ZARZĄDZENIE NR 119/2023
BURMISTRZA SOŚNICOWIC

z dnia 15 września 2023 r.

w sprawie wprowadzenia Procedury ochrony danych osobowych w ramach pracy zdalnej obowiązującej w Urzędzie Miejskim w Sośnicowicach

Na podstawie 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.U. UE. L. Nr 119, s. 1 ze zm.) zarządzam, co następuje:

§ 1. Procedurę szkolenia osób zaangażowanych w proces przetwarzania informacji obowiązującą w Urzędzie Miejskim w Sośnicowicach określa Załącznik 1 do niniejszego Zarządzenia.

§ 2. Wykonanie zarządzenia powierza się Sekretarzowi Gminy.

§ 3. Zarządzenie wchodzi w życie z dniem podpisania.

z up. Burmistrza
Sośnicowic

Bernard Wilczek

PROCEDURA OCHRONY DANYCH OSOBOWYCH W RAMACH PRACY ZDALNEJ

§ 1. Zakres podmiotowy procedury

1. Procedura ochrony danych osobowych w ramach pracy zdalnej, zwana dalej *„Procedurą”*, określa zasady postępowania z danymi osobowymi, zasady ich zabezpieczenia i ochrony podczas wykonywania pracy zdalnej.
2. Obowiązek stosowania *Procedury* dotyczy każdego pracownika wykonującego pracę zdalną bez względu na tryb jej uruchomienia.

§ 2. Podstawowe pojęcia

1) Pracodawca, administrator – należy przez to rozumieć pracodawcę pracownika wykonującego pracę zdalną;
2) Dane osobowe – należy przez to rozumieć dane osobowe w rozumieniu art. 4 pkt 1) RODO, czyli wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, czyli takiej osobie, 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;
3) IOD – należy przez to rozumieć Inspektora Ochrony Danych, powoływanego przez Administratora zgodnie z art. 37 RODO;
4) Przetwarzanie – należy przez to rozumieć operację lub zestaw operacji określonych w art. 4 pkt 2) RODO, 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; w szczególności, w odniesieniu do niniejszego regulaminu: rejestrowanie, przechowywanie, udostępnianie;
5) Naruszenie ochrony danych osobowych – takie naruszenie bezpieczeństwa, które prowadzi do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
6) RODO – należy przez to rozumieć 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.U. UE. L. Nr 119, s. 1 ze zm.).

§ 3. Dokumentacja ochrony danych osobowych

1. Każdy pracownik wykonujący pracę zdalną jest zobowiązany do stosowania obowiązujących u pracodawcy wewnętrznych aktów dotyczących ochrony informacji i danych osobowych, a także procedur lub instrukcji dotyczących działania systemów informatycznych obowiązujących u pracodawcy, w tym zasad uzyskiwania dostępu, przesyłania, przechowywania i wykonywania obowiązków związanych z przetwarzaniem danych osobowych.

2. W przypadku wątpliwości co do dopuszczalnego postępowania z danymi osobowymi, pracownik, po sprawdzeniu, czy dokumentacja ochrony danych osobowych nie reguluje takiego obszaru, kontaktuje się z wyznaczoną u pracodawcy osobą, tj. IOD, odpowiedzialnym informatykiem lub inną osobą odpowiedzialną za nadzór nad przetwarzaniem danych osobowych.

§ 4. Dostęp do danych osobowych i praca z danymi osobowymi

1. Pracownik wykonujący pracę zdalną, uzyskuje dostęp do danych osobowych, których przetwarzanie jest niezbędne do wykonywania obowiązków pracowniczych. Dostęp do danych osobowych możliwy jest po nadaniu pracownikowi upoważnienia do ich przetwarzania i trwa do momentu ustania zatrudnienia.
2. Nie jest dopuszczalne wykorzystywanie danych osobowych przetwarzanych w ramach pracy zdalnej w innym celu niż wykonywanie obowiązków służbowych.
3. Nie jest dopuszczalne korzystanie i zapisywanie na własnych nośnikach plików zawierających dane osobowe, których administratorem jest pracodawca, bez jego zgody i bez wcześniejszego zabezpieczenia przez dział IT.
4. Pracownik utrzymuje w tajemnicy otrzymane od pracodawcy dane dostępowe, w tym loginy i hasła oraz zabezpiecza je przed dostępem osób nieuprawnionych, w tym domowników. Szczegółowe zasady dotyczące zmiany hasła, jego budowy i przechowywania pracodawca może określić w dokumentacji ochrony danych osobowych.
5. Pracownik jest zobowiązany do pracy w ramach przydzielonego mu konta w systemie informatycznym. Nie jest dopuszczalne udostępnianie konta, loginu, hasła osobom nieuprawnionym, w tym innym pracownikom lub domownikom, ani też korzystanie z konta, loginu, hasła innego pracownika.
6. Dostęp do danych osobowych odbywa się w sposób zdalny i następuje poprzez:
   1) dostęp do skrzynki pocztowej pracownika w domenie pracodawcy;
   2) dostęp do systemu informatycznego przetwarzającego dane osobowe wynikającego z zakresu obowiązków;
   3) dostęp do określonych zasobów w infrastrukturze pracodawcy przy użyciu szyfrowanego połączenia zdalnego (np. VPN).
7. Nie jest dopuszczalne umożliwianie dostępu do danych, poczty elektronicznej lub systemów informatycznych osobom nieuprawnionym, próbującym uzyskać dostęp drogą telefoniczną lub mailową, podającym się za przedstawicieli serwisu lub konkretnych instytucji, bez ich weryfikacji i potwierdzenia w zakładzie pracy takiego kontaktu.
8. Komunikacja służbowa odbywa się w sposób zapewniający bezpieczeństwo informacji i danych osobowych, wyłącznie poprzez wskazane przez pracodawcę narzędzia i połączenia. Jeżeli pracownik przesyła załączniki zawierające dane osobowe muszą być one zaszyfrowane odpowiednim programem (np. zip). Nie należy przesyłać plików z danymi osobowymi (np. w celu pracy z danymi osobowymi), jeżeli możliwy jest dostęp do danych w systemie informatycznym.
9. Każdy pracownik korzystający z poczty elektronicznej jest zobowiązany do:
   1) przechowywania loginu i hasła do poczty elektronicznej w bezpiecznym miejscu, niedostępnym dla osób nieuprawnionych, w tym domowników,
   2) korzystania z poczty elektronicznej wyłącznie w celach służbowych,
   3) archiwizowania korespondencji służbowej przy użyciu dedykowanych temu celowi narzędzi poczty elektronicznej,

4) nieprzesyłania korespondencji służbowej na jakąkolwiek prywatną skrzynką pocztową.

10. Każdy pracownik korzystający z poczty elektronicznej i systemów teleinformatycznych jest zobowiązany do:
    1) stosowania zasad określonych w pkt 10 (powyżej),
    2) nieudostępniania danych dostępowych do systemów informatycznych osobom nieuprawnionym, w tym domownikom,
    3) niepobierania danych osobowych z systemów informatycznych w celu innym niż służbowy,
    4) pobierania i zapisywania tylko niezbędnych dokumentów.

§ 5. Obowiązki podczas spotkań zdalnych, wideokonferencji

1. Organizacja spotkań może nastąpić tylko przy użyciu dostarczonych przez pracodawcę rozwiązań informatycznych.
2. Podczas spotkań przebiegających z ujawnianiem wizerunków należy ograniczyć do minimum rejestrowanie spotkań.
3. W przypadku konieczności udostępniania konkretnych dokumentów podczas spotkań należy zamknąć używane wcześniej inne dokumenty, aplikacje, okna przeglądarek, aby udostępnić uczestnikom spotkania tylko i wyłącznie dedykowany dla nich plik.
4. Wszystkie pliki zapisywane w zespołach lub dedykowanej do tego przestrzeni w aplikacji do wideokonferencji należy cyklicznie przeglądać i usuwać po ustaniu ich przydatności.
5. Linki do wideokonferencji powinny być udostępniane tylko i wyłącznie uczestnikom spotkania, bezpiecznym kanałem komunikacji, zaproszenia powinny być kierowane wyłącznie na służbowe adresy e-mail.

§ 6. Przechowywanie danych osobowych i nośników

1. Pracownik odpowiada za bezpieczne przechowywanie danych osobowych, sprzętu i nośników służących do ich przetwarzania.
2. Nośniki oraz dokumentacja zawierająca dane osobowe nie powinna być pozostawiana bez nadzoru. Po zakończeniu pracy nośniki i dokumentacja powinny być schowane w miejscu zabezpieczonym przed osobami nieuprawnionymi (np. w szafce, szufladzie).

§ 7. Transport sprzętu i nośników danych

1. Pracownik odpowiada za bezpieczeństwo powierzonego mu sprzętu, nośników i dokumentacji podczas ich transportu. W szczególności nie jest dozwolone pozostawianie ich bez nadzoru (np. w środku transportu – samochodzie, komunikacji publicznej).
2. Przewożenie dokumentacji zawierającej dane osobowe powinno odbywać się w sposób zabezpieczający ją przed dostępem osób nieuprawnionych. W tym celu pracownik umieszcza dokumentację w teczce lub skoroszycie uniemożliwiającym zapoznanie się z treścią danych osobowych, a następnie w plecaku lub torbie.

§ 8. Szkolenia

1. Pracownik uczestniczy we wszystkich szkoleniach, warsztatach, instruktażach dotyczących ochrony danych osobowych i bezpieczeństwa informacji organizowanych przez pracodawcę, w tym w ramach pracy zdalnej.

2. Udział pracownika w wyżej wskazanych formach dokształcania ma charakter obowiązkowy oraz aktywny.

§ 9. Zgłaszanie incydentów

1. Każdy pracownik ma obowiązek zgłaszania wszelkich podejrzeń naruszeń ochrony danych osobowych. Pracownik zgłasza incydenty ochrony danych oraz ich podejrzenia osobom odpowiedzialnym w zakładzie pracy za ochronę danych osobowych (IOD lub inna osoba wskazana przez pracodawcę).
2. W przypadku zauważania nieprawidłowości w funkcjonowaniu systemów informatycznych pracownik podejmuje możliwe działania zabezpieczające jednocześnie z powiadomieniem właściwych osób, zgodnie z pkt 1.
3. Szczegółowy sposób postępowania w przypadku zauważenia incydentu ochrony danych określa dokumentacja ochrony danych osobowych obowiązująca u Pracodawcy.

§ 10. Stosowanie zabezpieczeń przez pracowników

Pracownik zobowiązany jest do dbałości o bezpieczeństwo danych osobowych przetwarzanych w ramach wykonywania obowiązków służbowych. W tym celu, podczas codziennej pracy pracownik:

1) ogranicza do niezbędnego minimum drukowanie plików zawierających dane osobowe i do sytuacji, gdy jest to konieczne;
2) niszczy robocze wydruki zawierające dane osobowe po ustaniu ich przydatności dla bieżącej pracy; nie można wyrzucać dokumentów zawierających dane osobowe do kosza, zniszczenie musi mieć charakter nieodwracalny, np. przy użyciu niszczarki lub nożyczek;
3) cyklicznie usuwa niepotrzebne pliki zawierające dane osobowe, pobrane w celu pracy z nimi;
4) przechowuje dokumentację zawierającą dane osobowe w sposób bezpieczny, zamkniętą w teczce, skoroszycie lub segregatorze, w miejscu niedostępnym dla osób postronnych (szafka, szuflada);
5) wylogowuje się z systemów informatycznych po zakończeniu pracy w nich;
6) zabezpiecza ekran przed dostępem innych osób, w tym domowników, poprzez stosowanie wygaszaczy ekranów lub każdorazowe wylogowanie się przed odejściem od ekranu;
7) nie korzysta i nie uruchamia programów i aplikacji pochodzących od nieznanych nadawców;
8) nie udostępnia domownikom komputerów przenośnych przeznaczonych do pracy, a jeżeli komputer stanowi własność pracownika, praca odbywa się wyłącznie na wydzielonych kontach systemowych.

…….

(data, pieczątka, podpis Administratora Danych Osobowych)