Polityka ochrony danych osobowych przetwarzanych w sposób tradycyjny oraz przy użyciu systemu informatycznego w Polskim Towarzystwie Badań Kanadyjskich

Podstawa prawna :

- 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 (RODO) oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

Polityka dotyczy wszystkich komputerów i systemów informatycznych przetwarzających dane osobowe oraz dokumentacji prowadzonej w sposób tradycyjny w stowarzyszeniu.

Spis treści

nośników informacji służących do przetwarzania danych.

12. Ustalenia w zakresie przetwarzania danych osobowych sposobem tradycyjnym.
13. Załączniki.

I . Pojęcia

1.1 Ustawa — rozumie się przez to 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 (RODO)

1.2 Administrator Danych Osobowych (ADO)– rozumie się przez to stowarzyszenie o nazwie Polskie Towarzystwo Badań Kanadyjskich Zwane dalej „Stowarzyszeniem") które decyduje o celach i środkach przetwarzania danych osobowych. Przy czym dla celów niniejszej Polityki (i tylko dla tych celów) wszędzie tam gdzie jest mowa w poniższym tekście o „siedzibie Stowarzyszenia" rozumie się pod tym pomieszczenie biurowe przy ul. Władysława Bojarskiego 1 lok. C.3.30 w Toruniu.

1.3 Inspektor Ochrony Danych (IOD) – osoba powołana zarządzeniem władz Stowarzyszenia, nadzorująca stosowanie środków technicznych i organizacyjnych przetwarzanych danych osobowych, odpowiednich do ryzyka, zagrożeń oraz kategorii danych objętych ochroną.

1.4 Dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, jeżeli jej tożsamość można określić bezpośrednio lub pośrednio , w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne; informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

1.5 Dane wrażliwe – dane o pochodzeniu rasowym lub etnicznym, poglądach politycznych, przekonaniach religijnych lub filozoficznych, przynależności wyznaniowej, partyjnej lub związkowej, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym.

1.6 Przetwarzanie danych - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

1.7 Zbiór danych - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

1.8 System informatyczny - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

1.9 Identyfikator użytkownika (login) - ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.

1.10 Hasło - ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

1.11 Uwierzytelnianie — rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

1.12 Rozliczalność – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

1.13 Integralność danych — rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.

1.14 Poufności danych — rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom.

II. Polityka ochrony danych

1. **Polityka ochrony danych** rozumiana jest jako wykaz praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji danych osobowych wewnątrz Stowarzyszenia. Obejmuje całokształt zagadnień związanych z problemem zabezpieczenia danych osobowych przetwarzanych zarówno tradycyjnie jak i w systemach informatycznych. Wskazuje działania przewidziane do wykonania oraz sposób ustanowienia zasad i reguł postępowania koniecznych do zapewnienia właściwej ochrony przetwarzanych danych osobowych.

2. **Deklaracja**
    1) Administrator danych mając świadomość, iż może wystąpić sytuacja przetwarzania danych wrażliwych określonych osób deklaruje dołożyć wszelkich starań, aby przetwarzanie odbywało się w zgodności z przepisami prawa.
    2) W celu zabezpieczenia danych osobowych przed nieuprawnionym udostępnieniem Administrator danych wprowadza określone niniejszym dokumentem zasady przetwarzania danych. Zasady te określa w szczególności niniejsza Polityka oraz będąca jej integralną częścią Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Dokumenty te są uzupełnione załącznikami do dokumentacji, na które składają się m.in.: wykazy zbiorów, miejsc ich przetwarzania oraz osób upoważnionych do przetwarzania danych.
    3) Mając świadomość, iż żadne zabezpieczenie techniczne nie gwarantuje 100%-towej szczelności systemu, konieczne jest, aby każdy pracownik, współpracownik, członek władz upoważniony do przetwarzania danych pełen świadomej odpowiedzialności, postępował zgodnie z przyjętymi zasadami i minimalizował zagrożenia wynikające z błędów ludzkich.
    4) W trosce o czytelny i uporządkowany stan materii, wprowadza się stosowne środki organizacyjne i techniczne zapewniające właściwą ochronę danych oraz nakazuje ich bezwzględne stosowanie, zwłaszcza przez osoby dopuszczone do przetwarzania danych.

5) ADO samodzielnie bądź poprzez Inspektora Ochrony Danych (jeżeli został powołany) prowadzi stałe monitorowanie stanu bezpieczeństwa tych danych w Stowarzyszeniu. W szczególności utrzymuje jak najwyższy stopień świadomości w zakresie wymagań Ustawy, w szczególności tego że dane osobowe muszą być:

a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”);

b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami („ograniczenie celu”);

c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”);

d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość”);

e) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania”);

f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub

niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność”).

zważywszy iż Administrator jest odpowiedzialny za przestrzeganie przepisów Ustawy w wyżej wymienionym zakresie i musi być w stanie wykazać ich przestrzeganie („rozliczalność”).

3. **Charakterystyka** - Administrator danych osobowych jest Stowarzyszeniem - podmiotem wpisanym do Krajowego Rejestru Sądowego pod numerem 0000129279, działającym głównie na mocy przepisów prawa zawartych w Ustawie – Prawo o stowarzyszeniach, Kodeksie Cywilnym i innych aktach prawnych.
4. **Wykaz zbiorów osobowych** - Na podstawie Ustawy **tworzy się wykaz zbiorów osobowych wraz ze wskazaniem programów komputerowych** służących do ich przetwarzania zgodnie z **załącznikiem nr 1** do niniejszej dokumentacji. Z uwagi na połączenie komputerów z siecią Internet, dla zbiorów przetwarzanych elektronicznie stosuje się adekwatne do stopnia ryzyka środki bezpieczeństwa.

5. **Wykaz miejsc przetwarzania.** Na podstawie przepisów Ustawy tworzy się wykaz pomieszczeń tworzących obszar fizyczny przetwarzania danych. Wyznaczają go pomieszczenia zlokalizowane w siedzibie Stowarzyszenia. Szczegółowy wykaz pomieszczeń, stanowi **załącznik nr 2** do niniejszej dokumentacji.

6. **Ewidencja osób upoważnionych do przetwarzania danych osobowych.** Zgodnie z art. 39 ust. 1 ustawy o ochronie danych osobowych wprowadza się ewidencję osób upoważnionych do przetwarzania danych, która stanowi **załącznik nr 3** do niniejszej dokumentacji. Ewidencja zawiera imię i nazwisko osoby upoważnionej. Osoby, które przetwarzają dane wrażliwe winny posiadać osobne upoważnienie wydane przez władze Stowarzyszenia, do takiego przetwarzania.

7. **Środki organizacyjne ochrony danych osobowych.** W celu stworzenia właściwych zabezpieczeń, które powinny bezpośrednio oddziaływać na procesy przetwarzania danych, wprowadza się następujące środki organizacyjne:

- Przetwarzanie danych osobowych w Stowarzyszeniu może odbywać się wyłącznie w ramach wykonywania zadań służbowych. Zakres uprawnień wynika z zakresu tych zadań.
- Zgodnie z art. 37 ust. 4 Ustawy, Administrator może powołać **Inspektora Ochrony Danych (IOD). Jeżeli Administrator nie powoła Inspektora, wykonuje czynności związane z ochroną danych osobowych samodzielnie.**
- Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające stosowne **upoważnienie**. Wzór upoważnienia stanowi **załącznik nr 4** do niniejszej dokumentacji.
- ADO prowadzi **ewidencję osób upoważnionych,** o której mowa w pkt 6 oraz na jej podstawie przygotowuje **Upoważnienia do przetwarzania danych**. Jeżeli przygotowania dokonuje IOD, to przedkłada je do podpisu ADO.
- Unieważnienie upoważnienia następuje na piśmie, wg wzoru stanowiącego **załącznik nr 5** do niniejszej dokumentacji.
- Zabrania się przetwarzania danych poza obszarem określonym w załączniku nr 2 do niniejszej instrukcji, chyba że przetwarzanie odbywa się w związku z czynnościami służbowymi poza siedzibą Stowarzyszenia (delegacje, sympozja, wykłady, zebrania, wystawy itd) bądź następuje za zgodą ADO w związku z czynnościami służbowymi na sprzęcie informatycznym odpowiednio zabezpieczonym, w sposób nie mniejszy niż w obszarze przetwarzania.
- Każdy upoważniony do przetwarzania danych **potwierdza pisemnie** fakt zapoznania się z niniejszą dokumentacją i zrozumie-

niem wszystkich zasad bezpieczeństwa. Wzór potwierdzenia stanowi **załącznik nr 6** do niniejszej dokumentacji.

- Obszar przetwarzania danych osobowych określony w załączniku nr 2 do niniejszej dokumentacji, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.
- Stałe przebywanie osób nieuprawnionych w w/w obszarze jest dopuszczalne za zgodą Administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych. Wzory zgody na przebywanie w pomieszczeniach dla osób nie posiadających upoważnienia, a także odwołania tej zgody, stanowią odpowiednio **załącznik nr 7** oraz **załącznik nr 8** do przedmiotowej dokumentacji. Jednocześnie, zważywszy iż obszar przetwarzania danych jest integralną częścią Uniwersytetu Mikołaja Kopernika w Toruniu (który prowadzi suwerenną politykę ochrony danych osobowych) pisemna zgoda nie jest wymagana w przypadku przebywania osób, których obecność związana jest z wykonywaniem obowiązków względem Uniwersytetu.
- Pomieszczenia stanowiące obszar przetwarzania danych powinny być zamykane na klucz.
- Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.
- Przed opuszczeniem pomieszczenia stanowiącego obszar przetwarzania danych należy zamknąć okna oraz usunąć z biurka wszystkie dokumenty i nośniki informacji zawierające dane osobowe oraz umieścić je w zamykanych szafach/szafkach .
- Przetwarzanie danych podawanych dobrowolnie może odbywać się tylko na podstawie pisemnej zgody podającego te dane wg wzoru określonego w **załączniku nr 10.**

8. Środki techniczne ochrony danych osobowych. Zbiory danych przetwarzane w Stowarzyszeniu zabezpiecza się poprzez:

1) Środki ochrony fizycznej.

- Zbiory danych osobowych przechowywane są w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi). Drzwi zamykane/otwierane są kartą dostępu.
- Zbiory danych osobowych przechowywane są w pomieszczeniach, w których okna są zamykane od wewnątrz. Zamontowane są żaluzje wewnętrze, uniemożliwiające podgląd pomieszczenia z zewnątrz, jeżeli są zasunięte.
- Zbiory danych osobowych w formie papierowej (dane osób fizycznych będących członkami Stowarzyszenia, współpracowników, w tym ewentualne dane wrażliwe) przechowywane są w zamkniętej szafie, zamykanej na klucz
- Kopie zapasowe/archiwalne zbiorów danych osobowych przechowywane są w zamykanej na klucz szafie.
- Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób ręczny mechaniczny za pomocą niszczarek dokumentów.

2) Środki sprzętowe, infrastruktury informatycznej i telekomunikacyjnej.

- Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
- Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.
- Zastosowano programy antywirusowe ESET NOD 32 ANTIVIRUS, AVAST

3) Środki ochrony w ramach systemowych narzędzi programowych i baz danych.

- Dostęp do zbiorów danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.

Dodatkowe środki ochrony technicznej systemu informatycznego, jak również wszystkie niezbędne informacje dotyczące jego pracy oraz zasad użytkowania, określa **Instrukcja zarządzania systemem informatycznym** służącym do przetwarzania danych osobowych opisana w pkt III niniejszej dokumentacji.

4) Podstawowa zasada Polskiego Towarzystwa Badań Kanadyjskich w zakresie przetwarzania danych osobowych

Towarzystwo przyjmuje za priorytet uzyskiwanie zgód osób fizycznych na przetwarzanie ich danych osobowych, przy czym za główny cel tego przetwarzania Towarzystwo uznaje zgodne ze statutem, ideami i zgodnością z prawem działanie i rozwój Towarzystwa. Wzory zgód określają **załączniki nr 10 i 11**.

III. Instrukcja zarządzania systemem informatycznym.

1. Charakterystyka systemu.

1) Sygnał internetowy dostarczany jest przez usługodawcę internetowego i odpowiednio zabezpieczony.
2) System zabezpieczony jest oprogramowaniem antywirusowym zainstalowanym na każdym urządzeniu.

2. Ogólne zasady pracy w systemie informatycznym.

1) ADO / IOD odpowiada za korygowanie niniejszej instrukcji w przypadku uzasadnionych zmian w przepisach praw-

nych dotyczących przetwarzania danych osobowych w systemach informatycznych, jak również zmian organizacyjno-funkcjonalnych.

2) Przetwarzanie danych w systemie informatycznym może być realizowane wyłącznie poprzez licencjonowane oprogramowanie.

3) Użytkownikom zabrania się:

a. udostępniania stanowisk roboczych osobom nieuprawnionym,

b. samowolnego instalowania i używania programów komputerowych,

c. korzystania z nielicencjonowanego oprogramowania oraz wykonywania jakichkolwiek działań niezgodnych z ustawą o ochronie praw autorskich,

d. umożliwiania dostępu do zasobów wewnętrznej informatycznych spółki oraz sieci internetowej osobom nieuprawnionym,

e. używania komputera bez zainstalowanego oprogramowania antywirusowego.

3. Procedury nadawania nadawanie uprawnień do przetwarzania danych oraz ich rejestrowanie w systemie informatycznym.

1) Do przetwarzania danych osobowych zgromadzonych w systemie informatycznym jak również w rejestrach tradycyjnych wymagane jest upoważnienie.

2) Wprowadza się rejestr osób upoważnionych do przetwarzania danych osobowych, który stanowi **załącznik nr 3** do niniejszej dokumentacji.

3) Uprawnienia do pracy w systemie informatycznym odbierane są czasowo, poprzez zablokowanie konta w przypadku zawieszenia w pełnieniu obowiązków.

4) Uprawnienia do przetwarzania danych osobowych odbierane są trwale w przypadku ustania członkostwa w Zarządzie Stowarzyszenia.
5) Osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia nawet w przypadku ustania stosunku członkostwa w Zarządzie Stowarzyszenia.

4. Stosowane metody i środki uwierzytelnienia oraz procedury związane i ich zarządzaniem i użytkowaniem.

1) System informatyczny przetwarzający dane osobowe wykorzystuje mechanizm identyfikatora i hasła jako narzędzi umożliwiających bezpieczne uwierzytelnienie.
2) Każdy sprzęt informatyczny, przypisany do danego użytkownika systemu informatycznego powinien posiadać odrębny identyfikator
3) Hasło nie powinno zawierać żadnych informacji, które można kojarzyć z użytkownikiem komputera np. osobiste dane użytkownika, tj. nazwisko, inicjały, imiona itp
4) Hasło nie powinno być zapisywane w miejscu dostępnym dla osób nieuprawnionych.
5) W przypadku, gdy istnieje podejrzenie, że hasło mogła poznać osoba nieuprawniona, użytkownik zobowiązany jest do natychmiastowej zmiany hasła, lub w razie problemów powiadomić o tym fakcie ADO/IOD.

5. Procedury rozpoczęcia , zawieszenia i zakończenia pracy.

1) Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje wprowadzenie hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione.

2) Użytkownik systemu jest odpowiedzialny za zabezpieczenie danych wyświetlanych przez system przed osobami nie mającymi uprawnień.
3) Zawieszenie pracy polega na opuszczeniu stanowiska pracy bez wylogowania się i jest dopuszczalne tylko w przypadku pozostania w pomieszczeniu.
4) Zabrania się opuszczania stanowiska pracy bez wcześniejszego wylogowania z systemu z zastrzeżeniem pkt 3.
5) Zakończenie pracy polega na wylogowaniu się z systemu i wyłączeniu komputera.

6. Procedury tworzenia kopii awaryjnych zbiorów danych oraz programów i narzędzi służących do ich przetwarzania.

1) Zbiory danych w systemie informatycznym są zabezpieczane przed utratą lub uszkodzeniem za pomocą:
    a) urządzeń zabezpieczających przed awarią zasilania lub zakłóceniami w sieci zasilającej (UPS)
    b) sporządzania kopii zapasowych zbiorów danych (kopie pełne).
2) Dane przechowywane na serwerze chronione są za pomocą kopii bezpieczeństwa. W szczególnych przypadkach – przed aktualizacją lub zmianą w systemie należy bezwarunkowo wykonać pełną kopię zapasową systemu.
3) Nośniki danych po ustaniu ich użyteczności należy pozbawić danych lub zniszczyć w sposób uniemożliwiający odczyt danych.

7. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji.

a) Dane osobowe, z zachowaniem należytej ostrożności, można przetwarzać na dyskach twardych komputerów stacjonarnych lub nośnikach informacji.

b) Przenośne nośniki danych powinny być zabezpieczone przed przypadkową utratą.

c) Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:

-likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,

-przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie,

-naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je, pod nadzorem ADO/IOD lub osoby odpowiedzialnej w Stowarzyszeniu za sektor informatyczny.

d) Nośniki kopii awaryjnych, które zostały wycofane z użycia, podlegają zniszczeniu po usunięciu danych osobowych.

8. Sposób zabezpieczenia systemu przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego.

W spółce zapewnia się ochronę antywirusową oraz zarządza systemem wykrywającym i usuwającym wirusy i inne niebezpieczne kody. System antywirusowy jest skonfigurowany w następujący sposób:

a) skanowanie dysków zawierających potencjalnie niebezpieczne dane następuje automatycznie po włączeniu komputera,

b) skanowanie wszystkich informacji przetwarzanych w systemie, a zwłaszcza poczty elektronicznej jest realizowane na bieżąco.

c) automatycznej aktualizacji wzorców wirusów.

W przypadkach wystąpienia infekcji użytkownik powinien niezwłocznie powiadomić o tym fakcie informatyka, ADO lub IOD.

2) W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy, osoba upoważniona przez ADO podejmuje działania

zmierzające do usunięcia zagrożenia. W szczególności działania te mogą obejmować:

a) usunięcie zainfekowanych plików, o ile jest to akceptowalne ze względu na prawidłowe funkcjonowanie systemu informatycznego,

b) odtworzenie plików z kopii awaryjnych po uprzednim sprawdzeniu, czy dane zapisane na kopiach nie są zainfekowane,

c) samodzielną ingerencję w zawartość pliku - w zależności od posiadanych narzędzi i oprogramowania.

9. Informacje o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia.

1) Informacje o udostępnieniu danych osobowych przetwarza się i przechowuje w segregatorze dotyczącym ochrony danych osobowych.

2) Za udostępnianie danych zgodnie z przepisami prawa odpowiedzialny jest ADO.

10. Przesyłanie danych poza obszar przetwarzania.

1) Urządzenia i nośniki zawierające dane osobowe, przekazywane poza obszar przetwarzania zabezpiecza się w sposób zapewniający poufność i integralność tych danych.

2) W wypadku przesyłania danych osobowych poza obszar przystosowany do transferu danych osobowych ADO/IOD może zastosować szczególne środki bezpieczeństwa, które obejmują zatwierdzenie przez ADO/IOD zakresu danych osobowych przeznaczonych do wysłania.

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

1. Przeglądy i konserwacje systemu oraz nośników informacji służących do przetwarzania danych mogą być wykonywane jedynie przez osoby posiadające upoważnienie wydane przez ADO.

2. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe muszą uwzględniać zachowanie wymaganego poziomu zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych, w szczególności poprzez bezpośredni nadzór prowadzony przez ADO/IOD lub osobę odpowiedzialną za sektor informatyczny.
3. W przypadku uszkodzenia zestawu komputerowego, nośniki danych, na których są przechowywane dane osobowe powinny zostać zabezpieczone przez informatyka lub ADO/IOD.
4. W przypadku konieczności przeprowadzenia prac serwisowych poza Stowarzyszeniem, dane osobowe znajdujące się w naprawianym urządzeniu muszą zostać w sposób trwały usunięte, chyba że z podmiotem tym zawarto umowę przetwarzania danych.
5. Jeżeli nie ma możliwości usunięcia danych z nośnika na czas naprawy komputera, należy zapewnić stały nadzór nad tym nośnikiem przez osobę upoważnioną do przetwarzania danych osobowych na nim zgromadzonych.

12. Zalecenia w zakresie przetwarzania danych osobowych sposobem tradycyjnym

1) Miejscem tworzenia, uzupełniania, przechowywania sposobem tradycyjnym dokumentacji , o której mowa w załączniku nr 1 do niniejszej dokumentacji , jest pomieszczenie na III piętrze budynku przy ul. Władysława Bojarskiego 1, lok. C 3.30 w Toruniu. Osoby prowadzące dokumentację zobowiązane są do zachowania tajemnicy służbowej.
2) Dokumentacji, o której mowa w punkcie 1) nie można wynosić poza teren określony wyżej, chyba że z wyraźnej i konkretnej potrzeby będącej w związku z interesem faktycznym/prawnym Stowarzyszenia, polecenia przełożonego lub nakazu upoważnionego organu państwowego wynika inaczej.
3) Dokumentację, o której mowa w punkcie 1) archiwizuje się zgodnie z praktyką archiwizacji w Stowarzyszeniu.

4) Osoby prowadzące dokumentację zobowiązane są do niezwłocznego poinformowania ADO/IOD o podejrzeniu dostępu do dokumentacji przez osoby nieupoważnione.

13. Załączniki.

Załącznik nr 1. Wykaz zbiorów osobowych przetwarzanych w Stowarzyszeniu.
Załącznik nr 2. Wykaz miejsc przetwarzania zbiorów osobowych w Stowarzyszeniu.
Załącznik nr 3. Wykaz osób upoważnionych do przetwarzania danych osobowych w Stowarzyszeniu.
Załącznik nr 4. Wzór upoważnienia do przetwarzania danych osobowych.
Załącznik nr 5. Wzór unieważnienia upoważnienia do przetwarzania danych osobowych.
Załącznik nr 6. Wzór potwierdzenia znajomości zasad bezpieczeństwa.
Załącznik nr 7. Wzór zgody na przebywanie w obszarze przetwarzania danych osobowych.
Załącznik nr 8. Wzór odwołania zgody na przebywanie w obszarze przetwarzania danych osobowych.
Załącznik nr 9. Wzór raportu z naruszenia bezpieczeństwa zasad ochrony danych osobowych.
Załącznik nr 10. Wzór zgody na przetwarzanie danych osobowych.
Załącznik nr 11. Wzór deklaracji członkowskiej z elementem zgody na przetwarzanie danych osobowych
Załącznik nr 12. Wzór umowy o powierzenie przetwarzania danych osobowych.