jest do zachowania ich w poufności oraz dołożenia wszelkich starań, aby dane osobowe nie zostały

przekazane osobom nieuprawnionym.

Rejestr użytkowników.

1. ADO (IOD jeśli został powołany) jest zobowiązany do prowadzenia i ochrony rejestru użytkowników i ich uprawnień w systemie informatycznym.
1. Rejestr musi odzwierciedlać aktualny stan systemu w zakresie użytkowników i ich uprawnień oraz umożliwić przeglądanie historii zmian w systemie informatycznym.
3. Rejestr - **załącznik nr 2 -** zawiera:
   a) imię i nazwisko użytkownika,
   b) identyfikator użytkownika,
   c) zakres uprawnienia,
   d) datę nadania uprawnień,
   e) datę odebrania uprawnień,
   f) przyczynę odebrania uprawnień,
   g) podpis ADO.

Rozdział V Postanowienia końcowe

1. **Polityka Ochrony Danych Osobowych jest dokumentem wewnętrznym i nie może być udostępniania osobom postronnym w żadnej formie.**
2. Wszelkie procedury i zasady opisane w niniejszym dokumencie są przestrzegane przez osoby upoważnione do przetwarzania danych osobowych ze szczególnym uwzględnieniem dobra osób których dane te dotyczą.
3. Powierzenie przetwarzania danych osobowych podmiotowi zewnętrznemu może być dokonanie jedynie w drodze umowy zawartej na piśmie z zastrzeżeniem, iż podmiot ten spełnia co najmniej takie same warunki bezpieczeństwa przetwarzania danych osobowych jak **infraTEAM**, - **załącznik nr 20.**
4. ADO/IOD jest zobowiązany zapoznać z treścią Polityki Ochrony Danych Osobowych każdego pracownika przetwarzającego dane osobowe w **infraTEAM.**
5. Wszystkie regulacje dotyczące systemów informatycznych, określone w Polityce Ochrony Danych Osobowych dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiejkolwiek innej formie.
6. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce Ochrony Danych Osobowych.

7. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych.
8. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła ADO/IOD (jeśli został powołany) można wszcząć postępowanie dyscyplinarne.
9. Kara dyscyplinarna orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności zgodnie z RODO oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
10. W sprawach nieuregulowanych w niniejszej Polityce Ochrony Danych Osobowych mają zastosowanie przepisy Rozporządzenia 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.U. UE L 119, s. 1).