ZARZĄDZENIE NR RO.SO.0050.20.2022

BURMISTRZA DOBREJ

z dnia 28 lutego 2022 r.

w sprawie: wprowadzenia **Regulaminu Ochrony Danych Osobowych w Urzędzie Miejskim w Dobrej**

Na podstawie:
- art. 24 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. 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 z 04.05.2016r.),
zarządzam się co następuje:

§ 1.

Wprowadzam do stosowania Regulamin Ochrony Danych Osobowych w Urzędzie Miejskim w Dobrej w brzmieniu stanowiącym **załącznik do niniejszego zarządzenia.**

§ 2.

Zobowiązuje wszystkich pracowników do przestrzegania Regulaminu Ochrony Danych Osobowych, pod groźbą konsekwencji służbowych, przewidzianych prawem.

§ 3.

Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ
DOBREJ
Tadeusz Gebler

Załącznik
do Zarządzenia Nr RO.SO.0050.20.2022
Burmistrza Dobrej
z dnia 28 lutego 2022 r.

Regulamin
Ochrony Danych Osobowych
w Urzędzie Miejskim w Dobrej

Niniejszy regulamin stanowi wykaz podstawowych obowiązków z zakresu przestrzegania zasad ochrony danych osobowych zgodnie z aktualnie obowiązującymi przepisami prawa, w tym w szczególności z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO) dla:

- *Pracowników;*
- *Współpracowników;*
- *Pracowników podmiotów trzecich, posiadających dostęp do danych osobowych przetwarzanych przez Administratora / Podmiot przetwarzający;*
- *Użytkowników systemów informatycznych z dostępem do danych osobowych przetwarzanych przez Administratora/Podmiot przetwarzający.*

Każda z w/w osób powinna zapoznać się z poniższym regulaminem oraz zobowiązać się do stosowania zasad w nim zawartych.

SPIS TREŚCI

1. Zasady bezpiecznego użytkowania sprzętu IT.

1) W przypadku, gdy użytkownik przetwarzający dane osobowe korzysta ze sprzętu IT zobowiązany jest do jego zabezpieczenia przed zniszczeniem lub uszkodzeniem. Za sprzęt IT rozumie się: komputery stacjonarne, monitory, drukarki, skanery, ksera, laptopy, służbowe tablety i telefony.
2) Użytkownik jest zobowiązany zgłosić zagubienie, utratę lub zniszczenie powierzonego mu Sprzętu IT.
3) Samowolne instalowanie, otwieranie (demontaż) sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) lub podłączanie jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego jest zabronione.
4) Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. klientom, pracownikom innych działów) wgląd do danych wyświetlanych na monitorach komputerowych – tzw. Polityka czystego ekranu.
5) Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu (wywołuje się go przez równoczesne naciśnięcie klawiszy „WINDOWS" oraz „L") lub wylogować się z systemu bądź z programu.
6) Po zakończeniu pracy, użytkownik zobowiązany jest:
    a) wylogować się z systemu informatycznego, a jeśli to wymagane - następnie wyłączyć sprzęt komputerowy,
    b) zabezpieczyć stanowisko pracy, w szczególności wszelkie nośniki magnetyczne i optyczne na których znajdują się dane osobowe.
7) Użytkownik jest zobowiązany do usuwania plików z nośników/dysków do których mają dostęp inni użytkownicy nieupoważnieni do dostępu do takich plików (np. podczas współużytkowania komputerów).
8) Jeśli użytkownik jest uprawniony do niszczenia nośników, powinien TRWALE zniszczyć sam nośnik lub trwale usunąć z niego dane (np. zniszczenie płyt DVD w niszczarce, zniszczenie twardego dysku, pendrive młotkiem).
9) Użytkownicy komputerów przenośnych na których znajdują się dane osobowe lub z dostępem do danych osobowych przez Internet zobowiązani są do stosowania zasad bezpieczeństwa zawartych w Regulaminie pracy zdalnej.
10) Dopuszcza się stosowanie szyfrowanych pendrive jedynie dopuszczonych do użytkowania przez Urząd.

2. Zasady bezpiecznego korzystania z oprogramowania.

1) Zobowiązuje się pracowników do korzystania tylko z legalnego oprogramowania wymienionego w ewidencji prowadzonej przez AS. Wzór „Ewidencji oprogramowania – licencji" stanowi załącznik nr 1 do Regulaminu.
2) Użytkownik nie ma prawa kopiować oprogramowania zainstalowanego na Sprzęcie IT przez Pracodawcę / Zleceniodawcę na swoje własne potrzeby ani na potrzeby osób trzecich.
3) Instalowanie jakiegokolwiek oprogramowania na Sprzęcie IT może być dokonane wyłącznie przez osobę upoważnioną.
4) Użytkownicy nie mają prawa do instalowania ani używania oprogramowania innego, niż przekazane lub udostępnione im przez Pracodawcę / Zleceniodawcę. Zakaz dotyczy między innymi instalacji oprogramowania z płyt

CD, programów ściąganych ze stron internetowych, a także odpowiadania na samoczynnie pojawiające się reklamy internetowe.

5) Użytkownicy nie mają prawa do zmiany parametrów systemu, które mogą być zmienione tylko przez osobę upoważnioną.
6) W przypadku naruszenia któregokolwiek z powyższych postanowień Pracodawca / Zleceniodawca ma prawo niezwłocznie i bez uprzedzenia usunąć nielegalne lub niewłaściwie zainstalowane oprogramowanie.
7) Naruszenia wyżej wymienionych ustaleń, ze względu na obowiązujące przepisy prawne, stanowią poważne naruszenie dyscypliny pracy.
8) Każdy z pracowników zobowiązany jest podpisać oświadczenie, stanowiące załącznik nr 2 do niniejszego regulaminu, o przyjęciu do wiadomości i stosowania ustaleń Regulaminu. Oświadczenie wpinane jest do akt osobowych pracowników

3. Zarządzanie uprawnieniami - procedura rozpoczęcia, zawieszenia i zakończenia pracy.

1) Każdy użytkownik (np. komputera stacjonarnego, laptopa, dysku sieciowego, programów w których użytkownik pracuje, poczty elektronicznej) musi posiadać swój własny indywidualny identyfikator (login) do logowania się.
2) Tworzenie kont użytkowników wraz z uprawnieniami (np. komputera stacjonarnego, laptopa, dysku sieciowego, programów w których użytkownik pracuje, poczty elektronicznej) odbywa się na polecenie przełożonych a wykonywane jest przez Administratora Systemu.
3) Konta użytkowników tworzone i anulowane są na podstawie upoważnienia zatwierdzonego przez Administratora – wzór upoważnienia stanowi załącznik nr 3 – Upoważnienie/Anulowanie upoważnienia do przetwarzania danych osobowych w systemie informatycznym lub w zbiorze w wersji papierowej.
4) Użytkownik nie może samodzielnie zmieniać swoich uprawnień (np. zostać administratorem Windows na swoim komputerze).
5) Każdy użytkownik musi posiadać indywidualny identyfikator. Zabronione jest umożliwianie innym osobom pracy na koncie innego użytkownika.
6) Zabrania się pracy wielu użytkowników na wspólnym koncie.
7) Użytkownik (np. komputera stacjonarnego, laptopa, dysku sieciowego, programów w których użytkownik pracuje, poczty elektronicznej) rozpoczyna pracę z użyciem identyfikatora i hasła.
8) Użytkownik jest zobowiązany do powiadomienia Administratora Systemu o próbach logowania się do systemu osoby nieupoważnionej, jeśli system to sygnalizuje.
9) W przypadku, gdy użytkownik podczas próby zalogowania się zablokuje system, zobowiązany jest powiadomić o tym Administratora Systemu.
10) Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. klientom, pracownikom innych działów) wglądu do danych wyświetlanych na monitorach – tzw. Polityka czystego ekranu.
11) Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu lub wylogować się z systemu. Jeżeli tego nie uczyni, po upływie 10 minut system automatycznie aktywuje wygaszacz.

12) Zabrania się uruchamiania jakiejkolwiek aplikacji lub programu na prośbę innej osoby, o ile nie została ona zweryfikowana jako pracownik komórki informatyki. Dotyczy to zwłaszcza programów przesłanych za pomocą poczty elektronicznej lub wskazanych w formie odnośnika internetowego.
13) Po zakończeniu pracy, użytkownik zobowiązany jest:
    a) wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy,
    b) zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe.

4. Polityka haseł.

1) Hasła powinny składać się z np. 8 znaków.
2) Hasła powinny zawierać duże litery + małe litery + cyfry (lub znaki specjalne).
3) Hasła nie mogą być łatwe do odgadnięcia. Nie powinny być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion i nazwisk osób bliskich, imion zwierząt, popularnych dat, popularnych słów, typowych zestawów: 123456.
4) Hasła nie powinny być ujawnianie innym osobom. Nie należy zapisywać haseł na kartkach i w notesach, nie naklejać na monitorze komputera, nie trzymać pod klawiaturą lub w szufladzie
5) W przypadku ujawnienia hasła –należy natychmiast go zmienić.
6) Hasła muszą być zmieniane co 30 dni.
7) Jeżeli system nie wymusza zmiany haseł, użytkownik zobowiązany jest do samodzielnej zmiany hasła.
8) Użytkownik systemu w trakcie pracy w aplikacji może zmienić swoje hasło.
9) Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności.
10) Zabrania się używania w serwisach internetowych takich samych lub podobnych haseł jak w systemie komputerowym firmy.

5. Zabezpieczenie dokumentacji papierowej z danymi osobowymi.

1) Upoważnieni pracownicy są zobowiązani do stosowania tzw. „Polityki czystego biurka". Polega ona na zabezpieczaniu (zamykaniu) dokumentów oraz nośników np. w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych po godzinach pracy lub podczas ich nieobecności w trakcie godzin pracy.
2) Upoważnieni pracownicy zobowiązani są do niszczenia dokumentów i wydruków w niszczarkach lub utylizacji ich w specjalnych bezpiecznych pojemnikach z przeznaczeniem do bezpiecznej utylizacji.
3) Zabrania się pozostawiania dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami, np. w korytarzach, na kserokopiarkach, drukarkach, w pomieszczeniach konferencyjnych.
4) Zabrania się wyrzucania niezniszczonych dokumentów na śmietnik lub porzucania ich na zewnątrz, np. na terenach publicznych miejskich lub w lesie.

8) Zabrania się samowolnego podłączania do komputerów modemów, telefonów komórkowych i innych urządzeń dostępowych (np.: typu BlueConnect, iPlus, OrangeGo). Zabronione jest też łączenie się przy pomocy takich urządzeń z Internetem w chwili, gdy komputer użytkownika podłączony jest do sieci firmowej.

8. Zasady korzystania z poczty elektronicznej.

1) Przesyłanie danych osobowych z użyciem maila poza organizację może odbywać się tylko przez osoby do tego upoważnione.
2) W przypadku przesyłania informacji wrażliwych wewnątrz organizacji bądź wszelkich danych osobowych poza organizację należy wykorzystywać mechanizmy kryptograficzne (hasłowanie wysyłanych plików, podpis elektroniczny).
3) W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 8 znaków: duże i małe litery i cyfry lub znaki specjalne a hasło należy przesłać odrębnym mailem lub inną metodą, np. telefonicznie lub SMS-em.
4) Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
5) Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.
6) WAŻNE: Nie należy otwierać załączników (plików) w mailach nadesłanych przez nieznanego nadawcę lub podejrzanych załączników nadanych przez znanego nadawcę.
7) WAŻNE: Nie należy otwierać stron internetowych wskazanych hiperlinkami w mailach, gdyż mogą to być hiperlinki do stron zainfekowanych lub niebezpiecznych.
8) Należy zgłaszać informatykowi przypadki podejrzanych emaili.
9) Użytkownicy nie powinni rozsyłać za pośrednictwem maila informacji o zagrożeniach dla systemu informatycznego, „łańcuszków szczęścia", itp.
10) Użytkownicy nie powinni rozsyłać, maili zawierających załączniki o dużym rozmiarze.
11) Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW".
12) Użytkownicy powinni okresowo kasować niepotrzebne maile.
13) Mail jest przeznaczony wyłącznie do wykonywania obowiązków służbowych.
14) Zakazuje się wysyłania korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych osób.
15) Zabrania się użytkownikom poczty elektronicznej konfigurowania swoich kont pocztowych do automatycznego przekierowywania wiadomości na adres zewnętrzny.
16) Przy korzystaniu z maila, Użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego.
17) Użytkownicy nie mają prawa korzystać z maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.
18) Użytkownik bez zgody Pracodawcy / Zleceniodawcy nie ma prawa wysyłać wiadomości zawierających dane osobowe dotyczące Pracodawcy / Zleceniodawcy, jego pracowników, klientów, dostawców lub kontrahentów za

pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej.

9. Ochrona antywirusowa.

1) Użytkownicy zobowiązani są do skanowania plików wprowadzanych z zewnętrznych nośników programem antywirusowym.
2) Zakazane jest wyłączanie systemu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe.
3) W przypadku stwierdzenia zainfekowania systemu lub pojawienia się komunikatów „np.; Twój system jest zainfekowany!, zainstaluj program antywirusowy", użytkownik obowiązany jest poinformować niezwłocznie o tym fakcie Administratora Systemu lub osobę upoważnioną.

10. Skrócona instrukcja postępowania w przypadku naruszenia ochrony danych osobowych.

1) Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadomienia Pracodawcy / Zleceniodawcy w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych.
2) Do sytuacji wymagających powiadomienia, należą:
   a) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
   b) niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
   c) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).
3) Do incydentów wymagających powiadomienia, należą:
   a) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
   b) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych),
   c) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).
4) Typowe przykłady incydentów wymagające reakcji:
   a) ślady na drzwiach, oknach i szafach wskazują na próbę włamania,
   b) dokumentacja jest niszczona bez użycia niszczarki,
   c) fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie,
   d) otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe,
   e) ustawienie monitorów pozwala na wgląd osób postronnych w dane osobowe,

6. Zasady wynoszenia nośników z danymi poza firmę/organizację.

1) 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, pendrive.
2) Dane osobowe wynoszone poza organizację na nośnikach elektronicznych muszą być zaszyfrowane (szyfrowane dyski, zahasłowane pliki).
3) Należy zapewnić bezpieczne przewożenie dokumentacji papierowej w plecakach, teczkach.
4) Należy korzystać ze sprawdzonych firm kurierskich.
5) W przypadku, gdy dokumenty przewozi pracownik, zobowiązany jest do zabezpieczenia przewożonych dokumentów przed zagubieniem i kradzieżą.
6) W sytuacji przekazywania nośników z danymi osobowymi poza obszar organizacji można stosować następujące zasady bezpieczeństwa:
    a) adresat powinien zostać powiadomiony o przesyłce,
    b) dane przed wysłaniem powinny zostać zaszyfrowane, a hasło podane adresatowi inną drogą,
    c) stosować bezpieczne koperty depozytowe,
    d) przesyłkę należy przesyłać przez kuriera.

7. Zasady korzystania z Internetu.

1) Użytkownik zobowiązany jest do korzystania z Internetu wyłącznie w celach służbowych.
2) Zabrania się zgrywania na dysk twardy komputera oraz uruchamiania jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą osoby upoważnionej do administrowania infrastrukturą IT (np. AS) i tylko w uzasadnionych przypadkach.
3) Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu.
4) Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo (na większości stron tego typu jest zainstalowane szkodliwe oprogramowanie infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem).
5) Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.
6) W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą "https:". Dla pewności należy „kliknąć" na ikonkę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel.
7) Należy zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku, portalu społecznościowego, e-sklepu, poczty mailowej) lub podania naszych loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet. Szczególnie tyczy się to żądania podania takich informacji przez rzekomy bank.

f) wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz organizacji bez upoważnienia Pracodawcy / Zleceniodawcy,
g) udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej i ustnej,
h) telefoniczne próby wyłudzenia danych osobowych,
i) kradzież, zagubienie komputerów lub CD, twardych dysków, Pen-drive z danymi osobowymi,
j) maile zachęcające do ujawnienia identyfikatora i/lub hasła,
k) pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów,
l) hasła do systemów przyklejone są w pobliżu komputera.

5) W pozostałych przypadkach należy postępować zgodnie z Zarządzeniem nr RO.SO.0050.52.2019 Burmistrza Dobrej z dnia 6 kwietnia 2019 roku w sprawie wprowadzenia instrukcji postępowania w przypadku naruszenia ochrony danych osobowych w Urzędzie Miejskim w Dobrej.

11. Obowiązek zachowania poufności i ochrony danych osobowych.

1) Każda z osób dopuszczona do przetwarzania danych osobowych jest zobowiązana do:
   a) przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez Pracodawcę / Zleceniodawcę zadaniach,
   b) zachowania w tajemnicy danych osobowych do których ma dostęp w związku z wykonywaniem zadań powierzonych przez Pracodawcę / Zleceniodawcę,
   c) niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez Pracodawcę / Zleceniodawcę,
   d) zachowania w tajemnicy sposobów zabezpieczenia danych osobowych,
   e) ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem.
2) Osoba dopuszczona do przetwarzania odbywa szkolenie z zasad ochrony danych osobowych.
3) Osoby zapoznane z treścią niniejszego Regulaminu ODO lub przeszkolone zobowiązane są podpisać Oświadczenie o poufności.
4) Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym lub osobom których tożsamości nie można zweryfikować lub osobom podszywającym się pod kogoś innego.
5) Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać się jasną podstawą prawną do dostępu do takich danych.
6) Zabrania się ujawniania na grupach dyskusyjnych, forach internetowych, blogach itp. jakichkolwiek szczegółów dotyczących funkcjonowania organizacji, w tym informacji na temat sprzętu i oprogramowania, z jakiego korzysta organizacja, oraz informacji kontaktowych innych, niż ogólnodostępne w materiałach zewnętrznych.

12. Postępowanie dyscyplinarne.

1) Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy.
2) Postępowanie sprzeczne z powyższymi zobowiązaniami, może też być uznane przez Pracodawcę / Zleceniodawcę za naruszenie przepisów karnych zawartych w ogólnym Rozporządzeniu o ochronie danych UE z dnia 27 kwietnia 2016 r.

13. Postanowienia końcowe.

1) Odpowiedzialnymi za realizację Instrukcji są wszyscy pracownicy mający dostęp do systemu komputerowego.
2) Za aktualizację niniejszej Instrukcji odpowiedzialny jest Administrator Systemu.
3) Nadzór nad realizacją Instrukcji pełni Inspektor Ochrony Danych /IOD/.
4) Instrukcja wchodzi w życie z dniem podpisania.

14. Specyfikacja dokumentacji dodatkowej – załączników.

1) Załącznik nr 1: Specyfikacja ewidencji oprogramowania – licencji,
2) Załącznik nr 2: Oświadczenie pracownika – przyjęcie do wiadomości i stosowania zapisów Zarządzenia,
3) Załącznik nr 3: Upoważnienie /Anulowanie upoważnienia do przetwarzania danych osobowych w systemie informatycznym oraz w zbiorze w wersji papierowej,
4) Załącznik nr 4: Metryka komputera.

BURMISTRZ
DOBREJ
Tadeusz Gebler

Załącznik Nr 1 do Regulaminu Ochrony Danych Osobowych w Urzędzie Miejskim w Dobrej

Specyfikacja ewidencji oprogramowania – licencji

Lp.	Nazwa	Wydawca	Opis	Liczba	Numer inwentaryzacyjny

BURMISTRZ
DOBREJ
Tadeusz Gebler

Załącznik Nr 2 do Regulaminu Ochrony Danych Osobowych w Urzędzie Miejskim w Dobrej

imię i nazwisko

stanowisko służbowe

OŚWIADCZENIE

Oświadczam, że przyjąłem/przyjęłam do wiadomości i stosowania przepisy Zarządzenia Nr __ z dnia .... r., a w szczególności, iż w Urzędzie Miejskim w Dobrej istnieje całkowity zakaz:

- samodzielnego podłączania jakichkolwiek urządzeń oraz nośników zewnętrznych do służbowych komputerów;
- dokonywania nieuprawnionych zmian w systemach informatycznych lub informacji w nich przetwarzanych;
- dokonywania nieuprawnionych prób testowania zauważonych podatności (luk w zabezpieczeniu systemu);
- dokonywania nieuprawnionych prób wyjaśniania incydentów;
- wykorzystywania Internetu i poczty elektronicznej do celów innych niż służbowe, a w szczególności:
  1) uznanych powszechnie za szkodliwe, niewłaściwe, niemoralne lub nielegalne;
  2) ściągania z Internetu i rozsyłania przy pomocy poczty elektronicznej informacji niezwiązanych z realizowanymi zadaniami służbowymi;
  3) nieprzestrzegania praw autorskich w stosunku do materiałów zamieszczonych w sieci;
  4) wprowadzania nieuprawnionych zmian w zatwierdzonej konfiguracji bazowej, stosowania nielegalnego oprogramowania, nieupoważnionego logowania się poza nominalnymi godzinami pracy (chyba, że pracownik posiada zgodę na inny czas pracy), prób dostępu do plików i folderów do których użytkownik nie ma dostępu;
- nieuprawnionego pozyskiwania informacji o zasobach informatycznych i środkach ich ochrony;
- nieuprawnionego instalowania oprogramowania, zwłaszcza oprogramowania, którego jednostka organizacyjna nie ma prawa używać np. z powodu braku wymaganych licencji.

Sprzęt informatyczny winien być użytkowany wyłącznie w celach służbowych. Na stanowiskach pracy mogą być wykorzystywane wyłącznie oprogramowania legalne oraz zawierające dane niezbędne do wykonywania zadań służbowych.

Instalacje oprogramowania na stanowiskach pracy w Urzędzie Miejskim w Dobrej dokonywane są z nośników znajdujących się w zasobach ww. jednostki przez upoważnione osoby.

Wykorzystywanie Internetu i poczty elektronicznej, a także infrastruktury sieciowej jest monitorowane. Wszelkie nieprzestrzeganie przepisów i ustaleń w przedmiotowym zakresie stanowić będzie poważne naruszenie obowiązków służbowych oraz dyscypliny pracy. Podejmowanie nieuprawnionych działań mogących obniżyć poziom bezpieczeństwa infrastruktury teleinformatycznej, wynikających z niezastosowania się do

reguł, o których mowa w niniejszym zarządzeniu, będzie uznane za działanie na szkodę Urzędu Miejskiego w Dobrej, jak również stanowić będzie naruszenie obowiązków pracowniczych i może być przyczyną pociągnięcia do odpowiedzialności służbowej lub karnej.
Za zainstalowane oprogramowania na serwerach Urzędu Miejskiego w Dobrej odpowiada Administrator Systemu. Administrator Systemu prowadzi kontrolę legalności oprogramowania, do której mogą być wykorzystywane programy kontrolne.

Nadzór nad wykonywaniem przepisów zarządzenia sprawuje Inspektor Ochrony Danych.

Zapoznanie się z w/w poleceniami potwierdzam własnoręcznym podpisem:

miejscowość	data	podpis składającego oświadczenie

BURMISTRZ
DOBREJ
Tadeusz Gebler

Załącznik Nr 3 do Regulaminu Ochrony Danych Osobowych w Urzędzie Miejskim w Dobrej

UPOWAŻNIENIE/ANULOWANIE UPOWAŻNIENIA*
do przetwarzania danych osobowych

w systemie informatycznym oraz w zbiorze w wersji papierowej

Z dniem ..... upoważniam/anuluję Upoważnienie

Panią/Pani/Pana*.....

Zatrudnionej/zatrudnionego w .....

(nazwa jednostki organizacyjnej)

a) do obsługi systemu informatycznego wg metryki komputera nr ...

w zakresie: ..... danych osobowych.

(WG) wglądu, (W) wprowadzania, (M) modyfikacji, (U) usuwania, (A) archiwizacji

b) do obsługi zbioru w wersji papierowej w zakresie pełnionych obowiązków służbowych na zajmowanym stanowisku.

Zobowiązuję Panią/Pana do przestrzegania przepisów dotyczących ochrony danych osobowych oraz wprowadzonych i wdrożonych do stosowania przez Administratora Danych „Polityki Bezpieczeństwa Informacji" oraz „Instrukcji zarządzania systemem informatycznym".

....

(miejscowość i data) (podpis Administratora Danych)

Wypełnia Administrator danego systemu:

Identyfikator użytkownika: .....

Data zarejestrowania w systemie: .....**

Data wyrejestrowania użytkownika
(zablokowania dostępu) z systemu: .....***

Podpis Administratora Systemu: .....

*) niepotrzebne skreślić
**) wypełnić w przypadku wydania upoważnienia
***) wypełnić w przypadku anulowania upoważnienia

BURMISTRZ DOBREJ
Tadeusz Gebler

Załącznik Nr 4 do Regulaminu Ochrony Danych Osobowych w Urzędzie Miejskim w Dobrej

Metryka komputera nr:

Data: ...

Komputer:

Numer Inwentarzowy:	
Referat:	
Nazwa:	

Użytkownik:

Imię, Nazwisko:	
E-mail:	
Nazwa Użytkownika:	

Sprzęt:

Urządzenie	Opis	Numer seryjny
Procesor		
RAM		
HDD		
VGA		
Audio		
Modem		
LAN		
Płyta		

System operacyjny:

Nazwa	Numer seryjny

Oprogramowanie:

Producent	Produkt	Numer seryjny

Pracownik oświadcza, że będzie korzystał jedynie z oprogramowania wymienionego w "metryce komputera".

.....

podpis Pracownika

Pracodawca oświadcza, iż wyposażył stanowisko pracy Pracownika w oprogramowanie komputerowe, wymienione w "metryce komputera", na używanie którego posiada aktualne licencje.

.....

podpis Pracodawcy

BURMISTRZ
DOBREJ
Tadeusz Gebler