Załącznik nr 2 do Statutu MKZP przy UGiM w Czerwieńsku

POLITYKA OCHRONY DANYCH OSOBOWYCH

Spis treści

Rozdział I

Przepisy Ogólne

Art. 1. Informacje wstępne

1. Polityka ochrony danych osobowych zwana dalej „Polityką” jest dokumentem wewnętrznym Międzyzakładowej Kasy Zapomogowo-Pożyczkowej przy Urzędzie Gminy i Miasta w Czerwieńska, zwanej dalej „Kasą”, opisującym zasady ochrony danych osobowych stosowane przez Administratora w celu spełnienia wymagań wynikających z:
   1) 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, sprost.: Dz. Urz. UE L 127 z 23.05.2018, s. 2);
   2) Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (t. j. Dz. U. z 2019 r. poz. 1781 ze. zm.);
   3) Ustawa z dnia 11 sierpnia 2021 r. o kasach zapomogowo-pożyczkowych (Dz.U. 2021 poz. 1666).
   4) Dobrych praktyk z zakresu bezpieczeństwa informacji oraz ochrony danych osobowych.

Art. 2. Definicje

1) **Administrator** – Międzyzakładowa Kasa Zapomogowo-Pożyczkowa przy Urzędzie Gminy i Miasta w Czerwieńska oznacza osobę fizyczną lub prawną lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. W rozumieniu niniejszej polityki ochrony danych pod pojęciem „Administratora” należy rozumieć MKZP;
2) **aktywa** – wszelkie elementy posiadające wartość dla podmiotu (zasoby ludzkie, finansowe, informacyjne, organizacyjne, technologiczne, i fizyczne) mogące służyć do przetwarzania danych osobowych;
3) **dane osobowe** – 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;

4) **dane osobowe zwykłe** – wszelkie dane osobowe nienależące do szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 RODO, jak również danych dotyczących wyroków skazujących lub czynów zabronionych;
5) **szczególnych kategorii dane osobowe** – dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej (w tym o korzystaniu z usług opieki zdrowotnej) ujawniające informacje o stanie jej zdrowia; dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne (przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej) oraz dane dotyczące seksualności lub orientacji seksualnej osoby fizycznej;
6) **Podmiot –** Międzyzakładowa Kasa Zapomogowo-Pożyczkowa przy Urzędzie Gminy i Miasta w Czerwieńska**;**
7) **Pracodawca –** zakład pracy zatrudniający członków MKZP;
8) **naruszenie ochrony danych osobowych** – 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;
9) **Odbiorca** - osoba fizyczna lub prawna, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią; Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców - przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;
10) **Ograniczenie przetwarzania** – oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
11) **Podatność -** słabość aktywu (zasobu) lub zabezpieczenia które może być wykorzystane przez jedno lub więcej zagrożeń;
12) **Przetwarzanie** – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie 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;

13) **Rejestr czynności przetwarzania danych osobowych –** rejestr czynności przetwarzania danych osobowych, o którym stanowi art. 30 ust. 1 RODO;
14) **RODO** – 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);
15) **Ryzyko** – potencjalna sytuacja, w której określone zagrożenie wykorzystując podatność aktywów lub grupy aktywów powodować może chociażby potencjalną szkodę majątkową lub niemajątkową dla MKZP;
16) **Użytkownik** - osoba posiadająca dostęp do systemu informatycznego przetwarzającego dane osobowe MKZP;
17) **Zagrożenie** – niepożądane działanie lub sytuacja, która może niekorzystnie wpłynąć na prawidłowość oraz bezpieczeństwo procesów realizowanych w MKZP, potencjalna przyczyna wystąpienia incydentu;
18) **Zgoda** – dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

Art. 3. Podmioty odpowiedzialne za ochronę i przetwarzanie danych osobowych

1. Administrator

1) wdraża odpowiednie środki techniczne i organizacyjne, mające na celu zabezpieczanie przetwarzanych danych oraz zapewnianie poufności, integralności i dostępności danych,
2) podejmuje odpowiednie działania w przypadku naruszenia ochrony danych osobowych lub podejrzenia naruszenia ochrony danych osobowych zgodnie z procedurą stanowiącą integralną część niniejszej Polityki,
3) upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnie zakresie,
4) prowadzi Rejestr czynności przetwarzania danych osobowych,
5) dopełnia wszelkie pozostałe obowiązki wymagane przez RODO i inne przepisy regulujące zasady przetwarzania danych osobowych w MKZP.

2. Użytkownicy

1) Użytkownicy dopuszczeni przez Administratora do przetwarzania danych osobowych, zobowiązani są do:
   a) zapoznania się z przepisami prawa w zakresie ochrony danych osobowych,
   b) niezwłocznego zawiadomienia Administratora o naruszeniach ochrony danych osobowych,
   c) stosowania określonych przez Administratora procedur i środków mających na celu zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym.

Art. 4. Zasady ochrony danych osobowych

1. Administrator zapewnia aby przetwarzanie danych osobowych odbywało się z poszanowaniem następujących zasad:
   1) dane osobowe muszą być przetwarzane zgodnie z prawem (legalizm);
   2) dane osobowe muszą być przetwarzane rzetelnie i uczciwie (rzetelność);
   3) dane osobowe muszą być przetwarzane w sposób przejrzysty dla osoby, której dane dotyczą (przejrzystość);
   4) dane osobowe muszą być przetwarzane w sposób adekwatny, stosowny oraz ograniczony do tego, co niezbędne do celów, w których dane są przetwarzane (minimalizacja);
   5) dane osobowe muszą być przetwarzane z dbałością o prawidłowość i aktualność danych (prawidłowość);
   6) dane osobowe muszą być przetwarzane nie dłużej niż to jest niezbędne do osiągnięcia celu przetwarzania danych osobowych (ograniczenie przechowywania);
   7) dane osobowe muszą być przetwarzane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami (ograniczenie celu);
   8) dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych (bezpieczeństwo).

Art. 5. Podstawy dopuszczalności przetwarzania danych osobowych

1. Przetwarzanie danych osobowych zwykłych dopuszczalne jest tylko wtedy, gdy zostanie spełniona jedna z przesłanek wynikających z art. 6 ust. 1 RODO.
2. W przypadku przetwarzania szczególnych kategorii danych osobowych podstawą dopuszczalności przetwarzania danych mogą być wyłącznie przesłanki wynikające z art. 9 ust. 2 RODO.
3. W przypadku przetwarzania danych osobowych na podstawie zgody osoby, której

dane dotyczą, należy stosować oświadczenie o wyrażeniu zgody na przetwarzanie danych osobowych.

Art. 6. Obowiązek informacyjny przy przetwarzaniu danych

1. Administrator realizuje obowiązek informacyjny w stosunku do osób fizycznych od których bezpośrednio są zbierane dane osobowe zgodnie z art. 13 ust. 1 i 2 RODO oraz w stosunku do osób, których dane zostały zebrane z innego źródła aniżeli bezpośrednio od osoby, której dane dotyczą zgodnie z art. 14 ust.1 i 2 RODO.
2. Zwolnienie z realizacji obowiązku informacyjnego wynikającego z art. 13 ust. 1 i 2 RODO znajduje zastosowanie w sytuacji, gdy osoba, której dane dotyczą dysponuje już tymi informacjami oraz w przypadkach uregulowanych w powszechnie obowiązujących przepisach prawa.
3. Wzór ogólny klauzuli informacyjnej zawierającej informacje, o których mowa w art. 13 ust. 1 i 2 RODO - służącej za podstawę do konstruowania szczegółowych klauzul informacyjnych na potrzeby Jednostki, stanowi **załącznik** do niniejszej Polityki.
4. Administrator realizuje obowiązek informacyjny z art. 13 ust. 1 i 2 RODO.
5. Zwolnienie z realizacji obowiązku informacyjnego na podstawie art. 14 ust.1 i 2, RODO znajduje zastosowanie, gdy zostanie spełniona jedna z przesłanek wyszczególnionych w art. 14 ust. 5 RODO.
6. Administrator realizuje obowiązek informacyjny z art. 14 ust. 1 i 2 RODO w sposób szczegółowo wskazany w źródłach prawa powszechnie obowiązującego.

Art. 7. Prawa osób, których dane dotyczą

1. Osobie, której dane są przetwarzane, przysługują następujące prawa:
   1) prawo dostępu do danych,
   2) prawo do sprostowania danych,
   3) prawo do usunięcia danych,
   4) prawo do ograniczenia przetwarzania danych,
   5) prawo do przenoszenia danych,
   6) prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.

Art. 8. Procedura nadawania upoważnień do przetwarzania danych osobowych

1. Do przetwarzania danych osobowych mogą mieć dostęp osoby posiadające pisemne upoważnienia do przetwarzania danych osobowych nadane przez Administratora, przy czym osoby te zobowiązane są złożyć oświadczenie o zachowaniu w tajemnicy

danych osobowych lub winny podlegać odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy.

2. Administrator przygotowuje stosowne upoważnienie do przetwarzania danych osobowych.
3. Administrator uprawniony jest do odwołania nadanego upoważnienia do przetwarzania danych osobowych w każdym czasie.
4. Zatwierdzone przez Administratora upoważnienie do przetwarzania danych osobowych rejestrowane jest w ewidencji.
5. Upoważnienia do przetwarzania danych osobowych przechowywane są siedzibie MKZP.

Art. 9. Rejestrowanie czynności przetwarzania danych

1. Wszystkie czynności przetwarzania realizowane przez Administratora zamieszcza się w Rejestrze czynności przetwarzania danych osobowych.
2. Administratorem, przygotowuje i aktualizuje rejestry, o których mowa w ust. 1.

Art. 10. Dostęp do danych osobowych przez podmioty trzecie

1. Administrator może przekazać podmiotowi trzeciemu (niebędącemu osobą, której dane dotyczą) przetwarzane przez siebie dane osobowe w ramach:
   1) udostępnienia jeżeli jest to przewidziane w powszechnie obowiązujących przepisach prawa,
   2) powierzenia jeżeli podmiot trzeci przetwarza dane w imieniu Administratora i na jego udokumentowane polecenie w rozumieniu art. 28 RODO.
2. W przypadku powierzenia przetwarzania danych konieczne jest zawarcie umowy powierzenia przetwarzania danych osobowych pomiędzy Administratorem oraz podmiotem przetwarzającym dane na zlecenie, który przetwarza dane w imieniu Administratora, bądź posłużenie się innym instrumentem prawnym, który podlega prawu Unii lub prawu polskiemu i wiąże zarówno podmiot przetwarzający, jak i Administratora.

Art. 11. Zasady anonimizacji danych osobowych

1. Na podstawie obowiązujących przepisów o dostępie do informacji zaleca się zastosowanie następujących zasad anonimizacji danych:
   1) w przypadku udostępniania informacji o osobie fizycznej anonimizacji – co do zasady – podlegają:
      a) imię i nazwisko,
      b) PESEL,

c) data i miejsce urodzenia,
d) adres zamieszkania, zameldowania lub pobytu,
e) numer tel.,
f) adres e-mail,
g) numer konta bankowego,
h) informacje o zobowiązaniach finansowych,
i) inne dane pozwalające zidentyfikować osobę fizyczną lub naruszyć jej prawa i wolności,

2) Anonimizacji nie podlega jednak imię i nazwisko usługodawcy lub nazwa firmy realizującej usługę, informacja o wykonanej usłudze oraz kwota, za jaką usługa została wykonana.

2. Zasady anonimizacji opisane w niniejszym rozdziale stanowią jedynie reguły ogólne anonimizacji i powinny być każdorazowo indywidualnie weryfikowane kiedy dochodzi do udostępniania danych.

Art. 12. Zasady postępowania z dokumentami papierowymi zawierającymi dane osobowe

1. W stosunku do dokumentów papierowych stanowiących wydruki z systemu informatycznego MKZP oraz wszelkie dokumenty zawierające dane osobowe, osoby upoważnione obowiązują następujące środki ostrożności:
   1) wydruki z systemu informatycznego i wszelkie dokumenty zawierające dane osobowe powinny być niedostępne dla osób nieuprawnionych,
   2) wydruki z systemu informatycznego i wszelkie dokumenty zawierające dane osobowe nie mogą być pozostawione w drukarce lub kserokopiarce ogólnodostępnej,
   3) wydruki niepotrzebne i nieprzydatne powinny być na bieżąco niszczone za pomocą niszczarki właściwej klasy,
   4) dokumenty zawierające dane osobowe, których nie można zniszczyć z przyczyn technicznych lub formalnych, powinny być składowane w miejscu z ograniczonym dostępem, systematycznie weryfikowane, a następnie archiwizowane zgodnie z obowiązującymi w tym zakresie przepisami.

Art. 13. Naruszenia ochrony danych osobowych

Administrator stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych osobowych Prezesowi Urzędu Ochrony Danych Osobowych.

Art. 14. Zasady korzystania z poczty elektronicznej

1. Użytkownik jest zobowiązany do korzystania z przyznanego mu adresu mailowego wyłącznie w celu prowadzenia korespondencji służbowej.
2. Użytkownik nie może używać służbowego adresu mailowego do celów prywatnych, w szczególności do rejestracji na portalach społecznościowych, dokonywania zakupów w sklepach internetowych.
3. Użytkownik powinien zachować szczególną ostrożność przy wpisywaniu adresu odbiorcy wiadomości.
4. Użytkownik podczas wysyłania maili do wielu adresatów jednocześnie, powinien użyć metody „Ukryte do wiadomości – UDW". Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości".
5. Użytkownik powinien zastosować zabezpieczenia kryptograficzne przy przesyłaniu załączników do wiadomości. Zabezpieczenia kryptograficzne mogą polegać na przesłaniu zahasłowanych plików w formie załącznika, niemniej hasło powinno być przekazane adresatowi za pośrednictwem innego źródła tj. sms, bądź podczas rozmowy telefonicznej po uprzednim zweryfikowaniu tożsamości adresata.
6. Użytkownik powinien zachować szczególną ostrożność podczas odbierania poczty elektronicznej, a w szczególności nie powinien otwierać plików i linków w niej zawartych, ani otwierać załączników jeżeli nie ma pewności co do autentyczności adresata wiadomości. Tego typu maile większości przypadków mogą zawierać załączniki ze szkodliwym kodem, które po „kliknięciu" infekują komputer Użytkownika oraz może istnieć realne ryzyko zaimplementowania kodu w pozostałych komputerach.
7. W wyniku działania takiego szkodliwego oprogramowania może dojść do poważnych incydentów, łącznie z pełną utratą danych osobowych lub zaszyfrowaniem przez kryptowirusy. W takim przypadku Użytkownik powinien poinformować o zdarzeniu Administratora.
8. Użytkownik powinien regularnie przeglądać folder spam i usuwać niepotrzebne wiadomości pocztowe.

Art. 15. Zasady korzystania z bankowości elektronicznej

1. Użytkownik, który wykonuje przelewy bankowe zobowiązany jest do regularnej zmiany hasła oraz nieprzechowywania go w formie pisemnej wraz z loginem.
2. Użytkownik zobowiązany jest do zapamiętania lub przechowywania hasła dostępu oraz innych danych służących do uwierzytelniania i autoryzacji w bezpiecznym

miejscu.

3. Użytkownik nie może opuścić stanowiska pracy bez wylogowania się i zamknięcia przeglądarki internetowej.
4. Użytkownik logujący się do bankowości elektronicznej nie powinien korzystać z nieznanych sieci bezprzewodowych.
5. W celu zalogowania się do systemu bankowości elektronicznej Użytkownik nie powinien wchodzić na stronę internetową banku za pośrednictwem linków znajdujących się w korespondencji elektronicznej.
6. Użytkownicy, obsługujący bankowość elektroniczną są zobligowani do zapoznania się z zasadami bezpieczeństwa teleinformatycznego przekazanymi przez bank, który obsługuje bankowość elektroniczną.

Rozdział II

Postanowienia końcowe

Art. 16. Informacje dotyczące Polityki ochrony danych osobowych

1. Każda osoba mająca dostęp do danych osobowych MKZP zobowiązana jest zapoznać się z niniejszą Polityką.
2. Zapisy dot. ochrony danych zawarte w niniejszym statucie winny podlegać przeglądom i aktualizacji w przypadku zmian w otoczeniu organizacyjno-prawnym Administratora.

Art. 17. Wykaz załączników

1) Załącznik Klauzula informacyjna o przetwarzaniu danych osobowych.