Załącznik nr 1
do Polityki ochrony danych osobowych w Fundacji Jesuit Refugee Service Poland (JRS)

REGULAMIN OCHRONY DANYCH OSOBOWYCH
w JRS na podstawie § 7 ust. 1 Zasady ochrony danych osobowych w JRS, wprowadza się do stosowania niniejszy Regulamin ochrony danych osobowych, zwany dalej „Regulaminem".

§ 1.

Podstawowe zasady ochrony danych osobowych

1. Osoby przetwarzające dane osobowe, przed dopuszczeniem ich do przetwarzania, zapoznają się z niniejszym Regulaminem.
2. Osoby zapoznane z treścią Regulaminu, zobowiązane są podpisać Oświadczenie o poufności.
3. Każda z osób dopuszczona do przetwarzania danych osobowych jest zobowiązana do:

1) przetwarzania danych osobowych wyłącznie w zakresie i celu określonym przez Administratora Danych Osobowych,
2) zachowania w tajemnicy danych osobowych, do których ma dostęp w związku z wykonywanymi zadaniami, właściwymi do zajmowanego stanowiska,
3) zachowania w tajemnicy sposobów zabezpieczenia danych osobowych,
4) ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem, dostępem do danych osobowych oraz przetwarzaniem.

4. Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie wykazują się podstawą prawną uprawniającą do dostępu do takich danych.
5. Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym lub osobom, których tożsamości nie można zidentyfikować.

§ 2.

Użytkowanie sprzętu elektronicznego

1. Użytkownicy pracują na własnych, przydzielonych im przez Administratora Danych Osobowych kontach. Zabronione jest umożliwianie innym osobom korzystanie z konta innego użytkownika.
2. Każdy użytkownik przetwarzający dane osobowe za pomocą sprzętu elektronicznego (np. na komputerze, na dysku sieciowym, w programie lub aplikacji, w poczcie elektronicznej) posiada swój własny indywidualny identyfikator (login) do logowania się.
3. Użytkownicy nie mogą samodzielnie zmieniać przyznanych im uprawnień.
4. Wszystkie osoby przetwarzające dane osobowe, korzystające ze sprzętu elektronicznego (np. z komputerów stacjonarnych, laptopów, monitorów, drukarek, skanerów, urządzeń kserujących, służbowych tabletów i telefonów) mają obowiązek jego ochrony przed jakimkolwiek zniszczeniem lub uszkodzeniem.
5. Zabronione jest samowolne otwieranie (demontaż) sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) lub podłączanie jakichkolwiek niedopuszczonych przez Administratora Danych Osobowych systemów informatycznych do systemu informatycznego.
6. W przypadku zagubienia, utraty lub zniszczenia sprzętu użytkownik ma obowiązek natychmiast zgłosić takie zdarzenie Administratorowi Danych Osobowych.

7. Użytkownicy sprzętu pracujący z danymi osobowymi muszą dbać o to, by osoby niepowołane nie miały możliwości wglądu do danych wyświetlanych na używanych komputerach.
8. W przypadku czasowego opuszczenia stanowiska pracy, użytkownik zobowiązany jest włączyć blokowany hasłem wygaszacz ekranu lub wylogować się z systemu lub programu.
9. Po zakończeniu pracy, użytkownik zobowiązany jest wylogować się z systemu informatycznego, następnie wyłączyć sprzęt komputerowy i zabezpieczyć stanowisko pracy, zgodnie z Polityką czystego biurka.
10. Należy używać programu antywirusowego. Zakazane jest wyłączanie programu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe.

§ 3.

Polityka haseł

1. Hasła powinny składać się z przynajmniej 9 znaków i zawierać duże litery + małe litery + cyfry (lub znaki specjalne).
2. Hasła powinny posiadać odpowiedni stopień skomplikowania. Dlatego nie mogą być łatwymi do odgadnięcia słowami.
3. Zabronione jest udostępnianie swoich haseł nieuprawnionym osobom. W przypadku ujawnienia hasła – należy natychmiast je zmienić.
4. Nie wolno haseł nigdzie zapisywać, ani naklejać np. na monitorze komputera, pod klawiaturą lub w szufladzie.
5. Hasła muszą być zmieniane co 3 miesiące. Jeżeli system nie wymusza zmiany haseł, należy samodzielnie zmienić hasło.

§ 4.

Zasady postępowania z dokumentacją papierową, zawierającą dane osobowe

1. Osoby pracujące z danymi osobowymi zobowiązane są do stosowania tzw. Polityki czystego biurka. Zgodnie z jej zasadami należy zabezpieczać dokumenty zawierające dane osobowe przed kradzieżą lub wglądem osób nieupoważnionych, zarówno w czasie godzin pracy, jak i po jej zakończeniu.
2. Osoby przetwarzające dane osobowe zobowiązane są niszczyć niepotrzebną dokumentację i jej wydruki zawierające dane osobowe – w niszczarkach.
3. Zabronione jest pozostawianie dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami.
4. Zabrania się wyrzucania niezniszczonych dokumentów na śmietnik lub porzucania ich na zewnątrz, poza obszar przetwarzania danych osobowych.

§ 5.

Wynoszenie nośników z danymi poza obszar przetwarzania danych osobowych

1. Użytkownicy nie mogą wynosić na zewnątrz, poza obszar przetwarzania danych osobowych, wymiennych elektronicznych nośników informacji (np. twardych dysków, pendrive, pamięci typu Flash, płyt) z zapisanymi danymi osobowymi, bez zgody Administratora Danych Osobowych.
2. Jeżeli dokumenty przewozi użytkownik, to on jest odpowiedzialny za zabezpieczenie przewożonych dokumentów przed zgubieniem i kradzieżą.
3. Dane osobowe w wersji papierowej muszą być bezpiecznie przewożone np. w torbach, plecakach, teczkach. W razie możliwości należy korzystać ze sprawdzonych firm kurierskich.

4. W przypadku, gdy dane na takich nośnikach wynoszone są poza obszar przetwarzania danych, powinny być właściwie zaszyfrowane.

§ 6.

Regulacje dotyczące korzystania z Internetu

1. Użytkownicy zobowiązani są do korzystania z Internetu wyłącznie w celach służbowych.
2. Zabronione jest uruchamianie jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomych źródeł. W przypadku takich działań użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu.

§ 7.

Korzystanie z poczty elektronicznej

1. E-mail służbowy należy wykorzystywać wyłącznie do wykonywania obowiązków służbowych.
2. Nie należy wysyłać korespondencji służbowej na prywatne skrzynki pocztowe użytkowników lub innych osób.
3. W przypadku wysyłania dokumentacji zawierającej dane osobowe za pośrednictwem poczty elektronicznej, należy zabezpieczać je hasłami.
4. Należy zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
5. Przed otwarciem załączników (plików) w mailach zawsze należy przeprowadzić wcześniejszą weryfikację nadawcy.
6. Nie należy „klikać” na hiperlinki w mailach, gdyż mogą to być hiperlinki do stron zainfekowanych lub niebezpiecznych.
7. W przypadku wysyłania poczty elektronicznej do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW”.
8. Należy okresowo kasować niepotrzebne maile.
9. Użytkownik bez zgody Administratora Danych Osobowych nie może wysyłać wiadomości zwierających dane osobowe za pośrednictwem prywatnej elektronicznej skrzynki pocztowej.

§ 8.

Odpowiedzialność dyscyplinarna

Przypadki świadomego naruszenia regulacji niniejszego Regulaminu ochrony danych osobowych lub nieuzasadnionego zaniechania obowiązków, mogą zostać uznane przez Administratora Danych Osobowych za ciężkie naruszenie obowiązków, na zasadach określonych w odrębnych przepisach.

Warszawa, 1 listopada 2022r.