Stowarzyszenie Rodów Grodzieńskich
Warszawa, ul. J. Kasprowicza 119 A/2
KRS 0000684080, REGON 367679556, NIP 1182148297

POLITYKA BEZPIECZEŃSTWA INFORMACJI

STOWARZYSZENIA RODÓW GRODZIEŃSKICH

Polityka wprowadzona została uchwałą nr 1/2017 Zarządu Stowarzyszenia Rodów Grodzieńskich z 13 lipca 2017 r.
w sprawie przyjęcia polityki bezpieczeństwa informacji Stowarzyszenia Rodów Grodzieńskich

PODSTAWY PRAWNE

- Konstytucja RP (art. 47 i 51).
- Konwencja nr 108 Rady Europy – dotycząca ochrony osób w związku z automatycznym przetwarzaniem danych osobowych.
- Dyrektywa PE i RE z dnia 24 października 1995 r. (95/46/EC) w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych.
- Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz. U. z 2015 poz. 2135 z późn. zm.).
- Rozporządzenie MSWiA z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100 poz. 1024).

PODSTAWOWE POJĘCIA

§ 1

- SRG – w tym dokumencie jest rozumiana, jako Stowarzyszenia Rodów Grodzieńskich z siedzibą 01-949 Warszawa, Kasprowicza 119a m. 2.
- Polityka – w tym dokumencie jest rozumiana jako „Polityka bezpieczeństwa" obowiązująca w SRG.
- Administrator Bezpieczeństwa Informacji (ABI) – osoba wyznaczona przez Administratora Danych Osobowych (Zarząd SRG) do nadzorowania przestrzegania zasad ochrony danych osobowych, oraz przygotowania dokumentów wymaganych przez przepisy ustawy o ochronie danych osobowych w SRG. ABI powołany jest uchwałą Zarządu SRG.
- Użytkownik – osoba upoważniona do przetwarzania danych osobowych. Użytkownikiem może być osoba zatrudniona, wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, odbywająca staż.
- Przetwarzanie danych – rozumie się to w tym dokumencie, jako jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie.
- Zabezpieczenie danych – wdrożenie i wykorzystywanie stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.

Stowarzyszenie Rodów Grodzieńskich
Warszawa, ul. J. Kasprowicza 119 A/2
KRS 0000684080, REGON 367679556, NIP 1182148297

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

I.1. Wykaz budynków w których przetwarzane są dane osobowe

§ 2

ADRES – BUDYNEK	POMIESZCZENIA
01-949 Warszawa, Kasprowicza 119a m. 2	Cały lokal

I.2 System przetwarzania danych osobowych

§ 3

W skład systemu wchodzą:

- dokumentacja papierowa (korespondencja, dokumenty pracowników i kontrahentów);
- wydruki komputerowe;
- procedury przetwarzania danych, w tym procedury awaryjne.

I.2.1 Cele i zasady funkcjonowania polityki bezpieczeństwa

§ 4

Realizując Politykę bezpieczeństwa informacji zapewnia ich:

- poufność – informacja nie jest udostępniana lub ujawniana nieupoważnionym osobom, podmiotom i procesom;
- integralność – dane nie zostają zmienione lub zniszczone w sposób nie autoryzowany;
- dostępność – istnieje możliwość wykorzystania ich na żądanie, w założonym czasie, przez autoryzowany podmiot;
- rozliczalność – możliwość jednoznacznego przypisania działań poszczególnym osobom;
- autentyczność – zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana;
- niezaprzeczalność – uczestnictwo w całości lub części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie jest niepodważalne;
- niezawodność – zamierzone zachowania i skutki są spójne.

§ 5

Polityka bezpieczeństwa informacji w SRG ma na celu zredukowanie możliwości wystąpienia negatywnych konsekwencji naruszeń w tym zakresie, to jest:

1. naruszeń danych osobowych rozumianych jako prywatne dobro powierzone SRG;
2. naruszeń przepisów prawa oraz innych regulacji;
3. utraty lub obniżenia reputacji SRG;
4. strat finansowych ponoszonych w wyniku nałożonych kar.

§ 6

Realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych SRG dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia, aby dane te były:

- przetwarzane zgodnie z prawem,

- zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,
- merytorycznie poprawne i adekwatne w stosunku do celu, w jakim są przetwarzane,
- przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

I.2.2 Kompetencje i odpowiedzialność w zarządzaniu bezpieczeństwem danych osobowych

§ 7

Za przetwarzanie danych osobowych niezgodnie z prawem, celami przetwarzania lub przechowywanie ich w sposób niezapewniający ochrony interesów osób, których te dane dotyczą grozi odpowiedzialność karna wynikająca z przepisów ustawy o ochronie danych osobowych lub pracownicza na zasadach określonych w kodeksie pracy lub kodeksie cywilnym

§ 8

Administrator Danych Osobowych (ADO) – Zarząd SRG:

- formułuje i wdraża warunki techniczne i organizacyjne służące ochronie danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem,
- decyduje o zakresie, celach oraz metodach przetwarzania i ochrony danych osobowych,
- odpowiada za zgodne z prawem przetwarzanie danych osobowych w SRG.

§ 9

Administrator Bezpieczeństwa Informacji (ABI) – osoba związana umową z SRG wyznaczony przez Zarząd:

- egzekwuje zgodnie z prawem przetwarzanie danych osobowych w SRG w imieniu ADO; wydaje upoważnienie do przetwarzania danych osobowych określając w nich zakres i termin ważności – wzór upoważnienia określa załącznik nr 1;
- prowadzi ewidencji osób upoważnionych do przetwarzania danych osobowych – wzór rejestru określa załącznik nr 2;
- ewidencjonuje oświadczenia osób upoważnionych o zaznajomieniu się z zasadami zachowania bezpieczeństwa danych – wzór oświadczenia określa załącznik nr 3;
- prowadzi rejestr zbiorów danych osobowych, według wzoru określonego w załączniku nr 7;
- określa potrzeby w zakresie stosowanych w SRG zabezpieczeń, wnioskuje do ADO o zatwierdzenie proponowanych rozwiązań i nadzoruje prawidłowość ich wdrożenia;
- udziela wyjaśnień i interpretuje zgodność stosowanych rozwiązań w zakresie ochrony danych osobowych z przepisami prawa;
- bierze udział w podnoszeniu świadomości i kwalifikacji osób przetwarzających dane osobowe w SRG i zapewnia odpowiedni poziom przeszkolenia w tym zakresie.

I.2.3 Zasady udzielania dostępu do danych osobowych

§ 10

Dostęp do danych osobowych może mieć wyłącznie osoba zaznajomiona z przepisami ustawy o ochronie danych osobowych oraz zasadami zawartymi w obowiązującej w SRG polityce bezpieczeństwa i instrukcji zarządzania systemem informatycznym, stanowiący załącznik nr 8. Osoba zaznajomiona z zasadami ochrony danych potwierdza to w pisemnym oświadczeniu.

§ 11

Dostęp do danych osobowych może mieć wyłącznie osoba posiadająca pisemne oraz imienne upoważnienie wydane przez ABI.

§ 12

ABI może wyznaczyć upoważnionych do przetwarzania danych osobowych pracowników SRG do nadzoru nad upoważnionymi pracownikami podmiotów zewnętrznych lub innymi upoważnionymi osobami przetwarzającymi dane osobowe w SRG.

I.2.4 Udostępnianie i powierzanie danych osobowych

§ 13

Dane osobowe mogą być udostępnione osobom i podmiotom z mocy przepisów prawa lub jeżeli w sposób wiarygodny uzasadnią one potrzebę ich posiadania, a ich udostępnienie nie naruszy praw i wolności osób, których one dotyczą.

§ 14

Udostępnienie danych może nastąpić na pisemny wniosek zawierający następujące elementy:

- adresat wniosku (administrator danych),
- wnioskodawca,
- podstawa prawna (wskazanie potrzeby),
- wskazanie przeznaczenia,
- zakres informacji.

§ 15

Administrator odmawia udostępnienia danych jeżeli spowodowałoby to naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób.

§ 16

Powierzenie danych może nastąpić wyłącznie w drodze pisemnej umowy, w której podmiot przyjmujący dane zobowiązuje się do przestrzegania obowiązujących przepisów ustawy o ochronie danych osobowych. Umowa powinna zawierać informacje o podstawia prawnej powierzenia danych, celu i sposobie ich przetwarzania.

§ 17

Każda osoba fizyczna, której dane przetwarzane są w SRG, ma prawo zwrócić się z wnioskiem o udzielenie informacji związanych z przetwarzaniem tych danych, prawo do kontroli i poprawiania swoich danych osobowych, a także w przypadkach określonych w art. 32 ust 1 pkt 7 i 8 ustawy o ochronie danych osobowych prawo wniesienia umotywowanego żądania

zaprzestania przetwarzania danych oraz sprzeciwu wobec przekazywania ich innym podmiotom.

§ 18

Sprawy związane z udzielaniem informacji w tym zakresie prowadzi ABI, udzielając informacji o zawartości zbioru danych na piśmie zgodnie ze wzorem w załączniku nr 4.

I.2.5 Bezpieczeństwo w przetwarzaniu danych osobowych w formie tradycyjnej

§ 19

Pomieszczenia, w których znajdują się przetwarzane zbiory danych osobowych pozostają zawsze pod nadzorem upoważnionego do ich przetwarzania pracownika. Opuszczenie pomieszczenia, w których znajdują się zbiory danych osobowych musi być poprzedzone zamknięciem zbioru danych w szafie na klucz. Przy planowanej dłuższej nieobecności pracownika pomieszczenie winno być zamknięte na klucz.

§ 20

Klucze do szaf, w których przechowywane są dane osobowe mają jedynie pracownicy upoważnieni do przetwarzania danych osobowych w zakresie zgodnym z kategorią danych.

§ 21

Korzystanie ze zbiorów danych osobowych przez osoby niezatrudnione w SRG powinno odbywać się po uzyskaniu upoważnienia lub skonsultowane z ABI w przypadku osób upoważnionych do przetwarzania tych danych na podstawie ogólnie obowiązujących przepisów.

I.3 Analiza ryzyka związanego z przetwarzaniem danych osobowych

I.3.1 Identyfikacja zagrożeń

§ 22

FORMA PRZETWARZANIA DANYCH	ZAGROŻENIA
dane przetwarzane w sposób tradycyjny	- oszustwo, kradzież, sabotaż; - zdarzenia losowe (powódź, pożar); - zaniedbania pracowników SRG (niedyskrecja, udostępnienie danych osobie nieupoważnionej); - niekontrolowana obecność nieuprawnionych osób w obszarze przetwarzania; - pokonanie zabezpieczeń fizycznych; - podsłuchy, podglądy; - ataki terrorystyczne; - brak rejestrowania udostępniania danych; - niewłaściwe miejsce i sposób przechowywania. dokumentacji;

dane przetwarzane w systemach informatycznych	- oszustwo, kradzież, sabotaż; - **z**aniedbania pracowników SRG (niedyskrecja, udostępnienie danych osobie nieupoważnionej); - niekontrolowana obecność nieuprawnionych osób w obszarze przetwarzania; - pokonanie zabezpieczeń informatycznych; - podsłuchy, podglądy; - ataki terrorystyczne; - pozostawienie sprzętu bez wylogowania się.

I.6.2 Sposób zabezpieczenia danych

§ 23

FORMA PRZETWARZANIA DANYCH	STOSOWANE ŚRODKI OCHRONY
dane przetwarzane w systemach informatycznych	- przetwarzanie danych osobowych tylko w komputerach specjalnie do tego przystosowanych, - zastosowanie haseł w dostępie do komputera; - przetwarzanie danych wyłącznie przez osoby posiadających upoważnienie nadane przez ABI; - zapoznanie pracowników z zasadami przetwarzania danych osobowych oraz obsługą systemu służącego do ich przetwarzania;
dane przetwarzane w sposób tradycyjny	- przechowywanie danych w pomieszczeniach zamykanych na zamki, - przechowywanie danych osobowych w szafach zamykanych na klucz, - osoby z ochrony wydające klucze tylko osobom upoważnionym, - przetwarzanie danych wyłącznie przez osoby posiadających upoważnienie nadane przez ABI, - zapoznanie pracowników z zasadami przetwarzania danych osobowych oraz obsługą systemu służącego do ich przetwarzania.

I.3.3 Określenie wielkości ryzyka

§ 24

Poziom ryzyka naruszenia bezpieczeństwa danych jest niski. Zastosowane techniczne i organizacyjne środki ochrony są adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych osobowych.

I.3.4 Identyfikacja obszarów wymagających szczególnych zabezpieczeń

§ 25

Uwzględniając kategorie przetwarzanych danych oraz zagrożenia zidentyfikowane w wyniku przeprowadzonej analizy ryzyka, stosuje się wysoki poziom bezpieczeństwa. ABI przeprowadza okresową analizę ryzyka dla poszczególnych systemów i na tej podstawie przedstawiają ADO propozycje dotyczące zastosowania środków technicznych i organizacyjnych, celem zapewnienia właściwej ochrony przetwarzanym danym.

INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA DANYCH

II.1 Istota naruszenia danych osobowych

§ 26

Naruszeniem danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych osobowych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu, a w szczególności:

- nieautoryzowany dostęp do danych;
- nieautoryzowane modyfikacje lub zniszczenie danych;
- udostępnienie danych nieautoryzowanym podmiotom;
- nielegalne ujawnienie danych;
- pozyskiwanie danych z nielegalnych źródeł.

II.2 Postępowanie w przypadku naruszenia danych osobowych

§ 27

Każdy pracownik oraz osoba pracująca na podstawie umowy cywilnej lub cywilno-prawnej w SRG, który stwierdzi fakt naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe, bądź posiada informację mogącą mieć wpływ na bezpieczeństwo danych osobowych jest zobowiązany niezwłocznie zgłosić to ABI.

§ 28

Każdy pracownik oraz osoba pracująca na podstawie umowy cywilnej lub cywilno-prawnej w SRG, który stwierdzi fakt naruszenia bezpieczeństwa danych ma obowiązek podjąć czynności niezbędne do powstrzymania skutków naruszenie ochrony oraz ustalić przyczynę i sprawcę naruszenia ochrony.

§ 29

W przypadku stwierdzenia naruszenia bezpieczeństwa danych należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia oraz nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia ABI.

§ 30

ABI podejmuje następujące kroki:

- zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości pracy SRG;
- może zażądać dokładnej relacji z zaistniałego naruszenia bezpieczeństwa danych osobowych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje w związku z zaistniałym naruszeniem;
- rozważa celowość i potrzebę powiadamiania o zaistniałym naruszeniu ADO, nawiązuje kontakt ze specjalistami spoza urzędu (jeśli zachodzi taka potrzeba).

§ 31

ABI dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych osobowych sporządzając raport wg wzoru stanowiącego załącznik nr 5 i przekazuje go ADO.

§ 32

ABI zasięga potrzebnych mu opinii i proponuje działania naprawcze (w tym także ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych osobowych).

II.3 Sankcje karne

§ 33

Wobec osoby, która w przypadku naruszenia ochrony danych osobowych nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami wszczyna się postępowanie dyscyplinarne.

§ 34

Kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia o naruszeniu danych osobowych nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą o ochronie danych osobowych.

Załączniki

Załącznik nr 1 – Upoważnienie do przetwarzania danych osobowych.
Załącznik nr 2 – Rejestr osób upoważnionych do przetwarzania danych osobowych.
Załącznik nr 3 – Oświadczenie pracownika o zapoznaniu się z zasadami zachowania bezpieczeństwa danych osobowych.
Załącznik nr 4 – Informacja o zawartości zbioru danych.
Załącznik nr 5 – Raportu z naruszenia bezpieczeństwa danych osobowych.
Załącznik nr 6 – Oświadczenie o zgodzie na przetwarzanie danych osobowych.
Załącznik nr 7 – Rejestr zbiorów danych osobowych.
Załącznik nr 8 – Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych.

Stowarzyszenie Rodów Grodzieńskich
Warszawa, ul. J. Kasprowicza 119 A/2
KRS 0000684080, REGON 367679556, NIP 1182148297

Załącznik nr 1

……, dn ……

UPOWAŻNIENIE NR…./20…
DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie przepisów art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2015 poz. 2135 z późn. zm.)

upoważniam

……

do przetwarzania danych osobowych zawartych w zbiorze/zbiorach danych o nazwie:
……
zgodnie z uprawnieniami wynikającymi z ustalonego zakresu czynności.

Zobowiązuję do zachowania tajemnicy o danych znajdujących się w w/w zbiorach, jak i sposobach ich zabezpieczenia. Obowiązek ten istnieje również po ustaniu zatrudnienia.

Upoważnienie ważne jest na czas …….

Upoważnienie może zostać odwołane lub utracić ważność wskutek wcześniejszego ustania zatrudnienia.

Oryginał upoważnienia należy zwrócić po jego odwołaniu lub ustaniu zatrudnienia.

Załącznik nr 2

REJESTR OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

L.p.	Imię i nazwisko	Zakres upoważnienia do przetwarzania danych osobowych	Data nadania uprawnień	Data odebrania uprawnień	Uwagi

Załącznik nr 3

……
(imię i nazwisko)

OŚWIADCZENIE
o zachowaniu poufności i zapoznaniu się z przepisami

Ja niżej podpisany/a oświadczam, iż zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których mam lub będę miał/a dostęp w związku z wykonywaniem zadań i obowiązków służbowych wynikających ze stosunku pracy, zarówno w czasie trwania umowy , jak i po jej ustaniu.

Oświadczam, że zostałem/am poinformowany/a o obowiązujących w Stowarzyszeniu Rodów Grodzieńskich zasadach dotyczących przetwarzania danych osobowych, określonych w „Polityce bezpieczeństwa informacji Stowarzyszenia Rodów Grodzieńskich" i zobowiązuję się ich przestrzegać. W szczególności oświadczam, że bez upoważnienia nie będę wykorzystywał/a danych osobowych ze zbiorów znajdujących się w SRG.

Zostałem/am zapoznany/a z przepisami ustawy o ochronie danych osobowych (Dz. U. 2002 r. Nr 101 poz. 926 z późn. zm.) oraz rozporządzenia MSWiA w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100 poz. 1024). Poinformowano mnie również o grożącej, stosownie do przepisów rozdziału 8 Ustawy o ochronie danych osobowych odpowiedzialności karnej. Niezależnie od odpowiedzialności przewidzianej w wymienionych przepisach, mam świadomość, ze złamanie zasad ochrony danych osobowych, obowiązujących w Stowarzyszeniu Rodów Grodzieńskich może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.

……..…….....
(podpis osoby upoważnionej)

Stowarzyszenie Rodów Grodzieńskich
Warszawa, ul. J. Kasprowicza 119 A/2
KRS 0000684080, REGON 367679556, NIP 1182148297

Załącznik nr 4

……, dnia …… r.

.....
(pieczęć SRG)

.....
(imię i nazwisko)
.....
.....
(adres)

INFORMACJA
o zawartości zbioru danych osobowych

W związku z Pani/Pana wnioskiem z dnia …… r. o udzielenie informacji związanych z przetwarzaniem danych osobowych w Stowarzyszenia Rodów Grodzieńskich działając na podstawie art. 33 ust. 1 ustawy o ochronie danych osobowych informuję, że zbiór danych zawiera następujące Pani/Pana dane osobowe:

.....

.....

Powyższe dane przetwarzane są w Stowarzyszenia Rodów Grodzieńskich w celu ..... z zachowaniem wymaganych zabezpieczeń i zostały uzyskane

.....
(podać sposób).

Powyższe dane nie były / były udostępniane .....

.....
(podać komu)

w celu .....
(podać cel przekazania danych)

Zgodnie z rozdziałem 4 ustawy o ochronie danych osobowych przysługuje Pani/Panu prawo do kontroli danych osobowych, prawo ich poprawiania, a także w przypadkach określonych w art. 32 ust. 1 pkt 7 i 8 ustawy, prawo wniesienia umotywowanego żądania zaprzestania przetwarzania danych oraz prawo sprzeciwu wobec przetwarzania danych w celach marketingowych lub wobec przekazywania danych innemu administratorowi danych osobowych.

.....
(podpis)

Stowarzyszenie Rodów Grodzieńskich
Warszawa, ul. J. Kasprowicza 119 A/2
KRS 0000684080, REGON 367679556, NIP 1182148297

Załącznik nr 5

……, dnia …… r.

.....
(pieczęć SRG)

RAPORT Z NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH SRG WOLNY UMYSŁ

1. Data: ..... r. Godzina: .....
2. Osoba powiadamiająca o zaistniałym zdarzeniu: .....
   .....
   (imię, nazwisko, stanowisko służbowe, nazwa użytkownika - jeśli występuje)
3. Lokalizacja zdarzenia: .....
   .....
   (np. nr pokoju, nazwa pomieszczenia)
4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:
   .....
   .....
   .....
5. Przyczyny wystąpienia zdarzenia:
   .....
   .....
6. Podjęte działania:
   .....
   .....
7. Postępowanie wyjaśniające:
   .....
   .....
   .....

.....
(podpis)

Stowarzyszenie Rodów Grodzieńskich
Warszawa, ul. J. Kasprowicza 119 A/2
KRS 0000684080, REGON 367679556, NIP 1182148297

Załącznik nr 6

…… ……, dn……
Imię i nazwisko

OŚWIADCZENIE

Zgodnie z art. 24 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych wyrażam zgodę na przetwarzanie moich danych osobowych przez administratora: Stowarzyszenia Rodów Grodzieńskich, zlokalizowany w 01-949 Warszawa, Kasprowicza 119a m., w celu:

.....

Dane będą przetwarzane w zbiorze danych osobowych o nazwie:

.....

Wiem, że podanie danych jest dobrowolne oraz, że mam prawo dostępu do treści swoich danych i ich poprawiania. Informujemy, że wyrażona zgoda może zostać w każdym czasie odwołana.

.....
(podpis)

Stowarzyszenie Rodów Grodzieńskich
Warszawa, ul. J. Kasprowicza 119 A/2
KRS 0000684080, REGON 367679556, NIP 1182148297

Załącznik nr 7

Rejestr zbiorów danych osobowych

L.p	Nazwa zbioru	Historia zmian w rejestrze	Data wykonania czynności	Oznaczenie Administrator Danych Osobowych	Oznaczenie przedstawiciela administratora o którym mowa w art. 31a Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych	Oznaczenie podmiotu, któremu powierzono przetwarzanie danych ze zbioru na podstawie art. 31 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych	Cel przetwarzani danych w zbiorze	Administrator danych przewiduje powierzenie przetwarzania danych innemu podmiotowi.	Opis kategorii osób, których dane są przetwa-rzane	Zakres danych przetwarzanych w zbiorze	Sposób zbierania danych do zbioru	Sposób udostępniania danych ze zbioru	Oznaczenie odbiorcy danych osobowych lub kategorii odbiorców, którym dane mogą być przekazywane	Informacja dotycząca ewentualnego przekazywania danych do państwa trzeciego
1	Członkowie	Wpis do rejestru	10.07.2017	Zarząd SRG	brak	brak	Zadania statutowe	tak	Dane osobowe emerytów, rencistów i inwalidów	Nazwisko i imię, PESEL, adres zamieszkania, numer telefonu, data i miejsce urodzenia	Dane zbierane są od osób, których dane osobowe dotyczą	Dane udostępniane są na podstawie wniosku złożonego przez wnioskodawcę zatwierdzanego	brak	Nie dotyczy
2	Wolontariat	Wpis do rejestru	10.07.2017	Zarząd SRG	brak	brak	Zadania statutowe	tak	Dane osobowe wolontariuszy	Nazwisko i imię, PESEL, adres zamieszkania, numer telefonu	Dane zbierane są od osób, których dane osobowe dotyczą	Dane udostępniane są na podstawie wniosku złożonego przez wnioskodawcę zatwierdzanego	brak	Nie dotyczy
3	Rejestr koresponde ncji	Wpis do rejestru	10.07.2017	Zarząd SRG	brak	brak	Zadania statutowe	tak	Dane osobowe nadawcy korespondencji	Imię i nazwisko, adres	Dane zbierane są od osób, których dane osobowe dotyczą	Dane udostępniane są na podstawie wniosku złożonego przez wnioskodawcę zatwierdzanego	brak	Nie dotyczy
4	Beneficjenci projektów	Wpis do rejestru	10.07.2017	Zarząd SRG	brak	brak	Zadania statutowe	tak	Dane osobowe osób korzystający z projektw PZERiI	Imię i nazwisko, adres	Dane zbierane są od osób, których dane osobowe dotyczą	Dane udostępniane są na podstawie wniosku złożonego przez wnioskodawcę zatwierdzanego	Brak	Nie dotyczy
5	Umowy cywilno-prawne	Wpis do rejestru	10.07.2017	Zarząd SRG	brak	brak	Zadania statutowe	tak	Dane osób wykonujące świadczenia na podstawie umów	Imię i nazwisko, adres zamieszkania, telefon, dane oddziału NFZ, Urząd Skarbowy, numer NIP, PESEL	Dane zbierane są od osób, których dane osobowe dotyczą	Dane udostępniane są na podstawie wniosku złożonego przez wnioskodawcę zatwierdzanego	brak	Nie dotyczy

Załącznik nr 8

Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych

1. Procedury rozpoczęcia i zakończenia pracy przeznaczone dla użytkowników systemu.

1.1. Rozpoczynając pracę, użytkownik włącza komputer i podaje hasło w celu uruchomienia systemu operacyjnego.
1.2. Jeżeli użytkownik pracuje w sieci, rejestruje się w systemie podając nazwę użytkownika sieci i hasło dostępu. Dla wysokiego poziomu bezpieczeństwa sieci teleinformatycznej obowiązkowe są hasła zawierające co najmniej 8 znaków, w tym małe lub duże litery lub znaki specjalne. Hasło powinno być zmieniane nie rzadziej niż co 30 dni.
1.3. Uruchomienie programów następuje po podaniu identyfikatora użytkownika i hasła. Pierwsze hasło dla użytkownika jest zakładane przez Administratora Systemu podczas wprowadzania jego identyfikatora. W takim przypadku przy pierwszym logowaniu użytkownik musi zmienić hasła. W przeciwnym razie użytkownik wpisuje hasło pod nadzorem administratora systemu. Przy zakładaniu hasła użytkownika, Administrator Systemu nadaje prawo użytkownikowi do dostępu do katalogów.
1.4. W przypadku, kiedy użytkownik musi opuścić stanowisko pracy, powinien wyjść z programu, włączyć wygaszasz ekranu albo wylogować komputer z sieci, aby uniemożliwić przeglądanie oraz ewentualne wprowadzenie danych.
1.5. Na stanowiskach pracujących pod systemem WINDOWS, jeżeli nie wykonuje się żadnych operacji, powinien być włączany wygaszacz ekranu, aby dalsza praca była niemożliwa bez podania hasła.
1.6. Po zakończeniu pracy użytkownik zamyka poprawnie uruchomione programy oraz system operacyjny.
1.7. Użytkownik wyłącza komputer.

2. Hasło.

2.1. W haśle nie należy stosować w szczególności popularnych nazw komputerowych, nazw znanych postaci bajkowych, literackich, filmowych. Hasło nie powinno kojarzyć się z użytkownikiem ani jego otoczeniem (imiona, nazwiska, adresy, daty itp.).
2.2. Hasło objęte jest tajemnicą.
2.3. Hasło nie może być udostępniane osobom trzecim ani przechowywane w dostępnym miejscu (kalendarz, szafka, biurko, monitor, pod klawiaturą itp.).

3. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności.

3.1. Ewidencję osób zatrudnionych przy komputerowym przetwarzaniu danych osobowych nadzoruje komputerowo Administrator Bezpieczeństwa Informacji.
3.2. Administrator Bezpieczeństwa Informacji w uzgodnieniu z użytkownikiem nadaje identyfikator do programu, uprawnienia oraz ustala hasło użytkownikiem.
3.3. Administrator Systemu nadaje uprawnienia do katalogów w sieci. Użytkownik może mieć tylko jeden identyfikator w systemie. Identyfikator raz przydzielony użytkownikowi, nie może być powtórnie nadany drugiemu użytkownikowi.
3.4. W przypadku, gdy użytkownik stracił prawa do wykonywania dotychczasowych zadań jego upoważnienie dopuszczające wygasa automatycznie i zostaje on usunięty z rejestru osób

przetwarzających oraz odebrane zostają mu nadane wcześniej prawa do systemu i katalogów sieciowych.

4. Sposób zabezpieczenia systemu teleinformatycznego przed oprogramowaniem złośliwym.
4.1. Stosowanie oprogramowania antywirusowego.
4.2.Wprowadzanie do sieci danych z zewnętrznych nośników dopuszczalne jest przez osoby upoważnione przez ABI.

5 **Sposób zabezpieczenia systemu teleinformatycznego przed utratą danych, spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.**
5.1. Stosowanie zasilaczy awaryjnych (UPS) i filtrów odgromowych.

6. Procedury i zasady obowiązujące przy pracy na stanowisku komputerowym.
6.1. Uruchomienie komputera następuje po podaniu hasła, które jest czasowo zmieniane.
6.2. Stanowisko komputerowe z uruchomionym systemem czy programem nie może być pozostawione bez kontroli pracującego na nim użytkownika.
6.3. Zabrania się użytkownikom:
6.3.1. udostępniania stanowisk komputerowych, haseł oraz ich zasobów informatycznych osobom nieupoważnionym,
6.3.2. wykorzystywania stanowiska komputerowego w celach innych niż wykonywanie obowiązków związanych z zakresem zadań powierzonym przez przełożonego,
6.3.3. samowolnego instalowania i używania programów komputerowych oraz przenoszenia sprzętu komputerowego,
6.3.4. kopiowania programów komputerowych oraz danych,
6.3.5. wynoszenia bez autoryzacji z siedziby danych przechowywanych elektronicznie lub na papierze,
6.3.6. odklejania naklejek świadczących o legalności oprogramowania oraz plomb zabezpieczających komputer,
6.3.7. używania elektronicznych nośników informacji podejrzanych o zainfekowanie wirusem.
6.4. Zobowiązuje się pracowników oraz osoby pracujące na podstawie umowy cywilnej lub cywilno-prawnej w SRG do:
6.4.1. ustawienia ekranów w sposób uniemożliwiający podgląd zawartości przez osoby nieupoważnione,
6.4.2. niszczenia w niszczarkach zbędnych wydruków zawierających dane osobowe,
6.4.3. przeglądania co najmniej raz dziennie poczty elektronicznej,
6.4.4. zgłaszania wszystkich nieprawidłowości w działaniu sprzętu i oprogramowania oraz prób nieautoryzowanego naruszenia zabezpieczeń.

7. Poziom bezpieczeństwa przetwarzania danych osobowych.
W SRG obowiązuje wysoki poziom bezpieczeństwa ochrony danych osobowych.

8. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.
8.1. Konserwacja baz danych i oprogramowania przeprowadzana jest przez Administratora Systemu.
8.2. Konserwacja sprzętu komputerowego przeprowadzana jest przez Administratora Systemu lub firmę zewnętrzną.

8.3. W przypadku awarii sprzętu, na którym znajdują się dane osobowe w zależności od uszkodzenia następuje:
8.3.1. naprawa na miejscu pod nadzorem Administratora Systemu,
8.3.2. demontowanie dysku i zabezpieczenie w SRG na czas naprawy,
8.3.3. przegrywanie danych przez Administratora Systemu na inny nośniki usunięcia danych z przekazywanego do naprawy sprzętu.
8.4. W przypadku przekazania komputerów innemu użytkownikowi lub jednostce organizacyjnej, dane z dysków twardych są usuwane przez Administratora Systemu w sposób uniemożliwiający ich odtworzenie.
8.5. W przypadku złomowania sprzętu komputerowego, nośniki informacji (dyski twarde) są fizycznie niszczone przez Administratora Systemu.

9. Procedury transportu przesyłek zawierających dane osobowe, przesyłek wartościowych lub transportu innych ważnych danych oraz przesłania danych.
9.1. Instrukcja obejmuje w szczególności transport przesyłek zawierających: nośniki z danymi osobowymi, wydruki przelewów, kopie baz danych i programów wykonane przez Administratora Systemu.
9.2. Przez transport należy rozumieć przenoszenie lub przewożenie przesyłek.
9.3. Transportu przesyłek dokonują pracownicy wyznaczeni przez ABI.
9.4. Transport przesyłek z danymi osobowymi lub innymi materiałami, może być realizowany pieszo lub pojazdem.
9.5. W przypadku przesłania danych osobowych mailem muszą one być spakowane i oznaczone hasłem, a hasło musi zostać przekazane do adresata inną drogą niż mailem (np.: SMS).

11. W przypadku stwierdzenia nie stosowania przez użytkowników Instrukcji, Administrator Systemu na polecenie ABI blokuje użytkownikowi prawo wejścia do sieci i korzystania z jej zasobów. Odblokowanie użytkownika w sieci następuje również na polecenie ABI.