REGULAMIN OCHRONY DANYCH OSOBOWYCH

MIEJSKI ZAKŁAD KOMUNIKACYJNY SP. Z O.O.
z siedzibą w Opolu przy ul. Luboszyckiej 19,
Opole 45-215
KRS: 0000033020, NIP: 7542490122,
REGON: 531313469

Pieczęć firmowa:	Podpis Administratora Danych Osobowych:	Data:

SPIS TREŚCI

1 Zasady bezpiecznego użytkowania sprzętu IT 4

2 Zasady korzystania z oprogramowania 5

3 Zasady korzystania z internetu 6

4 Zasady korzystania z poczty elektronicznej 6

5 Ochrona antywirusowa 7

6 Kontrola pracowników 7

7 Nadawanie upoważnień i uprawnień do przetwarzania danych osobowych 8

8 Polityka haseł 9

9 Procedura rozpoczęcia, zawieszenia i zakończenia pracy 9

10 Postępowanie z elektronicznymi nośnikami zawierającymi dane osobowe 10

11 Postępowanie z danymi osobowymi w wersji papierowej 10

12 Zapewnienie poufności danych osobowych 11

13 Skrócona instrukcja postępowania w przypadku naruszenia ochrony danych osobowych 11

14 Polityka kluczy 12

15 Postępowanie dyscyplinarne 13

WSTĘP

Realizując postanowienia Ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. 2016r., poz. 922 z zm.), ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. oraz wydane w oparciu o delegacje ustawą przepisy Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. (Dz. U. 2004r. Nr. 100 poz. 1024 z zm) w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych jakim powinny odpowiadać urządzenia i systemy informacyjne służące do przetwarzania danych osobowych wprowadza się zestaw reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji informacji wrażliwej pozwalający na zapewnienie ochrony danych osobowych.

Niniejszy regulamin stanowi wyciąg najistotniejszych zapisów zawartych w Polityce Bezpieczeństwa Ochrony Danych Osobowych oraz Instrukcji zarządzania systemami informatycznymi obowiązuje wszystkich Użytkowników, bez względu na rodzaj pracy i zajmowane stanowisko, zarówno Użytkowników etatowych Administratora Danych Osobowych, jak również współużytkowników (Użytkowników) wykonujących pracę na terenie zakładu na podstawie umów innych niż umowa o pracę, a mających upoważnienia do przetwarzania danych osobowych.

Ilekroć w Regulaminie jest mowa o:

- Administratorze Danych Osobowych (ADO) – rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, decydujące o celach i środkach przetwarzania danych osobowych. Administratorem danych osobowych jest Miejski Zakład Komunikacyjny Sp. z o.o.,

- Użytkowniku – rozumie się przez to upoważnionego przez Administratora Danych Osobowych, wyznaczonego do przetwarzania danych osobowych Użytkownika lub współużytkownika.

- Służbie IT- rozumie się przez to komórkę organizacyjną odpowiadającą za funkcjonowanie obszaru IT w przedsiębiorstwie.

1 Zasady bezpiecznego użytkowania sprzętu IT

1. Za sprzęt IT ADO uważa się w szczególności: komputery, laptopy, palmtopy, tablety, przenośne lub odłączalne banki pamięci w szczególności pendrive'y karty pamięci, dyski przenośne, dyski twarde, telefony komórkowe, smartfony, serwery, drukarki oraz inne narzędzia stanowiące własność ADO lub będące w użytkowaniu ADO wraz z oprogramowaniem służące do zbierania, przesyłania, opracowania, modyfikacji, przeglądania, przechowywania, zabezpieczania i prezentowania informacji, stanowiące własność ADO lub podmiotów kooperujących.

2. Sprzęt IT ADO jest przeznaczony do wykonywania obowiązków służbowych na rzecz ADO.

3. Użytkownik ponosi odpowiedzialność materialną za przekazany mu do użytku Sprzęt IT na zasadach odpowiedzialności za mienie powierzone. Przekazanie przenośnego sprzętu IT powinno zostać potwierdzone w protokole zdawczo – odbiorczym. Na protokole zostanie określone uprawnienie lub zakaz do wynoszenia sprzętu IT na zewnątrz.

4. Użytkownik zobowiązany jest korzystać ze Sprzętu IT w sposób zgodny z jego przeznaczeniem i instrukcją obsługi producenta, chronić go przed jakimkolwiek zniszczeniem lub uszkodzeniem i utrzymywać w należytym stanie technicznym.

5. Niedozwolone jest przechowywanie przez Użytkownika na Sprzęcie IT lub innych nośnikach danych należących do ADO prywatnych plików, za wyjątkiem prywatnych plików uzyskanych w sposób legalny i nienaruszających praw autorskich i licencyjnych.

6. Użytkownik jest zobowiązany nie dopuścić do ujawniania haseł dostępowych do systemów informatycznych ADO oraz do służbowej poczty elektronicznej (służbowego adresu e-mail) osobom nieuprawnionym.

7. Hasła dostępowe wykorzystywane przez Użytkownika powinny być cyklicznie zmienianie zgodnie z wytycznymi w punkcie 8 Polityka haseł nin. Regulaminu.

8. Użytkownik jest zobowiązany reagować na próby dostępu osób nieupoważnionych do sprzętu IT, a w szczególności podglądu danych na wydrukach i ekranach monitorów.

9. Użytkownik ma obowiązek natychmiast zgłosić ADO zagubienie, utratę lub zniszczenie powierzonego mu sprzętu IT.

10. Samowolne otwieranie (demontaż) Sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) lub podłączanie jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego jest zabronione.

11. ADO może monitorować pracę Użytkowników przy wykorzystaniu sprzętu IT, w celu kontroli jakościowej i ilościowej pracy, w tym poprzez monitoring służbowej skrzynki poczty elektronicznej, przy czym pracownicy objęci kontrolą są powiadomieni o tym fakcie.

12. ADO może kontrolować, czy Użytkownicy wykorzystują sprzęt IT do celów związanych z wykonywaniem ich obowiązków, w szczególności poprzez analizę wykazu połączeń i aktywności w sieci komputerowej oraz Internet.

13. W przypadku zmiany stanowiska pracy lub rozwiązania stosunku pracy lub rozwiązania, zakończenia innego rodzaju umowy łączącej, Użytkownik jest zobowiązany zwrócić Sprzęt IT ADO najpóźniej w ostatnim dniu zatrudnienia lub w ostatnim dniu świadczenia pracy lub usług na tym stanowisku.

14. Użytkownik jest zobowiązany do korzystania ze sprzętu IT zgodnie z instrukcją obsługi producenta lub zaleceniami służby IT. Użytkownik może ponieść koszty naprawy sprzętu IT w przypadku nieprawidłowej jego obsługi.

2 Zasady korzystania z oprogramowania

1. Użytkownik zobowiązuje się do korzystania wyłącznie z oprogramowania którego użytkowanie nie narusza zapisów licencji lub praw autorskich.

2. Użytkownik nie ma prawa instalować ani kopiować oprogramowania znajdującego się w zasobach ADO na swoje własne potrzeby ani na potrzeby osób trzecich bez zgody ADO.

3. Niedozwolone jest instalowanie na sprzęcie IT ADO jakiegokolwiek oprogramowania bez uprzedniej pisemnej zgody ADO lub upoważnionego pracownika Służby IT. Prawo do instalowania oprogramowania wynika z nadanych uprawnień.

4. Zmiana parametrów systemów mogą być wyłącznie przez osobę upoważnioną przez ADO w zakresie swoich uprawnień.

5. Instalowanie jakiegokolwiek oprogramowania na sprzęcie IT może być dokonane wyłącznie przez osobę upoważnioną w zakresie nadanych mu uprawnień.

6. Użytkownik ma prawo do użytkowania z oprogramowania przekazanego mu przez ADO.

7. Użytkownik nie ma prawa do zmiany parametrów systemu, które mogą być zmienione tylko przez osobę upoważnioną.

8. Użytkownik może pracować na innym komputerze niż tym, który został powierzony użytkownikowi, przy wykorzystaniu wyłącznie swojego loginu i hasła .

9. Użytkownik nie ma prawa wynoszenia poza siedzibę zakładu pracy jakiegokolwiek sprzętu komputerowego bez zgody ADO lub osoby przez niego wskazanej.

10. W przypadku naruszenia zasad odnoszących się do oprogramowana osoby upoważnione mają obowiązek usunąć nielegalnie lub niewłaściwie zainstalowane oprogramowanie, co może być wykonane bez uprzedzenia użytkownika.

3 Zasady korzystania z Internetu

1. Użytkownik ma prawo korzystać z Internetu w celu wykonywania obowiązków służbowych.

2. Przy korzystaniu z Internetu, użytkownik ma obowiązek przestrzegać prawa własności przemysłowej i praw autorskich.

3. Użytkownik nie ma prawa korzystać z Internetu w celu przeglądania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec obowiązujących zasad postępowania, a także grać w gry komputerowe w Internecie lub w systemie informatycznym ADO, ściągać z Internetu jakichkolwiek plików muzycznych, wideo, programów nie związanych z pracą.

4. W zakresie dozwolonym przepisami prawa, ADO zastrzega sobie prawo kontrolowania sposobu korzystania przez użytkownika z internetu pod kątem wyżej opisanych zasad. Ponadto, w uzasadnionym zakresie, ADO zastrzega sobie prawo kontroli czasu spędzanego i aktywności użytkownika w internecie. ADO może również blokować dostęp do niektórych treści dostępnych przez Internet, przy czym Użytkownicy objęci kontrolą są powiadomieni o tym fakcie.

4 Zasady korzystania z poczty elektronicznej i elektronicznych systemów przekazywania informacji

1. System Poczty Elektronicznej (adres e-mail) będący własnością ADO, komunikator oraz inne sposoby przekazywania informacji dostępne w komputerach którymi dysponuje ADO przeznaczone są do wypełniania obowiązków pracowniczych.

2. Użytkownik jest świadomy, że wszelkie wiadomości o charakterze prywatnym utworzone lub odebrane za pośrednictwem systemów przekazywania informacji przetwarzane są wyłącznie na jego własną odpowiedzialność.

3. Przy korzystaniu z systemów przekazywania informacji, Użytkownik ma obowiązek przestrzegać prawa własności przemysłowej, prawa autorskiego oraz zasad ochrony danych osobowych zawartych w przepisach prawa i regulacjach wewnętrznych ADO.

4. Użytkownik nie ma prawa korzystać z systemów przekazywania informacji w celu przeglądania lub rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania

5. Zakazuje się uczestnictwa w tzw. „łańcuszkach szczęścia" oraz innej aktywności w przekazywaniu informacji powielającej niechciane i niepożądane zachowania.

6. Użytkownik nie powinien otwierać przesyłek niewiadomego pochodzenia, nieoczekiwanej poczty, rozsyłanych reklam ani załączników będących ich częścią. Informacja o takiej korespondencji powinna być przekazywana Służbie IT.

7. W przypadku przesyłania plików danych osobowych do podmiotów zewnętrznych, Użytkownik zobowiązany jest do ich spakowania programem do kompresji i opatrzenia hasłem (8 znaków: duże , małe litery i cyfry lub znaki specjalne). Hasło należy przesłać odrębnym mailem. Dopuszcza się inne metody przekazywania danych o nie gorszym poziomie bezpieczeństwa.

5 Ochrona antywirusowa

1. Użytkownik zobowiązany są do skanowania plików wprowadzanych z zewnętrznych nośników programem antywirusowym.

2. Zakazane jest wyłączanie systemu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe.

3. W przypadku stwierdzenia zainfekowania systemu, Użytkownik obowiązany jest poinformować niezwłocznie o tym fakcie Służbę IT.

6 Kontrola pracowników

1. ADO ma prawo do prowadzenia stałej lub okresowej kontroli pracowników mającej na celu zapobieżenie zagarnięciu mienia ADO. Wszelkiego rodzaju kontrole odbywają się przez osoby upoważnione przez ADO z wyłączeniem kontroli osobistej.

2. W celu podniesienia poziomu bezpieczeństwa pracowników mienia oraz kontroli realizacji obowiązków pracowniczych, ADO ma prawo do monitorowania (przy wykorzystaniu telewizji przemysłowej oraz rejestratorów będących w posiadaniu kontrolerów):

   a. terenu zakładu pracy placów, ciągów komunikacyjnych, hal, pomieszczeń ogólnodostępnych oraz terenów przyległych znajdujących się w niedalekim sąsiedztwie w sposób ciągły;

   b. wnętrza oraz otoczenia autobusu w czasie jego jazdy i postoju zgodnie z Regulaminem Systemu Monitorowania;

   c. przebiegu kontroli biletowej i sytuacji po jej przeprowadzeniu w celu ochrony pracowników przed nieuzasadnionymi pomówieniami ze strony pasażerów.

3. Wszystkie pojazdy należące do spółki mogą być objęte monitoringiem GPS, np. do celów rozliczenia czasu pracy Użytkownika, jednocześnie ADO poinformuje Użytkownika, jaki zakres informacji będzie przez niego gromadzony (np. czas pracy w ruchu, czas postoju, dokładny adres postoju, szybkość przemieszczania się itd...)

7 Nadawanie upoważnień i uprawnień do przetwarzania danych osobowych

1. Za nadawanie upoważnień odpowiada osoba upoważniona przez ADO.

2. Osoba upoważniona jest informowana o zatrudnieniu nowego pracownika jak o zakończeniu stosunku pracy lub umowy zlecenia.

3. Każdy użytkownik systemu przed nadaniem upoważnienia musi:

   a. zapoznać się z niniejszym regulaminem;

   b. podpisać oświadczenie o poufności.

4. Osoba upoważniona nadaje pisemne upoważnienia Użytkownikom.

5. Upoważnienie nadawane jest do zbiorów w wersji papierowej i elektronicznej.

6. W przypadku, gdy upoważnienie udzielane jest do zbioru w wersji elektronicznej, nadawany jest użytkownikowi identyfikator w systemie oraz uprawniania nadawane przez Służbę IT.

7. W przypadku anulowania upoważnienia, identyfikator użytkownika jest blokowany w systemie.

8. Osoba upoważniona przez ADO odpowiada za aktualizację i anulowanie Upoważnień.

8 Polityka haseł

1. Hasło dostępu do zbioru danych składa się co najmniej z ośmiu (dużych i małych liter oraz z cyfr lub znaków specjalnych).
2. Zmianę hasła wymusza system lub użytkownik zobowiązany jest do manualnej zmiany hasła.
3. Użytkownik systemu w trakcie pracy w aplikacji może zmienić swoje hasło.
4. Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów.
5. Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności.
6. Zabronione jest zapisywanie haseł w sposób jawny oraz przekazywanie ich innym osobom.

9 Procedura rozpoczęcia, zawieszenia i zakończenia pracy

1. Użytkownik rozpoczyna pracę z systemem informatycznym przetwarzającym dane osobowe z użyciem identyfikatora i hasła.
2. Użytkownik jest zobowiązany do uniemożliwienia osobom nieuprawnionym (np. klientom) wglądu do danych wyświetlanych na monitorach komputerowych – tzw. „Polityka czystego ekranu”.
3. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu lub wylogować się z systemu.
4. Po zakończeniu pracy, użytkownik zobowiązany jest:
   a. wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy;
   b. zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe.

10 Postępowanie z elektronicznymi nośnikami zawierającymi dane osobowe

1. Elektroniczne nośniki, to: dyski twarde, dyski przenośne, pendrive'y, płyty CD, DVD, pamięci typu Flash.

2. Użytkownik nie może wynosić na zewnątrz firmy wymiennych elektronicznych nośników informacji z zapisanymi danymi osobowymi bez zgody bezpośredniego przełożonego.

3. Dane osobowe wynoszone poza firmę muszą być zaszyfrowane.

4. W przypadku uszkodzenia lub zużycia nośnika zawierającego dane osobowe należy go przekazać Służbie IT, która w razie konieczności może podjąć próbę ich odzyskania lub przekaże od zniszczenia.

5. Przekazywanie nośników z danymi osobowymi powinno być przeprowadzane z uwzględnieniem zasad bezpieczeństwa. Adresat powinien zostać powiadomiony o przesyłce, zaś nadawca powinien sporządzić kopię przesyłanych danych. Adresat powinien powiadomić nadawcę o otrzymaniu przesyłki. Jeżeli nadawca nie otrzymał potwierdzenia, zaś adresat twierdzi, że nie otrzymał przesyłki, użytkownik będący nadawcą powinien poinformować o zaistniałej sytuacji ADO.

11 Postępowanie z danymi osobowymi w wersji papierowej

1. Użytkownicy mają obowiązek dbać o czystość i porządek na stanowisku pracy i w jego najbliższym otoczeniu, a po zakończeniu pracy są zobowiązani do pozostawienia pracy w należytym porządku zgodnie z polityką „czystego biurka” i „polityką klucza” oraz między innymi do:

   a. użytkownicy wykonujący pracę biurową – zabezpieczenia akt i dokumentacji oraz do wyłączenia pracującego wyposażenia stanowisk pracy tj. komputerów, drukarek i innego sprzętu biurowego, a także zamknięcia okien i drzwi w pomieszczeniach;

   b. pozostali Użytkownicy – uporządkowania miejsca pracy oraz do należytego zabezpieczenia taboru służbowego, urządzeń, i narzędzi oraz do wyłączenia pracujących urządzeń.

2. Za bezpieczeństwo dokumentów i wydruków zawierających dane osobowe odpowiedzialne są osoby upoważnione (Użytkownicy) oraz kierownicy właściwych jednostek organizacyjnych.

3. Dokumenty i wydruki zawierające dane osobowe przechowuje się w pomieszczeniach zabezpieczonych fizycznie przed dostępem osób nieupoważnionych.

4. Użytkownik jest zobowiązany do stosowania „polityki czystego biurka". Polega ona na zabezpieczaniu dokumentów np. w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych.

5. Użytkownik jest zobowiązany do przewożenia dokumentów w sposób zapobiegający ich kradzieży, zagubieniu lub utracie.

6. Użytkownik jest zobowiązany do niszczenia dokumentów i tymczasowych wydruków w niszczarkach niezwłocznie po ustaniu celu ich przetwarzania.

12 Zapewnienie poufności danych osobowych

1. Użytkownik zobowiązany jest do zachowania w tajemnicy danych osobowych, do których ma lub będzie miał dostęp w związku z wykonywaniem zadań służbowych lub obowiązków pracowniczych lub zadań zleconych przez ADO.
2. Użytkownik zobowiązany jest do niewykorzystywania danych osobowych w celach pozasłużbowych bądź niezgodnych ze zleceniem o ile nie są one jawne.
3. Użytkownik zobowiązany jest do zachowania w tajemnicy sposobów zabezpieczenia danych osobowych o ile nie są one jawne.
4. Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym.

13 Skrócona instrukcja postępowania w przypadku naruszenia ochrony danych osobowych

1. Użytkownik zobowiązany jest do powiadomienia ADO w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych.

2. Typowe sytuacje, gdy użytkownik powinien powiadomić ADO:

   a. ślady na drzwiach, oknach i szafach wskazują na próbę włamania;

   b. dokumentacja jest niszczona bez użycia niszczarki;

   c. fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie;

   d. otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe;

   e. ustawienie monitorów pozwala na wgląd osób postronnych na dane osobowe;

f. wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz firmy bez upoważnienia ADO;

g. udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej i ustnej;

h. telefoniczne próby wyłudzenia danych osobowych;

i. kradzież sprzętu IT (komputerów, monitorów, drukarek, CD, DVD, dysków przenośnych, dysków twardych, pendrive'ów , kart pamięci i innego sprzętu);

j. maile zachęcające do ujawnienia identyfikatora i/lub hasła;

k. pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów;

l. hasła do systemów przechowywane są w pobliżu komputera.

14 Polityka kluczy

1. Polityka kluczy obejmuje wszystkie budynki i pomieszczenia firmy.
2. Polityka kluczy obowiązuje siedem dni w tygodniu, tzn. od poniedziałku do niedzieli 24 godziny na dobę.
3. Codzienny dostęp do pomieszczeń jest możliwy wyłącznie poprzez wyznaczone do tego wejścia i drzwi.
4. Zabrania się otwierania drzwi niewyznaczonych do tego bez wyrażenia zgody ADO lub osoby upoważnionej.
5. Klucze są wydawane wyznaczonym osobom.
6. Klucze zabezpieczające szafki, gabinety, biurka, szafy musza być jednoznacznie opisane.
7. W godzinach pracy klucze pozostają pod nadzorem Użytkowników upoważnionych, którzy ponoszą odpowiedzialność za ich należyte zabezpieczenie.
8. Pozostawienie kluczy w drzwiach, biurkach, szafkach podczas przerwy i kiedy w pobliżu znajdują się osoby nieupoważnione jest zabronione.

9. Po zakończeniu pracy klucze od biurek, szaf, gabinetów muszą być przechowywane w wyznaczonej do tego szafce.

15 Postępowanie dyscyplinarne

1. Przypadki, nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być traktowane jako ciężkie naruszenie obowiązków pracowniczych. Wobec Użytkownika, który w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjął działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.

2. Kara dyscyplinarna, orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity Dz. U. z 2016 r., poz. 922 z zm.) oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.