REGULAMIN OCHRONY DANYCH OSOBOWYCH W FUNDACJI EDUKACJA DLA DEMOKRACJI

WSTĘP

W związku z wejściem w życie RODO (Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.) i w celu zapewnienia ochrony przetwarzanych danych osobowych zarówno za pomocą systemów informatycznych jak i w wersji papierowej Fundacja Edukacja dla Demokracji przeprowadziła analizę ryzyka dot. danych osobowych.

Celem jak najlepszego zapoznania pracowników i współpracowników z zasadami ochrony danych osobowych, mając na względzie przepisy RODO dot. posługiwania się zrozumiałą i przystępną terminologią Fundacja, na podstawie wniosków z analizy ryzyka, przeprowadziła aktualizację dokumentacji przetwarzania danych osobowych.

Fundacja wdraża niniejszy jednolity dokument, który zastępuje dotychczasową dokumentację przetwarzania danych osobowych, obowiązującą w Fundacji od 12.2016 r. mianowicie:

- Politykę bezpieczeństwa (13 stron),
- Instrukcję zarządzania systemem informatycznym (24 strony),
- Regulamin ochrony danych w FED (12 stron).

§ 1
DEFINICJE

Ilekroć w niniejszym regulaminie jest mowa o:

1. RODO - rozumie się przez to Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
2. Administratorze danych – rozumie się przez to podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych (art. 4 pkt. 7) RODO). W niniejszym Regulaminie przez Administratora rozumie się Fundację Edukacja dla Demokracji z siedzibą w Warszawie, ul. Nowolipie 9/11, 00-150 Warszawa, dalej zwaną „Administratorem", lub „Fundacją".
3. Dokumentacji przetwarzania danych osobowych – rozumie się przez to niniejszy Regulamin ochrony danych osobowych oraz Analizę ryzyka dot. danych osobowych, wraz z załącznikami.
4. Użytkowniku uprzywilejowanym – należy przez to rozumieć osobę upoważnioną, posiadająca wyższe niż standardowo przyznawane na danym stanowisku, uprawnienia w systemie informatycznym;
5. Użytkowniku systemu – rozumie się przez to osobę upoważnioną, która otrzymała dostęp do sieci LAN umożliwiający korzystanie z sieci Internet oraz login i hasło do systemu;

Pozostałe pojęcia, używane w regulaminie, rozumie się jak w odpowiednich punktach RODO:

1. dane osobowe (lub „dane") – jak w art. 4 pkt. 1) RODO,
2. przetwarzanie (lub „przetwarzanie danych") – jak w art. 4 pkt. 2) RODO,
3. zbiór danych – jak w art. 4 pkt. 6) RODO,
4. podmiot przetwarzający – jak w art. 4 pkt. 8) RODO.

§ 2
POSTANOWIENIA OGÓLNE

Celem wdrożenia niniejszej dokumentacji jest ochrona interesów osób, których dane dotyczą poprzez zapewnienie należytej, adekwatnej do zdefiniowanego ryzyka, ochrony posiadanych zasobów informacyjnych.

Poprzez bezpieczeństwo danych osobowych należy rozumieć zapewnienie ich poufności, integralności, dostępności oraz rozliczalności, poprzez wdrożenie i eksploatację niezbędnych do tego celu mechanizmów technicznych i procedur organizacyjnych.

Regulamin obejmuje wszystkie zbiory danych osobowych przetwarzane przez administratora, zarówno w formie elektronicznej, jak i papierowej oraz dane osobowe przetwarzane poza zbiorami danych.

Regulamin są zobowiązani stosować wszyscy pracownicy administratora oraz inne osoby mające dostęp do danych osobowych, przy pomocy których administrator wykonuje swoje czynności.

§ 3
ADMINISTRATOR

1. Administrator stosuje środki techniczne i organizacyjne zapewniające ochronę danych osobowych odpowiednią do zagrożeń oraz kategorii przetwarzanych danych oraz zabezpiecza posiadane dane przed: ich udostępnieniem, zmianą, utratą, uszkodzeniem, zniszczeniem lub przetwarzaniem przez osobę nieupoważnioną.
2. Administrator dokłada należytej staranności w celu ochrony interesów osób, których dane osobowe dotyczą, w szczególności jest obowiązany zapewnić, aby dane: były przetwarzane **zgodnie z prawem**, zbierane **dla oznaczonych celów**, przetwarzane w określonym **czasie**, merytorycznie poprawne i **adekwatne w swym zakresie** do celów w jakich są zbierane, przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą oraz aby zapewniona była rozliczalność, integralność i poufność danych, gdzie przez:
    1) rozliczalność - rozumie się właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
    2) integralność danych - rozumie się właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
    3) poufność danych - rozumie się właściwość zapewniającą, że dane osobowe nie są udostępniane nieupoważnionym podmiotom.
3. Administrator w szczególności zapewnia:
    1) środki techniczne i organizacyjne niezbędne dla zapewnienia bezpiecznego przetwarzania danych w pomieszczeniach do tego przeznaczonych;
    2) system i sprzęt informatyczny umożliwiający bezpieczne przetwarzanie danych;
    3) że do przetwarzania danych osobowych zostały dopuszczone wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych;
    4) prowadzenie elektronicznej ewidencji osób upoważnionych, o których mowa w §5 oraz zawartych umów powierzenia, o których mowa w §6 (z możliwością wydruku);
    5) należyte i terminowe udzielanie informacji na wniosek osób, których dane są przetwarzane i które wystąpiły o wgląd do swoich danych;
    6) kontrolę nad tym jakie dane, kiedy i przez kogo zostały do zbiorów Administratora wprowadzone, ze zbiorów usunięte oraz komu i przez kogo przekazane.
4. Obowiązki Administratora wynikają wprost z przepisów RODO.
5. Do obowiązków administratora, zgodnie z art. 13. i 14. RODO, należy m.in. obowiązek przekazania osobom, których dane administrator przetwarza, wymaganych prawem informacji o Administratorze, przetwarzaniu i prawach osób. Wzór klauzul informacyjnych stanowi Załącznik nr 1 do niniejszego Regulaminu.

§ 4
PRZETWARZANIE DANYCH

1. Przetwarzanie danych jest dopuszczalne tylko jeśli istnieje ku temu podstawa prawna.
2. Administrator przetwarza dane, w szczególności na mocy następującej podstawy prawnej:
    1) RODO art. 6. pkt. 1 lit. a) – zgoda osoby, której dane są przetwarzane, z zastrzeżeniem § 4 pkt. 5. Regulaminu;
    2) RODO art. 6. pkt. 1 lit. b) – przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
    3) RODO art. 6. pkt. 1 lit. c) - jest to niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze (wynikającego np. z Kodeksu pracy, Ustawy o systemie ubezpieczeń społecznych, Ustawy o rachunkowości, Kodeksu cywilnego);
3. Administrator nie przetwarza danych osobowych szczególnych kategorii (zwanych „danymi wrażliwymi"), czyli ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz danych genetycznych, danych biometrycznych lub dotyczących zdrowia, seksualności lub orientacji seksualnej.
4. Przetwarzanie danych zawsze odbywa się w konkretnie określonym celu oraz w zdefiniowanym okresie czasu.
5. Jeżeli przetwarzanie odbywa się na podstawie zgody, powinny być dochowane wszystkie warunki określone w art. 7. RODO, w tym w szczególności:
    1) Administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych – oznacza to konieczność dowodu po stronie Administratora, dowód nie musi mieć jednak formy papierowej (drukowanej).
    2) Zgoda powinna być dobrowolna, innymi słowy m.in. brak wyrażenia zgody nie może uniemożliwiać świadczenia usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej usługi.
    3) Jeśli zgoda wyrażana jest w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.
    4) Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Osoba, której dane dotyczą, jest o tym informowana, zanim wyrazi zgodę. Wycofanie zgody musi być równie łatwe jak jej wyrażenie.
6. Przetwarzanie danych na mocy podstawy prawnej wskazanej w pkt.2. nie zdejmuje z Administratora obowiązku stosowania przepisów ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2013 r. poz. 1422) oraz ustawy z dnia 16 lipca 2004 r. prawo telekomunikacyjne (Dz.U. z 2014 r. poz. 243), które przewidują dalej idącą ochronę.
7. W razie jakichkolwiek wątpliwości co do ewentualnej zgodności z prawem planowanych działań związanych z przetwarzaniem danych, należy zwrócić się do wyznaczonej przez Administratora osoby odpowiedzialnej, w celu rozstrzygnięcia wątpliwości. Do ich rozstrzygnięcia nie należy zbierać ani przetwarzać przedmiotowych danych.

§ 5
OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Administrator nadaje upoważnienie do przetwarzania danych każdej osobie, która do przetwarzania danych będzie dopuszczona, w tym zwłaszcza osobom, współpracującym z administratorem na zasadzie umowy o pracę.
2. Upoważnienie powinno zwierać:
    1) datę z którą zostało nadane;
    2) datę z którą upoważnienie wygasa, jeżeli jest ono nadane na czas określony;
    3) zakres upoważnienia.
3. Osoba upoważniona przez Administratora ma obowiązek stosowania się do zapisów niniejszego Regulaminu.

4. Administrator odpowiada za zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych, co może odbywać się w postaci szkolenia.
5. Osoba upoważniona przez Administratora nie ma prawa do nadawania dalszych upoważnień, chyba że upoważnienie do przetwarzania danych osobowych nadane przez Administratora zawiera upoważnienie do nadawania dalszych upoważnień.
6. Każdy kto przetwarza dane osobowe obowiązany jest zachować w tajemnicy dane osobowe, do których posiada dostęp zarówno zamierzony jak i przypadkowy, sposoby zabezpieczania danych jak również wszelkie informacje, które powzięły w czasie przetwarzania danych. Obowiązek zachowania danych w tajemnicy jest bezterminowy.
7. Wzór upoważnienia stanowi Załącznik nr 2 do niniejszego Regulaminu.

§ 6
POWIERZENIE DANYCH

1. Administrator może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych. Podmiot, z którym zawarto umowę, jest podmiotem przetwarzającym.
2. Umowy powierzenia przetwarzania danych osobowych zawierane są w szczególności:
    1) ze specjalistami IT zajmującymi się systemami informatycznymi,
    2) z członkami komisji grantowych,
    3) z trenerami prowadzącymi szkolenia na zlecenie Fundacji,
    4) z podmiotami świadczącymi usługi pocztowe, ubezpieczeniowe, agencjami podróży,
    5) z podmiotami, od których Administrator pozyskuje granty.
3. Podmiot przetwarzający może przetwarzać dane wyłącznie w zakresie, w celu i w okresie przewidzianym w umowie.
4. Podmiot przetwarzający obowiązany jest przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające przetwarzanie danych, nie mniejsze od tych stosowanych przez administratora.
5. Wzór umowy powierzenia stanowi Załącznik nr 3 do niniejszego Regulaminu.
6. W ramach realizacji celów statutowych Fundacja może uzyskać dostęp do danych, których administratorami są inne podmioty. Oznacza to konieczność zawarcia umowy powierzenia. Fundacja może w ten sposób zostać podmiotem przetwarzającym, w szczególności w odniesieniu do grantobiorców programów dotacyjnych Fundacji.

§ 7
ODBIORCY DANYCH

1. Dane osobowe, których Administratorem jest Fundacja mogą być przekazywane innym odbiorcom, jeśli są spełnione przesłanki wynikające z przepisów prawa.
2. Do odbiorców danych przetwarzanych przez Administratora należą: banki, ZUS, US, Poczta Polska...
3. Administrator może nadawać dostęp do danych innym podmiotom, w szczególności sponsorom projektów, w ramach których dane są gromadzone, jeśli wymaga tego umowa dotacji oraz zawarte zostały umowy powierzenia danych.

§ 8
MIEJSCE PRZETWARZANIA DANYCH

4. Administrator przetwarza dane w swojej siedzibie, w pomieszczeniach do tego przeznaczonych w sposób uniemożliwiający dostęp do danych osobom nieuprawnionym.
5. Wszelkie dokumenty zwierające dane osobowe powinny być przechowywane w szafach lub pomieszczeniach zamykanych na klucz w siedzibie Fundacji.
6. Przebywanie osób nieuprawnionych w obszarze w którym przetwarzane są dane osobowe jest dopuszczalne za zgodą administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych

7. Osoba posiadająca klucze do budynków i pomieszczeń Fundacji, nie może ich przekazywać osobom nieuprawnionym, a ponadto zobowiązana minimalizować ryzyko ich utraty.
8. Osoba która utraciła posiadane klucze do pomieszczeń Administratora, niezwłocznie zgłasza tę okoliczność Administratorowi. Administrator w podejmuje wszelkie niezbędne środki techniczne i organizacyjne w celu zabezpieczenia pomieszczenia, do którego klucze utracono.

§ 10
SYSTEMY INFORMATYCZNE

1. Administrator używa następujących systemów informatycznych, w których przetwarzane są dane osobowe:
    1) systemem Windows z oprogramowaniem MS Office,
    2) Google Apps – skrzynki mailowe,
    3) program księgowy Finka FK,
    4) system wnioskodawczy (program RITA do k. 2018 r.): formularze.fed.org.pl,
    5) system wnioskodawczy (program Edukacji Globalnej): Witkac.pl.
    6) system wnioskodawczy (program Szkoła.PL): JotForm,
    7) system Android na służbowych smartfonach.
2. W systemach informatycznych służących do przetwarzania danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych (co najmniej za pomocą zabezpieczenia hasłem), w szczególności zapewnia się, aby:
    1) w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator;
    2) dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i podania hasła.
3. Obowiązuje zasada „jeden użytkownik = jeden login", nie można przekazywać innym użytkownikom swojego loginu, ani wykorzystywać raz przypisanego komuś loginu i hasła dla innego użytkownika.
4. W przypadku gdy dostęp do systemów wymaga hasła a dany system nie definiuje jego minimalnych parametrów, użytkownik ponosi odpowiedzialność za ustawienie hasła odpowiednio „silnego" (trudnego do odgadnięcia). Zaleca się, aby składa się ono co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.
5. Użytkownik ponosi pełną odpowiedzialność za utworzenie hasła (prócz pierwszego hasła do systemu nadawanego przez administratora systemu informatycznego, które użytkownik powinien zmienić niezwłocznie) i jego przechowywanie.
6. Zabronione jest:
    1) zapisywanie haseł w sposób jawny i umieszczania ich w miejscach ogólnodostępnych;
    2) stosowanie haseł opartych na skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących danej osoby, np. imiona, numery telefonów, daty urodzenia itp.;
    3) używanie tych samych haseł w różnych systemach operacyjnych i aplikacjach;
    4) udostępnianie haseł innym użytkownikom;
    5) przeprowadzanie prób łamania haseł;
    6) wpisywanie haseł „na stałe" (np. w skryptach logowania) oraz wykorzystywania opcji auto-zapamiętywania haseł (np. w przeglądarkach internetowych).
7. Administrator nie narzuca częstotliwości zmiany haseł, wymaga jednak niezwłocznej zmiany hasła przy podejrzeniu jego ujawnienia. Poszczególne systemy mogą wymuszać regularną zmianę haseł, niezależnie od zaleceń Administratora.
8. Dostępem do systemów (nadawanie, odbieranie, zawieszanie kont) zarządza administrator lub, w jego imieniu, użytkownik uprzywilejowany.
9. Administrator prowadzi ewidencję dostępów, w tym nadanych przywilejów.
10. System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed:
    1) nieuprawnionym dostępem,
    2) działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego;
    3) utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej (komputery stacjonarne).
11. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych.

12. Kopie zapasowe:
    1) przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem;
    2) usuwa się niezwłocznie po ustaniu ich użyteczności.
13. Osoba użytkująca komputer przenośny lub dyski zewnętrzne, w tym pendrive'y zawierające dane osobowe zachowuje szczególną ostrożność podczas ich transportu, przechowywania i użytkowania poza obszarem, w którym przetwarzane są dane osobowe, w tym stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.
14. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
    1) likwidacji - pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
    2) przekazania podmiotowi nieuprawnionemu do przetwarzania danych - pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
    3) naprawy - pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.
15. Administrator monitoruje wdrożone zabezpieczenia systemu informatycznego.
16. Administrator stosuje środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej.

§ 11
ZASADY BEZPIECZEŃSTWA PRZY PRZETWARZANIU DANYCH

1. Rozpoczęcie **pracy** w systemie informatycznym następuje po wprowadzeniu loginu i hasła.
2. Hasła i loginy do systemu informatycznego nie mogą być ujawniane nawet po utracie ich ważności.
3. Podczas przetwarzania danych należy zachować szczególną ostrożność i podjąć wszelkie możliwe środki umożliwiające zabezpieczenie oraz ochronę danych przed nieuprawnionym dostępem, modyfikacją, zniszczeniem lub ujawnieniem. W szczególności:
    1) Użytkownik ma obowiązek każdorazowego *blokowania ekranu* wygaszaczem chronionym hasłem przed odejściem od stanowiska pracy.
    2) *Przed zakończeniem pracy* użytkownik ma obowiązek upewnić się, czy dane zostały zapisane, aby uniknąć utraty danych.
    3) *Po zakończeniu pracy*, użytkownik obowiązany jest wylogować się ze wszystkich systemów informatycznych przetwarzających dane osobowe i z systemu operacyjnego, zabezpieczyć nośniki informacji (elektroniczne i papierowe) oraz wyłączyć komputer.
    4) W sytuacji, gdy *wgląd w wyświetlane na monitorze dane* może mieć nieuprawniona osoba, trzeba tymczasowo zmienić widok wyświetlany na monitorze, stosować odpowiednią nakładkę na monitor lub obrócić monitor (przymknąć ekran laptopa) w sposób uniemożliwiający wgląd w wyświetlaną treść.
4. Osoba przetwarzająca dane po zakończeniu pracy porządkuje swoje stanowisko, zabezpieczając dokumenty i nośniki elektroniczne z danymi w specjalnie do tego przeznaczonych szafach lub pomieszczeniach.
5. Każdy dokument zawierający dane a nieużyteczny niszczy się niezwłocznie.
6. Niszczenie dokumentów zawierających dane odbywa się jedynie za pomocą niszczarki gwarantującej odpowiedni stopień rozdrobnienia lub za pośrednictwem firmy zajmującej się niszczeniem dokumentów, po zawarciu umowy o powierzeniu przetwarzania danych osobowych.
7. Podczas korzystania z urządzeń wielofunkcyjnych należy zachować szczególną ostrożność. Dokumenty kopiowane bądź skanowane wyjmowane są z urządzenia wielofunkcyjnego niezwłocznie po ich użyciu. Dotyczy to również dokumentów powstałych na skutek kopiowania bądź skanowania.
8. Każdy użytkownik zobowiązany jest do przestrzegania zakazu prowadzenia rozmów, podczas których może dochodzić do wymiany informacji o danych osobowych lub informacji poufnych Administratora, jeśli rozmowy te odbywają się w miejscach publicznych, otwartych pomieszczeniach biurowych lub takich, które nie gwarantują zachowania poufności rozmów.
9. Użytkownik systemu informatycznego przetwarzającego dane osobowe niezwłocznie powiadamia administratora systemu w przypadku, gdy:

1) wygląd systemu, sposób jego działania, zakres danych lub sposób ich przedstawienia przez system informatyczny odbiega od standardowego stanu uznawanego za typowy dla danego systemu informatycznego;
2) niektóre opcje, dostępne użytkownikowi w normalnej sytuacji, przestały być dostępne lub też opcje niedostępne użytkownikowi w normalnej sytuacji, stały się dostępne.

10. Pracownikom Fundacji zostaje nadany dedykowany adres **skrzynki poczty elektronicznej** działający w domenie fed.org.pl i dostępny poprzez G Suite (Google Mail).
11. Dostęp do skrzynki mailowej zabezpieczony jest hasłem. Dodatkowo istnieje możliwość zabezpieczenia skrzynki za pomocą dodatkowego klucza (np. sms, kod wysyłany na telefon, tzw. dwustopniowa weryfikacja). Włączenie dwustopniowej weryfikacji zalecane jest dla osób, które pracują w programach „wschodnich" oraz osób, które często pracują poza biurem.
12. Informacja o służbowym adresie skrzynki pocztowej jest jawna i dostępna powszechnie, w tym może być dostępna na łamach witryny internetowej Administratora w postaci książki adresowej.
13. Nadany użytkownikowi adres skrzynki poczty elektronicznej służy wyłącznie do realizacji celów służbowych lub umownych. Informacje przesyłane za pośrednictwem sieci administratora danych (w tym do i z Internetu) nie stanowią własności prywatnej użytkownika.
14. Wszelka korespondencja elektroniczna niezwiązana z działalnością Administratora powinna być prowadzona przez prywatną skrzynkę poczty elektronicznej użytkownika.
15. Użytkownicy dokonujący wysyłki korespondencji masowej poza organizację, obowiązani są do ukrywania listy odbiorców w kopii (pole UDW lub BCC).
16. Należy dochować należytej staranności podczas przesyłania dokumentów zawierających dane za pomocą środków komunikacji elektronicznej, w szczególności należy upewnić się, czy przesyłane za pomocą poczty elektronicznej dokumenty trafiły do właściwego odbiorcy.
17. W przypadku przesyłania za pomocą środków komunikacji elektronicznej zestawień, spisów czy innych dokumentów zawierających liczne dane osobowe, przesyłany dokument należy zaszyfrować, a hasło przesłać w miarę możliwości innym środkiem komunikacji elektronicznej. W szczególności zasada ta dotyczy przekazywania danych poza obszar EOG, komunikacji z partnerami w ramach „wschodnich" projektów międzynarodowych.
18. Zabronione jest:
    1) wysyłanie materiałów służbowych na konta prywatne (np. celem pracy w domu);
    2) odbieranie e-maili z nieznanych źródeł;
    3) otwieranie załączników z plikami samorozpakowującymi się bądź wykonalnymi, np. exe, com;
    4) przesyłanie pocztą elektroniczną plików wykonywalnych typu: bat, com, exe;
    5) ukrywanie lub dokonywanie zmian tożsamości nadawcy;
    6) czytanie, usuwanie, kopiowanie lub zmiana zawartości skrzynek pocztowych innego użytkownika bez jego zgody;
    7) odpowiadanie na niezamówione wiadomości reklamowe lub wysyłane łańcuszki oraz na inne formy wymiany danych określanych spamem;
    8) posługiwanie się adresem służbowym e-mail w celu rejestrowania się na stronach handlowych, informacyjnych, chatach lub forach dyskusyjnych, które nie dotyczą zakresu wykonywanej pracy lub obowiązków umownych;
    9) wykorzystywanie poczty elektronicznej do reklamy prywatnych towarów lub usług, działalności handlowo-usługowej innej niż wynikającej z potrzeb Administratora lub do poszukiwania dodatkowego zatrudnienia.
19. W siedzibie Fundacji użytkownicy mają możliwość uzyskania dostępu do internetu, dostępne są 2 konta WiFi: *„Fundacja"* i *„Fundacja-gosc"* – pracownicy Fundacji są zobowiązani do używania sieci *„Fundacja"* (dostępnej również po sieci LAN). Sieć *„Fundacja-gosc"* dostępna jest dla gości Fundacji, w tym uczestników różnego rodzaju spotkań czy szkoleń. Zabrania się udostępniania hasła do sieci *„Fundacja"* osobom nieuprawnionym.
20. Zaleca się korzystanie ze stron internetowych po szyfrowanym protokole HTTPS.
21. Wprowadza się całkowity zakaz dostępu do treści uznanych za pornograficzne, jak również do protokołów umożliwiających wymianę plików w sieciach z naruszeniem przepisów prawa.
22. Dalsze ograniczenia dostępu do sieci Internet mogą być rekomendowane przez Administratora.

§ 12
UŻYTKOWANIE SPRZĘTU KOMPUTEROWEGO, OPROGRAMOWANIA, NOŚNIKÓW DANYCH

1. Do sprzętu komputerowego zalicza się między innymi:
    1) komputery stacjonarne;
    2) komputery przenośne;
    3) smartfony;
    4) drukarki;
    5) monitory;
    6) routery;
2. Administrator odpowiada za poprawne działanie sprzętu komputerowego. Stan ten administrator zapewnia we współpracy z podmiotem zewnętrznym.
3. W przypadku wykorzystywania urządzeń mobilnych (m.in. smartfon) wymaga się zastosowania następujących środków bezpieczeństwa:
    1) blokada ekranu (pin/hasło/symbol graficzny);
    2) szyfrowanie pamięci/karty pamięci;
    3) program antywirusowy;
    4) wyłączanie nieużywanych usług (wi-fi, gprs/lte, bluetooth, nfc);
    5) instalowanie oprogramowania z zaufanego źródła (np. Sklep Play);
    6) używanie aplikacji szyfrujących komunikację (zalecane: WhatsApp, Signal)
    7) ograniczenie korzystania z publicznych hotspotów.
4. Administrator jest zobowiązany do prowadzenia ewidencji posiadanego sprzętu komputerowego oraz oprogramowania wraz z dostarczoną dokumentacją oraz z wyszczególnieniem użytkownika.
5. Administrator ma obowiązek przechowywać karty gwarancyjne, klucze i licencje do oprogramowania.
6. Administrator ma prawo instalować wyłącznie licencjonowane oprogramowanie lub oprogramowanie, które nie wymaga opłaty licencyjnej, zgodnie z warunkami licencji.
7. Użytkownik jest zobowiązany do dbałości o sprzęt oraz oprogramowanie, w tym jego aktualizację, a także odpowiedzialny za zabezpieczenie go przed używaniem przez osoby nieuprawnione oraz do ochrony przed kradzieżą lub zagubieniem.
8. Użytkownik nie może samodzielnie zmieniać konfiguracji przekazanego sprzętu komputerowego oraz instalować lub usuwać oprogramowania, w tym nie może używać na przekazanym sprzęcie prywatnego oprogramowania.
9. W szczególności zabronione jest korzystanie z programów służących do przesyłania danych, które nie zostały zainstalowane domyślnie przez Administratora, bez jego uprzedniej zgody (np. DropBox).
10. Użytkownik nie może udostępniać powierzonego mu sprzętu służbowego, w szczególności urządzeń mobilnych, osobom trzecim.
11. Każdy użytkownik wymiennych nośników elektronicznych ponosi całkowitą odpowiedzialność za powierzony do użytkowania sprzęt oraz jest obowiązany do stosowania się do poniższych zasad:
    1) zabrania się pozostawiania bez opieki w miejscach publicznych nośników wymiennych przetwarzających informacje Administratora;
    2) komputery przenośne należy przewozić jako bagaż podręczny i dbać o jego bezpieczeństwo;
    3) użytkownik wykonując czynności zawodowe lub umowne w domu, powinien zadbać o należyte zabezpieczenie powierzonego sprzętu oraz dostępu do informacji przed nieautoryzowanym dostępem osób trzecich;
    4) zabrania się udostępniania osobom trzecim nośników elektronicznych informacji oraz powierzonego sprzętu będącego własnością Administratora;
    5) w przypadku utraty nośnika elektronicznego lub sprzętu komputerowego należy ten fakt bezzwłocznie zgłosić do bezpośredniego przełożonego, Administratora lub administratora systemu informatycznego. Bezpośredni przełożony lub administrator systemu informatycznego bezzwłocznie zgłaszają taki fakt do Administratora, ponieważ zagubienie nośnika przetwarzającego dane może wiązać się z utratą poufności informacji chronionych przez Administratora;
    6) problemy wynikające z nieprawidłowego funkcjonowania sprzętu komputerowego należy zgłaszać administratorowi systemu informatycznego.

12. Dopuszcza się korzystanie przez użytkowników systemu z prywatnych nośników danych (pendrive'y), w sytuacji kiedy jest to niezbędne. Używanie nośnika prywatnego powinno mieć jednak charakter doraźny a czas i zakres przechowywania na nich danych służbowych w tym danych osobowych powinien być ograniczony do niezbędnego minimum. Niedopuszczalna jest sytuacja, w której:
    1) pracownik Administratora przechowuje dane służbowe na 3 lub większej ilości nośników prywatnych,
    2) pracownik Administratora gromadzi na nośnikach prywatnych dane służbowe ponad doraźne potrzeby.
13. Użytkownicy systemu mają obowiązek skanowania każdego zewnętrznego elektronicznego nośnika informacji, który chcą wykorzystać.
14. W przypadku stwierdzenia pojawienia się wirusa i braku możliwości usunięcia go przez program antywirusowy, użytkownik ma obowiązek skontaktować się z administratorem.

§ 13
POSTĘPOWANIE W RAZIE ZAGROŻENIA DLA BEZPIECZEŃSTWA PRZETWARZANYCH DANYCH OSOBOWYCH

1. W przypadku podejrzenia naruszenia zasad bezpieczeństwa danych osobowych lub naruszenia zabezpieczeń stosowanych przez Administratora dla ochrony przetwarzanych danych osobowych osoba, która jako pierwsza stwierdziła możliwość naruszenia zasad bezpieczeństwa niezwłocznie zawiadamia Administratora o dostrzeżonych lub podejrzewanych naruszeniach.
2. Administrator w przypadku, o którym mowa w ust. 1 obowiązany jest przeprowadzić postepowanie wyjaśniające i ustalające skutki oraz przyczyny naruszenia lub narażenia na naruszenie zasad bezpieczeństwa i sposobów zabezpieczenia.