WÓJT GMINY ZAWIDZ

pow. Sierpc woj. mazowieckie

Zarządzenie nr 47/2025
Wójta Gminy Zawidz
z dnia 12 listopada 2025 r.

w sprawie wprowadzenia Polityki Ochrony Danych Osobowych w Urzędzie Gminy w Zawidzu Kościelnym

Na podstawie art. 24 ust. 1 i 2 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) (Dz.Urz. UE L 119, s. 1) zarządzam, co następuje:

§ 1.

Wprowadzam w Urzędzie Gminy w Zawidzu Kościelnym:

1. Politykę Ochrony Danych Osobowych, stanowiącą załącznik do niniejszego zarządzenia.
2. Instrukcję Zarządzania Systemami Informatycznymi, stanowiącą załącznik do niniejszego zarządzenia.

§ 2.

Zobowiązuję podległych pracowników do zapoznania z treścią wprowadzonych aktów w Urzędzie Gminy w Zawidzu Kościelnym.

§ 3.

Zarządzenie wchodzi z dniem podpisania.

WÓJT GMINY
Kamil Jan Różański

Polityka Ochrony Danych Osobowych

Urzędu Gminy w Zawidzu Kościelnym

Spis treści:

Strona nr

Załączniki:

- załącznik nr 1 - Wzór upoważnienia do przetwarzania danych osobowych
- załącznik nr 2 - Wzór oświadczenia o poufności i zapoznaniu się z przepisami
- załącznik nr 3 - Polityka czystego biurka
- załącznik nr 4 - wzór Rejestru Czynności Przetwarzania Danych
- załącznik nr 5 - wzór Rejestru Kategorii Czynności Przetwarzania
- załącznik nr 6 - wzór Rejestru Naruszeń Ochrony Danych
- załącznik nr 7 – Plan ciągłości działania

I. Podstawa prawna:

1. Niniejszy dokument zatytułowany „**Polityka ochrony danych osobowych**” (dalej jako **Polityka**) ma za zadanie stanowić mapę wymogów, zasad i regulacji ochrony danych osobowych w Urzędzie Gminy w Zawidzu Kościelnym (dalej jako **UGZ**).

   Niniejsza Polityka jest polityką ochrony danych osobowych w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1). (dalej jako **RODO**).

2. Polityka zawiera:
   1) opis zasad ochrony danych obowiązujących w UGZ;
   2) odwołania do załączników uszczegóławiających (wzorcowe procedury lub instrukcje dotyczące poszczególnych obszarów z zakresu ochrony danych osobowych wymagających doprecyzowania w odrębnych dokumentach);
3. Odpowiedzialny za wdrożenie i utrzymanie niniejszej Polityki jest Administrator Danych Osobowych.
4. Za monitorowanie przestrzegania Polityki odpowiada Inspektor Ochrony Danych Osobowych.
5. Za stosowanie niniejszej Polityki odpowiedzialni są wszyscy członkowie personelu UGZ. UGZ zapewnia możliwość zaznajomienia się z niniejszą Polityką podmiotom przetwarzającym dane osobowe na mocy umów powierzenia zawartych z UGZ.
6. UGZ zapewnia zgodność przetwarzania danych osobowych z regulacjami RODO oraz krajowymi przepisami dotyczącymi ochrony danych osobowych - szczególnie w odniesieniu do: pracowników, mieszkańców gminy, interesantów, a ponadto danych osobowych powierzonych do przetwarzania podmiotom trzecim.
7. Zapisy niniejszej polityki dotyczą również Urzędu Stanu Cywilnego w Zawidzu Kościelnym jako wyodrębnioną część Urzędu Gminy w Zawidzu Kościelnym.

II. Podstawowe pojęcia i skróty:

1) **Polityka** - oznacza niniejszą Politykę ochrony danych osobowych, o ile co innego nie wynika wyraźnie z kontekstu.
2) **RODO -** oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1).
3) **Dane -** oznaczają dane osobowe, wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, o ile co innego nie wynika wyraźnie z kontekstu.
4) **Dane wrażliwe -** oznaczają dane wymienione w art. 9 ust. 1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej
5) **Dane szczególne -** oznaczają dane specjalne karne oraz dane dzieci.
6) **Dane karne** - oznaczają dane wymienione w art. 10 RODO, tj. dane dotyczące wyroków skazujących i naruszeń prawa.
7) **Osoba** - oznacza osobę, której dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu.
8) **Podmiot przetwarzający** - oznacza organizację lub osobę, której UGZ powierzył przetwarzanie danych osobowych.
9) **Eksport danych** - oznacza przekazanie danych do państwa trzeciego lub organizacji międzynarodowej.
10) **IODO lub Inspektor -** oznacza Inspektora Ochrony Danych Osobowych
11) **RCPD lub Rejestr -** oznacza Rejestr Czynności Przetwarzania Danych Osobowych.
12) **RNOD -** oznacza Rejestr Naruszeń Ochrony Danych,
13) **Ustawa** – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych;

14) **Przetwarzanie danych osobowych** – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie.
15) **Administrator Danych Osobowych (ADO)** – Wójt gminy Zawidz;

III. Cele i zasady bezpieczeństwa ochrony danych osobowych:

1. **Filary ochrony danych osobowych w UGZ:**
   1) **Legalność** − UGZ dba o ochronę prywatności i przetwarza dane zgodnie z prawem.
   2) **Bezpieczeństwo** − UGZ zapewnia odpowiedni poziom bezpieczeństwa danych podejmując stale działania w tym zakresie.
   3) **Prawa osób** − UGZ umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.
   4) **Rozliczalność** − UGZ dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność.

2. **Zasady ochrony danych**

   UGZ działa w oparciu o podstawę prawną w szczególności- ustawa z dnia 8 marca 1990 r. o samorządzie gminnym, ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych, ustawa z dnia 21 sierpnia 1997 r. o gospodarce nieruchomościami, ustawy z dnia 27 marca 2003 r. o planowaniu i zagospodarowaniu przestrzennym, ustawa z dnia 13 września 1996 r. o utrzymaniu czystości i porządku w gminach, ustawy z dnia 7 czerwca 2001 r. o zbiorowym zaopatrzeniu w wodę i zbiorowym odprowadzeniu ścieków oraz ustawy z dnia 28 listopada 2014 r. prawo o aktach stanu cywilnego i zgodnie z prawem (legalizm);
   1) rzetelnie i uczciwie (rzetelność);
   2) w sposób przejrzysty dla osoby, której dane dotyczą (transparentność);
   3) w konkretnych celach i nie "na zapas" (minimalizacja);
   4) nie więcej niż potrzeba (adekwatność);
   5) z dbałością o prawidłowość danych (prawidłowość);
   6) nie dłużej niż potrzeba (czasowość);
   7) zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo).

3. System ochrony danych

System ochrony danych osobowych w UGZ składa się z następujących elementów:

1) **Inwentaryzacja danych. Ocena skutków dla ochrony danych. UGZ** każdorazowo w trakcie roku kalendarzowego - jak dodawane (odejmowane) są kolejne kategorie przetwarzanych danych dokonuje identyfikacji zasobów przetwarzanych danych osobowych, kategorii danych, zależności między zasobami danych, identyfikacji sposobów wykorzystania danych (inwentaryzacja), w tym:
   a) przypadków przetwarzania danych wrażliwych,
   b) przypadków przetwarzania danych osób, których UGZ nie identyfikuje (**dane niezidentyfikowane**);
   c) współadministrowania danymi.
2) **Rejestr.** UGZ opracowuje, prowadzi i utrzymuje Rejestr Czynności Przetwarzania Danych Osobowych oraz Rejestr Kategorii Czynności Przetwarzania. Rejestr jest narzędziem rozliczania zgodności z ochroną danych w UGZ.
3) **Umowy powierzenia przetwarzania danych. UGZ zawiera** z podmiotami lub osobami, którym powierza przetwarzanie danych osobowych odpowiednie umowy, stosownie do art. 28 RODO.
4) **Podstawy prawne. UGZ** zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania danych i rejestruje je w Rejestrze, w tym:
   a) utrzymuje system zarządzania zgodami na przetwarzanie,
   b) inwentaryzuje i uszczegóławia uzasadnienie przypadków, gdy przetwarza dane na podstawie prawnie uzasadnionego interesu,
5) **Obsługa praw jednostki.** UGZ spełnia obowiązki informacyjne względem osób, których dane przetwarza, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:
   a) **Obowiązki informacyjne.** Przekazuje osobom prawem wymagane informacje przy zbieraniu danych i w innych sytuacjach oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków.
   b) **Możliwość wykonania żądań.** Weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich przetwarzających.
   c) **Obsługa żądań.** Zapewnia odpowiednie nakłady i procedury, aby żądania osób były realizowane w terminach i w sposób wymagany RODO i dokumentowane.
   d) **Zawiadamianie o naruszeniach.** Stosuje procedury pozwalające na ustalenie

konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.

6) **Minimalizacja.** UGZ posiada zasady i metody zarządzania minimalizacją (*privacy by default*), a w tym:
   a) zasady zarządzania **adekwatnością** danych;
   b) zasady reglamentacji i zarządzania **dostępem** do danych;
   c) zasady zarządzania okresem **przechowywania** danych i weryfikacji dalszej przydatności;
7) **Bezpieczeństwo. UGZ** zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:
   a) przeprowadza analizy ryzyka dla czynności przetwarzania danych lub ich kategorii;
   b) przeprowadza oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie;
   c) dostosowuje środki ochrony danych do ustalonego ryzyka;
   d) stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych − zarządza incydentami. UGZ opracowuje, prowadzi i utrzymuje Rejestr Naruszeń Ochrony Danych Osobowych. Rejestr jest narzędziem rozliczania zgodności z ochroną danych.
   e) wydaje upoważnienia do przetwarzania danych osobowych dla pracowników i innych osób wykonujących czynności przetwarzania danych np. stażyści, praktykanci. Określa w upoważnieniu wyraźny zakres przetwarzania danych osobowych. **Wzór upoważnienia stanowi załącznik nr 1 do Polityki.**
   f) wydaje zobowiązania o zachowaniu tajemnicy i zapoznaniu się z przepisami. **Wzór zobowiązania stanowi załącznik nr 2 do Polityki.**
8) ***Privacy by design*.** UGZ zarządza zmianami mającymi wpływ na prywatność. W tym celu procedury uruchamiania nowych projektów lub zadań uwzględniają konieczność oceny wpływu zmiany na ochronę danych, zapewnienie prywatności (a w tym zgodności celów przetwarzania, bezpieczeństwa danych i minimalizacji) już w fazie projektowania zmiany, inwestycji czy na początku nowego projektu.

IV. Zabezpieczenia danych osobowych:

1. Ochrona danych polega na zabezpieczeniu informacji wprowadzonej, przetwarzanej,

przesyłanej w systemie informatycznym oraz na nośnikach informacji przed nielegalnym ujawnieniem, kradzieżą oraz nieuprawnioną modyfikacją lub usunięciem.

2. Dane osobowe mogą przetwarzać wyłącznie osoby posiadające upoważnienia do przetwarzania danych osobowych. Osoby upoważnione do przetwarzania danych mają obowiązek zachować w tajemnicy dane, które przetwarzają, oraz sposoby ich zabezpieczenia.
3. Fakt modyfikacji zbioru danych: struktury, lokalizacji, a także utworzenia nowego zbioru osoba upoważniona, która takiej modyfikacji dokonała ma obowiązek zgłosić ten fakt ADO.
4. Osoby nieupoważnione do przetwarzania danych osobowych mogą przebywać w obszarach przetwarzania danych osobowych jedynie za zgodą ADO lub w obecności osoby upoważnionej do przetwarzania danych osobowych.
5. Wszystkie pomieszczenia, w których przetwarza się dane osobowe są zamykane na klucz w przypadku opuszczenia pomieszczenia przez ostatniego pracownika upoważnionego do przetwarzania danych osobowych - także w godzinach pracy.
6. Klucze do pomieszczeń służbowych mogą posiadać i za nie odpowiadają tylko te osoby, które są do tego upoważnione.
7. Dane osobowe przechowywane w wersji tradycyjnej (papierowej) są przechowywane po zakończeniu pracy w zamykanych na klucz meblach biurowych, a tam gdzie jest to możliwe - w szafach metalowych lub pancernych. Klucze od szaf należy zabezpieczyć przed dostępem osób nieupoważnionych do przetwarzania danych osobowych.
8. Dokumenty zawierające dane osobowe, w wyjątkowych sytuacjach mogą być wynoszone poza miejsce przetwarzania jedynie w wypadku otrzymania akredytacji ADO z jednoczesnym zapewnieniem ochrony fizycznej ich przed niepożądanym dostępem osób nieupoważnionych. Odpowiedzialność za dokumentację ponosi pracownik, który otrzymał akredytację.
9. Dane osobowe w wersji papierowej, wydruki i kopie a także, w wersji elektronicznej na nośnikach typu płyty CD, DVD, dyskach przenośnych należy niszczyć w niszczarkach lub przekazywać do zniszczenia wynajętej do tego celu firmie. Dokumentacja niszczona w niszczarkach poddawana jest całkowitej utylizacji.
10. Sprzątanie pomieszczeń gdzie przetwarzane są dane osobowe odbywa się przez personel sprzątający, który został przeszkolony w zakresie ochrony danych osobowych oraz zapoznany z obowiązkiem zachowania tajemnicy. Sprzątanie odbywa się tylko z

założeniem, że zostaną zachowane przez pracowników przetwarzających dane osobowe zasady „czystego biurka i ekranu".

11. Użytkownicy nie mogą wynosić na zewnątrz organizacji wymiennych elektronicznych nośników informacji z zapisanymi danymi osobowymi bez zgody Pracodawcy / Zleceniodawcy. Do takich nośników zalicza się: wymienne twarde dyski, pen-drive, płyty CD, DVD, pamięci typu Flash.
12. Dane osobowe wynoszone poza organizację muszą być zaszyfrowane (szyfrowane dyski, zabezpieczone hasłem pliki).
13. Należy zapewnić bezpieczne przewożenie dokumentacji papierowej w plecakach, teczkach.
14. Należy korzystać ze sprawdzonych firm kurierskich.
15. W przypadku, gdy dokumenty przewozi pracownik, zobowiązany jest do zabezpieczenia przewożonych dokumentów przed zagubieniem i kradzieżą.
16. W sytuacji przekazywania nośników z danymi osobowymi poza obszar organizacji można stosować następujące zasady bezpieczeństwa:
    1) adresat powinien zostać powiadomiony o przesyłce;
    2) dane przed wysłaniem powinny zostać zaszyfrowane a hasło podane adresatowi inną drogą;
    3) stosować bezpieczne koperty depozytowe;
    4) przesyłkę należy przesyłać przez kuriera.

V. Instrukcja zarządzania systemami informatycznymi:

1. W celu ochrony danych przechowywanych w systemach informatycznych należy wykorzystywać wchodzące w ich skład mechanizmy zarówno sprzętowe jak i programowe oraz inne rozwiązania zwiększające bezpieczeństwo danych.
2. Przy przetwarzaniu danych osobowych w systemach teleinformatycznych stosuje się zasady „czystego biurka i ekranu", realizowane poprzez stosowanie wygaszacza ekranu, blokowania systemu za pomocą indywidualnych haseł lub kodów oraz ustawianie monitorów w taki sposób aby nie była widoczna informacja dla osób postronnych. **„Polityka czystego biurka" stanowi załącznik nr 3 do Polityki.**
3. Zabrania się udostępniania indywidualnego kodu dostępu i haseł innym osobom.
4. Zabronione jest usuwanie danych przez wyrzucenie ich do kosza na odpadki.

5. Zabrania się korzystania z prywatnych nośników informacji w systemach przetwarzających dane osobowe.
6. Zabrania się korzystania z sieci publicznej (World Wide Web) poprzez niebezpieczne przeglądarki internetowe lub nieznajomego pochodzenia witryny internetowe.
7. W przypadku żądania udostępniania danych pracownicy UGZ postępują zgodnie z przepisami dotyczącymi ochrony danych osobowych. Decyzję podejmuje ADO w porozumieniu z IODO.
8. Udostępnianie danych jest odnotowywane w systemach informatycznych, a w przypadku zbiorów danych w formie tradycyjnej odnotowanie informacji o udostępnianiu przechowuje ADO.
9. Dla danych osobowych przetwarzanych w systemach informatycznych stosuje się następujące zasady:
   1) kontrola dostępu do zbiorów danych osobowych;
   2) indywidualne identyfikatory użytkowników (pracowników przetwarzających dane osobowe);
   3) uwierzytelnianie użytkowników (potwierdzanie ich tożsamości).
10. W celu zabezpieczenia danych osobowych przed ich utratą lub uszkodzeniem:
    1) dla wszystkich systemów wdrożono procedury tworzenia kopii zapasowych;
    2) wszystkie systemy informatyczne wyposażono w awaryjne zasilanie;
    3) wdrożono oprogramowanie antywirusowe;
    4) dostęp do systemów z sieci publicznej jest kontrolowany za pomocą zapory sieciowej oraz filtrów antyspamowych i oprogramowania antywirusowego;
    5) przy przesyłaniu danych wrażliwych przez sieć publiczną użytkownicy są zobowiązani stosować oprogramowanie szyfrujące;
    6) zastosowano środki fizyczne chroniące urządzenia przed osobami nieupoważnionymi przez ADO do dostępu do danych osobowych oraz zagrożeniami ze strony sił natury.
11. Użytkowników systemów przetwarzających dane osobowe obowiązuje następująca polityka haseł:
    1) minimalna długość hasła wynosi 8 (osiem) znaków;
    2) zmiana hasła następuje nie rzadziej, niż co 30 dni;
    3) hasło może się powtórzyć dopiero po 6 zmianie;
    4) hasło zawiera małe i wielkie litery oraz cyfry i znaki specjalne.
12. Jeżeli system informatyczny środkami technicznymi nie wymusza zasad ujętych

powyżej, użytkownik zobowiązany jest do przestrzegania powyższych zasad, a tym samym do okresowej zmiany hasła i dobrania odpowiedniej jego długości.

13. Użytkownik, który utracił hasło, zobowiązany jest zgłosić ten fakt bezzwłocznie ADO, który ustali nowe hasło.
14. Zabezpieczanie danych przed ich utratą uszkodzeniem, lub nieupoważnionym przetworzeniem w pozostałych przypadkach:
    1) W przypadku naprawy, przekazania, likwidacji nośnika (papier, dysk twardy, płyta kompaktowa, pamięć przenośna, dyskietka, taśma magnetyczna itp.), który zawiera dane osobowe podmiotowi nieupoważnionemu do przetwarzania danych, należy zapewnić trwałe wymazanie informacji stanowiących dane osobowe, z wyłączeniem sytuacji, kiedy naprawy, przekazania, likwidacji nośnika dokonuje podmiot z którym ADO w tym zakresie zawarł umowę powierzenia;
    2) W przypadku korzystania z komputerów przenośnych zawierających dane osobowe należy zachować szczególną ostrożność podczas używania komputera poza obszarem przetwarzania danych. W szczególności należy stosować mechanizmy szyfrowania plików lub baz danych, wbudowanych w system operacyjny. Po ustaniu konieczności przetwarzania danych na komputerze przenośnym, należy je trwale usunąć z nośnika danych;
    3) Ekrany komputerów, na których przetwarzane są dane osobowe, są chronione wygaszaczami. Monitory należy ustawić tak, aby ograniczyć dostęp do danych osobom nieupoważnionym do przetwarzania danych;
    4) W pomieszczeniach gdzie przetwarzane dane osobowe są szczególnie narażone na ich przetworzenie przez osoby nieuprawnione stosuje się zabezpieczenia fizyczne w postaci odgrodzenia stref przetwarzania danych osobowych poprzez montaż np.: przezroczystych szyb, drzwi, drewnianych półek, lad, blatów. Powyższe odgrodzenia mają na celu zabezpieczenie strefy szczególnie narażonych na przetwarzanie danych osobowych przed nieuprawnionym dostępem do strefy więcej niż jednej osoby bez wiedzy upoważnionego pracownika do przetwarzania danych osobowych, w pomieszczeniach gdzie zachowanie zasady „czystego biurka" jest ze względów logistycznych, fizycznych (brak miejsca) nie jest możliwe do zrealizowania. Wstęp do strefy przetwarzania danych osobowych następuje za zgodą upoważnionego pracownika.

15. Zgodnie z art. 32 RODO, Administrator powinien zapewnić zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego. Administrator opracował procedury przywracania, opisane w „Planie ciągłości działania" stanowiącym **Załącznik nr 7 do niniejszej polityki.**
16. Szczegółowy zakres zarządzania systemami informatycznymi określony jest w odrębnym dokumencie.

VI. Rejestry:

1. Rejestr Czynności Przetwarzania Danych (RCPD)

1) RCPD stanowi formę dokumentowania czynności przetwarzania danych osobowych w UGZ. RCPD pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności.
2) UGZ prowadzi RCPD, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe.
3) RCPD jest jednym z podstawowych narzędzi umożliwiających rozliczanie większości obowiązków ochrony danych.
4) W RCPD, dla każdej czynności przetwarzania danych, którą UGZ uznał za odrębną dla potrzeb RCPD, UGZ odnotowuje co najmniej:
   a) nazwę czynności,
   b) cel przetwarzania,
   c) opis kategorii osób,
   a) opis kategorii danych,
   b) podstawę prawną przetwarzania, wraz z wyszczególnieniem kategorii uzasadnionego interesu UGZ, jeśli podstawą jest uzasadniony interes,
   c) sposób zbierania danych,
   d) opis kategorii odbiorców danych (w tym przetwarzających),
   e) informację o przekazaniu poza EU/EOG;
   f) ogólny opis technicznych i organizacyjnych środków ochrony danych.

2) Wzór RCPD stanowi **Załącznik nr 4 do Polityki - "Wzór Rejestru Czynności**

Przetwarzania Danych". Wzór Rejestru zawiera także kolumny nieobowiązkowe. W kolumnach nieobowiązkowych UGZ rejestruje informacje w miarę potrzeb i możliwości, z uwzględnieniem tego, że pełniejsza treść RCPD ułatwia zarządzanie zgodnością ochrony danych i rozliczenie się z niej. Rejestr sporządzony jest w formie elektronicznej pliku XLS.

2. Rejestr Kategorii Czynności Przetwarzania (RKCP)

1) RKCP stanowi formę dokumentowania czynności przetwarzania danych osobowych w UGZ jako przetwarzający w imieniu innego Administratora Danych. RKCP pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności.
2) UGZ prowadzi RKCP, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe.
3) RKCP jest jednym z podstawowych narzędzi umożliwiających rozliczanie większości obowiązków ochrony danych.
4) W RKCP, dla każdej czynności przetwarzania danych, którą UGZ uznał za odrębną dla potrzeb RKCP, UGZ odnotowuje co najmniej:
   a) Kategorie przetwarzań,
   b) Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa,
   c) Nazwa i dane kontaktowe administratora,
   d) dane inspektora ochrony danych administratora,
   e) informacje czy dane są przekazywane do państwa trzeciego i organizacji międzynarodowej.
5) Wzór RCPD stanowi **Załącznik nr 5 do Polityki - "Wzór Rejestru Kategorii Czynności Przetwarzania".** Wzór Rejestru zawiera także kolumny nieobowiązkowe. W kolumnach nieobowiązkowych UGZ rejestruje informacje w miarę potrzeb i możliwości, z uwzględnieniem tego, że pełniejsza treść RKCP ułatwia zarządzanie zgodnością ochrony danych i rozliczenie się z niej. Rejestr sporządzony jest w formie elektronicznej pliku XLS.

3. Rejestr Naruszeń Ochrony Danych (RNOD)

1) RNOD stanowi formę dokumentowania naruszeń ochrony danych osobowych w UGZ.

RNOD pełni rolę sprawdzenia naruszeń oraz środków zaradczych, naprawczych, które w związku z tym wdraża UGZ, a także jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności.

2) UGZ prowadzi RNOD, w którym gromadzi i monitoruje naruszenia ochrony danych osobowych.
3) RNOD jest jednym z podstawowych narzędzi umożliwiających rozliczanie obowiązku monitorowania naruszeń ochrony danych i stosowania działań zaradczych.
4) W RNOD, dla każdego naruszenia ochrony danych, UGZ odnotowuje co najmniej:
   a) naruszenie,
   b) Data i godzina zgłoszenia podejrzenia naruszenia,
   c) Data oraz godzina stwierdzenia naruszenia,
   d) Data naruszenia/okres, którego dotyczy,
   e) Kategoria i ilość osób, których dotyczy naruszenie,
   f) Miejsce naruszenia,
   g) Okoliczności naruszenia - opis charakteru naruszenia, analiza zdarzenia, przyczyny wystąpienia,
   h) Opis skutków/konsekwencji naruszenia
   i) Podjęte działania - opis środków zastosowanych lub proponowanych do wdrożenia w celu zaradzenia naruszeniu, w tym zastosowane środki zastosowane w celu zminimalizowania jego negatywnych skutków,
   j) Czy zachodzi obowiązek poinformowania Urzędu Ochrony Danych Osobowych,
   k) Czy zachodzi obowiązek poinformowania osoby/osób, których naruszenie dotyczy.
5) Wzór RNOD stanowi **Załącznik nr 6 do Polityki - "Wzór Rejestru Naruszeń Ochrony Danych".** Wzór Rejestru zawiera także kolumny nieobowiązkowe.

W kolumnach nieobowiązkowych UGZ rejestruje informacje w miarę potrzeb i możliwości, z uwzględnieniem tego, że pełniejsza treść RNOD ułatwia zarządzanie zgodnością ochrony danych i rozliczenie się z niej. Rejestr sporządzony jest w formie elektronicznej pliku XLS.

4. Podstawy przetwarzania

1) UGZ dokumentuje w RCPD podstawy prawne przetwarzania danych dla

poszczególnych czynności przetwarzania.

2) Wskazując ogólną podstawę prawną (zgoda, umowa, obowiązek prawny, żywotne interesy, zadanie publiczne/władza publiczna, uzasadniony cel) UGZ dookreśla podstawę w czytelny sposób, gdy jest to potrzebne.
3) UGZ wdraża metody zarządzania zgodami umożliwiające rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej konkretnych danych w konkretnym celu, oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności (sprzeciw, ograniczenie itp.).

VII. Zgłaszanie naruszeń:

1. Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu

1) W przypadku naruszenia w UGZ ochrony danych osobowych, ADO bez zbędnej zwłoki - w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia - zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55 RODO, 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 naruszenia w UGZ ochrony danych osobowych musi co najmniej:
   a) 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;
   b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
   c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
   d) opisywać środki zastosowane lub proponowane przez UGZ w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

2. Zawiadamianie o naruszeniu ochrony danych osobowych osoby, której naruszenie

dotyczy

1) Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, UGZ bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.
2) Zawiadomienie musi być sporządzone jasnym i prostym językiem, opisywać charakter naruszenia ochrony danych osobowych oraz zawierać co najmniej:
   a) informacje o IODO,
   b) konsekwencjach naruszenia,
   c) środkach zaradczych.
3) UGZ zwolniony jest z obowiązku zawiadomienia osoby jeśli:
   a) wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie,
   b) zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby,
   c) wymagałoby ono niewspółmiernie dużego wysiłku.

3. Opis zdarzeń naruszających ochronę danych

1) Podział zagrożeń:

   a) Zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych.

   b) Zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania, błędy pracowników), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych.

   c) Zagrożenia zamierzone, świadome i celowe - najpoważniejsze zagrożenia, naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na: nieuprawniony dostęp z zewnątrz (włamanie do systemu, włamanie do pomieszczeń), nieuprawniony dostęp do systemu z jego wnętrza, udostępnienie danych osobom nieupoważnionym, nieuprawniony przekaz danych, pogorszenie

jakości sprzętu i oprogramowania, bezpośrednie zagrożenie materialnych składników systemu.

2) Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu ochrony danych osobowych, to w szczególności:

   a) Sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.,

   b) Niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy,

   c) Awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru,

   d) Pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,

   e) Jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,

   f) Nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych,

   g) Stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),

   h) Nastąpiła niedopuszczalna manipulacja danymi osobowymi, w tym również kradzież danych lub ich wyłudzenie,

   i) Ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń,

   j) Praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony informacji - np. praca przy komputerze lub w sieci osoby, która nie jest

formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.,

k) Ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki", itp.,

l) Podmieniono lub zniszczono nośniki z danymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane,

m) Rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur ochrony danych osobowych (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na informacjach służbowych w celach prywatnych, itp.),

n) Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania informacji (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, płytach CD w formie niezabezpieczonej itp.

VIII. Inspektor Ochrony Danych Osobowych:

1. Wyznaczenie Inspektora Ochrony Danych

1) Status prawny i zadania Inspektora ochrony danych regulują przepisy Rozdziału IV Sekcji 4 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.
2) Inspektor ochrony danych w wykonywaniu swoich zadań podlega bezpośrednio ADO.
3) Do zadań Inspektora ochrony danych należy w szczególności:
   a) informowanie ADO oraz pracowników UGZ, którzy przetwarzają dane osobowe o obowiązkach wynikających z rozporządzenia RODO oraz innych przepisów Unii Europejskiej lub państw członkowskich o ochronie danych i doradzanie im w tych sprawach;
   b) monitorowanie przestrzegania rozporządzenia RODO, innych przepisów dotyczących ochrony danych osobowych oraz prowadzenie szkoleń wewnętrznych

zwiększających świadomość personelu UGZ w zakresie zasad dotyczących ochrony danych,

c) pełnienie funkcji punktu kontaktowego dla właściwych organów i podmiotów zewnętrznych w kwestiach związanych z przetwarzaniem przez UGZ danych osobowych.

4) IODO nie rzadziej niż raz na rok przeprowadza kontrolę wewnętrzną stosowania dokumentacji ochrony danych osobowych oraz rozwiązań technicznych i organizacyjnych w UGZ.
5) Z kontroli o której mowa w pkt. 4 IODO sporządza protokół, określający zakres kontroli, stan stosowania regulacji ochrony danych osobowych, a także zalecenia co do dalszego przetwarzania.

IX. Postanowienia końcowe:

1. W sprawach nieobjętych niniejszym dokumentem mają zastosowanie odpowiednie przepisy prawa w szczególności rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1) oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.
2. Każda osoba upoważniona do przetwarzania danych osobowych w UGZ jest obowiązana do zapoznania się oraz stosowania postanowień Polityki.
3. Polityka wchodzi w życie z dniem ogłoszenia.

Załącznik nr 7 do Polityki

Plan ciągłości działania

SPIS TREŚCI

1 PLAN AWARYJNY ODTWORZENIA SYSTEMU INFORMATYCZNEGO PO AWARII KRYTYCZNEJ

1. **Zasady postępowania przy odtworzeniu systemu informatycznego w lokalizacji podstawowej:**
   1) w przypadku stwierdzenia krytycznej awarii dysku podstawowego w centrali, osoba upoważniona podpina dysk zapasowy, konfiguruje, zgrywa dane z kopii zapasowej;
   2) po uruchomieniu dysku osoba upoważniona podłącza go do sieci;
   3) przewidywany czas operacji uruchomienia dysku zapasowego – 3 godziny.
2. **Zasady postępowania przy odtworzeniu systemu informatycznego w lokalizacji alternatywnej:**
   1) w przypadku zniszczenia miejsca serwerowni wraz z serwerem, należy zaplanowaną uprzednio lokalizację przeznaczyć na alternatywną serwerownię;
   2) przygotowanie serwerowni wymaga: zapewnienia energii elektrycznej, UPS, łącz telekomunikacyjnych;
   3) po uruchomieniu serwera osoba upoważniona podłącza go do sieci;
   4) przewidywany czas operacji uruchomienia serwera zapasowego – 2 dni.

2 PLAN AWARYJNY NA WYPADEK BRAKU ZASILANIA W SIECI KOMPUTEROWEJ

1. Sieć komputerowa podłączona jest do UPS wyposażonego w baterie wystarczające na około 2 godz. pracy.
2. W przypadku dłuższej awarii sieci zasilającej osoba upoważniona bądź Administrator Danych Osobowych zobowiązany jest do powiadomienia wszystkich użytkowników o konieczności zakończenia pracy w systemach.

3. Administrator Danych Osobowych wykonuje kopie podstawowych danych w cyklu miesięcznym na dysk zewnętrzny.
4. Dyski zapasowe przechowywane są w miejscu niedostępnym dla szerszego grona osób.

3 PLAN AWARYJNY NA WYPADEK UTRATY DOSTĘPU DO SIECI INTERNET

1. W przypadku niedostępności internetu awaria jest zgłaszana do Operatora internetu na numer wyznaczony na zgłoszenia.
2. W przypadku niedostępności systemów specjalistycznych awaria zgłaszana jest do Administratora danego systemu.