ZAŁĄCZNIK 1
DO ZARZĄDZENIA NR 7/2023

KODEKS DOBRYCH PRAKTYK RODO
w związku z przetwarzaniem danych osobowych, w tym również podczas pracy w trybie zdalnym
Łódzki Zakład Usług Komunalnych
ul. Nowe Sady 19, 94-102 Łódź

Niniejszy dokument stanowi wytyczne dla Pracowników i innych osób, które przetwarzają dane osobowe w Łódzkim Zakładzie Usług Komunalnych, w tym również podczas wykonywania pracy zdalnej.

Wszyscy Pracownicy i inne osoby zobowiązane są do zachowania odpowiedniego poziomu bezpieczeństwa przetwarzania danych osobowych, zabezpieczenia danych osobowych przed zagrożeniami, w tym przed ich udostępnieniem osobom nieupoważnionym, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.

I. Definicje i pojęcia.

1. **Administrator Danych Osobowych (dalej: Administrator/Jednostka)**: Łódzki Zakład Usług Komunalnych, ul. Nowe Sady 19, 94-102 Łódź tel.: +48 (42) 272 34 50, e-mail: zaklad@lzuk.lodz.pl
2. **ASI:** Administrator systemów informatycznych, który zobowiązany jest, z upoważnienia Administratora, do zarządzania systemami, programami w jednostce.
3. **Bezpieczeństwo informacji:** stan, w którym informacja jest chroniona przed wieloma różnymi zagrożeniami w taki sposób, aby zapewnić ciągłość prowadzenia działalności, zminimalizować straty i maksymalizować zwrot nakładów na inwestycje i działania o charakterze biznesowym; niezależnie od tego, jaką formę informacja przybiera lub za pomocą jakich środków jest udostępniana lub przechowywana, zawsze powinna być w odpowiedni sposób chroniona; bezpieczeństwo informacji oznacza w szczególności zachowanie: poufności, integralności, dostępności i rozliczalności;
4. **Dane osobowe:** oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"). Możliwa do zidentyfikowania osoba fizyczna, to osoba którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden, bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.
5. **Hasło**: ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi.
6. **Identyfikator**: ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
7. **Inspektor ochrony danych**: oznacza Inspektora ochrony danych, o którym mowa w art. 37 RODO.
8. **Integralność danych**: właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
9. **Kodeks**: niniejszy Kodeks Dobrych Praktyk RODO w związku z przetwarzaniem danych osobowych, w tym również podczas pracy w trybie zdalnym.
10. **Kopia bezpieczeństwa**: kopie plików danych lub plików oprogramowania tworzone na nośnikach wymiennych lub dysku komputera w celu ich odtworzenia w przypadku utraty lub uszkodzenia danych;
11. **Odbiorca danych**: każdy, komu udostępniane są dane osobowe, z wyłączeniem:
    a. organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.
12. **Osoba upoważniona do przetwarzania danych osobowych**: osoba, która upoważniona została do przetwarzania danych osobowych przez Administratora na piśmie.
    a. osoby upoważnionej do przetwarzania danych;

b. osoby, której dane dotyczą.

13. **Poufność danych:** właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom.
14. **Praca zdalna -** praca wykonywana całkowicie lub częściowo w miejscu wskazanym przez Pracownika i każdorazowo uzgodnionym z Pracodawcą, w tym pod adresem zamieszkania Pracownika, w szczególności przy wykorzystaniu środków bezpośredniego porozumiewania się na odległość
15. **Pracodawca:** Dyrektor Łódzkiego Zakładu Usług Komunalnych z siedzibą w Łodzi.
16. **Pracownik** - osoba zatrudniona w Łódzkim Zakładzie Usług Komunalnych na podstawie stosunku pracy bez względu na podstawę nawiązania stosunku pracy, rodzaj stanowiska, rodzaj umowy o pracę i czas jej trwania, również jeśli realizacja tej umowy wiąże się z wykonywaniem obowiązków na rzecz Pracodawcy w miejscu ich stałego wykonywania wyznaczonym przez Pracodawcę.
17. **Proces zarządzania bezpieczeństwem systemów informatycznych:** całość działań organizacyjno-technicznych i prawnych podejmowanych przez Jednostkę mających na celu właściwą ochronę informacji oraz minimalizację skutków w przypadku incydentów bezpieczeństwa.
18. **Przetwarzający dane**: podmiot, któremu zostało powierzone przetwarzanie danych osobowych na podstawie umowy, zgodnie z art. 28 RODO.
19. **Przetwarzanie danych**: operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich 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.
20. **RODO:** Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 7 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s. 1).
21. **System informatyczny (dalej: system)**: sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych; w systemie tym pracuje co najmniej jeden komputer centralny i system ten tworzy sieć teleinformatyczną.
22. **Trwałe usunięcie informacji**: sposób postępowania z nośnikiem informacji mający na celu usunięcie zapisanych na nim informacji tak, aby ich odtworzenie w całości lub w części było niemożliwe;
23. **Ustawa:** Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. 2019, poz. 1781).
24. **Uwierzytelnianie:** działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.
25. **Użytkownik**: Pracownik, współpracownik, osoba upoważniona do przetwarzania danych osobowych, w tym osoba której nadano identyfikator i przyznano hasło;
26. **Zagrożenie:** stan faktyczny, który może spowodować naruszenie bezpieczeństwa informacji;
27. **Zasada wiedzy koniecznej:** zasada, że dostęp osób zatrudnionych w jednostce do zasobów informacyjnych ograniczony jest wyłącznie do informacji, które są im niezbędne do wykonania powierzonych zadań.

II. Zakres przedmiotowy Kodeksu.

1. Kodeks ma zastosowanie do każdego zbioru danych osobowych:
   a. przetwarzanych w systemach informatycznych;
   b. zapisanych w formie elektronicznej na zewnętrznych nośnikach;
   c. zapisanych i przechowywanych w formie papierowej.

III. Zakres podmiotowy Kodeksu.

1. Do stosowania postanowień Kodeksu obowiązani są wszyscy Pracownicy i inne osoby, które przetwarzają dane osobowe w jednostce, jak również całkowicie lub częściowo w miejscu wskazanym przez Pracownika i każdorazowo uzgodnionym z Pracodawcą, w tym pod adresem zamieszkania Pracownika, w szczególności przy wykorzystaniu środków bezpośredniego porozumiewania się na odległość.
2. Przed przystąpieniem do pracy przez Pracownika lub innej osoby zatrudnionej w jednostce obowiązkowe jest zapoznanie się z wszystkimi regulacjami dotyczącymi przetwarzania danych obowiązującymi u Pracodawcy.
3. Fakt zapoznania się z regulacjami, o których mowa w pkt. 2, potwierdzany jest m.in. poprzez podpisanie oświadczenia o zapoznaniu się z niniejszym Kodeksem.

IV. System informatyczny.

1. Na System informatyczny w jednostce składają się:
   a. urządzenia:
      — serwery
      — stacje robocze
      — drukarki i urządzenia wielofunkcyjne
   b. programy:
      — oprogramowanie biurowe;
      — oprogramowanie antywirusowe;
      — oprogramowanie specjalistyczne (np. kadrowe, księgowe, techniczne).
2. Elementy Systemu opisane w pkt. 1 są wykorzystywane do przetwarzania danych przez Administratora i podlegają one regularnej kontroli w celu zapewnienia bezpieczeństwa przetwarzanych danych.

V. Klasyfikacja systemów informatycznych.

1. Każdy system informatyczny eksploatowany w jednostce wymaga zaklasyfikowania do określonej kategorii ze względu na poziom poufności, integralności i dostępności przetwarzanych informacji oraz na rodzaj informacji i wagę systemu dla ciągłości świadczenia usług.
2. Systemy informatyczne eksploatowane w jednostce są skategoryzowane i opisane.
3. Za sklasyfikowanie systemów informatycznych eksploatowanych w jednostce odpowiada ASI.
4. Klasyfikacja systemów informatycznych podlega akceptacji Administratora.

VI. Zarządzanie dostępem.

1. Dostęp do systemów informatycznych musi być zabezpieczony z wykorzystaniem obowiązujących w jednostce mechanizmów bezpieczeństwa w postaci rozwiązań organizacyjno-technicznych i prawnych uwzględniających kategorię systemu oraz wrażliwość informacji przetwarzanych w systemie.
2. Mechanizmy bezpieczeństwa muszą zapewniać rozliczalność w stopniu uwzględniającym kategorię systemu oraz wymagania wynikające z przepisów prawa i przepisów wewnętrznych Jednostki.
3. W szczególności każdemu użytkownikowi systemu informatycznego musi być przydzielony niepowtarzalny identyfikator.
4. Każdy użytkownik systemu informatycznego zobowiązany jest do eksploatowania systemów informatycznych zgodnie z opisanymi procedurami.
5. Dostęp do systemów informatycznych wygasa:

a. zgodnie z zasadą wiedzy koniecznej (osoby uprawnione mają dostęp jedynie do zasobów, które są niezbędne do wykonywania przez nich obowiązków);
b. po upływie okresu, na który został przyznany;
c. w przypadku zawinionego naruszenia bezpieczeństwa systemu lub bezpieczeństwa przetwarzanych danych.

6. Zasady szczegółowe:
   a. poszczególnym osobom upoważnionym do przetwarzania danych osobowych przydziela się konta opatrzone niepowtarzalnym identyfikatorem, umożliwiające dostęp do danych, zgodnie z zakresem upoważnienia do ich przetwarzania;
   b. ASI przydziela Pracownikowi upoważnionemu do przetwarzania danych, konto w systemie informatycznym, dostępne po wprowadzeniu prawidłowego identyfikatora i uwierzytelnieniu hasłem;
   c. w razie potrzeby ASI może przydzielić konto opatrzone identyfikatorem, osobie upoważnionej do przetwarzania danych osobowych, nieposiadającej statusu Pracownika;
   d. pierwsze hasło wymagane do uwierzytelnienia się w systemie przydzielane jest przez ASI po nadaniu, przez Administratora, upoważnienia do przetwarzania danych osobowych, w którym jest mowa o zachowaniu poufności.
   e. do zagwarantowania poufności i integralności danych osobowych konieczne jest przestrzeganie przez użytkowników swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowania się do zaleceń.

VII. Cele i zasady bezpieczeństwa systemu.

1. Stosowanie zabezpieczeń ma na celu zapewnienie optymalnego poziomu bezpieczeństwa przetwarzanych w systemie danych, stosownie do ich rodzaju oraz ewentualnych zagrożeń.
2. Zapewnienie odpowiedniego poziomu bezpieczeństwa następuje poprzez stosowanie zasad, zgodnie z którymi:
   a. osoby nieupoważnione nie mają dostępu do systemu;
   b. użytkownicy mają ograniczony dostęp do systemu, zgodnie z postanowieniami niniejszego Kodeksu;
   c. użytkownicy wykorzystują oddane im do dyspozycji narzędzia zgodnie z zaleceniami, zachowując wymogi należytej staranności.

VIII. Poziom bezpieczeństwa.

1. Uwzględniając kategorie danych osobowych oraz konieczność zachowania bezpieczeństwa ich przetwarzania w systemie informatycznym połączonym z siecią publiczną, wprowadza się „poziom wysoki" bezpieczeństwa.
2. Zastosowanymi środkami bezpieczeństwa są:
   a. środki ochrony organizacyjne;
   b. środki ochrony fizyczne;
   c. środki ochrony techniczne.

IX. Nadawanie uprawnień w systemach informatycznych.

1. Dostęp do systemu informatycznego służącego do przetwarzania danych osobowych może uzyskać wyłącznie osoba upoważniona do przetwarzania danych osobowych przez Administratora, lub osobę przez upoważnioną przez Administratora i zarejestrowana jako użytkownik.
2. W jednostce przetwarzać dane mogą jedynie osoby posiadające ww. upoważnienie, które złożyły oświadczenia o zachowaniu poufności przetwarzanych danych.

3. Użytkownik obowiązany jest do zachowania w tajemnicy loginu oraz hasła, w szczególności nieudostępniania go innym użytkownikom, niezapisywania w powszechnie dostępnych miejscach.

X. Dezaktywacja konta użytkownika.

1. Dezaktywacja kont z systemu informatycznego dokonywane jest przez ASI.
2. Dezaktywacja konta następuje w przypadku:
   a. rozwiązania stosunku pracy;
   b. wygaśnięcia stosunku pracy;
   c. ustania innego stosunku prawnego, w ramach którego zatrudniony był użytkownik;
   d. przejścia użytkownika do innej Jednostki organizacyjnej;
   e. cofnięcia upoważnienia do przetwarzania danych osobowych.
3. Dopuszcza się ponowną aktywację wcześniej zdezaktywowanego konta, z zastrzeżeniem wygaszenia uprawnień tego konta wraz z ponownym przydzieleniem uprawnień.
4. Dopuszcza się przekazywanie kont pocztowych innym użytkownikom, ze względu na konieczność zachowania ciągłości korespondencji dotyczącej konkretnej Jednostki organizacyjnej – na podstawie stosownego wniosku, z zastrzeżeniem usunięcia oraz archiwizacji wiadomości historycznych.
5. Postanowień pkt. 4 nie stosuje się do imiennych kont użytkowników.
6. Postanowień działu X nie stosuje się w sytuacji zmiany postanowień lub rodzaju umowy, na podstawie której użytkownik zatrudniony jest w jednostce, o ile zachowana jest ciągłość zatrudnienia.

XI. Zawieszenie konta użytkownika.

1. Zawieszenie dostępu użytkownika do systemów informatycznych dokonuje ASI, na podstawie stosownego wniosku.

XII. Kontrola bezpieczeństwa.

1. Codzienna kontrola bezpieczeństwa powinna być wykonywana przez użytkowników i polega w szczególności na sprawdzeniu, czy nie doszło do:
   a. próby nieautoryzowanego dostępu do systemu;
   b. próby nieautoryzowanej zmiany oprogramowania;
   c. próby nieautoryzowanej modyfikacji danych;
   d. ujawnienia lub udostępnienia innym osobom nazwy lub hasła;
   e. uszkodzenia lub zniszczenia urządzeń systemu.
2. W razie stwierdzenia nieprawidłowości w zakresie bezpieczeństwa użytkownik powiadamia niezwłocznie ASI.

XIII. Metody i środki uwierzytelniania - nazwa i hasło użytkownika.

1. Uwierzytelnienie użytkownika w Systemie informatycznym następuje po podaniu nazwy użytkownika oraz hasła.
2. Nazwa użytkownika stanowi identyfikator, który w sposób jednoznaczny przypisany został konkretnemu użytkownikowi.
3. Identyfikator składa się z ciągu znaków.
4. Niedopuszczalne jest funkcjonowanie kilku takich samych nazw użytkowników w ramach danego systemu. Raz przypisana nazwa nie podlega zmianie i nie może zostać wykorzystana w przyszłości przez innego użytkownika.
5. W przypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniej zarejestrowanego użytkownika ASI nadaje inny identyfikator, odstępując od zasady określonej w pkt 4.
6. Hasło powinno składać się z unikalnego zestawu znaków, liter oraz cyfry lub znaków specjalnych.

7. Hasło nie może być:
   a. identyczne z identyfikatorem użytkownika;
   b. identyczne z imieniem lub nazwiskiem użytkownika;
   c. odnosić się do innych cech szczególnych użytkownika;
   d. ponowieniem hasła stosowanego wcześniej, jeżeli od ostatniego zastosowania danej kombinacji nie upłynął rok.
8. Niedopuszczalne jest zapamiętywanie haseł w systemie.
9. Pierwsze nadane hasło ulega zmianie przez użytkownika podczas pierwszego użycia.
10. Użytkownik odpowiada za działania wykonywane w systemie przy użyciu jego nazwy oraz za zachowanie hasła w tajemnicy.
11. Użytkownik ma obowiązek zmieniać hasło nie rzadziej niż co 90 dni.
12. Okresowe zmiany hasła są wykonywane osobiście przez użytkownika.
13. ASI ma prawo do zmiany hasła w przypadku zapomnienia go przez użytkownika, na wniosek Kierownika Jednostki organizacyjnej Pracownika.

XIV. Zasady korzystania ze stacji roboczej.

1. Przed rozpoczęciem pracy użytkownik obowiązany jest sprawdzić stan urządzeń oraz dokonać oględzin swojego stanowiska pracy w celu wykrycia ewentualnych nieprawidłowości mogących świadczyć o naruszeniu bezpieczeństwa danych osobowych.
2. W pomieszczeniu, w którym przetwarzane są dane osobowe, mogą znajdować się osoby postronne tylko za zgodą i w towarzystwie użytkownika.
3. Przed osobami postronnymi należy chronić ekrany komputerów (ustawienie monitora powinno uniemożliwiać podgląd), a także wydruki leżące na biurkach oraz w otwartych szafach.
4. Rozpoczęcie pracy:
   a. włączenie monitora i stacji roboczej;
   b. zalogowanie się poprzez wprowadzenie nazwy użytkownika i hasła;
   c. uruchomienie programu użytkowego.
5. Zawieszenie pracy w przypadku czasowego opuszczenia stanowiska pracy:
   a. zablokowanie sesji na stacji roboczej;
   b. odblokowanie sesji po podaniu hasła.
6. W przypadku bezczynności na stacji roboczej przez czas przekraczający 10 minut automatycznie włącza się wygaszacz ekranu, który powinien być zaopatrzony w hasło umożliwiające ponowne podjęcie pracy na stacji roboczej.
7. Zakończenie pracy:
   a. zakończenie pracy programu zgodnie z instrukcją obsługi;
   b. wylogowanie z systemu;
   c. wyłączenie stacji roboczej i monitora.
8. Krótkotrwała przerwa w pracy, podczas której użytkownik nie opuszcza stanowiska roboczego, nie wymaga zamykania aplikacji, wylogowania.
9. Każdorazowa zmiana użytkownika stacji roboczej musi poprzedzać wylogowanie się użytkownika, który poprzednio z niej korzystał.

XV. Zasady korzystania z urządzeń przenośnych.

1. Przetwarzanie danych poza obszarem przetwarzania na urządzeniu przenośnym wymaga zgody Administratora..

2. O ile to możliwe, przy przetwarzaniu danych osobowych na urządzeniach przenośnych obowiązują procedury określone w niniejszym Kodeksie, obowiązujących Regulaminach oraz Instrukcjach, dotyczące pracy na komputerach stacjonarnych, w tym:
    a. zabezpieczenia dostępu hasłem;
    b. zastosowanie oprogramowania i zabezpieczeń analogicznie do rozwiązań przyjętych na stacjonarnych stacjach roboczych.
3. Pliki zawierające dane osobowe przechowywane na urządzeniach przenośnych są opatrzone hasłem dostępu.
4. Obowiązuje zakaz używania urządzeń przenośnych przez osoby inne niż użytkownicy, którym zostały one powierzone.
5. Obowiązuje zakaz przetwarzania na urządzeniach przenośnych całych zbiorów danych lub szerokich z nich wypisów.
6. Osoba wykorzystująca urządzenie przenośne obowiązana jest do:
    a. wykorzystywania go wyłącznie do określonych celów, mieszczących się w zakresie upoważnienia;
    b. nieudostępniania urządzenia nieupoważnionym osobom;
    c. zachowania szczególnej ochrony przed kradzieżą, zwłaszcza podczas transportu;
    d. zaniechania jakichkolwiek zmian oprogramowania.
7. W przypadku konieczności zmiany, aktualizacji albo naprawy urządzenia należy zgłosić ten fakt bezpośredniemu przełożonemu, który powyższe zgłasza do ASI.
8. Administrator, w razie potrzeby, wskazuje w dokumencie powierzenia urządzenia przenośnego osobie upoważnionej do przetwarzania danych osobowych konieczność i częstotliwość sporządzania kopii zapasowych danych przetwarzanych na urządzeniu przenośnym oraz określa zasady:
    a. postępowania w razie nieobecności w pracy wynoszącą 1 miesiąc. Jeżeli urządzenie przenośne nie może być zwrócony przed okresem nieobecności, to użytkownik tego komputera powinien niezwłocznie powiadomić o tym bezpośredniego przełożonego oraz Administratora i uzgodnić z nim zwrot urządzenia;
    b. zwrotu sprzętu w razie ustania stosunku zatrudnienia.

XVI. Ochrona antywirusowa.

1. W jednostce istnieje bezwzględny wymóg instalacji oprogramowania antywirusowego na każdym stanowisku roboczym, zarówno na komputerach stacjonarnych, jak i przenośnych wykorzystywanych do przetwarzania danych.
2. Sprawdzanie obecności wirusów komputerowych w systemie informatycznym oraz ich usuwanie odbywa się przy wykorzystaniu oprogramowania zainstalowanego na serwerach, stacjach roboczych oraz komputerach przenośnych przez ASI.
3. Oprogramowanie, o którym mowa w ust. 2, sprawuje ciągły nadzór (ciągła praca w tle) nad pracą systemu i jego zasobami oraz serwerami i stacjami roboczymi.
4. Niedopuszczalne jest wyłączanie lub zmiana ustawień oprogramowania antywirusowego przez użytkowników.
5. Użytkownik jest obowiązany zawiadomić ASI o pojawiających się komunikatach, wskazujących na wystąpienie zagrożenia wywołanego szkodliwym oprogramowaniem.
6. Użytkownicy mogą korzystać z zewnętrznych nośników danych tylko na stanowisku wydzielonym z sieci komputerowej ASI po uprzednim sprawdzeniu zawartości nośnika oprogramowaniem antywirusowym.

7. Niedopuszczalne jest otwieranie plików pobranych z Internetu lub korzystania z zewnętrznych nośników bez uprzedniego przeskanowania zawartości nośnika przez program antywirusowy.
8. Przesyłanie danych osobowych pocztą elektroniczną dopuszczalne jest tylko w postaci zaszyfrowanej.

XVII. Bezpieczeństwo oprogramowania.

1. Oprogramowanie stosowane w jednostce może pochodzić wyłącznie ze źródeł legalnych oraz posiadać aktualną i kompletną dokumentację użytkownika, eksploatacyjną i techniczną.
2. Zgrywanie na urządzenia informatyczne oraz uruchamianie jakichkolwiek nielegalnych oprogramowań lub pochodzących z nielegalnych źródeł oraz plików pobranych z niewiadomego źródła jest zabronione.
3. Instalacja i deinstalacja dokonywana jest wyłącznie przez ASI.
4. Użytkownicy obowiązani są do powstrzymania się od jakiejkolwiek ingerencji w oprogramowanie.
5. Wszelkie oprogramowanie wykorzystywane w jednostce musi być użytkowane z poszanowaniem praw własności intelektualnej, a w szczególności zgodnie z ustawą z 4.02.1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz. U. z 2022 r. poz. 2509).
6. Wszelkie działania związane z utrzymaniem i eksploatacją systemu informatycznego mogą być podejmowane wyłącznie przez upoważniony, wykwalifikowany personel Jednostki lub upoważnione osoby.

XVIII. Naprawy urządzeń komputerowych z chronionymi danymi osobowymi.

1. Wszelkie naprawy urządzeń komputerowych oraz zmiany w systemie informatycznym przeprowadzane są – o ile to możliwe – przez Pracowników lub podmiot zewnętrzny pod nadzorem ASI.
2. Naprawy i zmiany w systemie informatycznym przeprowadzane przez serwisanta prowadzone są pod nadzorem w siedzibie ASI – o ile to możliwe – lub poza siedzibą ASI, po uprzednim nieodwracalnym usunięciu danych w nich przetwarzanych, a jeśli wiązałoby się to z nadmiernymi utrudnieniami, to po podpisaniu umów powierzenia przetwarzania danych osobowych.
3. Jeśli nośnik danych (dysk, dyskietka, płyta lub inne) zostanie uszkodzony i nie można go odczytać ani usunąć z niego danych, należy go zniszczyć mechanicznie w niszczarce, w obecności ASI.

XIX. Przechowywanie elektronicznych nośników informacji zawierających dane osobowe.

1. Zakazuje się przetwarzania danych osobowych na zewnętrznych nośnikach magnetycznych, optycznych i innych oraz ich przesyłania pocztą elektroniczną bez uprzedniego zaszyfrowania.
2. Na nośnikach, o których mowa w pkt. 1, dopuszczalne jest przetwarzanie jedynie jednostkowych danych osobowych.
3. W przypadku posługiwania się nośnikami danych pochodzącymi od podmiotu zewnętrznego użytkownik jest zobowiązany do sprawdzenia go programem antywirusowym na wyznaczonym w tym celu stanowisku komputerowym oraz do oznakowania tego nośnika.
4. Nośniki magnetyczne raz użyte do przetwarzania danych osobowych nie mogą być wykorzystywane do innych celów, mimo usunięcia danych.

XX. Bezpieczeństwo nośników informacji.

1. Zasady ogólne:
   a. wszystkie nośniki informacji podlegają właściwej ochronie stosownie do klasyfikacji informacji, na wszystkich etapach ich używania, od momentu zapisu informacji, aż do momentu wycofania

z użycia lub fizycznego zniszczenia opisanego w Kodeksie oraz obowiązujących Regulaminach oraz Instrukcjach;

b. za zapewnienie właściwej ochrony nośników informacji odpowiada ich użytkownik;
c. osoby korzystające z nośników informacji powinny być świadome zagrożeń i zobowiązane są do zachowania należytej staranności poprzez zastosowanie obowiązujących środków organizacyjno-technicznych i prawnych;
d. w przypadku wycofywania z użycia nośników informacji zawierających informacje stanowiące tajemnicę, na osobie, której nośnik przekazano do używania, spoczywa obowiązek wykonania procedury opisanej w Kodeksie.

2. Zasady szczegółowe:
   a. urządzenia przenośne oraz nośniki danych wynoszone z siedziby Administratora nie powinny być pozostawiane bez nadzoru w miejscach publicznych. Komputery przenośne należy przewozić w służbowych torbach;
   b. nie należy pozostawiać bez kontroli dokumentów, nośników danych i sprzętu w miejscach publicznych, ani też w samochodach;
   c. informacje przechowywane na urządzeniach przenośnych lub komputerowych nośnikach danych należy chronić przed uszkodzeniami fizycznymi, a ze względu na działanie silnego pola elektromagnetycznego należy przestrzegać zaleceń producentów dotyczących ochrony sprzętu;
   d. wykorzystywanie komputerów przenośnych w miejscach publicznych jest dozwolone, o ile otoczenie, w którym znajduje się osoba upoważniona do przetwarzania danych osobowych, stwarza warunki minimalizujące ryzyko zapoznania się z danymi przez osoby nieupoważnione. W konsekwencji korzystanie z komputera przenośnego będzie z reguły niedozwolone w restauracjach czy środkach komunikacji publicznej;
   e. niedozwolone jest udostępnianie domownikom komputera przenośnego należącego do Administratora. Użytkownik powinien zachować w tajemnicy wobec domowników identyfikator i hasło, których podanie jest konieczne do rozpoczęcia pracy na komputerze przenośnym.

XXI. Definicja naruszenia bezpieczeństwa systemu.

1. Za naruszenie bezpieczeństwa systemu informatycznego uznawany jest każdy stwierdzony fakt oraz uzasadnione podejrzenie, w szczególności:
   a. nieuprawnionego ujawnienia danych, udostępnienia;
   b. naruszenia hasła dostępu i identyfikatora (system nie reaguje na hasło lub je ignoruje bądź można przetwarzać dane bez wprowadzenia hasła);
   c. częściowego lub całkowitego braku danych albo dostępu do danych w zakresie szerszym niż wynikający z przyznanych uprawnień;
   d. braku dostępu do właściwej aplikacji lub zmiany zakresu wyznaczonego dostępu do zasobów serwera;
   e. wykrycia wirusa komputerowego,
   f. zauważenia elektronicznych śladów próby włamania do systemu informatycznego;
   g. znacznego spowolnienia działania systemu informatycznego;
   h. podejrzenia kradzieży sprzętu komputerowego lub dokumentów zawierających dane osobowe;
   i. istotnej zmiany położenia sprzętu komputerowego;
   j. zauważenia śladów usiłowania lub dokonania włamania do pomieszczeń lub zamykanych szaf;
   k. umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną;
   l. spowodowane szkód przez zainstalowanie ściągniętego z Internetu oprogramowania w związku, z którym doszło do naruszenia bezpieczeństwa danych.
   m. uszkodzenia lub zniszczenie danych lub jakiegokolwiek elementu systemu informatycznego.

2. Tryb postępowania:
   a. każdy użytkownik systemu posiadający informacje o naruszeniu albo uzasadnione podejrzenie naruszenia bezpieczeństwa systemu informatycznego obowiązany jest bezzwłocznie poinformować o danym fakcie bezpośredniego przełożonego oraz ASI;
   b. użytkownik do czasu przybycia na miejsce ASI lub innej osoby upoważnionej podejmuje tylko takie czynności, które zmierzają do:
      — zabezpieczenia śladów naruszenia,
      — zapobieżenia dalszym zagrożeniom,
      — powstrzymania skutków naruszenia,
      — ustalenia przyczyny i sprawcy naruszenia ochrony,
      — rozważenia wstrzymania bieżącej pracy w celu zabezpieczenia miejsca zdarzenia,
      — przygotowania opisu incydentu.
   c. Pracownik nie opuszcza bez uzasadnionej przyczyny miejsca zdarzenia do czasu przybycia ASI lub osoby przez niego wskazanej;
   d. ASI po otrzymaniu zawiadomienia, o którym mowa w pkt 1, powinien niezwłocznie:
      — przeprowadzić postępowanie wyjaśniające w celu ustalenia okoliczności naruszenia ochrony danych osobowych,
      — podjąć działania chroniące system przed ponownym naruszeniem.
   e. w przypadku stwierdzenia faktycznego naruszenia bezpieczeństwa systemu sporządzić raport naruszenia bezpieczeństwa systemu informatycznego;
   f. Administrator danych osobowych w porozumieniu z ASI, może zarządzić, w razie potrzeby, odłączenie części systemu informatycznego dotkniętej incydentem od pozostałej jego części;
   g. w razie odtwarzania danych z kopii zapasowych ASI obowiązany jest upewnić się, że odtwarzane dane zapisane zostały przed wystąpieniem incydentu (dotyczy to zwłaszcza przypadków infekcji wirusowej);
   h. Administrator podejmuje decyzję o dalszym trybie postępowania, powiadomieniu właściwych organów oraz podjęciu innych szczególnych czynności zapewniających bezpieczeństwo systemu informatycznego bądź zastosowaniu środków ochrony fizycznej.

XXII. W przypadku stwierdzenia podejrzenia, iż mogło dojść do ujawnienia danych w postaci wejścia w posiadanie informacji o danych osobowych przez osoby niepożądane, Pracownik jest zobowiązany postępować zgodnie z obowiązującą Procedurą Postępowania w Przypadku Naruszenia Ochrony Danych Osobowych.

XXIII. Główne zasady postępowania przy przetwarzaniu danych.

1. Zasada legalności – przetwarzać dane zgodnie z prawem.
2. Zasada celowości – zbierać dane dla oznaczonych, zgodnych z prawem celów i nie poddawać ich dalszemu przetwarzaniu niezgodnemu z tymi celami. Cele te powinny być określone nie później niż w momencie ich zbierania.
3. Zasada merytorycznej poprawności – dbać o merytoryczną poprawność danych, tj. należy pamiętać aby dane osobowe były zgodne z prawdą, pełne (kompletne) i aktualne.
4. Zasada adekwatności danych – dbać o adekwatność danych w stosunku do celów, w jakich są przetwarzane.
5. Zasada ograniczenia czasowego – przechowywać dane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to nie- zbędne do osiągnięcia celu przetwarzania.

XXIV. Prawo dostępu do danych.

1. Osoba, której dane dotyczą ma prawo do uzyskania od Administratora potwierdzenia, czy przetwarzane są jej dane osobowe a jeśli tak, to jest uprawniona do uzyskania dostępu do nich oraz do uzyskania informacji takich jak:
   a. cele przetwarzania;
   b. kategorie danych;
   c. informacje o odbiorcach lub kategoriach odbiorców, którym dane zostaną udostępnione;
   d. planowany okres przechowywania / kryteria ustalania tego okresu;
   e. informacji o przysługujących prawach:
      — dostęp do treści swoich danych (podstawa prawna: art.15 RODO);
      — sprostowanie danych (podstawa prawna: art.16 RODO);
      — usunięcie danych (podstawa prawna: art. 17 RODO);
      — ograniczenie przetwarzania (podstawa prawna: art. 18 RODO);
      — przenoszenie danych (podstawa prawna: art. 20 RODO);
      — wniesienie sprzeciwu (podstawa prawna: art. 21 RODO);
      — cofnięcie wyrażanej zgody na przetwarzanie danych, przy czym cofnięcie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie wyrażonej zgody przed jej cofnięciem (podstawa prawna: art.15 RODO);
   f. informacje o prawie wniesienia skargi do organu nadzorczego (podstawa prawna: art. 77 RODO);
   g. jeżeli dane nie pochodzą od osoby, której dotyczą to wszelki informacje o ich źródle;
   h. informacje o profilowaniu.

1. Należy pamiętać iż w razie zgłoszenia swoich praw tj. chęci skorzystania przez osobę fizyczną z przysługujących jej praw zawsze należy o tym poinformować bezpośredniego przełożonego oraz Pracodawcę..

XXV. Pozostałe zasady pracy zdalnej.

1. Wszystkie osoby wykonujące obowiązki w trybie pracy zdalnej zobowiązane są do zachowania odpowiedniego poziomu bezpieczeństwa w związku z korzystaniem z systemów informatycznych, urządzeń informatycznych, telefonów komórkowych oraz dokumentów zawierających dane osobowe.
2. Do wszelkich systemów informatycznych i urządzeń informatycznych oraz mobilnych dostęp posiadają tylko upoważnione osoby, zgodnie z nadanymi upoważnieniami oraz zgodnie z zasadami i procedurami panującymi w Jednostce. Wszelkie odstępstwa powinny być zgłaszane Pracodawcy.
3. Wykorzystywanie systemów, urządzeń informatycznych oraz powierzonego mienia powinno być zawsze zgodne z zachowaniem należytej staranności, jak również zgodne z zaleceniami Pracodawcy, który może wydawać w tym zakresie bieżące wskazówki, polecenia oraz wytyczne postępowania.
4. W celu zachowania wysokiego poziomu bezpieczeństwa korzystania z systemów i urządzeń informatycznych oraz sprzętu przy wykonywaniu pracy zdalnej, korzystanie z tych systemów i sprzętów w celach prywatnych jest bezwzględnie zakazane, zaś dopuszczenie się wszelkich odstępstw od realizacji tego zakazu wiązać się może z odpowiedzialnością dyscyplinarną Pracownika, bądź inną, w razie wystąpienia szkód lub innego rodzaju uszczerbków, bądź naruszeń.
5. Należy odpowiednio zabezpieczyć stanowisko pracy, w szczególności należy zabezpieczyć wszelkie nośniki danych, dokumenty i wydruki zawierające dane osobowe przed jakąkolwiek możliwością zapoznania się z nimi przez osoby postronne, jak również należy zadbać o bezpieczeństwo komputera oraz innych urządzeń, na których mogą być przechowywane dane osobowe.
6. Pracownik zobowiązany jest do korzystania z nadanego mu adresu mailowego (także tymczasowego w celu wykonywania pracy w miejscu wykonywania pracy zdalnej) wyłącznie do prowadzenia wszelkiej korespondencji służbowej z innymi Pracownikami, bądź klientami Administratora.

7. Przy prowadzeniu korespondencji w formie e-mail – w zakresie związanym z bezpieczeństwem danych osobowych - Pracownik zobowiązany jest do działania w sposób nie naruszający praw innych użytkowników i odbiorców wiadomości oraz nie będzie przenosił prawa do korzystania ze swojej skrzynki pocztowej na jakiekolwiek osoby trzecie.
8. Pracownik powinien stosować odpowiednie środki ostrożności zapobiegające wprowadzeniu wirusów do systemu poczty elektronicznej, natomiast w razie wątpliwości powinien zasięgnąć porady ASI, bądź innej upoważnionej osoby.
9. Bezwzględnie zabrania się udostępniania przez Pracownika jakimkolwiek innym osobom jakichkolwiek haseł dostępu do kont, PIN-ów, a ponadto zabrania się notowania i przechowywania przez Pracownika haseł w sposób narażający na ich odczytanie przez osoby postronne.
10. Z uwagi na konieczność zapewnienia ochrony interesu i bezpieczeństwa danych osobowych Administrator zastrzega sobie prawo do wglądu we wszystkie wiadomości Pracownika o charakterze służbowym (zarówno w skrzynce odbiorczej, jak i nadawczej), przy czym kontrola służbowej korespondencji Pracowników oraz ich poczty elektronicznej może nastąpić w obecności Pracownika.
11. Za poprawność wprowadzenia adresu e-mail odbiorcy, odpowiedzialność ponosi Pracownik, zgodnie z obowiązkiem przestrzegania zasady merytorycznej poprawności danych. Zaleca się szczególną ostrożność przy wprowadzaniu adresu e-mail pamiętając o niebezpieczeństwie powstania incydentu/sytuacji zagrożenia dla danych osobowych (w takich wypadkach zastosowanie mają obowiązujące u Administratora procedury postępowania na wypadek powstania incydentu).
12. Zabrania się otwierania plików załączonych do nadesłanej przez nieznanego nadawcę korespondencji email. Bezwzględnie należy weryfikować nadawcę wiadomości, natomiast w razie jakichkolwiek wątpliwości, Pracownik zobowiązany jest skontaktować się w tej kwestii z ASI, bądź inną upoważnioną osobą.
13. Pracownik zobowiązany jest do ochrony danych osobowych oraz innych danych stanowiących tajemnicę służbową przed osobami postronnymi, w tym także osobami wspólnie z nim mieszkającymi.
14. W razie sytuacji budzących wątpliwość Pracownika w kwestiach związanych ze sposobem zabezpieczenia miejsca pracy zdalnej, należy skontaktować się z Pracodawcą, bądź osobami do tych celów upoważnionymi.
15. Niedopuszczalne jest przetwarzanie - w formie pracy zdalnej - danych posiadających klauzulę niejawności „zastrzeżone” lub wyższą. W razie otrzymania tego rodzaju informacji, Pracownik zobligowany jest skontaktować się z Pracodawcą lub inną osobą upoważnioną.
16. Informacje, niezależnie od nośnika, na którym zostały zapisane (np. pen-drive, dyski twarde itp.), przeznaczone do użytku służbowego (stanowiące własność Administaratora), mogą być wykorzystywane przez Pracownika wyłącznie do celów związanych z wykonywaniem obowiązków służbowych.
17. W przypadku wystąpienia kradzieży lub zgubienia urządzenia przenośnego zawierającego dane osobowe, Pracownik zobowiązany jest natychmiast powiadomić o tym fakcie administratora danych osobowych i inspektora ochrony danych osobowych, a powiadomienie powinno zawierać informacje, jakiego rodzaju dane były na tym urządzeniu przechowywane, oraz czy utracony nośnik informacji był zaszyfrowany.
18. Zabrania się podłączania do komputera i innych urządzeń wyposażanych w port USB powierzonych Pracownikowi do pracy w systemie zdalnym innych nośników, niż udostępnione Pracownikowi przez Administratora, chyba że doszło do w tej kwestii do odmiennych ustaleń z Administratorem, zaś komputer został wyposażony w stosowne zabezpieczenia i programy antywirusowe.
19. Korzystanie z sieci Internet na urządzeniach informatycznych przekazanych Pracownikowi w celu wykonywania pracy w trybie zdalnym dozwolone jest wyłącznie w celach służbowych.

20. Zabrania się wchodzenia – za pomocą służbowego komputera - na strony, na których prezentowane są informacje o charakterze przestępczym, hakerskim, pornograficznym, lub innym zakazanym przez prawo ze względu na wysokie ryzyko zainfekowania urządzeń i systemów informatycznych.
21. Ustawienia przeglądarki powinny mieć wyłączone w opcjach „autouzupełnianie" formularzy oraz zapamiętywanie haseł.
22. Pracownik w związku z wykonywaniem pracy w trybie zdalnym powinien pamiętać o przestrzeganiu zasady merytorycznej poprawności danych osobowych tj. należy pamiętać aby dane osobowe były prawidłowe i aktualne, zaś w razie potrzeby na bieżąco uaktualniane.
23. W związku z obowiązkiem przestrzegania zasady merytorycznej poprawności danych Pracownik powinien zadbać również o to aby wiadomość, która może zawierać załączniki (np. umowy, pisma) trafiła pod adres e-mail wskazany przez osobę uprawnioną wraz z treścią zgodną i aktualną z obowiązującym stanem faktycznym. W razie zaniedbań dotyczących powyższej zasady administrator danych osobowych może wyciągnąć konsekwencje służbowe wobec Pracownika dopuszczającego się takiego niedopełnienia.
24. Dane osobowe przetwarzane w związku z wykonywaniem pracy zdalnej mają być przetwarzane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami. Z kolei cele te powinny być określone nie później niż w momencie zbierania tych danych. Ponadto brak wskazania celu powoduje niemożność przetwarzania tych danych osobowych.

POSTANOWIENIA KOŃCOWE

XXVI. Obowiązki.

1. W kwestii Pani/Pana obowiązków zawodowych, z którymi związane jest przetwarzanie danych osobowych pozyskanych przez Pracodawcę, zobowiązuje Panią/Pana do:
   a. zapoznania się z obowiązującą dokumentacją ochrony danych osobowych oraz stosowania się do niej, a w razie wątpliwości do konsultowania się z Inspektorem ochrony danych osobowych;
   b. stosowania wszelkich instrukcji oraz zasad dotyczących przetwarzania danych osobowych, w tym nieudostępniania jakichkolwiek danych osobowych osobom trzecim bez zgody pracodawcy, nie wynoszenia żadnych nośników, dokumentów, czy informacji zawierających dane osobowe bez zgody pracodawcy;
   c. niezwłocznego informowania i zgłaszania Pracodawcy, zgodnie z Procedurą Postępowania w Przypadku Naruszenia Ochrony Danych Osobowych, będącą integralną częścią Polityki Ochrony Danych Osobowych obowiązującej w Jednostce, wszelkich incydentów związanych z naruszeniem zasad dotyczących ochrony danych osobowych.
2. Jest Pani/Pan zobowiązana/-y do przestrzegania następujących codziennych zasad związanych z obsługą i przetwarzaniem danych osobowych:
   a. niedozwolone jest kopiowanie dowodu osobistego lub innego dokumentu tożsamości bez konkretnej podstawy prawnej;
   b. należy przestrzegać zasad związanych z dyskretnym przetwarzaniem danych osobowych w obecności innych osób – osoba ma prawo do poufnego przetwarzania jego danych;
   c. udzielanie osobom postronnym/nieupoważnionym jakichkolwiek informacji na temat osoby fizycznej (np. innego klienta, innego Pracownika Administratora, nawet z grona osób najbliższych osobie pytającej o dane), będzie uznane za naruszenie podstawowych obowiązków pracowniczych i skutkować może nawet dyscyplinarnym zwolnieniem Pracownika oraz pociągnięciem go do odpowiedzialności odszkodowawczej;
   d. przy realizacji wniosków i spraw, pytania powinny zmierzać jedynie do uzyskania informacji w niezbędnym zakresie;

e. rozmowa telefoniczna sama w sobie jest przetwarzaniem danych osobowych klienta, więc należy zwracać uwagę na zakres oraz cel udzielanych w czasie rozmowy informacji (nie należy udzielać informacji na temat konkretnych danych osobowych z uwagi na znacznie ograniczoną możliwość weryfikacji rozmówcy i możliwość nagrywania rozmów przez osoby dzwoniące);
f. klientom należy udzielać informacji w przejrzystym i dostosowanym do konkretnej sytuacji języku bez nadmiernego formalizmu;
g. swoje obowiązki należy wykonywać w granicach upoważnienia do przetwarzania danych osobowych, a w sytuacjach wątpliwych należy na bieżąco konsultować się z Administratorem lub Inspektorem ochrony danych;
h. należy działać z tzw. należytą starannością i świadomością podczas podejmowania określonych czynności i decyzji;
i. należy weryfikować stan stanowiska pracy przed jej rozpoczęciem i po jej zakończeniu oraz zwracać uwagę na wszelkie budzące wątpliwość sytuacje;
j. w przypadku kradzieży, zniszczenia lub zagubienia danych, jak również w sytuacji wystąpienia innych incydentów należy niezwłocznie powiadomić Administratora;
k. wszelkie interwencje w sprawach należy załatwiać wyłącznie w pokojach za zamkniętymi drzwiami i bez udziału osób trzecich;
l. nie należy wyjaśniać jakichkolwiek spraw na korytarzach, poza pokojami, a zwłaszcza w obecności osób trzecich.

XXVII. Stosowanie Kodeksu.

1. Kodeks jest dokumentem wewnętrznym Jednostki i jest objęty obowiązkiem zachowania w poufności przez wszystkie osoby, którym zostanie ujawniony.
2. W sprawach nieokreślonych niniejszym Kodeksem należy stosować zasady opisane w Regulaminach, Instrukcjach oraz innych dokumentach obowiązujących u Administratora.
3. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się z niniejszym Kodeksem oraz złożyć stosowne oświadczenie, potwierdzające znajomość jej treści.
4. Niezastosowanie się do procedur określonych w niniejszym Kodeksie oraz w Regulaminach, Instrukcjach oraz innych dokumentach obowiązujących u Administratora, przez Pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52 ustawy z 26.06.1974 r. – Kodeks pracy (t,j. Dz.U. z 2022 r. poz. 1510).
5. Potrzeba przestrzegania Kodeksu dobrych praktyk RODO u Administratora wynika z następujących okoliczności:
   a. RODO wymaga aby konkretna podstawa przetwarzania danych wynikała z konkretnego przepisu prawnego;
   b. Pracownicy muszą wiedzieć, że w tym zakresie nie ma dowolności;
   c. Pracownikom nie wolno pozyskiwać ani ujawniać danych wedle własnego uznania;
   d. Pracownicy zawsze muszą wskazać podstawę prawną dla każdej procedury związanej z przetwarzaniem danych;
   e. w sytuacji wystąpienia nieprawidłowości i ukarania podmiotu publicznego za niezgodne z RODO przetwarzanie danych, każda nałożona kara może być dodatkowo traktowana jako naruszenie obowiązków służbowych Pracownika i dyscypliny budżetowej, co może rodzić indywidualną odpowiedzialność dyscyplinarną, karną lub cywilną.