ZARZĄDZENIE Nr 49/2024

STAROSTY TURECKIEGO

z dnia 25 czerwca 2024 r.

w sprawie wprowadzenia w Starostwie Powiatowym w Turku procedur dotyczących bezpieczeństwa udostępnianych danych osobowych

Na podstawie art. 34 ust. 1 ustawy z dnia 5 czerwca 2018 r. o samorządzie powiatowym (Dz. U. z 2024 r. poz. 107), art. 4 ust. 1 pkt 1 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2022 r. poz. 902), rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2007 r. w sprawie Biuletynu Informacji Publicznej (Dz.U. z 2007 r. Nr 10 poz. 68) oraz art. 24 ust. 1 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 - RODO z dnia 27 kwietnia 2016 r. (Dz. Urz. UE.L Nr 119, str. 1 ze zm.) zarządzam, co następuje:

§ 1.

1. Wprowadza się w Starostwie Powiatowym w Turku **procedurę Korzystania ze Służbowej Poczty Elektronicznej.**
2. Procedura, o której mowa w ust. 1 stanowi załącznik nr 1 do niniejszego zarządzenia.

§ 2.

1. Wprowadza się w Starostwie Powiatowym w Turku **procedurę Retencji Danych w Systemie Poczty Elektronicznej.**
2. Procedura, o której mowa w ust. 1 stanowi załącznik nr 2 do niniejszego zarządzenia.

§ 3.

1. Wprowadza się w Starostwie Powiatowym w Turku **procedurę ustalania okresu publikowania treści zawierających dane osobowe w BIP oraz dokonywania przeglądu danych udostępnionych w BIP**.
2. Procedura, o której mowa w ust. 1 stanowi załącznik nr 3 do niniejszego zarządzenia.

§ 4.

1. Wprowadza się w Starostwie Powiatowym w Turku **procedurę inwentaryzacji umów powierzenia przetwarzania.**
2. Procedura, o której mowa w ust. 1 stanowi załącznik nr 4 do niniejszego zarządzenia.

§ 5.

1. Wykonanie niniejszego zarządzenia powierza się naczelnikom wydziałów, kierownikom biur i pracownikom zatrudnionym na samodzielnych stanowiskach pracy.
2. Zarządzenie wchodzi w życie z dniem podpisania.

STAROSTA
Jan Smak

Inspektor
Ochrony Danych
Robert Wojdyła

RADCA PRAWNY
Magdalena Mikołajczyk
Pz-3856

Załącznik nr 1 do Zarządzenia nr 40/2024 Starosty Tureckiego

w sprawie wprowadzenia w Starostwie Powiatowym w Turku

procedur dotyczących bezpieczeństwa udostępnianych danych osobowych

Procedura Korzystania ze Służbowej Poczty Elektronicznej

Wstęp

Poczta elektroniczna stanowi kluczowy element współczesnej komunikacji w ramach organizacji jak i w sferze osobistej oferując możliwość szybkiego i skutecznego przesyłania wiadomości zarówno w obrębie organizacji, jak i na skalę globalną.

Niemniej jednak, użytkowanie e-maila nie jest wolne od ryzyka. Istnieje możliwość, że wiadomości mogą zostać przechwycone, nieautoryzowane zapisane, odczytane lub nawet przekazane dalej przez osoby trzecie. Dodatkowo, nieoficjalne uwagi lub komentarze zamieszczone w treści e-maili lub w załącznikach mogą być błędnie zrozumiane przez adresatów, co potencjalnie prowadzi do konfliktów lub komplikacji prawnych. Jednym z głównych ryzyka jest również masowe wysyłanie wiadomości, które ujawniają prywatne adresy e-mail odbiorców, co stanowi naruszenie prywatności i ochrony danych osobowych. Z tego powodu, kluczowe jest ścisłe przestrzeganie zasad bezpiecznego korzystania z poczty elektronicznej, aby zminimalizować ryzyko i zapewnić odpowiednią ochronę przesyłanych danych. W obecnych czasach, odpowiednie zarządzanie i bezpieczne użytkowanie poczty elektronicznej są niezbędne do ochrony danych osobowych, bezpieczeństwa informacji i zapewnienia prywatności komunikacji.

1. Przedmiot Procedury

Niniejsza procedura ma na celu określenie jednolitych zasad korzystania z systemu służbowej poczty elektronicznej. Dokument ten został opracowany w celu zapewnienia, że wszystkie działania związane z używaniem poczty elektronicznej w ramach organizacji są realizowane w sposób bezpieczny, efektywny oraz zgodny z obowiązującymi przepisami o ochronie danych. Procedura ta dotyczy każdego pracownika mającego dostęp do firmowego systemu poczty e-mail oraz określa standardy postępowania, mające na celu minimalizację zagrożeń związanych z ochroną i przetwarzaniem danych osobowych i firmowych.

2. Cele Procedury

Głównym celem niniejszej procedury jest:

1) Zapewnienie spójności i zgodności w korzystaniu z służbowej poczty elektronicznej wśród wszystkich pracowników.

2) Ochrona poufności i integralności informacji przekazywanych drogą elektroniczną.
3) Zminimalizowanie ryzyka wystąpienia incydentów bezpieczeństwa, w tym nieautoryzowanego dostępu do informacji, ich utraty lub uszkodzenia.
4) Promowanie odpowiedzialnego i świadomego korzystania z narzędzi komunikacji elektronicznej.
5) Zapewnienie zgodności z obowiązującymi przepisami prawa dotyczącymi ochrony danych osobowych i tajemnicy przedsiębiorstwa.

3. Zakres Obowiązujących Zasad

Procedura dotyczy wszystkich aspektów związanych z korzystaniem z poczty elektronicznej, w tym, ale nie ograniczając się do:

1) Ustanowienie jasnych wytycznych dotyczących dozwolonego użytku służbowej poczty elektronicznej.
2) Definiowanie procedur zabezpieczeń, takich jak stosowanie haseł, szyfrowanie wiadomości oraz regularne aktualizacje oprogramowania antywirusowego.
3) Określenie zasad dotyczących archiwizacji korespondencji elektronicznej i zarządzania cyklem życia informacji.
4) Wskazanie odpowiednich działań w przypadku wykrycia podejrzanych lub nieautoryzowanych działań związanych z pocztą elektroniczną.
5) Podkreślenie znaczenia prywatności i poufności w komunikacji elektronicznej, wskazując na odpowiedzialność każdego użytkownika za ochronę przekazywanych danych.

4. Zasady Korzystania z Służbowej Poczty Elektronicznej - Szczegółowe Wytyczne

1) **Przeznaczenie Służbowe:** Użycie służbowej poczty elektronicznej jest wyłącznie zarezerwowane dla celów zawodowych, co oznacza, że każdy pracownik jest zobowiązany do wykorzystywania tego narzędzia ściśle w zakresie wykonywania powierzonych mu zadań. Jakiekolwiek wykorzystanie poczty do celów prywatnych jest niezgodne z polityką jednostki.
2) **Własność Korespondencji:** Wszystkie e-maile generowane, odbierane lub wysyłane przez pracowników są uznawane za własność organizacji. Jednostka zastrzega sobie prawo do dostępu do wszystkich wiadomości e-mail w ramach prowadzonej działalności, zgodnie z obowiązującym prawem.
3) **Odpowiedzialność za Bezpieczeństwo Informacji:** Oczekuje się, że użytkownicy służbowej poczty elektronicznej będą postępować z najwyższą ostrożnością, aby zabezpieczyć wszelkie przekazywane informacje przed nieautoryzowanym dostępem, zmianą, utratą lub zniszczeniem. Wszelkie działania, które mogą zwiększyć ryzyko naruszenia bezpieczeństwa danych, powinny być unikane.
4) **Wyłączność Użycia Przydzielonych Adresów:** Każdy pracownik ma prawo korzystać wyłącznie z adresu e-mail, który został mu przydzielony przez organizację. Używanie kont pocztowych przypisanych do innych pracowników, jak również udostępnianie swojej skrzynki pocztowej innym, nieupoważnionym osobom, jest surowo zabronione.
5) **Raportowanie Nieprawidłowości:** W przypadku wystąpienia jakichkolwiek nieprawidłowości w funkcjonowaniu systemu poczty elektronicznej lub pojawienia się

wątpliwości dotyczących bezpieczeństwa używania e-maila, pracownik jest zobowiązany do niezwłocznego zgłoszenia tego faktu kierownikowi jednostki, administratorom serwerów pocztowych oraz inspektorowi ochrony danych.

6) **Ochrona Danych Osobowych:** Wszystkie dane osobowe przesyłane za pośrednictwem poczty elektronicznej muszą być odpowiednio zabezpieczone i zaszyfrowane, najlepiej poprzez wysyłanie ich w załącznikach chronionych hasłem.

5. Ustawienia i Zarządzanie Konfiguracją Wiadomości E-mail

1) **Inicjalne Ustawienia:** Przed rozpoczęciem użytkowania służbowej skrzynki e-mail, każdy pracownik zobowiązany jest do skonfigurowania podstawowych ustawień swojego konta, utworzenia profesjonalnego podpisu e-mail, który powinien być zgodny ze standardami przyjętymi w jednostce.
2) **Autoodpowiedź podczas Nieobecności:** W przypadku planowanej nieobecności (np. urlopu), pracownik jest zobowiązany do aktywacji funkcji autoodpowiedzi, informującej o czasowej niedostępności oraz wskazującej alternatywny kontakt do osoby zastępującej w tym czasie.
3) **Delegowanie Dostępu do Skrzynki:** Ustawienie przekierowania otrzymywanych wiadomości na adres e-mail innego pracownika wymaga uzyskania wcześniejszej zgody bezpośredniego przełożonego. Zgoda ta powinna być udokumentowana pisemnie lub za pomocą e-maila.
4) **Podpisywanie Wiadomości z Ogólnego Adresu:** W przypadku korzystania przez kilku pracowników z jednego, ogólnego adresu e-mail (np. kontakt@urząd.pl), konieczne jest indywidualne podpisywanie się imieniem i nazwiskiem w treści każdej wysyłanej wiadomości, aby zapewnić jasność komunikacji.
5) **Autoodpowiedź po Zakończeniu Współpracy:** W sytuacji ustania stosunku pracy na koncie e-mailowym pracownika zostanie ustawiona autoodpowiedź informująca o zakończeniu zatrudnienia oraz wskazująca kontakt do osoby, która przejmuje obowiązki.
6) **Staranność w Przygotowaniu Wiadomości:** Przy tworzeniu i wysyłaniu każdej wiadomości e-mail, należy zachować szczególną staranność w zakresie dokładności treści, prawidłowego doboru załączników oraz precyzyjnego adresowania do odbiorców. W przypadku wysłania informacji do osoby nieupoważnionej należy bezzwłocznie poinformować o zaistniałej sytuacji Kierownika jednostki i inspektora ochrony danych osobowych.
7) **Zarządzanie Skrzynką Odbiorczą:** Zaleca się regularne przeglądanie i porządkowanie zawartości skrzynki odbiorczej, w tym usuwanie nieaktualnych wiadomości oraz organizowanie pozostałych w odpowiednich folderach w celu ułatwienia zarządzania korespondencją i optymalizacji pracy. Przetwarzanie danych osobowych na kontach pocztowych musi odbywać się zgodnie z przepisami i instrukcją kancelaryjną. Dane osobowe, których przetwarzanie nie jest uzasadnione wykonywanymi zadaniami lub przepisami archiwizacji należy niezwłocznie usunąć.

6. Zarządzanie Bezpieczeństwem Informacji w Komunikacji E-mailowej

1) **Zabezpieczanie Danych Osobowych:** Wszelkie przesyłane dane osobowe, takie jak imiona, nazwiska czy adresy e-mail, a także inne dane muszą być szyfrowane i

przekazywane w formie załączników zabezpieczonych hasłem. Takie podejście zapobiega nieautoryzowanemu dostępowi do informacji, nawet w przypadku przechwycenia wiadomości.

2) **Zabezpieczanie Plików przez Kompresję:** Powszechną metodą ochrony przesyłanych plików jest ich kompresja do formatu archiwum, które następnie zabezpiecza się silnym hasłem. Taki sposób zabezpieczenia dodatkowo minimalizuje ryzyko dostępu do zawartości przez osoby nieuprawnione.
3) **Wymogi dotyczące Haseł:** Hasła stosowane do zabezpieczania dokumentów i archiwów powinny być skomplikowane, unikatowe i nieoparte na słownikowych kombinacjach. Muszą się składać z co najmniej 8 znaków, liter, cyfr oraz znaków specjalnych.
4) **Komunikacja Haseł:** Hasło do zabezpieczonego dokumentu lub archiwum powinno być przekazywane odbiorcy za pomocą alternatywnego kanału komunikacji, np. poprzez rozmowę telefoniczną lub za pomocą innej platformy komunikacyjnej, smsem, co zapobiega jego przechwyceniu.
5) **Stałe Hasła dla Zaufanych Odbiorców:** Możliwe jest uzgodnienie stałego hasła dla ciągłej korespondencji z określonym odbiorcą, co ułatwia proces szyfrowania i dekodowania informacji. Jako alternatywę, można użyć informacji znanej tylko wybranemu odbiorcy jako hasła, które nie będzie wymagało oddzielnej komunikacji. Takie hasło należy okresowo zmieniać, nie rzadziej niż raz na miesiąc.

7. Zasady Adresowania Wiadomości E-mail

1) **Cel Komunikacji:** Każda wysyłana wiadomość powinna być skierowana do określonego odbiorcy lub odbiorców z konkretnym celem. Należy upewnić się, że treść e-maila jest adekwatna do kontekstu komunikacji z daną osobą.
2) **Selekcja Adresatów:** W polu "Do/To" powinni znaleźć się wyłącznie ci adresaci, od których oczekuje się bezpośredniego zaangażowania lub odpowiedzi na treść wiadomości. Jest to kluczowe dla zapewnienia skuteczności komunikacji oraz uniknięcia niepotrzebnego przeciążenia informacyjnego.
3) **Użycie Pola DW/CC:** Dodanie adresata w polu "DW (Do Wiadomości)/CC (Carbon Copy)" oznacza, że otrzymuje on kopię wiadomości w celach informacyjnych. Należy jednak pamiętać, aby używać tego pola z rozwagą, by nie przekazywać informacji osobom, dla których nie jest ona przeznaczona.
4) **Ochrona Prywatności Adresatów:** Wszelkie wiadomości, które ujawniają adresy e-mail wielu odbiorców, powinny być wysyłane z zachowaniem szczególnej ostrożności. Jeśli adresy e-mail odbiorców są służbowe i istnieje świadomość wspólnego zaangażowania w daną sprawę, dopuszczalne jest ich ujawnienie. W przeciwnym razie zaleca się stosowanie pola BCC/UDW, aby chronić prywatność adresatów.
5) **Komunikacja z Nieobecnymi:** W przypadku wysyłania wiadomości do osoby nieobecnej lub rzadko sprawdzającej pocztę, zaleca się skierowanie korespondencji również do osoby odpowiedzialnej za dany obszar lub podejmującej decyzje. Dzięki temu minimalizowane jest ryzyko opóźnień lub braku reakcji na ważne wiadomości.
6) **Masowa Korespondencja:** W przypadku planowania wysyłki masowej korespondencji, należy skonsultować się z działem IT w celu wyboru najbardziej odpowiedniego narzędzia lub oprogramowania, które ułatwi zarządzanie taką komunikacją, zapewniając jej efektywność i zgodność z polityką ochrony danych.

8. Zakazane Praktyki w Użytkowaniu Służbowej Poczty Elektronicznej

W celu zapewnienia profesjonalnej, etycznej i bezpiecznej komunikacji elektronicznej, użytkownikom służbowej poczty elektronicznej wyraźnie zabrania się następujących działań:

1) **Nieodpowiednia Zawartość i Reprezentacja:**
   a) **Nielegalne i Nieodpowiednie Treści:** Zakazane jest tworzenie, wysyłanie lub przechowywanie treści, które mogą być uznane za nielegalne, obraźliwe, dyskryminacyjne lub nieetyczne a także treści o charakterze rasistowskim, seksistowskim, pornograficznym, propagującym terroryzm, oraz wszelkie inne materiały uznawane powszechnie za nieodpowiednie.
   b) **Nieautoryzowana Reprezentacja:** Używanie poczty elektronicznej do reprezentowania pracodawcy bez wyraźnego upoważnienia jest zabronione.
   c) **Prywatna Korespondencja:** Wykorzystywanie służbowej poczty elektronicznej do celów prywatnych, osobistych lub niezwiązanych z działalnością pracodawcy jest niedozwolone.
   d) **Podszywanie się:** Wysyłanie wiadomości e-mail z cudzego konta lub w cudzym imieniu, włączając w to manipulację nagłówkiem "From" / "Od", jest surowo zakazane.
   e) **Masowa Korespondencja:** Ręczne rozsyłanie masowej korespondencji jest niedozwolone. W przypadku konieczności wysłania masowych wiadomości należy skorzystać z narzędzi do mailingu, po uprzedniej konsultacji z działem IT.
   f) **Działania Niezgodne z Prawem:** Wykorzystywanie poczty elektronicznej do jakichkolwiek działań niezgodnych z prawem, nieetycznych lub szkodliwych dla jednostki jest zabronione.
2) **Nieautoryzowany Dostęp i Manipulacja:** Zabrania się przechwytywania, podglądania, zapisywania, modyfikowania lub ujawniania treści wiadomości e-mail należących do innych osób, chyba że jest to uzasadniona konieczność i odbywa się z odpowiednim upoważnieniem.
3) **Użycie Zewnętrznych Kont Pocztowych:** Używanie prywatnych kont pocztowych do celów służbowych jest zakazane.
4) **Przekierowywanie Wiadomości:** Aby zapobiec wyciekom informacji, zabrania się automatycznego przekierowywania wiadomości e-mail do zewnętrznych systemów pocztowych.

Procedura ta stanowi kompleksowy zestaw wytycznych mających na celu zapewnienie, że komunikacja e-mailowa w organizacji jest prowadzona w sposób bezpieczny, profesjonalny i zgodny z najlepszymi praktykami ochrony danych. Jej naruszenie traktowane jest jako naruszenie obowiązków pracowniczych i wiązać będzie się z nałożeniem stosownych kar dyscyplinarnych na pracownika.

STAROSTA
Jan Smak

Załącznik nr 2 do Zarządzenia nr 40/2024 Starosty Tureckiego

w sprawie wprowadzenia w Starostwie Powiatowym w Turku

procedur dotyczących bezpieczeństwa udostępnianych danych osobowych

Procedura Retencji Danych w Systemie Poczty Elektronicznej

Cel Procedury

Celem niniejszej procedury jest określenie zasad zarządzania czasem przechowywania danych osobowych oraz innych informacji w systemie poczty elektronicznej, w celu zapewnienia zgodności z wymogami prawnymi dotyczącymi ochrony danych osobowych oraz ograniczenia czasu przechowywania do okresu niezbędnego dla celów przetwarzania.

1. Zakres i Obowiązki

Procedura obejmuje wszystkich użytkowników systemu poczty elektronicznej w organizacji i nakłada na nich obowiązek przestrzegania zasad retencji danych. Każdy użytkownik jest zobowiązany do aktywnego udziału w procesie zarządzania danymi i odpowiedzialny za eliminację danych niepotrzebnych lub przestarzałych zgodnie z ustalonymi okresami retencji.

2. Zasady Ogólne

Poczta elektroniczna stanowi narzędzie służbowe, przeznaczone wyłącznie do komunikacji służbowej. Zakazuje się wykorzystywania poczty do celów prywatnych.

Użytkownicy zobowiązani są do niezwłocznego usuwania wiadomości e-mail, których okres przechowywania upłynął, zgodnie z określonymi w procedurze okresami retencji.

Procedura dotyczy wszystkich rodzajów wiadomości: przychodzących, wychodzących, roboczych, spamu, oraz wszelkich powiadomień.

3. Okresy Retencji

Okresy retencji są ustalane indywidualnie dla różnych typów korespondencji, w zależności od ich znaczenia, wymogów prawnych, typu sprawy i właściwej instrukcji kancelaryjnej w tym między innymi:

1) Korespondencja związana z udzielaniem odpowiedzi na pytania klientów: przechowywana przez okres 5 lat od zakończenia korespondencji.

2) Korespondencja z kontrahentami: przechowywana przez okres 5 lat od zakończenia współpracy.
3) Zapytania ofertowe - 5 lat od momentu otrzymania oferty.
4) CV - ..... od momentu otrzymania CV, o ile jest prowadzona rekrutacja lub kandydat wyraził zgodę na przechowywanie CV do kolejnych procesów rekrutacji.
5) Zapytania w trybie dostępu do informacji publicznej - ..... od momentu udzielenia odpowiedzi.
6) Żądania związane z przetwarzaniem danych - ..... od momentu zakończenia korespondencji.
7) Korespondencja dotycząca postępowań administracyjnych - ..... od momentu zakończenia korespondencji.
8) Zgłoszenia sygnalistów - ..... od momentu zakończenia korespondencji.
9) Korespondencja wewnętrzna, dotycząca spraw administracyjnych – 5 lat od momentu zakończenia korespondencji.

4. Praktyki Zarządzania Danych

Użytkownicy powinni:

Regularnie przeglądać swoją skrzynkę pocztową w celu identyfikacji i usuwania wiadomości, których okres przechowywania upłynął.

Wykorzystywać funkcjonalności systemu poczty elektronicznej, takie jak grupowanie wiadomości według wątków, oznaczanie wiadomości etykietami oraz korzystanie z automatycznego archiwizowania, aby ułatwić zarządzanie retencją danych.

Usuwać kopie robocze, spam, prywatne wiadomości oraz nieistotne powiadomienia niezwłocznie po ich zidentyfikowaniu.

Pobierać ważne załączniki na dysk zewnętrzny lub wewnętrzny system zarządzania dokumentami przed usunięciem wiadomości e-mail.

5. Monitorowanie i Kontrola

Administrator systemu poczty elektronicznej jest odpowiedzialny za monitorowanie przestrzegania procedury retencji danych przez użytkowników i za wysyłanie okresowych przypomnień o konieczności przeprowadzania retencji danych.

6. Przechowywanie Danych po Zakończeniu Współpracy

Dane z poczty elektronicznej użytkownika są przechowywane przez okres maksymalnie 3 miesięcy po zakończeniu współpracy, pod warunkiem, że były wykorzystywane wyłącznie do celów służbowych.

Aby zapewnić efektywną retencję informacji zawartych w systemie poczty elektronicznej, użytkownik powinien stosować się do następujących praktyk:

1) **Grupowanie Wiadomości:** Wykorzystywanie funkcji grupowania wiadomości według wątków umożliwia lepszą organizację i łatwiejsze zarządzanie korespondencją.
2) **Oznaczanie Wiadomości dla Retencji:** Klasyfikowanie wiadomości lub wątków poprzez nadawanie im odpowiednich etykiet lub przenoszenie do dedykowanych folderów, zgodnie z typem korespondencji, ułatwia identyfikację terminów retencji.
3) **Regularny Przegląd Korespondencji:** Systematyczne, miesięczne przeglądanie korespondencji w celu usunięcia wiadomości, których okres przechowywania wygasł, zgodnie z ustalonymi terminami retencji.
4) **Usuwanie Niepotrzebnych Wiadomości:** Natychmiastowe usuwanie kopii roboczych, wiadomości uznanych za spam, prywatnych oraz innych nieistotnych komunikatów, jak automatyczne powiadomienia.
5) **Wykorzystanie Automatyzacji:** Korzystanie z funkcji automatycznego archiwizowania i usuwania wiadomości, zgodnie z ustalonymi okresami retencji, aby usprawnić proces zarządzania danymi.
6) **Zapisywanie Ważnych Załączników:** Pobieranie istotnych dokumentów załączonych do wiadomości e-mail, takich jak umowy czy wnioski, na dysk. Wiadomości, które nie są już potrzebne, powinny być usuwane po zapisaniu ważnych załączników.
7) **Opróżnianie Kosza:** Regularne, co najmniej raz w miesiącu, opróżnianie folderu z usuniętymi wiadomościami, aby zwolnić miejsce i utrzymać porządek w systemie poczty.

Po zakończeniu współpracy dane z poczty e-mail użytkownika są przechowywane przez ustalony okres, wymagający od użytkownika korzystania z poczty wyłącznie w celach służbowych i niezwłocznego usuwania korespondencji prywatnej.

W związku z utrzymaniem dyscypliny retencji danych, administrator systemu poczty elektronicznej regularnie wysyła przypomnienia do wszystkich użytkowników o konieczności przeglądu i usuwania przestarzałych danych, zgodnie z obowiązującymi procedurami retencji.

Dane zawarte w systemie poczty elektronicznej użytkownika są utrzymywane przez określony czas po zakończeniu współpracy z organizacją, co zobowiązuje użytkownika do odpowiedzialnego zarządzania swoją skrzynką mailową:

STAROSTA
Jan Smak

Opracował: Robert Wojdyła – Inspektor Ochrony Danych Osobowych

Załącznik nr 3 do Zarządzenia nr 40/2024 Starosty Tureckiego
w sprawie wprowadzenia w Starostwie Powiatowym w Turku
procedur dotyczących bezpieczeństwa udostępnianych danych osobowych

Procedura ustalania okresu publikowania treści zawierających dane osobowe w BIP oraz dokonywania przeglądu danych udostępnionych w BIP

1. Wstępna analiza zawartości

Osoba odpowiedzialna za treść przygotowywaną do opublikowania w Biuletynie Informacji Publicznej (BIP) musi upewnić się, czy zawiera ona informacje dotyczące konkretnych lub potencjalnie identyfikowalnych osób fizycznych, czyli dane osobowe

2. Kwalifikacja informacji

Jeśli treść informacji nie obejmuje danych osobowych, pracownik merytoryczny przekazuje ją do redaktora BIP w celu publikacji
Jeżeli treść informacji obejmuje dane osobowe dokonuje się weryfikacji zgodnie z pkt. nr 3 poniżej.

3. Weryfikacja zgodności z przepisami

Gdy informacja zawiera dane osobowe, konieczne jest dokonanie oceny treści informacji, aby ustalić, czy istnieje prawny obowiązek ujawnienia danych osobowych, zgodnie z obowiązującymi przepisami prawa. Przykładowo, taka konieczność może wystąpić przy publikowaniu oświadczeń majątkowych.

Jeśli ustalono podstawę prawną do ujawnienia danych osobowych, należy zweryfikować, czy zakres danych osobowych w informacji jest zgodny z przepisami prawa. W przypadku jakichkolwiek rozbieżności, konieczne jest dokonanie odpowiednich zmian, w szczególności ograniczenia zakresu danych

Po ustaleniu podstawy prawnej, pracownik merytoryczny ustala czas publikacji informacji w Biuletynie Informacji Publicznej (BIP), uwzględniając podstawę prawną ujawnienia danych oraz jednolity rzeczowy wykaz akt obowiązujących w jednostce.

W przypadku wątpliwości co do czasu publikacji, pracownik merytoryczny konsultuje się z archiwistą zatrudnionym w jednostce.

4. Sprawdzenie z Inspektorem Ochrony Danych (IOD)

Inspektor Ochrony Danych (IOD), bazując na przekazanych informacjach, dokonuje weryfikacji zgodności informacji przeznaczonej do publikacji z przepisami dotyczącymi ochrony danych oraz rejestrem czynności przetwarzania.

Informacja, przed przekazaniem do Inspektora Ochrony Danych (IOD), musi być kompletna i zawierać następujące elementy:

1) Podstawę prawną dotyczącą ujawnienia danych osobowych, w tym konkretnie wskazane artykuły lub paragrafy aktu prawnego, które nakładają taki obowiązek,
2) Określenie czasu publikacji informacji w Biuletynie Informacji Publicznej (BIP), aby IOD mógł właściwie ocenić zgodność publikacji z przepisami o ochronie danych.

Pracownik, który przygotował informację, ma obowiązek udzielenia Inspektorowi Ochrony Danych wszelkich potrzebnych wyjaśnień dotyczących przygotowanej treści.

Po zweryfikowaniu informacji, Inspektor Ochrony Danych przekazuje ją, wraz z ustalonym czasem publikacji, pracownikowi merytorycznemu, aby uzyskać jego akceptację jako administratora danych do publikacji informacji w Biuletynie Informacji Publicznej.

5. Akceptacja przez administratora danych

Informacja, która została zaakceptowana, jest przekazywana redaktorowi Biuletynu Informacji Publicznej (BIP) w celu dokonania publikacji.

6. Publikacja

Redaktor Biuletynu Informacji Publicznej (BIP) publikuje informację, ustawiając w systemie zarządzania treścią (CMS) czas, w którym ma być ona widoczna dla użytkowników.

7. Okresowe przeglądy

Okresowe przeglądy treści opublikowanych w Biuletynie Informacji Publicznej (BIP) odbywają się raz w roku, zgodnie z terminem ustalonym przez administratora danych.

8. Zespół odpowiedzialny za przegląd

Za przeprowadzanie przeglądów treści w Biuletynie Informacji Publicznej (BIP) odpowiada zespół składający się z Inspektora Ochrony Danych (IOD) oraz redakcji BIP. Administrator ma również możliwość wyznaczenia innych osób, które będą zaangażowane w czynności związane z przeglądem BIP.

9. Weryfikacja treści

Przeglądowi podlegają wszystkie treści publicznie dostępne w BIP. Zespół odpowiedzialny za przegląd BIP dokonuje weryfikacji opublikowanych treści pod kątem obecności danych, które mogą w sposób pośredni lub bezpośredni ujawniać tożsamość osób fizycznych.

Weryfikacji podlegają również mechanizmy automatycznego archiwizowania/zakończenia czasu publikacji w systemie zarządzania treścią (CMS), oraz poprawność ich ustawiania przez redaktorów Biuletynu Informacji Publicznej (BIP) w chwili publikacji treści.

10. Ocena i usunięcie przestarzałych treści

Jeśli analizowana informacja zawiera dane osobowe, zespół przeprowadza ocenę, czy treści, których czas publikacji minął, powinny zostać usunięte. Ocena ta opiera się na następujących kryteriach:

1) czasie określonym w przepisach prawa, na podstawie których informacja została ujawniona
2) Wymaganiach wynikających z jednolitego rzeczowego wykazu akt w jednostce
3) Rejestrze czynności przetwarzania danych

Opracował: Robert Wojdyła – Inspektor Ochrony Danych Osobowych

4) Czy cel przetwarzania danych osobowych nadal istnieje lub nie

Jeśli zespół ustali, że cel ujawnienia danych osobowych w Biuletynie Informacji Publicznej (BIP) został zrealizowany lub przestał być aktualny, podejmuje decyzję o usunięciu informacji.

11. Raportowanie i usunięcie treści

Z przeglądu jest sporządzany raport, który jest podpisywany przez wszystkie osoby biorące udział w przeglądzie. Po zaakceptowaniu raportu przez administratora danych, redaktorzy Biuletynu Informacji Publicznej (BIP) usuwają informacje wskazane w raporcie z BIP. Wzór raportu stanowi załącznik nr 1 do niniejszej procedury.

STAROSTA
Jan Smak

Załącznik nr 1 do
procedury ustalania okresu publikowania treści
zawierających dane osobowe w BIP
oraz dokonywania przeglądu danych udostępnionych w BIP

RAPORT Z PRZEGLĄDU DANYCH OSOBOWYCH W OŚWIADCZENIACH MAJĄTKOWYCH W BIP

Data przeglądu: .....
Uczestnicy przeglądu:

1. [Imię i nazwisko uczestnika 1] - [Stanowisko]
2. [Imię i nazwisko uczestnika 2] - [Stanowisko]
3. [Imię i nazwisko uczestnika 3] - [Stanowisko]

Opis przeprowadzonego przeglądu: *Przeprowadziliśmy szczegółowy przegląd danych osobowych zawartych w oświadczeniach majątkowych udostępnionych w Biuletynie Informacji Publicznej (BIP). Celem przeglądu było ocenienie zgodności przetwarzania danych osobowych z wymogami Rozporządzenia Ogólnego o Ochronie Danych Osobowych (RODO).*

Szczegółowe wyniki przeglądu:

1. **Identyfikacja danych osobowych:** *Zidentyfikowaliśmy wszystkie dane osobowe zawarte w oświadczeniach majątkowych, takie jak imię, nazwisko, adres zamieszkania, numer identyfikacyjny PESEL, oraz wszelkie inne dane identyfikujące.*
2. **Ocena zgodności z zasadami RODO:** *Przeprowadziliśmy analizę zgodności przetwarzania danych osobowych z zasadami RODO, w tym legalności, celowości, adekwatności, dokładności, ograniczenia przechowywania danych oraz integralności i poufności.*
3. **Ocena zabezpieczeń danych:** *Sprawdziliśmy, czy zastosowane zabezpieczenia danych osobowych są wystarczające i adekwatne do ryzyka związanego z przetwarzaniem danych, w tym oświadczeń majątkowych.*
4. **Identyfikacja niezgodności:** *Zidentyfikowaliśmy wszelkie niezgodności w przetwarzaniu danych osobowych zawartych w oświadczeniach majątkowych oraz potencjalne obszary wymagające poprawy zgodnie z wymogami RODO.*

Wnioski i zalecenia:

Stwierdzenie zgodności: *Informujemy, że przetwarzanie danych osobowych w oświadczeniach majątkowych jest zgodne z przepisami RODO oraz obowiązującymi przepisami prawa. Okresy retencji są zgodne z przepisami prawa.*

LUB

Opracował: Robert Wojdyła – Inspektor Ochrony Danych Osobowych

Stwierdzenie niezgodności: *W związku z przeprowadzonym przeglądem danych osobowych zawartych w oświadczeniach majątkowych za lata ..... udostępnionych w Biuletynie Informacji Publicznej (BIP), Komisja zaleca niezwłoczne usunięcie informacji, dla których ustał już uzasadniony czas publikacji.*
W szczególności dotyczy to informacji dostępnych w zakładce ".....".
Podjęcie działań w celu usunięcia tych danych osobowych jest niezbędne z uwagi na zgodność z obowiązującymi przepisami prawa, w szczególności z Rozporządzeniem Ogólnym o Ochronie Danych Osobowych (RODO), oraz w trosce o zachowanie poufności i integralności danych osobowych.

Monitoring i audyt: *Zalecamy regularne monitorowanie i audyt zgodności z RODO, aby zapewnić ciągłą zgodność z przepisami o ochronie danych osobowych, zwłaszcza w kontekście oświadczeń majątkowych.*

Podpis uczestników komisji:

1. .....
2. .....
3. .....

Okres, którego dotyczy przegląd :
.....

Podstawa prawna przeglądu:
art. 5 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), zwanego dalej RODO, w tym art. 5 ust. 1 lit. c) RODO - zasada minimalizacji danych, art. 5 ust. 1 lit. e) RODO - zasada ograniczenia przechowywania.

Zakres przeglądu:
Rodzaj dokumentu – zakładka .....
Publikowane dane osobowe.....

Wnioski:
Dane są adekwatne, prawidłowe, zgodne z art. 5 RODO i przetwarzane na podstawie art.6 ust.1 lit. c RODO.

Podpis IOD .....

Podpis ADO .....

STAROSTA

Jan Smak

Opracował: Robert Wojdyła – Inspektor Ochrony Danych Osobowych

Załącznik nr 4 do Zarządzenia nr 40/2024 Starosty Tureckiego

w sprawie wprowadzenia w Starostwie Powiatowym w Turku

procedur dotyczących bezpieczeństwa udostępnianych danych osobowych

Procedura inwentaryzacji umów powierzenia przetwarzania

§ 1.

1. Niniejsza procedura ma na celu wprowadzenie zasad inwentaryzacji umów powierzenia przetwarzania danych osobowych, które Administrator Danych Osobowych zawarł z podmiotem zewnętrznym w celu realizacji usługi.
2. Powierzenie odbywa się na podstawie umowy lub innego instrumentu prawnego.

§ 2.

1. Administrator decydując się na powierzenie przetwarzania danych osobowych dokonuje wyboru usługobiorcy- podmiotu przetwarzającego po wcześniejszym:
    1) przeanalizowaniu czy korzystając z usług podmiotu przetwarzającego, podmiot ten zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych zapewniających ochronę powierzonych danych,
    2) Przekazaniu i wypełnieniu przez podmiot przetwarzający ankiety diagnozującej gwarancje, o których mowa w pkt. 1 powyżej,
    3) zaopiniowaniu przez Inspektora Ochrony Danych powierzenia danych osobowych
    4) określeniu w umowie powierzenia obowiązków podmiotu przetwarzającego
    5) zaopiniowaniu umowy powierzenia przez radcę prawnego i inspektora ochrony danych osobowych,
2. Administrator odpowiada za kontrolę przetwarzania danych osobowych, które zostały powierzone procesorowi.

§ 3.

1. Inwentaryzację umów powierzenia przetwarzania przeprowadza się następującymi metodami:

1) ciągłą – polegającą na bieżącym sprawdzaniu i monitorowaniu powierzenia przetwarzania na podstawie przygotowanych przez pracowników Administratora ankiet, pytań kontrolnych i rozmów z podmiotem przetwarzającym,
2) okresową – polegającą na przeprowadzeniu kontroli rzeczywistej umów powierzenia w dniu sprawdzania - audyt
3) doraźną – przeprowadzaną w miarę potrzeb jednostki, np. w przypadku orzeczeń sądu, decyzji Prezesa Urzędu Ochrony Danych Osobowych,
4) wyrywkową – polegającą na ustaleniu stanu rzeczywistego np. podczas audytu zgodności z RODO

2. Zaleca się przeprowadzić:
   1) Co roku - inwentaryzację okresową;
   2) W razie potrzeb - inwentaryzację doraźną oraz wyrywkową.
3. Inwentaryzację przeprowadza się w drodze weryfikacji, poprzez porównanie zawartych umów cywilnoprawnych, zarządzeń lub innych instrumentów prawnych związanych z przekazaniem danych na zewnątrz z Rejestrem Czynności Przetwarzania oraz ich faktyczną weryfikację.
4. Inwentaryzacja ma na celu wykazanie czy pracownik merytoryczny w sposób prawidłowy zakwalifikował daną umowę jako wymagającą zawarcia umowy powierzenia przetwarzania danych osobowych czy nie wymagającą zawarcia umowy powierzenia przetwarzania danych.
5. Każdy pracownik merytoryczny przed przekazaniem danej umowy do podpisu kierownikowi jednostki zobowiązany jest poinformować inspektora ochrony danych osobowych o zawieranych umowach oraz uzyskać opinię IODa o konieczności zawarcia lub nie umowy powierzenia przetwarzania danych
6. Po zinwentaryzowane umowy powierzenia wpisuje się odpowiednią adnotację o inwentaryzacji do Rejestru Umów Powierzenia.
7. W przypadku stwierdzenia, że pracownik w sposób rażący nie przekazał informacji o zamiarze powierzenia przetwarzania danych w sytuacji, gdy w sposób oczywisty taka sytuacja miała miejsce Inspektor Ochrony Danych zgłasza to kierownikowi jednostki, jeśli uzna, że zaniedbanie mogło narazić Administratora na karę lub inną odpowiedzialność.

§ 5

1. Po przeprowadzonej kontroli przedstawia się Administratorowi protokół.

2. W przypadku stwierdzenia braków podpisanej umowy - IOD rekomenduje podpisanie umowy powierzenia przetwarzania lub przyjęcia innego instrumentu prawnego.
3. W przypadku stwierdzenia, że przekazana czynność nie stanowi powierzenia przetwarzania, a dokonano podpisania umowy - IOD wnosi o dostosowanie sytuacji przekazania do stanu prawnego. W takiej sytuacji informuje ADO, że powierzenie przetwarzania nastąpiło bez jego wiedzy i zgody.
4. IOD dokonuje odpowiedniego wpisu do Rejestru Czynności Przetwarzania.

STAROSTA
Jan Smak

Opracował: Robert Wojdyła – Inspektor Ochrony Danych Osobowych