

System zarządzania informacją przy sąsiedzkich usługach opiekuńczych



Fundusze Europejskie
dla Rozwoju Społecznego

Dofinansowane przez
Unię Europejską



Dokument przygotowany w ramach projektu „Dobre Wsparcie dla NGO” numer projektu FERS.04.12-IP.04-0042/24 (dalej Projekt), współfinansowanego przez Unię Europejską w ramach Programu Fundusze Europejskie dla Rozwoju Społecznego 2021-2027 (FERS 2021-2027).



System zarządzania informacją przy sąsiedzkich usługach opiekuńczych

Wprowadzenie

Celem opracowania jest stworzenie ramowego standardu zarządzania informacją w organizacjach pozarządowych realizujących sąsiedzkie usługi opiekuńcze, w tym realizowanych w ramach projektu „Dobre Wsparcie dla NGO”. System powinien wspierać efektywne gromadzenie, przetwarzanie, przechowywanie i ochronę danych w sposób zgodny z obowiązującym prawem (w tym RODO) oraz z najlepszymi praktykami w zakresie bezpieczeństwa informacji i IT. Polityka zapewnia zgodność z obowiązującymi przepisami prawa, w tym z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO), oraz wdrożenie standardów bezpieczeństwa informacji.

Definicje

Organizacje pozarządowe - niebędące jednostkami sektora finansów publicznych, w rozumieniu przepisów o finansach publicznych, i nie działające w celu osiągnięcia zysku, osoby prawne lub jednostki nieposiadające osobowości prawnej utworzone na podstawie przepisów ustaw, w tym fundacje i stowarzyszenia¹

Dane osobowe – oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

Szczególne kategorie danych osobowych - ujawniają pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, członkostwo w związkach zawodowych i obejmują przetwarzanie danych genetycznych, dane

¹ art. 3 ust. 2 ustawy z dnia 24 kwietnia 2003 r. o działalności pożytku publicznego i o wolontariacie (Dz.U. z 2025 r. poz. 1338 t.j.)

Dokument przygotowany w ramach projektu „Dobre Wsparcie dla NGO” numer projektu FERS.04.12-IP.04-0042/24 (dalej Projekt), współfinansowanego przez Unię Europejską w ramach Programu Fundusze Europejskie dla Rozwoju Społecznego 2021-2027 (FERS 2021-2027).



biometryczne w celu jednoznacznej identyfikacji osoby fizycznej, dane dotyczące zdrowia, dane dotyczące życia seksualnego osoby lub orientację seksualną.

W zależności od obowiązującego prawa, specjalne kategorie danych osobowych mogą również zawierać informacje o środkach zabezpieczenia społecznego lub postępowaniach administracyjnych i karnych oraz o sankcjach.

Przetwarzanie danych – oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

Podopieczny – osoba korzystająca z sąsiedzkich usług opiekuńczych świadczonych przez organizację.

Personel – pracownicy, wolontariusze i współpracownicy organizacji oraz opiekunowie świadczący sąsiedzkie usługi opiekuńcze.

Administrator danych (ADO) - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. W ramach niniejszego dokumentu jest nim Organizacja pozarządowa, która przetwarza dane osobowe w ramach realizowanych usług.

IOD – Inspektor Ochrony Danych lub wyznaczona osoba odpowiedzialna za ochronę danych w Organizacji.



Podstawy prawne:

1. 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. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2019 poz. 1781 ze zm.).
3. Ustawa z dnia 24 kwietnia 2003 r. o działalności pożytku publicznego i o wolontariacie (Dz.U. 2025 poz. 1338).
4. Ustawa z dnia 12 marca 2004 r. o pomocy społecznej (Dz.U. 2025 poz. 1214).
5. Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. 2024 poz. 1513 ze zm.)
6. Obwieszczenie Ministra Pracy, Polityki Społecznej i Rodziny z dnia 24 maja 2024 r. w sprawie ogłoszenia jednolitego tekstu rozporządzenia Ministra Polityki Społecznej w sprawie specjalistycznych usług opiekuńczych
7. Ustawa z dnia 11 września 2019 r. o realizowaniu usług społecznych przez centrum usług społecznych (Dz.U. 2019 poz. 1818)



Opracowanie standardu zarządzania informacją

Opracowanie standardu zarządzania informacją w organizacji wynika ze specyfiki i kontekstu działań organizacji pozarządowych. Organizacje pozarządowe często dysponują ograniczonymi zasobami technicznymi i kadrowymi, jednocześnie gromadząc, przetwarzając, archiwizując dane osobowe, w tym dane wrażliwe.

W przypadku sąsiedzkich usług opiekuńczych opiekun powinien mieć stały dostęp do danych osobowych podopiecznego, szczególnie w zakresie danych dotyczących stanu zdrowia. Dane te mogą być przetwarzane i przekazywane między innymi pracownikom placówek ochrony zdrowia, urzędnikom, pracownikom organizacji pozarządowych.

Standaryzacja procesów informacyjnych obejmuje stosowanie jednolitych formularzy, procedur i systemów elektronicznych przez wszystkie osoby wskazane przez organizację w procesie świadczenia sąsiedzkich usług opiekuńczych.

W procesie zarządzania informacjami obowiązuje **zasada minimalizacji danych**, czyli gromadzenie wyłącznie tych danych, które są niezbędne oraz **segmentacja dostępu**, to jest ograniczenie dostępu do danych tylko do osób uprawnionych. Zgodnie z art. 5 RODO obowiązują również zasady:

1. zgodności z prawem, rzetelności i przejrzystości, - art. 5 ust. 1 pkt a
2. ograniczenia celu – art. 5 ust. 1 pkt b
3. prawidłowości – art. 5 ust. 1 pkt d
4. ograniczenia przechowywania – art. 5 ust. 1 pkt e
5. integralności i poufności – art. 5 ust. 1 pkt f

Wśród najlepszych praktyk zarządzania informacją znajdują się zasady:

- Bezpieczeństwo wielowarstwowe czyli połączenie rozwiązań organizacyjnych (polityki i procedury), technicznych (szyfrowanie, backupy), i proceduralnych (szkolenia personelu)
- Rozwiązania chmurowe – wykorzystanie certyfikowanych dostawców usług IT z odpowiednimi gwarancjami zgodności z RODO.

Przy opracowywaniu standardów przetwarzania informacji bardzo ważne jest ustanowienie kontekstu, co ma na celu określenie ram, w jakich zarządzanie ryzykiem będzie prowadzone. Przede wszystkim należy:

1. Określić rodzaj organizacji i jej otoczenia, w tym zrozumienie, czym zajmuje się organizacja, jakie są jej cele i jakie uwarunkowania prawne (poza RODO), organizacyjne i technologiczne mają wpływ na przetwarzanie danych. W kontekście organizacji



pozarządowych świadczących sąsiedzkie usługi opiekuńcze Administrator Danych Osobowych (ADO) powinien realizować następujące cele:

- a) **Realizacja zadań z zakresu pomocy społecznej i usług opiekuńczych**, w tym:
 - przyjmowanie i weryfikacja wniosków o przyznanie sąsiedzkich usług opiekuńczych,
 - kwalifikowanie osób do objęcia wsparciem,
 - prowadzenie dokumentacji niezbędnej do udzielenia pomocy,
 - monitorowanie jakości i zakresu świadczonych usług.
- b) **Zarządzanie personelem i współpracownikami realizującymi usługi**, obejmujące m.in.:
 - rekrutację, szkolenie i nadzór nad osobami świadczącymi usługi sąsiedzkie (np. wolontariuszami lub osobami zatrudnionymi na umowy cywilnoprawne),
 - przetwarzanie danych kontaktowych i rozliczeniowych,
 - zapewnienie zgodności działań z obowiązującymi procedurami i standardami opieki.
- c) **Zapewnienie bezpieczeństwa osób objętych wsparciem**, w tym:
 - przetwarzanie danych niezbędnych do kontaktu w sytuacjach nagłych (np. kontakt do rodziny, opiekunów medycznych),
 - dokumentowanie incydentów i sytuacji wymagających interwencji służb ratunkowych lub socjalnych,
 - podejmowanie działań mających na celu ochronę życia, zdrowia lub mienia podopiecznych.
- d) **Zapewnienie rozliczalności i transparentności działań ADO**, poprzez:
 - prowadzenie ewidencji świadczeń i czasu pracy usługodawców,
 - sporządzanie sprawozdań na potrzeby organów nadzorczych i jednostek finansujących (np. samorządów, urzędów, grantodawców),
 - realizację obowiązków wynikających z przepisów o rachunkowości, finansach publicznych oraz kontroli wewnętrznej.
- e) **Ewaluacja i rozwój systemu usług sąsiedzkich**, tj.:
 - analizowanie danych w celu oceny skuteczności i efektywności świadczenia usług,
 - planowanie i wdrażanie działań usprawniających,
 - współpraca z partnerami (np. organizacjami pozarządowymi, instytucjami pomocy społecznej) w ramach projektów rozwojowych, przy zachowaniu zasad minimalizacji danych.

- 2. Zidentyfikować czynności przetwarzania danych, w tym sporządzenie Rejestru Czynności Przetwarzania (RCP) zgodnie z art. 30 RODO, który obejmuje opis celów, kategorii danych, odbiorców, planowanych terminów usunięcia i stosowanych zabezpieczeń.



Rejestr Czynności Przetwarzania stanowi załącznik nr 3 do Systemu zarządzania informacją

3. Zidentyfikować aktywa, czyli określić zasoby - osoby, sprzęt, oprogramowanie, dokumenty, które są zaangażowane w przetwarzanie danych i które mogą być narażone na zagrożenia.
4. Ustalić kryteriów akceptacji ryzyka: Zdefiniowanie, jaki poziom ryzyka jest uznawany za akceptowalny (niski, średni, wysoki) dla organizacji, po wdrożeniu zabezpieczeń.

Ustalając standardy należy oszacować ryzyko składające się z trzech podetapów -identyfikacji, analizy i oceny.

1. Identyfikacja obejmuje identyfikację ryzyka i podatności:
 - a) Identyfikacja ryzyka - identyfikacja zagrożeń - Określenie, co może spowodować naruszenie ochrony danych (np. awaria sprzętu, atak hakerów, błąd ludzki, klęski żywiołowe).
 - b) Identyfikacja podatności (słabości) - ustalenie słabych punktów w systemach, procedurach lub u pracowników, które mogą zostać wykorzystane przez zagrożenia (np. brak aktualizacji oprogramowania, słabe hasła, brak szkoleń).
2. Analiza ryzyka obejmuje analizę incydentów i skutków:
 - a) Analiza incydentów - określenie prawdopodobieństwa wystąpienia danego zdarzenia (naruszenia) w wyniku połączenia zagrożenia i podatności.
 - b) Analiza skutków - ocena potencjalnego wpływu naruszenia na prawa i wolności osób fizycznych (np. dyskryminacja, szkody majątkowe lub niemajątkowe, utrata kontroli nad danymi).
3. Ocena Ryzyka czyli określenie poziomu ryzyka w oparciu o ustalone kryteria (np. matryca ryzyka) i wynik analizy (prawdopodobieństwo x skutek) ustala się poziom ryzyka (np. Niski, Średni, Wysoki).

Działania określone jako ryzyka, które zostały uznane za nieakceptowalne (zazwyczaj wysokie), wymagają podjęcia natychmiastowych działań.

Po oszacowaniu ryzyka należy podjąć decyzje o sposobie reakcji na zidentyfikowane ryzyka. Dostępne są cztery podstawowe opcje:

1. Redukcja (ograniczenie) ryzyka. Polega na wdrożeniu dodatkowych środków bezpieczeństwa (technicznych i organizacyjnych), które mają obniżyć



prawdopodobieństwo lub skutki naruszenia (np. szyfrowanie, pseudonimizacja, dodatkowe szkolenia, kontrola dostępu). Jeśli ryzyko jest wysokie, należy wdrożyć środki, które je skutecznie zmniejszą. Jeśli ryzyko pozostaje wysokie pomimo podjętych działań, administrator ma obowiązek przeprowadzić Ocenę Skutków dla Ochrony Danych (DPIA) (art. 35 RODO) i ewentualnie skonsultować się z Urzędem Ochrony Danych Osobowych (UODO).

2. Akceptacja ryzyka. Jest to świadoma decyzja o tolerowaniu ryzyka, które jest na poziomie akceptowalnym dla organizacji.
3. Unikanie ryzyka to zakończenie operacji przetwarzania danych, która jest głównym źródłem wysokiego ryzyka.
4. Przeniesienie ryzyka, np. poprzez ubezpieczenie się od konsekwencji naruszenia.

Zarządzanie ryzykiem przy czynnościach dotyczących danych osobowych to proces ciągły. Stąd też niezbędne jest monitorowanie i kontrolowanie zabezpieczeń oraz analiza występujących ryzyk poprzez:

1. Wdrożenie środków zaradczych - wprowadzenie w życie zaplanowanych zabezpieczeń (środków technicznych i organizacyjnych).
2. Ciągłe monitorowanie czyli regularne sprawdzanie i ocena skuteczności wdrożonych zabezpieczeń (np. poprzez audyty, testy, przeglądy).
3. Systematyczny przegląd i aktualizacja całej analizy ryzyka (np. raz w roku). Dodatkowo działania takie powinny być przeprowadzane każdorazowo w przypadku istotnych zmian w procesach przetwarzania, technologii lub otoczeniu prawnym.
4. Utrzymywanie aktualnej i kompletnej dokumentacji z całego procesu zarządzania ryzykiem, w tym rejestru zidentyfikowanych ryzyk i podjętych działań.

Gromadzenie danych

1. Dane osobowe podopiecznych, rodzin i wolontariuszy zbierane są poprzez formularze papierowe i/lub elektroniczne.



2. Każdy formularz zawiera klauzulę informacyjną RODO zawierającą kluczowe informacje dotyczące przetwarzania danych osobowych. Zgodnie z art. 13 RODO administrator podczas pozyskiwania danych osobowych podaje jej wszystkie następujące informacje:²
- a) swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela;
 - b) gdy ma to zastosowanie – dane kontaktowe inspektora ochrony danych;
 - c) cele przetwarzania danych osobowych, oraz podstawę prawną przetwarzania;
 - d) prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią;
 - e) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
 - f) gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz informacje o sposobach uzyskania kopii zabezpieczeń lub o miejscu ich udostępnienia.
 - g) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
 - h) informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
 - i) informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem (jeżeli dotyczy);
 - j) informacje o prawie wniesienia skargi do organu nadzorczego;

² Rozporządzenie 2016/679 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), art. 13 pkt. 1 i 2

Dokument przygotowany w ramach projektu „Dobre Wsparcie dla NGO” numer projektu FERS.04.12-IP.04-0042/24 (dalej Projekt), współfinansowanego przez Unię Europejską w ramach Programu Fundusze Europejskie dla Rozwoju Społecznego 2021-2027 (FERS 2021-2027).



- k) informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
- l) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Przykładowa klauzula RODO została ujęta w załączniku 1 do Systemu zarządzania informacjami.

- 3. W przypadku pozyskania danych osobowych od innej osoby, niż ta, której dane dotyczą, Administrator Danych Osobowych podaje osobie, której dane dotyczą oprócz informacji podanych powyżej, źródło pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych;³
- 4. Zbierane są tylko dane niezbędne do realizacji usług (np. imię, nazwisko, adres, dane kontaktowe, informacje o potrzebach opiekuńczych). W przypadku podopiecznych, opiekun ma dostęp do danych wrażliwych, np. orzeczenie o niepełnosprawności, stan zdrowia podopiecznego. Dane te mogą być przetwarzane jedynie w sytuacji kontaktu z pracownikami placówek ochrony zdrowia, tylko i wyłącznie za wiedzą i zgodą podopiecznego jedynie w zakresie wskazanym w art. 9 RODO.

Przetwarzanie danych

- 1. Dane przetwarzane wyłącznie w zakresie realizacji usług opiekuńczych zgodnie z zapisami art. 9 RODO.
- 2. Dane osobowe mogą być przetwarzane jeżeli spełniony jest jeden z poniższych warunków:⁴
 - a) osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach
 - b) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej

³ Rozporządzenie 2016/679 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), art. 14

⁴ Rozporządzenie 2016/679 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), art. 9 pkt 2, ppkt a, b, c, h

Dokument przygotowany w ramach projektu „Dobre Wsparcie dla NGO” numer projektu FERS.04.12-IP.04-0042/24 (dalej Projekt), współfinansowanego przez Unię Europejską w ramach Programu Fundusze Europejskie dla Rozwoju Społecznego 2021-2027 (FERS 2021-2027).



- c) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;
 - d) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego
- 3. W przypadku opiekunów świadczących sąsiedzkie usługi opiekuńcze dane są przetwarzane wyłącznie w celach przygotowania umów zlecenia na realizację świadczeń oraz realizacji rozliczeń tychże świadczeń
 - 4. W przypadku podopiecznych korzystających z usług opiekuńczych, dane są przetwarzane przez ośrodki pomocy społecznej w celu ustalenia sytuacji życiowej i zdrowotnej oraz ustalenia konieczności świadczenia sąsiedzkich usług opiekuńczych.
 - 5. Do danych osobowych podopiecznego ma dostęp opiekun świadczący sąsiedzkie usługi opiekuńcze. Dane te może przetwarzać i udostępniać wyłącznie za wiedzą i zgodą podopiecznego i wyłącznie w sytuacjach związanych z zakresem świadczonych usług ustalonych na podstawie decyzji administracyjnej Ośrodka Pomocy Społecznej.
 - 6. W przypadku korzystania z narzędzi technologicznych, np. aplikacji do zarządzania sąsiedzkimi usługami opiekuńczymi, zabezpieczanie danych osobowych obejmuje techniczne i organizacyjne środki, takie jak szyfrowanie danych w spoczynku i w transmisji, stosowanie silnych metod uwierzytelniania (np. hasła, biometria, OTP), minimalizacja zbieranych danych zgodnie z RODO, regularne aktualizacje aplikacji i systemów oraz stosowanie zabezpieczeń sieciowych jak VPN. Jednocześnie aplikacja rejestruje logi dostępu i zmian.
 - 7. W przypadku współpracy z podmiotami zewnętrznymi, którym przekazywane są dane osobowe, konieczne jest zawarcie umów powierzenia przetwarzania danych.

Przechowywanie danych

- 1. Dane osobowe należy przechowywać w sposób zgodny z zasadą ograniczenia przechowywania (retencja danych), czyli nie dłużej niż jest to niezbędne do realizacji celu, dla którego zostały zebrane, oraz w formie umożliwiającej identyfikację osoby, której dotyczą.
- 2. Dane osobowe przechowywane w systemie elektronicznym, z kopią zapasową szyfrowaną i przechowywaną w bezpiecznym miejscu.
- 3. Dokumentacja w formie papierowej powinna być przechowywana w zamykanych szafach, z kontrolą dostępu.
- 4. Dane osobowe przechowywane powinny być tylko przez okres niezbędny do realizacji usług i zgodny z polityką retencji.

Dokument przygotowany w ramach projektu „Dobre Wsparcie dla NGO” numer projektu FERS.04.12-IP.04-0042/24 (dalej Projekt), współfinansowanego przez Unię Europejską w ramach Programu Fundusze Europejskie dla Rozwoju Społecznego 2021-2027 (FERS 2021-2027).



Ochrona danych

1. Ochrona danych osobowych ma na celu zapewnienie prywatności osób fizycznych poprzez ochronę ich danych przed nieuprawnionym użyciem zgodnie z aktualnymi przepisami, w tym Rozporządzeniem 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) (RODO) oraz Ustawą z 10 maja 2018 r. o ochronie danych osobowych i Ustawą z 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 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. W obrębie ochrony danych osobowych stosuje się zasad bezpieczeństwa RODO (integralność, poufność, dostępność).
3. Organizacja powołuje Administratora Danych Osobowych, który monitoruje, kontroluje i analizuje ryzyka w obrębie danych osobowych
4. Organizacja stosuje zabezpieczenia techniczne: szyfrowanie, uwierzytelnianie wieloskładnikowe, aktualizacje systemów, firewall, programy antywirusowe
5. Organizacja prowadzi szkolenia personelu w zakresie ochrony danych i bezpieczeństwa IT.
6. W przypadku naruszenia bezpieczeństwa danych obowiązuje procedura reagowania i zgłaszania incydentu do AOD oraz – jeśli wymagane – do Prezesa UODO w ciągu 72 godzin.
7. Dane są usuwane w sposób bezpieczny: niszczenie dokumentów papierowych, nadpisywanie i kasowanie danych cyfrowych
8. Organizacja ustala procedury reagowania na incydenty naruszenia bezpieczeństwa danych (np. wyciek, zgubienie dokumentacji). Wzór procedury reagowania i zgłaszania incydentu stanowi załącznik nr 2 do Standardu zarządzania informacjami

Technologie wspierające

W obrębie ochrony danych osobowych organizacja może korzystać z rozwiązań technologicznych w tym z:

1. rozwiązań chmurowych zgodnych z RODO i posiadających certyfikaty bezpieczeństwa (ISO/IEC 27001),
2. aplikacji mobilnych do raportowania i planowania pracy,

Dokument przygotowany w ramach projektu „Dobre Wsparcie dla NGO” numer projektu FERS.04.12-IP.04-0042/24 (dalej Projekt), współfinansowanego przez Unię Europejską w ramach Programu Fundusze Europejskie dla Rozwoju Społecznego 2021-2027 (FERS 2021-2027).



3. systemów CRM/ERP dedykowanych NGO,
4. komunikatorów do wymiany informacji w zespole.

Rekomendacje organizacyjne, techniczne i proceduralne

Aby zapewnić ochronę danych osobowych rekomenduje się:

1. Wyznaczenie Inspektora Ochrony Danych (IOD) lub osoby odpowiedzialnej w organizacji za dane osobowe.
2. Opracowanie i wdrożenie polityki ochrony danych.
3. Prowadzenie regularnych audytów wewnętrznych.
4. Szyfrowanie danych w spoczynku i w transmisji.
5. Tworzenie kopii zapasowych wykonywanych, co najmniej raz dziennie i testowane.
6. Wdrożenie uwierzytelniania wieloskładnikowego.
7. Opracowanie procedury zgłaszania i obsługi incydentów bezpieczeństwa
8. Opracowanie procedury nadawania i odbierania uprawnień dostępowych.
9. Opracowanie procedury retencji i bezpiecznego usuwania danych (shredder, demagnetyzacja, kasowanie).

Postanowienia końcowe

1. Za wdrożenie i nadzorowanie zasad systemu zarządzania informacją odpowiada zarząd organizacji oraz ADO
2. AOD lub osoba wyznaczona prowadzi rejestr czynności przetwarzania danych.
3. Każdy pracownik i wolontariusz jest zobowiązany do przestrzegania zasad systemu zarządzania informacją
4. Organizacja przeprowadza coroczne audyty bezpieczeństwa danych.
5. Zasady systemu zarządzania informacją wchodzi w życie z dniem zatwierdzenia przez zarząd Organizacji.
6. Naruszenie zasad systemu zarządzania informacją może skutkować odpowiedzialnością dyscyplinarną lub cywilnoprawną.

Podsumowując, kluczowe dla zgodności z RODO jest wykazanie, że administrator w sposób świadomy i metodyczny podchodzi do oceny i minimalizacji ryzyka naruszenia praw i wolności osób, których dane dotyczą.



Załącznik 1 do System zarządzania informacją przy sąsiedzkich usługach opiekuńczych

KLAUZULA INFORMACYJNA RODO

1. Administrator danych osobowych

Administratorem Pani/Pana danych osobowych jest:

[pełna nazwa jednostki organizującej usługi, np. Gmina X / Centrum Usług Społecznych w X / Ośrodek Pomocy Społecznej w X],

.....
z siedzibą przy [adres siedziby],.....
reprezentowana przez.....

Kontakt z administratorem:

e-mail: [adres e-mail jednostki]

tel.: [numer telefonu]

adres korespondencyjny: [adres urzędu / instytucji]

2. Inspektor ochrony danych

Administrator wyznaczył Inspektora Ochrony Danych (IOD).

Z Inspektorem można kontaktować się w sprawach związanych z przetwarzaniem danych osobowych:

e-mail: [adres e-mail IOD]

adres: [adres korespondencyjny IOD, jeśli inny niż administratora]

3. Cel i podstawa prawna przetwarzania danych

Pani/Pana dane osobowe przetwarzane są w celu:

Dokument przygotowany w ramach projektu „Dobre Wsparcie dla NGO” numer projektu FERS.04.12-IP.04-0042/24 (dalej Projekt), współfinansowanego przez Unię Europejską w ramach Programu Fundusze Europejskie dla Rozwoju Społecznego 2021-2027 (FERS 2021-2027).



- a) rozpatrzenia wniosku o przyznanie sąsiedzkich usług opiekuńczych,
- b) organizacji, realizacji i monitorowania usług sąsiedzkich,
- c) prowadzenia dokumentacji świadczenia usług oraz rozliczeń finansowych,
- d) zapewnienia bezpieczeństwa i jakości świadczenia usług.

Podstawą prawną przetwarzania danych jest:

- a) art. 6 ust. 1 lit. c RODO – obowiązek prawny ciążyący na administratorze wynikający z:
 - o ustawy z dnia 12 marca 2004 r. o pomocy społecznej,
 - o rozporządzenia Ministra Rodziny i Polityki Społecznej z dnia 25 sierpnia 2021 r. w sprawie usług sąsiedzkich,
 - o ustawy z dnia 24 kwietnia 2003 r. o działalności pożytku publicznego i o wolontariacie,
- b) art. 6 ust. 1 lit. e RODO – przetwarzanie niezbędne do wykonania zadania realizowanego w interesie publicznym,
- c) w przypadku danych szczególnych kategorii (np. dotyczących zdrowia) – art. 9 ust. 2 lit. b i h RODO, tj. przetwarzanie niezbędne do świadczenia usług opiekuńczych w zakresie zabezpieczenia społecznego i ochrony zdrowia.

4. Zakres przetwarzanych danych osobowych

Administrator może przetwarzać następujące kategorie danych:

- 1) dane identyfikacyjne (imię, nazwisko, PESEL, adres zamieszkania),
- 2) dane kontaktowe (numer telefonu, adres e-mail),
- 3) informacje o sytuacji rodzinnej, mieszkaniowej i materialnej,
- 4) dane dotyczące stanu zdrowia (jeśli są niezbędne do właściwego świadczenia usług opiekuńczych),
- 5) dane dotyczące realizacji usług (np. godziny wsparcia, rodzaj czynności, opinie o jakości usług).

5. Odbiorcy danych osobowych

Dane mogą być przekazywane wyłącznie:

- upoważnionym pracownikom administratora i osobom realizującym usługi sąsiedzkie,
- organom i instytucjom publicznym uprawnionym na podstawie przepisów prawa (np. MRiPS, OPS, CUS, instytucjom kontrolującym),
- podmiotom przetwarzającym dane w imieniu administratora (np. dostawcom systemów informatycznych, biuram rachunkowym) – wyłącznie na podstawie umowy powierzenia i w zakresie niezbędnym do realizacji celu.

Dane nie będą przekazywane poza Europejski Obszar Gospodarczy (EOG) ani organizacjom międzynarodowym.

6. Okres przechowywania danych

Pani/Pana dane osobowe będą przechowywane:

- przez okres świadczenia usług sąsiedzkich oraz
- przez 5 lat od zakończenia realizacji usług, lub przez dłuższy czas, jeżeli przepisy prawa wymagają zachowania dokumentacji administracyjnej przez inny okres.



7. Prawa osoby, której dane dotyczą

Przysługuje Pani/Panu prawo do:

- dostępu do swoich danych oraz uzyskania ich kopii,
- sprostowania danych (poprawienia nieprawidłowych lub uzupełnienia niekompletnych danych),
- ograniczenia przetwarzania danych,
- wniesienia sprzeciwu wobec przetwarzania danych,
- wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych,
ul. Stawki 2, 00-193 Warszawa.

Jeśli przetwarzanie odbywa się na podstawie zgody (np. zgoda na wykorzystanie wizerunku, udział w materiałach promocyjnych) – ma Pani/Pan prawo do cofnięcia tej zgody w dowolnym momencie, bez wpływu na zgodność z prawem przetwarzania dokonanego przed jej cofnięciem.

8. Obowiązek podania danych

Podanie danych osobowych jest obowiązkowe, jeśli wynika z przepisów prawa i jest niezbędne do przyznania i realizacji usług sąsiedzkich.

Brak podania wymaganych danych może uniemożliwić przyznanie lub świadczenie usług.

9. Zautomatyzowane podejmowanie decyzji

Pani/Pana dane osobowe nie będą przetwarzane w sposób zautomatyzowany, w tym nie będą podlegały profilowaniu.

(miejscowość i data)

(czytelny podpis osoby wymagającej wsparcia)



Załącznik 2 do System zarządzania informacją przy sąsiedzkich usługach opiekuńczych

INSTRUKCJA REAGOWANIA I ZGŁASZANIA INCYDENTU OCHRONY DANYCH OSOBOWYCH DO ADMINISTRATORA DANYCH OSOBOWYCH

Cel wydania instrukcji i jej zakres przedmiotowy

1. Instrukcja określa zasady postępowania wszystkich osób upoważnionych do przetwarzania danych osobowych zatrudnionych przy przetwarzaniu danych osobowych przez Administratora Danych Osobowych, dalej „ADO”, w przypadku naruszenia ich bezpieczeństwa.
2. Naruszeniem zabezpieczenia danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych osobowych, udostępnienia lub umożliwienia dostępu do nich osobom

nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia lub usunięcia, a w szczególności:

- 1) nieautoryzowany dostęp do danych;
- 2) nieautoryzowane modyfikacje lub zniszczenie danych;
- 3) udostępnienie danych nieautoryzowanym podmiotom;
- 4) nielegalne ujawnienie danych.

3. Wobec osoby, która w przypadku naruszenia danych osobowych nie podjęła

Dokument przygotowany w ramach projektu „Dobre Wsparcie dla NGO” numer projektu FERS.04.12-IP.04-0042/24 (dalej Projekt), współfinansowanego przez Unię Europejską w ramach Programu Fundusze Europejskie dla Rozwoju Społecznego 2021-2027 (FERS 2021-2027).



działania określonego w niniejszej instrukcji, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami wszczyna się postępowanie dyscyplinarne lub porządkowe. Kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia o naruszeniu danych osobowych nie wyklucza odpowiedzialności karnej tej osoby zgodnie z aktualnie obowiązującym przepisami oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

Rodzaje incydentów świadczących o możliwości naruszenia bezpieczeństwa danych

1. Naruszenie ochrony danych osobowych” oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
2. Wyróżnia się następujące rodzaje naruszeń:
 - 1) „naruszenie poufności”, które polega na ujawnieniu lub udostępnieniu danych osobie nieuprawnionej;
 - 2) „naruszenie integralności”, które sprowadza się do zmiany treści danych osobowych, czyli ich modyfikowania, w sposób nieautoryzowany;
 - 3) „naruszenie dostępności”, które wiąże się z trwałą utratą dostępu do danych lub ich zniszczeniem.
3. O możliwości wystąpienia naruszenia bezpieczeństwa danych osobowych mogą świadczyć:
 - 1) nadmierne w stosunku do wykonywanych zadań (zakresu upoważnienia), uprawnienia użytkownika do zasobów danych;
 - 2) niestabilna praca systemu teleinformatycznego;
 - 3) korzystanie z zasobów danych poza miejscem przetwarzania/godzinami pracy (bez zgody przełożonego);
 - 4) nowe „podejrzane” (nieznane) konta użytkowników w systemie;
 - 5) wysoka aktywność kont, które długo pozostawały niewykorzystane;



- 6) zanotowanie w krótkim czasie dużej liczby nieudanych prób logowania;
- 7) anomalie w pracy systemu lub programu (świadczące np. o obecności wirusa komputerowego);
- 8) naruszenie lub wadliwe funkcjonowanie zabezpieczeń fizycznych w pomieszczeniach, w
których następuje przetwarzanie danych osobowych (uszkodzone zamki, okna, drzwi, itp.).

Postępowanie w przypadku podejrzenia naruszenia bezpieczeństwa danych

1. Każda osoba upoważniona, która stwierdzi lub podejrzewa fakt naruszenia danych osobowych, jest zobowiązana niezwłocznie zgłosić to swojemu bezpośredniemu przełożonemu, który zgłasza ten fakt Inspektorowi Ochrony Danych, zwanemu dalej „IOD”.
2. Każda osoba upoważniona, która stwierdzi fakt naruszenia danych osobowych ma obowiązek podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony oraz zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia.
3. ADO lub upoważniona przez niego osoba dokonuje wstępnej identyfikacji zaistniałego zdarzenia i na podstawie dostępnych informacji oraz analizy okoliczności kwalifikuje zdarzenie (lub serię zdarzeń) jako:
 - 1) zdarzenie niemające cech naruszenia bezpieczeństwa, np. zaplanowana przerwa techniczna;
 - 2) błąd w działaniu elementu systemu teleinformatycznego, infrastruktury teleinformatycznej lub infrastruktury biurowej;
 - 3) awaria techniczna czasowo blokująca dostępność informacji;
 - 4) zdarzenie niskiej kategorii – związane z naruszeniem bezpieczeństwa ochrony danych, a
szczególnie jej integralności i poufności, nie generujące kar finansowych, jednak powodujący pośrednio lub bezpośrednio utrudnienia w realizacji jakiegokolwiek procesu przetwarzania;



- 5) zdarzenie średniej kategorii – związane z naruszeniem bezpieczeństwa ochrony danych skutkujące pośrednio lub bezpośrednio zatrzymaniem realizacji jakiegokolwiek procesu
ustawowego i/lub stratami finansowymi oraz możliwością konsekwencji prawnych i/lub utraty wizerunku;
 - 6) zdarzenie wysokiej kategorii – związane z naruszeniem bezpieczeństwa ochrony danych, którego skutkiem jest destrukcja (zniszczenie, utrata) kluczowych zasobów i przerwanie funkcjonowania procesów funkcjonowania organizacji
4. **Przy analizie naruszeń, należy wziąć pod uwagę:**
- 1) charakter zdarzenia i jego znaczenie związane z naruszeniem bezpieczeństwa ochrony danych osobowych;
 - 2) miejsce wystąpienia zdarzenia - identyfikacja punktu, w którym nastąpiło zdarzenie (lokalizacja pomieszczenia, serwer, stacja robocza itp.);
 - 3) zakres zasobów dotkniętych naruszeniem;
 - 4) identyfikację zasobów potrzebnych przy dalszych działaniach w ramach postępowania ze zdarzeniem związanym z naruszeniem bezpieczeństwa ochrony danych;
 - 5) możliwości rozszerzania się naruszenia i sposoby jego ograniczania;
 - 6) rodzaj ujawnionej informacji (jeśli ma zastosowanie - np. dane osobowe);
 - 7) szacunkowy czas, po którym skutki naruszenia zostaną zlikwidowane, jeżeli nie ma możliwości natychmiastowego usunięcia stanu naruszenia bezpieczeństwa ochrony danych;
 - 8) skutki organizacyjne i prawne (wstępny szacunek).
5. **W przypadku, gdy zasięg i szacunkowy czas trwania powoduje zakwalifikowanie naruszenia do wysokiej kategorii, ADO powiadamia niezwłocznie Prezesa Urzędu Ochrony Danych Osobowych (PUODO), a następnie przeprowadza dochodzenie wyjaśniające.**
6. **W przypadku, gdy rodzaj i zasięg incydentu, zidentyfikowany na którymkolwiek z etapów postępowania, uzasadnia potrzebę powiadomienia organów ścigania, to decyzję o sposobie i terminie powiadomienia**



podejmuje ADO.

7. ADO podejmuje następujące kroki:

- 1) zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości i ciągłości pracy;
 - 2) odbiera dokładną relację z zaistniałego naruszenia bezpieczeństwa danych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje w związku z zaistniałym naruszeniem;
 - 3) nawiązuje kontakt ze specjalistami zewnętrznymi (jeśli zachodzi taka potrzeba).
8. ADO 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)

Ograniczanie skutków naruszeń

1. Dokumentacja naruszenia podlega rygorom ochrony przez tworzenie autoryzowanych kopii tych elementów, które mają zastosowanie przy postępowaniu z naruszeniem, w tym: rejestry



urządzeń, systemów operacyjnych i aplikacji, kopie zapasowe, pliki konfiguracyjne i systemowe, bezpieczne przechowywanie tych kopii, przyjęcia dokumentacji oraz jej wszystkich części.

2. ADO przeprowadza bieżące działania zmierzające do ograniczenia skutków naruszenia i zidentyfikowania jego źródła. W tym celu może spowodować zablokowanie części systemu lub dostępnych usług.

Odtwarzanie systemu

1. Osoba upoważniona przez ADO przystępuje do odtworzenia systemu po zidentyfikowaniu i usunięciu lub zablokowaniu źródła naruszenia.
2. Odtwarzanie systemu odnosi się do punktu odtworzenia, co do którego ASI ma uzasadnioną pewność, że nie zawiera źródła naruszenia.
3. Zasoby w postaci oprogramowania oraz danych są odtwarzane z oryginalnych źródeł dystrybucji oprogramowania oraz kopii zapasowych.
4. ADO może podjąć decyzję o podjęciu przetwarzania danych mimo braku pewności usunięcia źródła naruszenia, jeśli szacowane negatywne skutki braku przetwarzania przewyższają potencjalne ryzyko podjęcia działania.

Zgłaszanie naruszenia ochrony danych do UODO

1. W przypadku naruszenia ochrony danych osobowych, ADO bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je Urzędowi Ochrony Danych Osobowych, chyba że jest mało prawdopodobne, by naruszenie to **skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.**

2. Zgłoszenie musi co najmniej:

- 1) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których



- dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
- 2) zawierać imię i nazwisko oraz zawierać imię i nazwisko oraz dane kontaktowe ADO lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
 - 3) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
 - 4) opisywać środki zastosowane lub proponowane przez ADO w celu zapobiegania naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach - środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
3. Jeżeli informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.
4. ADO dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego artykułu.
5. Zgłoszenia można dokonać za pomocą formularza dostępnego na stronie www.uodo.gov.pl na cztery sposoby:
- 1) elektronicznie poprzez wypełnienie dedykowanego formularza dostępnego bezpośrednio na platformie www.biznes.gov.pl;
 - 2) elektronicznie poprzez wysłanie wypełnionego formularza na elektroniczną skrzynkę podawczą ePUAP: UODO/SkrytkaESP
 - 3) elektronicznie poprzez wysłanie wypełnionego formularza za pomocą pisma ogólnego dostępnego na platformie www.biznes.gov.pl;
 - 4) tradycyjną pocztą, wysyłając wypełniony formularz na adres Urzędu.

Zawiadamianie osób o naruszeniu ochrony ich danych osobowych

1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, ADO bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

Dokument przygotowany w ramach projektu „Dobre Wsparcie dla NGO” numer projektu FERS.04.12-IP.04-0042/24 (dalej Projekt), współfinansowanego przez Unię Europejską w ramach Programu Fundusze Europejskie dla Rozwoju Społecznego 2021-2027 (FERS 2021-2027).



2. Zawiadomienie jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w art. 33 ust. 3 lit. b), c) i d) RODO.
3. Nie dokonuje się zawiadomienia osób w następujących przypadkach, gdy:
 - 1) ADO wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
 - 2) ADO zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą
 - 3) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.



Formularz zgłoszenia incydentu naruszenia bezpieczeństwa danych przez pracownika

Dane zgłaszającego:

Imię i nazwisko	
Stanowisko	
Jednostka organizacyjna/dydaktyczna/ samodzielne stanowisko	
Telefon kontaktowy	
E-mail	

Wskazanie, w którym miejscu wystąpiło naruszenie:

Sieci	
System teleinformatyczny	



Dokumentacja papierowa, zbór
danych

Data i godzina stwierdzenia naruszenia:

Charakterystyka naruszenia:

Opisać szczegółowo na czym polegało naruszenie ochrony danych osobowych, w tym:
- opis zdarzenia ze wskazaniem np. faktu zniszczenia, utraty, nieuprawnionej modyfikacji danych, ujawnienia danych, nieuprawnionego dostępu do danych wraz z okolicznościami tego zdarzenia:

.....
.....
.....

Na czym polegało naruszenie?

Zgubienie, kradzież nośnika/urządzenia
Dokumentacja papierowa (zawierająca dane osobowe) zgubiona, skradziona lub pozostawiona w niezabezpieczonej lokalizacji
Korespondencja papierowa utracona przez operatora pocztowego lub otwarta przed

zwróceniem jej do nadawcy
Nieuprawnione uzyskanie dostępu do informacji/systemu
Nieuprawnione uzyskanie dostępu do informacji poprzez złamanie zabezpieczeń
Złośliwe oprogramowanie ingerujące w poufność, integralność i dostępność danych
Uzyskanie poufnych informacji przez pozornie zaufaną osobę w oficjalnej komunikacji elektronicznej, takiej jak e-mail czy komunikator internetowy
Nieprawidłowe usunięcie/zniszczenie danych osobowych z nośnika/urządzenia elektronicznego przed jego zbyciem przez administratora
Niezamierzona publikacja
Dane osobowe wysłane do niewłaściwego odbiorcy
Ujawnienie danych niewłaściwej osobie
Ustne ujawnienie danych osobowych
Inne

.....
.....
.....



Przyczyna naruszenia:

Wewnętrzne działanie niezamierzone
Wewnętrzne działanie zamierzone
Zewnętrzne działanie niezamierzone
Zewnętrzne działanie zamierzone

Opisać możliwe konsekwencje naruszenia ochrony danych osobowych:

Naruszenie ma wpływ na:
poufność (nieuprawnione lub przypadkowe ujawnienie bądź udostępnienie danych)
integralność (wprowadzenie nieuprawnionych zmian podczas odczytu, zapisu, transmisji lub przechowywania)
dostępność (brak możliwości wykorzystania danych na żądanie, w założonym czasie, przez do tego uprawnioną

Kategorie danych osobowych, których dotyczy naruszenie:

nazwiska i imiona
nazwa użytkownika i/lub hasło
imiona rodziców
dane dot. zarobków
data urodzenia
nazwisko rodowe matki
nr rachunku bankowego
seria i numer dowodu osobistego
adres zamieszkania lub pobytu
numer telefonu
numer ewidencyjny PESEL
wizerunek
adres e-mail
inne.....

przybliżona liczba osób, których mogło dotyczyć
naruszenie.....
przybliżona liczba wpisów danych osobowych, których dotyczy
naruszenie.....



Dane szczególnej kategorii przetwarzania:

dane o pochodzeniu rasowym lub etnicznym
dane o poglądach politycznych
dane o przekonaniach religijnych lub światopoglądowych
dane o przynależności do związków zawodowych
dane dotyczące seksualności lub orientacji seksualnej
dane dotyczące zdrowia
dane genetyczne
dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej

Możliwe konsekwencje (opisać konsekwencje dla osoby, której dane dotyczą):

utrata kontroli nad własnymi danymi osobowymi
ograniczenie możliwości realizowania praw z art. 15-22 RODO
ograniczenie możliwości realizowania praw
dyskryminacja
kradzież lub sfalszowanie tożsamości
strata finansowa
naruszenie dobrego imienia
utrata poufności danych osobowych chronionych tajemnicą zawodową
inne:

.....

Czy naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych:

NIE

TAK

.....

podpis osoby zgłaszającej

Zarejestrowano w rejestrze naruszeń ochrony danych osobowych w dniu

.....

godz. poz. rejestru

Rejestr czynności przetwarzania

Nazwa i dane kontaktowe administratora	
Nazwa	Centrum Szkoleniowe Gielar Sp. z o.o.
Adres	ul. Jagiellońska 82/1, 70-362 Szczecin
Email	biuro@gielar.pl
Telefon	884858285

Inspektor Ochrony Danych (jeśli powołano)	
Nazwa	Damian Otolski
Adres	ul. Jagiellońska 82/1, 70-362 Szczecin
Email	ido@gielar.pl
Telefon	884858285

Przedstawiciel (jeśli wyznaczono)	
Nazwa	
Adres	
Email	
Telefon	

*Kolorem czerwonym oznaczono informacje wymagane w rejestrze przez art. 30 ust. 1 RODO

	1	2	3	4	5	6	7
LP.	Nazwa czynności przetwarzania	Jednostka organizacyjna (departament, dział itp.)	Cel przetwarzania	Kategorie osób	Kategorie danych	Podstawa prawna	Źródło danych
			Art.. 30 ust. 1 pkt b	Art.. 30 ust. 1 pkt c	Art.. 30 ust. 1 pkt c		
1.	Rekrutacja podopiecznych	Koordinator sąsiedzkich usług opiekuńczych	Rekrutacja uczestników	Kandydacji do uczestniczenia w projekcie	Dane identyfikacyjne, dane adresowe, dane o wykształceniu, dane wrażliwe	RODO art.. 30, 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, Dz.Urz.UE.L Nr 119	Formularz rekrutacyjny
2.	Rekrutacja i proces zatrudnienia opiekunów	Koordinator sąsiedzkich usług opiekuńczych	Rekrutacja opiekunów, przygotowywanie umów cywilno-prawnych i umów o pracę	Kandydaci do pracy	Dane identyfikacyjne, dane adresowe, dane o wykształceniu	RODO art.. 30, 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, Dz.Urz.UE.L Nr 119	Formularz rekrutacyjny
3.	Umowy z dostawcami usług będącymi przedsiębiorcami prowadzącymi jednoosobowe działalności gospodarcze lub wspólnikami spółek handlowych oraz osoby przez nich wspakane	Koordinator sąsiedzkich usług opiekuńczych	Przygotowywanie umów na realizację usług	Wykonawcy usług, przedsiębiorcy przystępujący do postępowania w drodze zamówień publicznych	Dane identyfikacyjne, dane adresowe, dane o wykształceniu	RODO art.. 30, 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, Dz.Urz.UE.L Nr 119	Formularz zgłoszeniowy

8	9	10	11	12	13
Planowany termin usunięcia kategorii danych <i>(jeżeli jest to możliwe)</i>	Nazwa współadministratora i dane kontaktowe <i>(jeżeli dotyczy)</i>	Nazwa podmiotu przetwarzającego i dane kontaktowe <i>(jeżeli dotyczy)</i>	Kategorie odbiorców <i>(innych niż podmiot przetwarzający)</i>	Nazwa systemu lub oprogramowania	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa zgodnie z art. 32 ust. 1 <i>(jeżeli jest to możliwe)</i>
Art.. 30 ust. 1 pkt f	Art.. 30 ust. 1 pkt a	Art.. 30 ust. 1 pkt d	Art.. 30 ust. 1 pkt d		Art.. 30 ust. 1 pkt g

14	15	16
DPIA (jeśli tak, lokalizacja raportu)	Transfer do kraju trzeciego lub org. międzynarodowej	
	Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu)	Jeśli transfer i art. 49 ust. 1 akapit drugi - dokumentacja odpowiednich zabezpieczeń
	Art. 30 ust. 1 pkt e	Art. 30 ust. 1 pkt e