Zmiany w wydaniu 15 dotyczą dodania zasad przetwarzania danych osobowych w związku z wykonywaniem pracy zdalnej.

OPIS POSTĘPOWANIA

Każdy pracownik Urzędu, praktykant i stażysta (dalej w instrukcji jako „pracownik") jest obowiązany przestrzegać zasad bezpieczeństwa informacji oraz zasad ochrony danych osobowych zawartych w tej instrukcji. Nieprzestrzeganie poniższych zasad stanowi ciężkie naruszenie obowiązków pracowniczych i może spowodować poniesienie przez pracownika, stażystę lub praktykanta konsekwencji określonych w obowiązujących przepisach.

Kierownik komórki organizacyjnej ma obowiązek egzekwować przestrzeganie w podległej komórce zapisów niniejszej instrukcji oraz utrzymywać aktualność zapisu potwierdzającego fakt zapoznania się przez podległych pracowników, stażystów i praktykantów z treścią tej instrukcji i zobowiązania do przestrzegania jej postanowień (wzór oświadczenia w formie listy stanowi załącznik nr 1 do instrukcji.

Niezachowanie w tajemnicy informacji wewnętrznych określonych jako tajemnica pracodawcy oraz zasad ochrony danych osobowych stanowi ciężkie naruszenie przez pracownika Urzędu Miasta Płocka, stażystę lub praktykanta obowiązków pracowniczych i może spowodować poniesienie przez pracownika, stażystę lub praktykanta konsekwencji określonych w obowiązujących przepisach.

Pracodawca ma prawo kontrolować niezależnie od czasu pracy poszczególne pomieszczenia biurowe Urzędu Miasta Płocka oraz ich wyposażenie, powierzone pracownikom, pod względem przestrzegania przez pracowników zasad bezpieczeństwa informacji.

1. Polityka kluczy i zasady przebywania na terenie Urzędu Miasta Płocka, zwanego dalej „Urzędem"

1) Pracownik Urzędu może pobrać tylko te klucze do pomieszczeń, do których został on upoważniony. Lista osób upoważnionych do pobrania danego klucza znajduje się na stanowisku ochrony właściwym dla danego budynku. Kierownik komórki organizacyjnej jest zobowiązany do przekazania do Wydziału Techniczno – Gospodarczego informacji o osobach upoważnionych do pobrania kluczy w podległej komórce. Za kompletność i poprawność listy odpowiedzialny jest wyznaczony pracownik Wydziału Techniczno - Gospodarczego.
2) Klucze do pomieszczeń należy zdać po zakończeniu pracy na stanowisku ochrony właściwym dla danego budynku.
3) Klucze do mebli biurowych przeznaczonych do przechowywania aktywów informacyjnych należy zabezpieczyć w pomieszczeniu indywidualnie, ujawniając miejsce zabezpieczenia wyłącznie współpracownikom z danego pomieszczenia. Sposób zabezpieczenia kluczy powinien uniemożliwiać osobom postronnym łatwe znalezienie kluczy, a tym samym dostanie się do zawartości mebli.

4) Klucze do podręcznych magazynków, będących w dyspozycji komórek organizacyjnych mogą być przechowywane w pomieszczeniach tych komórek, pod warunkiem zapewnienia właściwego zabezpieczenia, analogicznie do kluczy do mebli z aktywami informacyjnymi.
5) Zapasowe klucze do pomieszczeń przechowywane są w Wydziale Techniczno - Gospodarczym.
6) Pokój należy chronić przed nieuprawnionym dostępem. W szczególności zakazane jest pozostawianie otwartego, niedozorowanego pomieszczenia lub osoby trzeciej (interesanta) samego w pomieszczeniu.
7) Kody do pomieszczeń wyposażonych w elektroniczny system kontroli dostępu lub system alarmowy należy bezwzględnie chronić przed ujawnieniem innym osobom. Postępowanie z kodami systemów dostępu reguluje odrębna instrukcja ZSZ.
8) Zabronione jest zostawianie klucza w drzwiach po zewnętrznej stronie, także w czasie obecności pracownika w pokoju, oraz po wewnętrznej stronie - w przypadku, gdy drzwi pozostają otwarte (np. dla zapewnienia cyrkulacji powietrza).
9) Przy opuszczaniu pomieszczeń wyposażonych w system alarmowy należy ten system aktywować.

2. Rodzaje informacji

1) Wszystkie informacje w Urzędzie, których dotyczy niniejsza instrukcja, niezależnie od ich formy utrwalenia (papierowa, elektroniczna), zostały podzielone na trzy grupy o takich samych poziomach ochrony, ale różnych zasadach udostępniania.

Kategoria główna	Kategoria podrzędna I
Informacje jawne	Informacje publicznie dostępne
Informacje wewnętrzne	Informacje wewnętrzne dostępne
	Informacje wewnętrzne wrażliwe
	Tajemnica pracodawcy
Informacje chronione	Informacje chronione ustawowo

- **Informacje publicznie dostępne –** oznaczają informacje dostępne dla każdego obywatela (publikowane w Biuletynie Informacji Publicznej lub udostępniane na wniosek w trybie ustawy o dostępie do informacji publicznej).
- **Informacje wewnętrzne dostępne** – oznaczają informacje dostępne w organizacji dla wszystkich pracowników (zwykle publikowane w wewnętrznej sieci intranetowej).
- **Informacje wewnętrzne wrażliwe** – oznaczają informacje dostępne w organizacji dla części pracowników (zwykle publikowane w wewnętrznej sieci intranetowej pod linkiem zabezpieczonym hasłem dostępu).
- **Tajemnica pracodawcy –** oznacza informacje chronione w organizacji, których ujawnienie może narazić pracodawcę na szkodę.
- **Informacje chronione ustawowo** – informacje określone w ustawie o ochronie informacji niejawnych, ustawie o ochronie danych osobowych oraz inne tajemnice prawnie chronione.

2) Lista grup informacji, zakwalifikowanych jako „Tajemnica pracodawcy", zawarta jest w tabeli stanowiącej **załącznik nr 2** do instrukcji.
3) Szczególne zasady postępowania z informacjami podlegającymi ochronie na podstawie przepisów prawa powszechnego określają te przepisy oraz regulacje wewnętrzne wydane w celu określenia sposobu ich stosowania w Urzędzie.
4) Dokumenty w Urzędzie oznacza się zgodnie z przyporządkowaną im kategorią informacji.
5) Na terenie Urzędu obowiązuje **zasada czystego biurka**, co oznacza, że wszelkie dokumenty (bez względu na ich przynależność do danej grupy informacji) należy po zakończeniu pracy zabezpieczyć przed nieuprawnionym dostępem w meblach zamykanych na klucz. Zasada ta nie dotyczy pokoi o statusie szafy. W pokojach tych osoby trzecie wykonujące prace na rzecz Urzędu (sprzątanie, prace instalacyjne, itp.) mogą przebywać tylko w obecności pracowników z danego pokoju.
6) W każdym obszarze kontrolowanym przez Urząd obowiązuje **zasada wolnej drukarki**, co oznacza, że wszelkie wydruki (bez względu na ich przynależność do danej grupy informacji) należy zabrać z drukarki bezpośrednio po wydrukowaniu.
7) W przypadku konieczności pozbycia się dużej ilości danych utrwalonych w formie papierowej (bez względu na ich przynależność do danej grupy informacji), należy je opakować w karton lub mocny foliowy worek, oznaczyć etykietą „do zniszczenia" i przekazać do Archiwum zakładowego.
8) Aktywa informacyjne są przechowywane w zamkniętych pomieszczeniach. Po godzinach pracy należy je zabezpieczyć w zamykanych na klucz meblach (dotyczy pomieszczeń sprzątanych po godzinach pracy). Wynoszenie poza miejsce przechowywania, kopiowanie, udostępnianie wewnątrz Urzędu (np. do innej komórki organizacyjnej) oraz udostępnianie na zewnątrz (poza Urząd) musi być poprzedzone zgodą bezpośredniego przełożonego. Niszczenie tych informacji musi być wykonywane obowiązkowo w niszczarce do dokumentów. Informacje w wersji elektronicznej, w razie konieczności należy skasować z dysku lub nośnika zewnętrznego.
9) Postępowanie z informacjami, których poziom ochrony zdefiniowano jako „Tajemnica pracodawcy" wiąże się z obowiązkiem zachowania dodatkowych reguł, określanych dla każdej informacji bądź grupy informacji przez właściwego kierownika komórki organizacyjnej (właściciela aktywów odpowiedzialnego za ich bezpieczeństwo) – zależnie od sposobu przetwarzania, miejsca przechowywania i innych specyficznych okoliczności mających wpływ na bezpieczeństwo tych informacji. Sposób określenia i zakomunikowania pracownikom tych reguł należy do uznania kierownika komórki organizacyjnej.

3. Zasady dotyczące korzystania z nośników elektronicznych

1) Zabronione jest używanie nośników nie będących własnością pracodawcy.
2) Używanie pamięci przenośnych np. pendrive, stanowiących zarówno własność pracodawcy jak i klientów, wymaga każdorazowego przeskanowania programem antywirusowym.
3) Wszystkie nośniki zawierające jakiekolwiek dane stanowiące własność pracodawcy muszą być chronione przed utratą (np. zagubieniem, kradzieżą itp.) poprzez chowanie ich po zakończonym dniu pracy do zamkniętych mebli. Nośniki należy szczególnie chronić w trakcie przebywania poza obszarem kontrolowanym

przez Urząd. Nośniki danych można wynosić poza obszar kontrolowany przez Urząd jedynie jeżeli jest to niezbędne z uwagi na wykonywane obowiązki służbowe.
4) Należy bezwzględnie przestrzegać zasad prawidłowej eksploatacji nośników określonych przez producenta (nie narażanie na nadmierną ekspozycję promieni światła, wahań temperatury, silnych pól elektromagnetycznych).
5) Należy dbać o to, by dane nie podlegały nadmiernej dystrybucji. Należy usuwać z nośników dane nieistotne, nieaktualne oraz takie, których przechowywanie nie jest już w żaden sposób uzasadnione. W przypadku, gdy danych nie da się usunąć z nośnika (np. w przypadku płyt CD), nośnik należy zniszczyć.
6) Niszczenie nośników przeprowadza się w specjalnie przystosowanych do tego niszczarkach. Nośniki typu pendrive oraz wszelkie inne nie podlegające zniszczeniu przez użytkownika nośniki należy przekazać do Referatu Teleinformatyki.
7) Bez względu na zawartość, nośniki uszkodzone należy zniszczyć w sposób opisany powyżej. Należy pamiętać, że uszkodzone nośniki również podlegają ochronie do czasu ich zniszczenia.

4. Zasady korzystania z komputerów osobistych

1) Komputer osobisty jest własnością pracodawcy i może być wykorzystywany wyłącznie w celach służbowych (dotyczy również komputerów przekazanych Urzędowi przez inne podmioty).
2) Pracodawca ma prawo kontrolować sposób korzystania przez pracowników ze służbowego sprzętu komputerowego.
3) Na komputerze można pracować wyłącznie na swoim indywidualnym koncie, lub w przypadku kont do użytku ogólnego (np. Dysponent, Internet) koncie ogólnym przyznanym przez Referatu Teleinformatyki. Stacje robocze, komputery przenośne oraz systemy informatyczne wykorzystywane w Urzędzie muszą być zabezpieczone przed nieuprawnionym dostępem poprzez zastosowanie w systemie operacyjnym odpowiedniego hasła. Musi ono spełniać poniższe wymagania chyba, że zasady zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Urzędzie stanowią inaczej lub za zgodą IOD Kierownik Referatu Teleinformatyki w udokumentowanej formie dopuścił odstępstwo, zapewniając za pomocą innych rozwiązań utrzymanie odpowiedniego poziomu zabezpieczeń.

Zasady prawidłowo skonstruowanych haseł:

a) składa się z co najmniej 8 znaków,
b) ma małe i wielkie litery, cyfry i znaki specjalne jednocześnie,
c) wszystkie hasła ustawione domyślnie przez producenta lub dostawcę muszą być zmienione,
d) hasła startowe nadane przez Administratorów należy zmienić podczas pierwszego logowania,
d) zmiana hasła następuje nie rzadziej niż co 30 dni,
e) zabrania się zapisywania hasła pod programowalnym klawiszem,
f) w przypadku ujawnienia hasła należy je bezzwłocznie zmienić,
g) zabrania się wielokrotnego wykorzystania tych samych haseł (zmienione hasło nie może być identyczne z którymś z ostatnich 5 haseł),
h) należy chronić hasło przed ujawnieniem podczas wpisywania,

i) hasła nie mogą być łatwe do zidentyfikowania, czyli **należy unikać**: imion, nazwisk rodziny, dzieci i znajomych, popularnych nazw komputerowych, dat urodzenia, nazw użytkowników komputerów, wyrazów złożonych z sekwencji odczytywanej z klawiatury (np qwerty), żadnych z powyższych pisanych wspak lub z dołączoną cyfrą,

j) da się je łatwo zapamiętać bez potrzeby ich zapisywania.

4) Pozostałe zasady dotyczące haseł:

a) nigdy nie przyklejaj kartek z hasłem na monitorze, pod klawiaturą, ani w żadnym innym miejscu w pobliżu komputera,

b) nie wykorzystuj pamięci przeglądarki do zapamiętywania hasła dostępowego do wykorzystywanych systemów informatycznych oraz podpisu elektronicznego,

c) w przypadku pięciokrotnie błędnie wpisanego hasła do systemu Mdok, konto użytkownika zostaje automatycznie zablokowane,

d) odblokowanie konta dokonywane jest przez uprawnionego administratora systemu Mdok na wniosek użytkownika przesłany za pomocą HelpDesku lub w przypadku braku dostępu do HelpDesku - za pomocą poczty elektronicznej na adres: pomocmdok@plock.eu.

5) Użytkownik komputera nie może instalować oraz usuwać oprogramowania bez zgody Referatu Teleinformatyki. Niedopuszczalne jest również uruchamianie oprogramowania „bezinstalacyjnego" typu „Portable" oraz jego przechowywania na stacjach roboczych.

6) Na komputerze Urzędu nie można przechowywać żadnych plików naruszających prawa własności intelektualnej lub inne regulacje prawne (np. zachęcających do popełnienia przestępstwa, szerzących nienawiść rasową itp.).

7) Przy opuszczaniu stanowiska pracy komputer musi zostać zablokowany tak, by przed ponownym rozpoczęciem pracy konieczne było ponowne wpisanie hasła. Aby zablokować komputer należy wcisnąć jednocześnie klawisze [ALT] + [CTRL] + [DEL], a następnie wybrać opcję „zablokuj komputer" lub nacisnąć jednocześnie klawisze WIN + L.

8) Zabronione są wszelkie ingerencje w sprzęt komputerowy i oprogramowanie, w szczególności dotyczy to:

a) modyfikowania konfiguracji sprzętowej komputera, ustawień BIOS,

b) niszczenia lub usuwania plomb gwarancyjnych i oznaczeń,

c) modyfikowania lub usuwania plików będących częścią systemu operacyjnego lub oprogramowania zainstalowanego na komputerze,

d) uruchamiania systemów LiveCD z nośników CD/DVD oraz pamięci typu Flash.

9) Użytkownik powinien wykonywać kopie zapasowe danych, które nie posiadają wersji elektronicznej w systemie Mdok, a są istotne dla ciągłości działania komórki. Nośniki CD/DVD do wykonywania kopii i przechowywania danych są udostępniane przez Wydział Techniczno - Gospodarczy. Wszelkie wykonane kopie muszą być odpowiednio zabezpieczone przed dostępem osób niepowołanych oraz oznaczone w sposób umożliwiający identyfikację zawartości nośnika (imię, nazwisko, opis danych, czas sporządzenia kopii). Systemy dziedzinowe oraz poczta elektroniczna nie wymagają dodatkowej archiwizacji przez pracownika.

10) Zabrania się pracownikom Urzędu kopiowania bądź wysyłania pocztą elektroniczną danych będących własnością pracodawcy, bez zgody bezpośredniego przełożonego.

5. Polityka korzystania z mobilnych urządzeń teleinformatycznych

1) Dla komputerów przenośnych obowiązują także wszystkie zasady zdefiniowane dla komputerów osobistych.
2) Pracownik dysponujący komputerem przenośnym stanowiącym własność pracodawcy, może go wynosić poza budynek Urzędu tylko jeśli posiada do tego stosowne upoważnienie. Lista osób upoważnionych przez Kierownika Referatu Teleinformatyki do wynoszenia komputerów przenośnych poza budynki Urzędu znajduje się w Referacie Teleinformatyki. Upoważnienie jest wydawane przez Kierownika Referatu Teleinformatyki na pisemny wniosek właściwego kierownika komórki organizacyjnej lub Prezydenta bądź właściwego Zastępcę Prezydenta, Sekretarza i Skarbnika, jeśli wniosek dotyczy kierowników komórek organizacyjnych, wskazujący informacje podlegające przechowywaniu bądź przetwarzaniu na komputerze przenośnym. Kierownik Referatu Teleinformatyki wydając upoważnienie w razie potrzeby poleca dostosowanie poziomu zabezpieczeń komputera przenośnego do warunków pracy poza siedzibą Urzędu.
3) Nośniki danych komputerów przenośnych podlegają obowiązkowemu szyfrowaniu.
4) Należy chronić komputer przenośny przed fizycznym uszkodzeniem poprzez zachowanie odpowiednich warunków eksploatacji oraz środków ostrożności w trakcie jego użytkowania i transportu.
5) Należy chronić komputer przenośny / tablet/ smartfon przed kradzieżą lub zagubieniem poprzez zachowanie odpowiednich środków ostrożności, w szczególności nie pozostawiać go bez opieki w miejscach publicznych, pokojach hotelowych, salach konferencyjnych, przedziałach pociągów lub w samochodach w widocznym miejscu.
6) W przypadku kradzieży komputera przenośnego należy niezwłocznie powiadomić bezpośredniego przełożonego oraz Pełnomocnika ds. ZSZ. Jeżeli zdarzenie nastąpiło poza siedzibą Urzędu należy niezwłocznie powiadomić policję. Jeżeli w komputerze przenośnym znajdowały się dane osobowe należy niezwłocznie powiadomić Inspektora Ochrony Danych.
7) Zabrania się pracownikom Urzędu kopiowania, bez zgody bezpośredniego przełożonego, na prywatne mobilne urządzenia teleinformatyczne danych stanowiących własność bądź powierzonych pracodawcy.
8) W przypadku przechowywania na prywatnym urządzeniu mobilnym takich danych pracownik ma obowiązek zachowania szczególnej ostrożności podczas korzystania z urządzenia mobilnego w miejscach publicznych, salach konferencyjnych i innych niezabezpieczonych obszarach. Zaleca się stosowanie środków ochrony, aby uniknąć nieautoryzowanego dostępu do tych urządzeń lub ujawnienia informacji przechowywanych i przetwarzanych przez te urządzenia.
9) Pracodawca zastrzega sobie prawo, z uwzględnieniem prawa użytkownika do prywatności, do usunięcia z urządzenia mobilnego danych stanowiących własność pracodawcy, gdy użytkownik przestanie być uprawniony do dostępu do informacji.
10) Zabrania się pracownikom Urzędu korzystania z prywatnych mobilnych urządzeń teleinformatycznych w godzinach pracy, z wyjątkiem przerw określonych Regulaminem pracy oraz sytuacji zgłoszonych bezpośredniemu przełożonemu lub Inspektorowi Ochrony Danych. Korzystanie w godzinach pracy z prywatnych tabletów i laptopów w celach innych niż służbowe (np. przeglądanie plików multimedialnych, uczestniczenie w portalach o charakterze społecznościowym i towarzyskim, korzystanie z serwisów internetowych niezwiązanych z obowiązkami pracowniczymi) stanowi naruszenie dyscypliny pracy.

6. Zasady korzystania z poczty elektronicznej

1) Poczta elektroniczna powinna być wykorzystywana do celów służbowych w ramach czynności realizowanych na rzecz Urzędu.
2) Osoba korzystająca z poczty elektronicznej jest odpowiedzialna za poufność przekazywanych oraz przechowywanych w ten sposób informacji.
3) Osoba korzystająca z poczty elektronicznej jest odpowiedzialna za poufność hasła dostępowego do swojego konta pocztowego. Hasło musi zostać zmienione w przypadku ujawnienia lub podejrzenia zaistnienia takiego faktu.
4) Poczta elektroniczna nie może być wykorzystywana wbrew interesom Urzędu, w szczególności chronionym w myśl ustawy o ochronie informacji niejawnych oraz ochronie danych osobowych. Nie może być również wykorzystywana do czynów noszących znamiona przestępstwa. Pracodawca zastrzega sobie prawo dostępu do zawartości poczty służbowej pracowników.
5) W przypadku otrzymania przesyłki oznaczonej jako spam bądź noszącej znamiona spamu należy dokonać weryfikacji na podstawie nadawcy, tematu oraz załącznika. Należy ze szczególną ostrożnością traktować wszystkie przesyłki otrzymane od nadawców, z którymi nie prowadzono dotychczas korespondencji, bądź od których przesyłka nie jest oczekiwana.
6) Niedozwolone jest otwieranie odnośników (linków) umieszczonych w wiadomościach e-mail, o ile nie prowadzą one do treści, których bezpieczeństwo jest wiadome użytkownikowi (np. linki do informacji na stronach instytucji sektora administracji publicznej oraz innych zweryfikowanych nadawców).
7) Wszelkie podejrzane wiadomości, lub załączniki muszą być niezwłocznie zgłoszone do Referatu Teleinformatyki w celu weryfikacji. Użytkownik ponosi pełną odpowiedzialność za ewentualne szkody powstałe w wyniku uruchomienia szkodliwego skryptu.
8) Zawartość przesyłek przekazywanych za pośrednictwem poczty elektronicznej nie może zawierać treści szkodliwych lub obraźliwych, takich jak: pornografia, propagowanie przemocy, nawoływanie do rasizmu, terroryzmu itp. Użytkownik poczty elektronicznej jest zobowiązany do usuwania przesyłek zawierających wyżej wymienione treści lub takich, co do których ma podejrzenie, że stanowią one zagrożenie wirusowe. Zakazane jest rozprzestrzenianie przesyłek o wyżej wymienionym charakterze.
9) W przypadku przesyłania danych osobowych poza organizację należy wysyłać pliki zaszyfrowane lub spakowane (np. programem 7-Zip, WinZip, WinRar) i zabezpieczone hasłem, przy czym hasło powinno być przesłane do odbiorcy innym kanałem dystrybucyjnym np. telefonicznie lub SMS
10) W przypadku konieczności zapewnienia poufności przesyłanych danych w drodze ochrony kryptograficznej, należy skontaktować się z Referatem Teleinformatyki, który dokona szyfrowania danych, jego ekspedycji oraz odbierze od adresata potwierdzenie otrzymania danych, lub dokona modyfikacji klienta poczty, umożliwiającej użytkownikowi samodzielne stosowanie przyjętych w Urzędzie technik kryptograficznych.
11) Podczas wysyłania maili do wielu adresatów jednocześnie, **użytkownik zobowiązany jest** użyć funkcji „Ukryte do wiadomości – UDW”. Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości”.

7. Zasady bezpiecznego korzystania z zasobów sieci www

1) Korzystanie z zasobów sieci www powinno być związane z czynnościami wykonywanymi przez pracownika w ramach powierzonych zadań.
2) Pracownik – niezależnie od zabezpieczeń stosowanych na poziomie organizacji – jest zobowiązany do przestrzegania następujących zasad:
   a) niedozwolone jest pobieranie jakichkolwiek treści niezwiązanych z czynnościami służbowymi,
   b) w przypadku okien pop-up (reklamy) należy zamknąć je, nie klikając na zawartość,
   c) zabrania się rejestracji i logowania się na stronach budzących podejrzenie co do bezpieczeństwa informacji oraz uruchamiania wszelkich skryptów, programów, apletów mogących prowadzić do zainfekowania komputera. Użytkownik ponosi odpowiedzialność za ewentualne następstwa naruszenie w/w zasad.

8. Zasady korzystania z sieci komputerowej

1) W sieci komputerowej Urzędu znajdować się mogą tylko i wyłącznie zasoby informatyczne będące własnością Urzędu, wszelkie inne muszą posiadać autoryzację odpowiedniego kierownika oraz wyznaczonego pracownika Referatu Teleinformatyki.
2) Zakazana jest ingerencja w strukturę sieci, w szczególności jej samodzielna rozbudowa lub przebudowa oraz podejmowanie jakichkolwiek czynności mogących negatywnie wpłynąć na bezpieczeństwo (np. używanie skanerów sieciowych).

9. Zasady informowania interesantów przez telefon i pocztę elektroniczną

1) Drogą telefoniczną lub poprzez pocztę elektroniczną można udzielać wyłącznie informacji o klauzuli „Informacje jawne". Zabronione jest w szczególności przekazywanie jakichkolwiek informacji wymagających identyfikacji odbiorcy, np. haseł do kont pocztowych, danych osobowych. Nie jest dopuszczalne stosowanie jakichkolwiek odstępstw od tej zasady, uwarunkowanych statusem odbiorcy (np. osoba zajmująca wysokie stanowisko w hierarchii służbowej, nawet jeśli jest znana dysponentowi informacji i uważa on, iż zidentyfikował rozmówcę - kierownik komórki organizacyjnej, radny Rady Miasta Płocka, Prezydent Miasta Płocka), bądź kontekstem sytuacyjnym (potrzeba "natychmiastowego" dostępu do informacji).
2) Powyższe nie dotyczy informacji zabezpieczonych kryptograficznie za pomocą oprogramowania dopuszczonego do stosowania w Urzędzie.
3) W przypadku prośby o przekazanie powyższych informacji należy poinformować osobę o konieczności zwrócenia się w formie pisemnej lub stawienia się osobiście.

10. Sposób zgłaszania incydentów naruszających bezpieczeństwo informacji, w tym bezpieczeństwo danych osobowych

1) Każdy pracownik Urzędu zobowiązany jest do zgłaszania incydentów bezpieczeństwa. W celu zgłoszenia zauważonego incydentu należy skontaktować się w dowolny sposób (HelpDesk, rozmowa telefoniczna, e-mail) z pracownikiem Zespołu Systemów Zarządzania / IOD / Referat Teleinformatyki.

2) Lista przykładowych incydentów bezpieczeństwa informacji (nie jest to lista zamknięta):

- ✔ znaleziono klucze do pomieszczenia / kartę zbliżeniową
- ✔ nieprawidłowe działanie systemu kontroli dostępu (uszkodzony zamek, niedziałający system kontroli dostępu)
- ✔ niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów
- ✔ pozostawiony klucz w drzwiach
- ✔ naruszenie zasady czystego biurka i wolnej drukarki
- ✔ włamanie do Urzędu, kradzież sprzętu w organizacji
- ✔ pożar, powódź lub inne szkodliwe działania sił natury
- ✔ włamanie do systemu, kradzież informacji Urzędu
- ✔ atak wirusowy na system teleinformatyczny
- ✔ podejrzenie ujawnienia hasła dostępu
- ✔ nieautoryzowane usunięcie / modyfikacja danych
- ✔ udostępnienie, w dowolnej formie, danych osobowych osobom nieupoważnionym
- ✔ znalezienie niezabezpieczonego nośnika z danymi
- ✔ zagubienie dokumentów lub nośników z danymi osobowymi
- ✔ obecność plików naruszających ustawę o prawie autorskim i prawach pokrewnych / plików o treściach naruszających inne regulacje prawne (np. zachęcających do popełnienia przestępstwa, szerzących nienawiść rasową itp.)
- ✔ inne incydenty związane z systemem teleinformatycznym.

3) O awariach związanych z funkcjonowaniem systemów teleinformatycznych (np.: awaria komputera, awaria zasilania, awaria sieci) należy niezwłocznie poinformować pracownika Referatu Teleinformatyki.

4) W przypadku stwierdzenia incydentów naruszających bezpieczeństwo przetwarzania danych osobowych należy niezwłocznie powiadomić Inspektora Ochrony Danych.

11. Sposób zgłaszania niewłaściwego funkcjonowania oprogramowania lub dysfunkcji sprzętu komputerowego

1) W przypadku stwierdzenia niewłaściwego funkcjonowania oprogramowania lub stwierdzenia dysfunkcji sprzętu komputerowego należy:

a) odnotować objawy problemu oraz wszelkie komunikaty pojawiające się na ekranie (np. za pomocą zrzutu ekranu z wykorzystaniem klawisza PrntScr),

b) przerwać korzystanie ze stacji roboczej i niezwłocznie powiadomić Referat Teleinformatyki za pomocą systemu HelpDesk na stronie helpdesk.plock.eu,

c) dopuszczalne jest zgłaszanie uszkodzeń droga telefoniczną tylko w przypadku braku możliwości dokonania zgłoszenia poprzez system HelpDesk.

2) Bezwzględnie zabronione jest samodzielne ingerowanie w niewłaściwie funkcjonujące oprogramowanie bądź jakiekolwiek komponenty systemu operacyjnego.

3) W przypadku stwierdzenia niewłaściwego funkcjonowania oprogramowania służącego do przetwarzania danych osobowych należy niezwłocznie powiadomić Inspektora Ochrony Danych.

12. Wybrane zasady bezpieczeństwa pożarowego

1) Każdy pracownik Urzędu, bez względu na zajmowane stanowisko i pełnioną funkcję, ma obowiązek zapoznać się i przestrzegać ustaleń i zasad zawartych w instrukcjach bezpieczeństwa pożarowego dla poszczególnych budynków Urzędu.

2) Na terenie budynków Urzędu zabrania się:

a) włączania do sieci gwarantowanej urządzeń innych niż jednostki centralne komputerów oraz monitory,

b) posługiwania się odbiornikami energii z otwartą spiralą grzejną oraz bez wyłączników termicznych,

c) opuszczania pomieszczeń z pozostawionymi bez nadzoru odbiornikami energii, które nie są przystosowane do pracy ciągłej,

d) wychodzenia z pomieszczeń bez sprawdzenia, czy nie zachodzi niebezpieczeństwo powstania pożaru lub wybuchu,

e) układanie przewodów zasilających odbiorniki energii elektrycznej pod wykładzinami oraz zwiniętych w zwojach,

f) używania otwartego ognia i palenia papierosów poza wyznaczonym miejscem.

3) Szczegółowe zasady postępowania z urządzeniami elektrycznymi po zakończeniu pracy i opuszczeniu pomieszczeń biurowych:

a) czajnik elektryczny jest urządzeniem bezpiecznym pod warunkiem użytkowania go zgodnie z instrukcją obsługi. Zaleca się jednak, przed opuszczeniem miejsca pracy, zestawienie ostudzonego czajnika z podstawy grzejnej i pozostawienie podstawy podłączonej do prądu;

b) urządzenia typu chłodziarka, kuchenka mikrofalowa i ekspres do kawy są odbiornikami przystosowanymi do pracy ciągłej (nie wymagają odłączania od zasilania);

c) w przypadku podłączenia do listwy zasilająco–filtrującej urządzeń elektrycznych nieprzystosowanych do pracy ciągłej należy odłączyć je przyciskiem „włącz-wyłącz" znajdującym się na listwie, bez konieczności odłączania listwy z gniazda zasilającego;

d) **komputery, drukarki oraz skanery** są urządzeniami przystosowanymi do pracy ciągłej. Urządzenia te po zakończeniu pracy muszą zostać wyłączone przyciskiem funkcyjnym, nie należy odłączać urządzeń od zasilania;

e) **bazy telefonów** są przystosowane do stałego podłączenia do zasilania. Baza telefonu musi być zasilana ponieważ służy jako ładowarka bezprzewodowej słuchawki telefonu;

f) **niszczarki** należy wyłączać z gniazd sieciowych;

g) **urządzenia wielofunkcyjne**, tak jak i zwykłe drukarki, powinny być na stałe podłączone do zasilania. Ich codzienne wyłączanie, a zwłaszcza odłączanie od zasilania na kilka dni, może spowodować ich uszkodzenie. Urządzenia po zakończeniu pracy muszą zostać wyłączone tylko przyciskiem funkcyjnym, nie należy odłączać urządzeń od zasilania;

h) **ładowarki smartfonów/tabletów** - zalecane jest odłączanie ładowarek po każdorazowym naładowaniu urządzenia i nie pozostawianie ich podłączonych do sieci przez dłuższy okres czasu co może powodować nagrzewanie się ładowarki i w konsekwencji może być przyczyną pożaru. Problem dotyczyć może szczególnie tanich ładowarek podatnych na awarie i nie przeznaczonych do pracy ciągłej.

13. Ogólne zasady przetwarzania danych osobowych w Urzędzie Miasta Płocka

1) Kierownicy komórek organizacyjnych sprawują bieżącą kontrolę zasad ochrony przetwarzania danych osobowych określonych w przepisach prawa i uregulowaniach wewnętrznych.
2) Kierownik komórki organizacyjnej stwarza właściwe warunki organizacyjno-techniczne gwarantujące bezpieczeństwo przetwarzania danych osobowych w podległej mu komórce organizacyjnej.
3) Kierownik komórki organizacyjnej:
   a) określa pomieszczenia, w których przetwarzane są dane osobowe,
   b) wyznacza użytkowników danych osobowych,
   c) zgłasza Inspektorowi Ochrony Danych :
      • zamiar rozpoczęcia przetwarzania nowych zbiorów danych osobowych,
      • zmiany skutkujące powstaniem obowiązku aktualizacji rejestru czynności przetwarzania prowadzonego przez Inspektora Ochrony Danych (podstawa prawna, cel przetwarzania, zakres przetwarzanych danych, kategorie osób których dane dotyczą, kategorie odbiorców danych, okres przechowywania danych) oraz rejestru kategorii czynności przetwarzania (dane administratora, kategorie przetwarzań dokonywanych w imieniu administratora);
      • wystąpienie naruszenia ochrony danych osobowych.
4) Kierownik komórki organizacyjnej zgłasza Administratorowi Danych Osobowych:
   a) **konieczność** wydania upoważnienia do przetwarzania danych osobowych,
   b) **konieczność** zmiany zakresu upoważnienia do przetwarzania danych osobowych,
   c) **zmianę danych** personalnych osoby posiadającej upoważnienie do przetwarzania danych osobowych,
   d) **konieczność** odebrania upoważnienia do przetwarzania danych osobowych,
   e) **wystąpienie** naruszenia ochrony danych osobowych.

14. Inspektor Ochrony Danych

Inspektor Ochrony Danych:

1) monitoruje zgodność przetwarzania danych osobowych z regulacjami dotyczącymi ochrony danych osobowych;
2) opracowuje i aktualizuje dokumentację przetwarzania danych osobowych oraz monitoruje przestrzeganie zasad w niej określonych;
3) informuje administratora danych osobowych oraz pracowników przetwarzających dane osobowe o obowiązkach ciążących na nich na mocy przepisów o ochronie danych osobowych ;
4) monitoruje szkolenie osób upoważnionych do przetwarzania danych osobowych z zakresu przepisów o ochronie danych osobowych;
5) prowadzi rejestr czynności przetwarzania danych osobowych oraz rejestr kategorii czynności przetwarzania w Urzędzie Miasta Płocka;
6) prowadzi rejestr naruszeń ochrony danych osobowych;
7) udziela, na żądanie, zaleceń co do oceny skutków dla ochrony danych i monitoruje jej wykonanie;
8) przygotowuje pisemne upoważnienia do przetwarzania danych osobowych;

9) prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych;
10) współpracuje z organem nadzorczym ;
11) opiniuje projekt umowy powierzenia przetwarzania danych osobowych;
12) pełni funkcję punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem.

15. Podstawowe zasady przetwarzania danych osobowych:

1) Zakres uprawnień i obowiązków użytkowników określa treść upoważnienia oraz indywidualny zakres czynności.
2) Ekrany monitorów, na których wyświetlone są dane osobowe, muszą być ustawione w sposób uniemożliwiający osobom postronnym wgląd w dane.
3) W przypadku pracy w innym programie niż program przetwarzający dane osobowe, użytkownik zobowiązany jest do wylogowania się z programu przetwarzającego dane osobowe.
4) Użytkownicy mają obowiązek zgłaszania kierownikowi komórki organizacyjnej wszelkich incydentów mogących wpłynąć na naruszenie bezpieczeństwa ochrony danych osobowych.
5) Tradycyjne (ręczne) zbiory danych osobowych oraz materiały źródłowe dla baz zinformatyzowanych muszą być przechowywane w meblach zamykanych na klucz. W sytuacjach uzasadnionych formą zbioru i sposobem jego przetwarzania (np. dokumentacja budowlana) dopuszcza się odstąpienie od tego wymogu pod warunkiem odpowiedniego zabezpieczenia pomieszczenia w trakcie pracy i po jej zakończeniu (sprzątanie wyłącznie w godzinach pracy, w obecności jednego z pracowników, wykluczona obecność osób postronnych).
6) Obowiązuje bezwzględny zakaz używania nośników informatycznych bez uprzedniego sprawdzenia ich za pomocą programu antywirusowego.
7) Pomieszczenia, w których przetwarzane są dane osobowe muszą być zamykane podczas nieobecności w nich osób upoważnionych.
8) Osoby postronne mogą przebywać w pomieszczeniach, w których znajdują się dane osobowe, tylko w obecności osób upoważnionych.
9) Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym wglądu do danych wyświetlanych na monitorach komputerowych – tzw. Polityka czystego ekranu.
10) Każdy użytkownik systemu informatycznego przetwarzającego dane osobowe posiada unikalny identyfikator, bez którego praca w systemie nie jest możliwa.
11) Bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.
12) Hasło użytkownika wymaga zmiany co najmniej raz na miesiąc.
13) Hasła użytkownika, umożliwiające dostęp do oprogramowania przetwarzającego dane osobowe, utrzymuje się w tajemnicy również po upływie ich ważności.
14) Kierownik komórki organizacyjnej jest zobowiązany do niezwłocznego informowania kierownika Referatu Teleinformatyki o każdej zmianie zakresu uprawnień podległych pracowników do dostępu do systemu teleinformatycznego przetwarzającego dane osobowe (rozwiązanie umowy o pracę, zmiana zakresu przetwarzania danych osobowych, cofnięcie upoważnienia do przetwarzania danych osobowych).

16. Powierzenie przetwarzania danych osobowych

1) Przetwarzanie danych osobowych może zostać powierzone innemu podmiotowi.
2) Dane osobowe mogą być powierzone wyłącznie podmiotom, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi przepisów z zakresu ochrony danych osobowych.
3) Kierownik komórki organizacyjnej powinien być w stanie wykazać, że podmiot przetwarzający spełnia warunek określony w ust. 2. Spełnienie warunku można wykazać poprzez wskazanie, że np.: podmiot przetwarzający jest podmiotem wyspecjalizowanym w świadczeniu określonej kategorii usług; podmiot przetwarzający wdrożył politykę prywatności; podmiot przetwarzający jest zobowiązany do przestrzegania tajemnicy zawodowej.
4) Umowa powierzenia musi mieć formę pisemną i określać jej przedmiot, czas trwania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, prawa i obowiązki administratora.
5) Dopuszczalne jest stosowanie klauzuli powierzenia przetwarzania danych osobowych w umowach głównych, jeżeli powierzenie przetwarzania jest tylko jednym z elementów umowy.
6) Inspektor Ochrony Danych opiniuje projekt umowy powierzenia przetwarzania danych osobowych. Fakt powierzenia przetwarzania danych osobowych odnotowywany jest w rejestrze umów prowadzonym w Urzędzie.

17. Upoważnienie do przetwarzania danych osobowych

1) Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez Administratora Danych Osobowych.
2) Kierownik komórki organizacyjnej lub osoba przez niego upoważniona, przekazuje Administratorowi Danych Osobowych pisemny wniosek o potrzebie nadania /odebrania upoważnienia z podaniem danych personalnych pracownika (imienia, nazwiska), określeniem zbioru danych, którego upoważnienia ma dotyczyć i okresu czasu na jaki ma być wydane (wzór wniosku stanowi **załącznik nr 3** do instrukcji).
3) Zakres upoważnienia do przetwarzania danych osobowych wynika z indywidualnego zakresu czynności każdego pracownika.
4) Upoważnienie przygotowuje Inspektor Ochrony Danych i przekazuje do podpisania Administratorowi Danych Osobowych.
5) Inspektor Ochrony Danych prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych.
6) Odebranie upoważnienia do przetwarzania danych osobowych następuje w przypadku zmiany zakresu obowiązków skutkującej zaprzestaniem przetwarzania danych osobowych.
7) Odebranie upoważnienia następuje w takim samym trybie jak przy wydaniu upoważnienia.
8) Odebranie lub modyfikacja uprawnień użytkownika w systemie informatycznym służącym do przetwarzania danych osobowych następuje w przypadku rozwiązania umowy o pracę, bądź zmiany zakresu obowiązków związanych z przetwarzaniem danych osobowych – w zakresie tej zmiany.

9) Odebranie lub modyfikacja uprawnień użytkownika w systemie informatycznym następuje w takim samym trybie jak przy nadawaniu uprawnień.

18. Obowiązki użytkowników:

1) Wszystkich użytkowników obowiązuje:
   a) obowiązek przetwarzania danych osobowych wyłącznie w zakresie i celu określonym w powierzonych do realizacji zadaniach,
   b) zakaz wykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań,
   c) obowiązek ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych oraz przetwarzaniem,
   d) zakaz udostępniania i umożliwiania dostępu do danych osobowych osobom nie posiadającym stosownego upoważnienia,
   e) zamykanie drzwi i okien po zakończeniu pracy,
   f) zdawanie kluczy na portiernię po zakończeniu pracy,
   g) zakaz wynoszenia z Urzędu komputerów, na których znajdują się zbiory danych osobowych,
   h) informowanie o zauważonym incydencie, mogącym mieć wpływ na bezpieczeństwo przetwarzania danych osobowych,
   i) stosowania wprowadzonych zabezpieczeń,
   j) przetwarzanie danych osobowych zgodnie z obowiązującymi zasadami,
   k) zakaz ujawniania hasła,
   l) zakaz utrwalania hasła w sposób umożliwiający jego kompromitację,
   ł) zmiana hasła zgodnie z przyjętą polityką haseł, w przypadku gdy system sam nie wymusza zmiany.
2) Wszyscy użytkownicy zobowiązani są do zachowania w tajemnicy:
   a) danych osobowych, w których przetwarzaniu brali udział,
   b) szczegółów struktury i funkcjonowania systemu informatycznego przetwarzającego dane osobowe,
   c) zasad ochrony danych osobowych,
   d) mechanizmów stosowanych do identyfikacji i uwierzytelniania użytkownika.

19.Udostępnianie danych osobowych

1) Dane osobowe udostępniane są osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.
2) Dane osobowe, poza danymi wymienionymi w art. 9 i 10 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 (dalej zwane RODO) mogą być udostępnione innym osobom lub podmiotom niż wymienionym w pkt 1, jeżeli spełniają one co najmniej jedną z przesłanek przetwarzania danych osobowych określonych w art. 6 RODO, a udostępnienie danych nie naruszy praw i wolności osób, których dane dotyczą.

3) Dane osobowe udostępnia się na pisemny, umotywowany wniosek, który zawiera informacje umożliwiające wyszukanie w zbiorze żądanych danych, ich zakres i przeznaczenie.
4) O udostępnieniu danych osobowych decyduje Kierownik komórki organizacyjnej, w której dane są przetwarzane.
5) Kierownik komórki organizacyjnej prowadzi rejestr udostępnień danych osobowych zawierający informacje kiedy, komu, jakie dane zostały udostępnione i na jakiej podstawie prawnej.

20. Bezpieczeństwo danych osobowych

1) Każdy użytkownik danych osobowych ma obowiązek niezwłocznego powiadomienia kierownika komórki organizacyjnej o wszelkich nieprawidłowościach w działaniu systemu informatycznego służącego do przetwarzania danych osobowych, mogących wskazywać na możliwe naruszenie zabezpieczenia systemu, w szczególności gdy:
   a) zakłócony zostanie tok pracy procedur zapewniających ochronę przetwarzania,
   b) pojawi się odpowiedni komunikat alarmowy z tych procedur,
   c) stan urządzeń wchodzących w skład systemu wskazuje na umyślne zakłócenie jego pracy,
   d) stan przeglądu danych osobowych w systemie wskazuje na obecność wirusa komputerowego lub inną nieprzypadkową anomalię,
   e) stwierdzono ujawnienie osobom nieupoważnionym danych osobowych strzeżonych elementami systemu zabezpieczeń,
   f) stwierdzono rażące złamanie dyscypliny pracy w zakresie bezpieczeństwa informacji, (np.; nie zamknięto pomieszczeń, dane przetwarza osoba nieupoważniona, itp.).
2) Kierownik komórki organizacyjnej powiadamia niezwłocznie Administratora Danych Osobowych oraz Inspektora Ochrony Danych o zaistniałych incydentach.
3) Inspektor ochrony danych, we współpracy z Referatem Teleinformatyki, ocenia otrzymane informacje.
4) W przypadku wykrycia naruszenia zabezpieczenia systemu informatycznego Inspektor ochrony danych organizuje działania zmierzające do:
   a) ograniczenia lub przerwania procesu przetwarzania danych;
   b) przeanalizowania przez administratora sieci komputerowej i administratora bazy danych osobowych, wszelkich logów systemu;
   c) skontrolowania poprawności i integralności baz danych oraz związanego z nimi oprogramowania;
   d) przywrócenia stanu baz danych i oprogramowania sprzed naruszenia, w przypadku gdy kontrola, o której mowa w poprzednim punkcie wykaże błędy;
   e) sporządzenia pełnego raportu z naruszenia;
   f) na podstawie danych z raportu sprecyzowania rodzaju dokonanego naruszenia;
   g) zabezpieczenia dowodów zdarzenia;
   h) określenia osób odpowiedzialnych za usunięcie skutków naruszenia;
   i) przygotowania, w razie konieczności, wraz z administratorem sieci komputerowej i administratorem bazy danych osobowych, wniosku o poprawę zabezpieczeń systemu informatycznego i baz danych;
   j) przekazania raportu i wniosków z ww. prac do kierownika Referatu Teleinformatyki;

k) powiadomienia o zdarzeniu Administratora danych osobowych.

5) W przypadku zaobserwowania zakłóceń w działaniu systemu Inspektor ochrony danych organizuje działania zmierzające do:

a) ustalenia, czy zakłócenie zagraża procesowi przetwarzania danych;

b) jeżeli zakłócenie zagraża procesowi przetwarzania danych, ustalenia sposobu naprawy i przeciwdziałania na przyszłość;

c) dokładnego opisu zakłócenia;

d) zebrania opinii użytkowników danych osobowych, administratorów sieci i baz danych na temat zaistniałych zakłóceń;

e) przekazania opisu zakłóceń i opinii do kierownika Referatu Teleinformatyki.

21. Oprogramowanie do przetwarzania danych osobowych

1) W procesie przetwarzania danych w Urzędzie można wykorzystywać jedynie oprogramowanie zatwierdzone pod względem technicznym i funkcjonalnym przez Referat Teleinformatyki.

2) Do przetwarzania danych osobowych na terenie Urzędu można wykorzystywać wyłącznie sprzęt komputerowy będący jego własnością, wypożyczony, wzięty w leasing lub powierzony w związku z przetwarzaniem danych osobowych.

3) Zabrania się wykorzystania przez pracowników w systemach informatycznych przetwarzających dane osobowe napędów z wymiennymi nośnikami umożliwiającymi zapis informacji, poza udokumentowanymi wyjątkami wynikającymi z konieczności prawidłowej realizacji zadań.

4) Osoba użytkująca przenośny komputer, służący do przetwarzania danych osobowych, obowiązana jest zachować szczególną ostrożność podczas transportu i przechowywania tego komputera poza obszarem wyznaczonym w Urzędzie do przetwarzania danych osobowych, w celu zapobieżenia dostępowi do tych danych osobie niepowołanej, a w szczególności powinna zabezpieczyć dostęp do komputera hasłem i nie zezwalać na używanie komputera osobom nieupoważnionym do dostępu do danych osobowych.

22. Praca z danymi osobowymi

1) Podczas rozpoczynania pracy należy przestrzegać następującej procedury:

a) przed rozpoczęciem pracy w systemie informatycznym użytkownik musi wprowadzić do systemu swój identyfikator i hasło,

b) każdy użytkownik danych osobowych ma obowiązek obserwowania zachowania się systemu informatycznego i niezwłocznego powiadomienia Inspektora Ochrony Danych oraz uprawnionego administratora systemu o wszelkich nieprawidłowościach w działaniu systemu informatycznego mogących wskazywać na możliwe naruszenie zabezpieczenia systemu informatycznego.

2) Podczas przerwy w pracy:

a) stacja robocza powinna być automatycznie blokowana z użyciem hasła,

b) należy zamknąć pomieszczenie zgodnie z przyjętymi zasadami bezpieczeństwa.

3) Podczas kończenia pracy należy bezwzględnie przestrzegać następującej procedury:

a) prawidłowo zamknąć wszystkie używane aplikacje (wylogować się z systemu),

b) prawidłowo zamknąć system operacyjny na użytkowanym komputerze,
c) wyłączyć komputer,
d) zniszczyć wszystkie zbędne wydruki w sposób uniemożliwiający odczytanie zawartych na nich danych lub zabezpieczyć potrzebne później dokumenty,
e) zamknąć pomieszczenie zgodnie z przyjętymi zasadami bezpieczeństwa.

4) Jeżeli podczas wyłączania aplikacji lub systemu operacyjnego pracownik zauważy jakiekolwiek nieprawidłowości, powinien o tym fakcie natychmiast poinformować Inspektora Ochrony Danych oraz administratora systemu.

5) Nośniki należy przechowywać w bezpiecznym miejscu – mebel zamykany na klucz w pomieszczeniu, do którego osoby postronne nie mają niekontrolowanego dostępu.

6) Zabrania się kopiowania dokumentów zawierających dane osobowe dla potrzeb innych niż niezbędne do przetwarzania tych danych zgodnie z określonym celem przetwarzania.

23. Zasady przetwarzania danych osobowych w związku z wykonywaniem pracy zdalnej

1) Zasady bezpiecznego przetwarzania danych osobowych określone w niniejszej instrukcji mają również zastosowanie do przetwarzania takich danych w ramach pracy zdalnej.

2) W przypadku pracy zdalnej z wykorzystaniem sprzętu własnego pracownika, obowiązują ponadto następujące zasady:

a) pracownik uzyskuje dostęp wyłącznie do danych zawartych w poczcie elektronicznej, portalu pracowniczym, systemie Mdok i wewnętrznej książce telefonicznej;

b) dostęp systemu informatycznego UMP następuje po instalacji na komputerze pracownika stosownego oprogramowania zgodnie z instrukcją otrzymaną od pracowników Referatu Teleinformatyki Urzędu Miasta Płocka i zestawieniu łącza VPN;

c) pracownik zobowiązany jest do stworzenia oddzielnego konta użytkownika systemu w pracy na prywatnym sprzęcie komputerowym, wykorzystywanym do pracy zdalnej. Konto użytkownika powinno posiadać ograniczone uprawnienia i być chronione silnym hasłem oraz nieudostępniane osobom trzecim;

d) zabronione jest wykonywanie wydruków dokumentów zawierających dane osobowe oraz utrwalanie dokumentów zawierających dane osobowe na prywatnych nośnikach danych;

e) zabronione jest udostępnianie danych osobom nieuprawnionym, w tym wspólnie z pracownikiem zamieszkującym;

e) przesyłanie danych można dokonywać wyłącznie przez łącze VPN;

f) w przypadku przerw w pracy oraz po jej zakończeniu pracownik zobowiązany jest wylogować się z programów wykorzystywanych do pracy zdalnej.

3) W przypadku pracy zdalnej z wykorzystaniem sprzętu stanowiącego własność pracodawcy, obowiązują ponadto następujące zasady:

a) przekazany sprzęt można wykorzystywać wyłącznie do realizacji zadań służbowych;

b) zabronione jest podłączania drukarek i urządzeń wielofunkcyjnych;

c) zabronione jest wykonywanie wydruków dokumentów zawierających dane osobowe oraz utrwalanie dokumentów zawierających dane osobowe na prywatnych nośnikach danych;

d) zabronione jest udostępnianie danych osobom nieuprawnionym, w tym wspólnie z pracownikiem zamieszkującym;
e) w przypadku przerw w pracy oraz po jej zakończeniu pracownik zobowiązany jest wylogować się z programów wykorzystywanych do pracy zdalnej oraz z systemu;
4) Przed przejściem na pracę zdalną wymagana jest zamiana hasła dostępu do systemu informatycznego na stanowisku pracy pracownika w Urzędzie.
5) Przed przejściem na pracę zdalną pracownik zobowiązany jest zapoznać się z zasadami ochrony danych osobowych W Urzędzie Miasta Płocka, w tym w zakresie pracy zdalnej. Fakt tego zapoznania się pracownik potwierdza składając oświadczenie na porozumieniu lub we wniosku o pracę zdalną.
6) Pracownik ma obowiązek zgłoszenia wszelkich incydentów bezpieczeństwa i ochrony danych osobowych, a także podejrzenia ich wystąpienia oraz wszelkich nieprawidłowości w zakresie ochrony danych osobowych. Zgłoszenia należy dokonać kierownikowi właściwej komórki organizacyjnej oraz inspektorowi ochrony danych na adres mail: iod@plock.eu.
7) Nieprzestrzeganie zasad ochrony danych może być kwalifikowane jako ciężkie naruszenie podstawowych obowiązków pracowniczych.

24. Realizacja obowiązku informacyjnego

1) Kierownicy komórek organizacyjnych zapewniają realizację ciążącego na Administratorze Danych obowiązku informacyjnego.

2) Obowiązek informacyjny realizowany jest w następujący sposób:
   a) jeżeli do załatwiania spraw w Urzędzie Miasta Płocka wykorzystywany jest formularz, w którego treści są pola przeznaczone na dane osobowe – klauzulę umieszcza się pod treścią formularza,
   b) przypadku braku określonych wzorów formularzy, klauzula informacyjna musi być zawarta w opisie procedury załatwiania sprawy znajdującym się w BIP.

3) Treść klauzuli informacyjnej musi być dostosowana do specyfiki danego przetwarzania, zwłaszcza w zakresie określenia celu przetwarzania danych osobowych, podstawy prawnej przetwarzania, odbiorców lub kategorii odbiorców danych osobowych, okresu przechowywania, informacji o prawach osoby, której dane dotyczą oraz obowiązkowości lub dobrowolności podania danych osobowych i konsekwencjach ich niepodania.

4) Podstawowy wzór klauzuli informacyjnej stanowi **załącznik nr 5** do instrukcji.

25. Zachowanie tajemnicy skarbowej

Do zachowania tajemnicy skarbowej mają zastosowanie wszystkie środki ochrony wymienione w tej instrukcji.

1) Pracownicy, którzy, w ramach wykonywania czynności służbowych, mają dostęp do informacji stanowiących tajemnicę skarbową zobowiązani są do złożenia na piśmie przyrzeczenia, którego wzór stanowi załącznik nr 4 do instrukcji.
2) Obowiązek określony w pkt 1 obejmuje również stażystów i praktykantów, którzy w ramach odbywanych staży i praktyk wykonują czynności związane z dostępem do danych stanowiących tajemnicę skarbową.

3) Zachowanie tajemnicy skarbowej obowiązuje również po ustaniu zatrudnienia, zakończeniu stażu lub praktyki.
4) Kierownik komórki organizacyjnej, w której przetwarzane są informacje stanowiące tajemnicę skarbową, odpowiada za złożenie przez zobowiązanych pracowników przyrzeczeń określonych w pkt 1.
5) Oryginały dokumentów przyrzeczeń należy przekazać do akt osobowych pracownika.

Załącznik nr 1: Wzór oświadczenia w postaci listy potwierdzającej zapoznanie podległych pracowników, stażystów i praktykantów z zapisami instrukcji P-5/In-13.

…….
pieczęć komórki organizacyjnej

LISTA PRACOWNIKÓW, STAŻYSTÓW i PRAKTYKANTÓW
zapoznanych z zapisami
Instrukcji podstawowych zasad bezpieczeństwa informacji
dla pracowników Urzędu Miasta Płocka
wyd. 15 z dnia ……..

Oświadczam, że zapoznałem się z postanowieniami instrukcji P-5/In-13 dotyczącymi zasad bezpieczeństwa informacji i zasad ochrony danych osobowych oraz zobowiązuję się do ich przestrzegania.

l.p.	Imię i nazwisko pracownika/stażysty/ praktykanta	Symbol komórki organizacyjnej (do poziomu Zespołu)	Data złożenia podpisu	Podpis stwierdzający zapoznanie się z treścią instrukcji P-5/In-13 oraz zobowiązanie do przestrzegania jej postanowień.

Załącznik nr 2: Grupy informacji z poziomem ochrony „Tajemnica pracodawcy" (z uwzględnieniem regulacji wynikających z odrębnych przepisów prawa powszechnego)

l.p.	Grupa informacji	Opis grupy informacji	Informacje stanowiące tajemnicę pracodawcy
1.	**Dokumentacja związana z planowaniem strategicznym oraz przestrzennym**	Informacje związane z projektami planów zagospodarowania przestrzennego, rozwoju Miasta, wnioskami o dofinansowanie z funduszy rozwojowych i strukturalnych, projekty realizowane w formule partnerstwa publiczno – prywatnego (PPP) oraz analizy, opracowania i sprawozdania dot. powyższych kwestii	1. koncepcje rozwojowe, zwłaszcza o charakterze unikalnym, 2. analizy oraz opracowania diagnostyczne i prognostyczne, 3. zamierzenia i plany inwestycyjne Miasta oraz informacje dot. pozyskiwania terenów pod te inwestycje, 4. negocjacje prowadzone w sprawach nabycia nieruchomości pod inwestycje i do zasobu w drodze wykupu lub zamiany, w tym również operaty szacunkowe określające wartość tych nieruchomości, 5. negocjacje prowadzone w sprawach ustanowienia służebności na rzecz Gminy Płock, w tym operaty szacunkowe określające wysokość wynagrodzenia z tytułu jej ustanowienia, 6. karty opisu projektu dofinansowania oraz informacje uzyskane w celu ich wypełnienia, 7. kody dostępu do kart projektów, 8. opracowywane i składane wnioski o pozyskanie środków unijnych, wraz z załącznikami, 9. projekty miejscowych planów zagospodarowania przestrzennego oraz studiów uwarunkowań i kierunków zagospodarowania przestrzennego Miasta – przed ich skierowaniem do uzgodnienia i zaopiniowania, 10. dokumentacja analityczna dla potrzeb sporządzenia koncepcji poprzedzających wykonanie opracowań planistycznych, 11. analizy funkcji oraz cech zabudowy i zagospodarowania terenu na etapie przed sporządzeniem projektu decyzji, 12. informacje zawarte w analizach mających na celu ustalenie sytuacji prawnej majątku spółki, stanu i perspektyw rozwoju przedsiębiorstwa spółki, oszacowania wartości przedsiębiorstwa, oceny realizacji obowiązków wynikających z tytułu wymagań przepisów ochrony środowiska w procesie prywatyzacji, 13. roczne sprawozdania finansowe spółek z udziałem Miasta i sprawozdania z działalności spółki oraz sprawozdania rad nadzorczych do czasu ich zatwierdzenia przez zwyczajne zgromadzenia wspólników / zwyczajne walne zgromadzenia; sprawozdania finansowe spółek sporządzone w trakcie roku obrotowego; raporty biegłych rewidentów z badania

			sprawozdania finansowego; przychody i koszty spółki w trakcie roku obrotowego, 14. informacje związane z przygotowaniem i realizacją projektów w formule partnerstwa publiczno-prywatnego, w tym w szczególności analizy przedrealizacyjne, dokumentacja przebiegu dialogu konkurencyjnego oraz zapisy umowy PPP objęte tajemnicą przedsiębiorcy, 15. informacje dotyczące obsługi inwestorów, w tym w szczególności: zapytania inwestorskie, informacje przekazywane inwestorom, szczegóły negocjacji z inwestorami.
2.	**Informacje związane z podmiotami zewnętrznymi**	Dane osób fizycznych oraz firm i instytucji zewnętrznych związanych z inwestowaniem lub załatwiających sprawy administracyjne	1. informacje przetargowe dla potencjalnych oferentów, 2. dokumentacja oraz informacje uzyskane od inwestorów w trakcie procesu prywatyzacji, 3. dane przedsiębiorcy i konsumenta w sprawach o naruszenie indywidualnych i zbiorowych interesów konsumentów, 4. dokumentacja powierzona przez klienta
3.	**Akty prawa miejscowego i regulacje wewnętrzne na etapie tworzenia**	Projekty uchwał i aktów administracyjnych	1. projekty uchwał do czasu przekazania ich pod obrady Rady Miasta, 2. projekty aktów administracyjnych do czasu podpisania przez Prezydenta, 3. projekty innych uregulowań prawnych do czasu zatwierdzenia.
4.	**Dokumentacja pracownicza**	Informacje związane z zatrudnieniem i rozwojem zawodowym pracowników Urzędu oraz podmiotów podległych	1. wysokości składników wynagrodzeń pracowników Urzędu, 2. wysokości składników wynagrodzeń, w tym dodatków motywacyjnych dla dyrektorów miejskich placówek oraz kierowników miejskich jednostek organizacyjnych, 3. projekty decyzji kadrowych i dyscyplinarnych dot. pracowników Urzędu oraz kierowników miejskich jednostek organizacyjnych, 4. testy kwalifikacyjne dla kandydatów do pracy oraz test dla osób kończących służbę przygotowawczą.
5.	**Dokumentacja systemów informatycznych**	Dokumentacja funkcjonowania systemów teleinformatyki i dokumentacja użytkowników systemów teleinformatycznych.	1. informacje dot. funkcjonowania sieci teleinformatycznych i innych z nimi związanych, a w szczególności: - klucze szyfrujące dostęp do punktów dystrybucyjnych, - techniczne szczegóły budowy punktów dystrybucyjnych, - konfigurację urządzeń sterujących ruchem sieci w tym hasła dostępowe, - informacje o ruchu, o funkcjonowaniu centrali, o zastrzeżonych numerach), 2. informacje dot. funkcjonowania systemów informatycznych obejmujące m. in. szczegóły konfiguracji serwerów (SO, baz danych,

Załącznik nr 3: Wzór wniosku o nadanie / odebranie upoważnienia do przetwarzania danych osobowych

.....
(pieczęć komórki organizacyjnej)

Płock, dnia .....

Prezydent Miasta Płocka

Wniosek o nadanie/odebranie* upoważnienia do przetwarzania danych osobowych

Imię i nazwisko użytkownika danych osobowych:.....

Zbiór danych osobowych do którego nadane są uprawnienia:
.....
.....

Okres obowiązywania upoważnienia:
.....

.....
(podpis wnioskodawcy)

*- niewłaściwe skreślić

Załącznik nr 4: Wzór przyrzeczenia w sprawie zachowania tajemnicy skarbowej

Płock, ...

.....

pieczęć nagłówkowa UMP

PRZYRZECZENIE

Ja niżej podpisana/y ....., zgodnie z obowiązkiem wynikającym z art. 294 § 2 ustawy z dnia 29 sierpnia 1997 roku – Ordynacja Podatkowa, składam przyrzeczenie następującej treści:

„Przyrzekam, że będę przestrzegał tajemnicy skarbowej. Oświadczam, że są mi znane przepisy o odpowiedzialności karnej za ujawnienie tajemnicy skarbowej".

Mam świadomość, że zachowanie tajemnicy skarbowej obowiązuje również po ustaniu zatrudnienia, zakończeniu stażu lub praktyki.

.....

(czytelny podpis osoby składającej przyrzeczenie)

Otrzymują:

1. Osoba składająca przyrzeczenie
2. a/a - Akta osobowe pracownika

Załącznik nr 5: Klauzula informacyjna

Informacje dotyczące przetwarzania danych osobowych:

1. Administratorem przetwarzanych Państwa danych osobowych jest Gmina – Miasto Płock, 09-400 Płock, pl. Stary Rynek 1;

2. Kontakt z inspektorem ochrony danych – iod@plock.eu;

3. Państwa dane osobowe przetwarzane będą w celu (*wpisać tytuł formularza czego dotyczy procedura lub określić rodzaj realizowanego zadania*) zgodnie z przepisami (*podać tytuł aktu prawnego*);

4. Odbiorcami Państwa danych osobowych będą wyłącznie podmioty uprawnione do uzyskania danych osobowych na podstawie przepisów prawa. (*jeżeli będą inni odbiorcy np. ZUS, NFZ, urząd skarbowy, archiwum państwowe, banki, kancelarie adwokackie, podmioty przetwarzające dane na podstawie umów powierzenia, placówki ochrony zdrowia, firmy windykacyjne, podmioty świadczące usługi na rzecz administratora np. pocztowe – należy skreślić wyraz „wyłącznie" i dodać „oraz" …….. (tu wymienić te podmioty)*;

5. Państwa dane osobowe będziemy przechowywać przez okres ….(*okres przechowywania wynika bądź z przepisów prawa materialnego, bądź jest określony w jednolitym rzeczowym wykazie akt);*

6. Mają Państwo prawo do:
a) dostępu do swoich danych osobowych oraz otrzymania ich kopii,
b) sprostowania (poprawiania) swoich danych osobowych,
c) ograniczenia przetwarzania danych osobowych,
d) usunięcia danych osobowych gdy dane nie są już niezbędne dla celów, dla których były zebrane,
e) przenoszenia danych,
f) sprzeciwu,
g) wniesienia skargi do organu nadzorczego, którym jest Prezes Urzędu Ochrony Danych Osobowych.

7. *zapis alternatywny*

Podanie przez Państwa danych osobowych jest obowiązkowe na mocy (*powołać przepis prawa*).

lub

Podanie danych osobowych jest dobrowolne, jednakże odmowa podania danych będzie skutkować odmową realizacji wniosku *(zawarciem umowy)*.

Objaśnienia:

Ad pkt 3)

Treść punktu musi być dostosowana do podstawy przetwarzania danych.
Podana we wzorze treść dotyczy przypadku, kiedy przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze.

Autor dokumentu:	**Zatwierdził merytorycznie:**	**Zatwierdził do użytkowania**
Anna Domańska – Zespół Systemów Zarządzania Rafał Frankowski – Pełnomocnik ds. Cyfryzacji	Daniel Urbański – Dyrektor Wydziału Organizacyjnego Andrzej Kobylski – Inspektor Ochrony Danych	Magdalena Niedziałkowska – Dyrektor Wydziału Koordynacji Procesów Zarządzania - Pełnomocnik ds. ZSZ

W przypadku przetwarzania danych na podstawie umowy, celem i zarazem podstawą będzie realizacja postanowień umowy ……..(podać rodzaj umowy).
W przypadku przetwarzania danych na podstawie zgody podstawą prawną będzie wyrażona zgoda.

Ad pkt 4)

Wykaz podmiotów będącymi odbiorcami danych lub kategorii odbiorców musi odpowiadać faktycznym odbiorcom danych (np. przy przechowywaniu bezterminowym czyli aktach kategorii „A" odbiorcą będzie archiwum państwowe, ale przy przechowywaniu terminowym czyli aktach kategorii „B..." archiwum odbiorcą nie będzie; odbiorcą danych kadrowo płacowych będzie NFZ, a nie będzie odbiorcą danych z zakresu spraw geodezyjnych).

Ad pkt 5)

Okres przechowywania wynika z RWA lub jest określony w przepisach prawa materialnego (np. ustawa o dowodach osobistych – 10 lat przechowywania wniosków dowodowych licząc od śmierci wnioskodawcy). Nie wystarczy samo powołanie się na przepisy o narodowym zasobie archiwalnym. Takie rozwiązanie jest dopuszczalne, gdy w przepisach prawa materialnego i w RWA brak jest ustalonego okresu przechowywania, ale podać wtedy trzeba sposób, w jaki zostanie czas przechowywania ustalony. W przypadku akt kategorii „A" - dane przechowywane będą bezterminowo jako dokumentacja stanowiąca materiały archiwalne kategorii „A", zgodnie z przepisami o narodowym zasobie archiwalnym i archiwach.

Ad pkt 6)

Zakres uprawnień osób, których dane dotyczą zależy do podstawy przetwarzania danych osobowych.
Następujące uprawnienia przysługują zawsze:

a) prawo dostępu do swoich danych osobowych,
b) prawo do sprostowania (poprawiania) swoich danych osobowych,
c) prawo do ograniczenia przetwarzania,
d) prawo do usunięcia danych osobowych, gdy dane nie są już niezbędne dla celów, dla których były zebrane
e) prawo do wniesienia skargi do organu nadzorczego, którym jest Prezes Urzędu Ochrony Danych Osobowych.

Prawa, które przysługują w zależności od podstawy przetwarzania danych:

a) prawo do usunięcia danych – przysługuje także, gdy podstawą przetwarzania jest zgoda osoby, której dane dotyczą, a osoba ta cofnęła swoją zgodę,
b) prawo do przenoszenia danych – przysługuje, gdy spełnione są dwa warunki:
- gdy przetwarzanie odbywa się na podstawie zgody lub na podstawie umowy, oraz
- przetwarzanie odbywa się w sposób zautomatyzowany.

c) prawo sprzeciwu – przysługuje wobec przetwarzania danych osobowych opartego na art. 6 ust. 1 lit. e lub f RODO.
UWAGA! - prawo do usunięcia danych nie przysługuje, gdy mamy do czynienia z dokumentami stanowiącymi kategorię „A".