REGULAMIN OCHRONY DANYCH OSOBOWYCH – WYCIĄG Z POLITYKI BEZPIECZEŃSTWA

w

DDC Spółce z ograniczoną odpowiedzialnością Spółce komandytowej
(zwanym dalej „ADO" lub „DDC")

§1
REGULAMIN OCHRONY DANYCH OSOBOWYCH

1. Regulamin ochrony danych osobowych (zwany dalej „Regulaminem") stanowi wyciąg podstawowych uprawnień i obowiązków członków personelu DDC oraz procedur związanych z przetwarzaniem danych osobowych, określonych w Polityce bezpieczeństwa wdrożonej do stosowania w DDC.
2. Postanowienia Regulaminu obowiązują wszystkich członków personelu DDC, tj. pracowników, osoby współpracujące na podstawie umów o współpracy, umów zlecenia, umów o dzieło, praktykantów, stażystów i innych (zwanych dalej łącznie „Personelem" lub „Użytkownikami").

§2
OGÓLNE ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

1. Członek Personelu DDC uprawniony jest do przetwarzania danych osobowych wyłącznie w zakresie ustalonym indywidualnie w nadanym mu upoważnieniu i tylko w celu wykonywania powierzonych mu obowiązków.
2. Członek Personelu DDC upoważniony do przetwarzania danych osobowych zobowiązany jest do zachowania w tajemnicy tych danych oraz sposobów ich zabezpieczenia stosowanych w DDC.
3. Członek Personelu DDC zobowiązany jest do:
   1) zachowania w tajemnicy przetwarzanych danych osobowych oraz stosowanych przez ADO środków bezpieczeństwa, w szczególności sposobów zabezpieczenia danych osobowych i złożenia w zakresie przestrzegania tego zobowiązania oświadczenia na piśmie;
   2) odpowiedniego zabezpieczenia danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem Ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;
   3) przestrzegania zasad przetwarzania danych osobowych, w szczególności poprzez stosowanie przyjętych i wdrożonych w DDC procedur oraz wytycznych mających na celu zgodne z prawem i bezpieczne przetwarzanie danych osobowych

§3
POSTĘPOWANIE Z DANYMI OSOBOWYMI A WYKONYWANIE OBOWIĄZKOW SŁUŻBOWYCH

Członkowie Personelu DDC wykonując swoje obowiązki służbowe zobowiązani są zapewnić bezpieczeństwo przetwarzanym danym osobowym, w szczególności poprzez:

1) niepozostawianie osób postronnych w pomieszczeniu, w którym przetwarza się dane osobowe pod nieobecność osoby upoważnionej do przetwarzania danych osobowych,

2) nieużywanie powtórne jednostronnie zadrukowanych dokumentów, na których znajdują się dane osobowe, zaś w przypadku ustania ich przydatności niezwłocznego ich usuwania przy użyciu niszczarki;

3) usuwanie przy użyciu niszczarki wszelkich wydruków zawierających dane osobowe, które nie będą wykorzystywane w pracy, przed opuszczeniem miejsca pracy po zakończeniu dnia pracy;

4) chowanie do szaf zamykanych na klucz wszelkich akt, dokumentów i wydruków zawierających dane osobowe, przed opuszczeniem stanowiska pracy po zakończeniu dnia pracy;

5) zamykanie okien w razie opuszczenia pomieszczenia, w tym zwłaszcza po zakończeniu dnia pracy.

§4
PRZETWARZANIE DANYCH OSOBOWYCH PRZY UŻYCIU SYSTEMU INFORMATYCZNEGO

1. Członkowie Personelu DDC korzystając z systemu informatycznego, w tym urządzeń elektronicznych, komputerów, laptopów, tabletów, telefonów komórkowych (smartphonów), programów lub aplikacji komputerowych oraz zewnętrznych nośników danych zobowiązani są zapewnić bezpieczeństwo przetwarzanych danych osobowych.

2. Obowiązek określony w ust. 1 powyżej winien być realizowany w szczególności poprzez:

1) przestrzegania swoich uprawnień w systemie informatycznym, tj. właściwe korzystanie z baz danych oraz używanie tylko własnego identyfikatora i hasła oraz stosowania się w tym zakresie do zaleceń ADO;

2) niepodłączanie do listew podtrzymujących napięcie, przeznaczonych dla sprzętu komputerowego, innych urządzeń, szczególnie tych łatwo powodujących spięcia;
3) dbanie o prawidłową wentylację komputerów, w szczególności poprzez niezastawienie i nieprzykrywanie otworów wentylacyjnych;
4) strzeżenie nośników danych, w tym akt, płyt CD i DVD, pamięci przenośnych i komputerów przenośnych, w szczególności poprzez niepozostawienie ich bez nadzoru w miejscach, w których narażone są na nieuprawnione pozyskanie przez osoby trzecie;
5) zabezpieczenie nośnika, na którym zapisano hasła, w taki sposób by był niedostępny dla osób trzecich;
6) kończenie pracy na stacji roboczej po uprzednim zapisaniu wszystkich zmian i prawidłowym wylogowaniu się z systemu i wyłączeniu komputera;
7) usuwanie dokumentów elektronicznych i innych plików wytworzonych lub modyfikowanych w celach służbowych, w szczególności tych zawierających dane osobowy, z prywatnego komputera, tabletu, telefonu komórkowego (także z kosza) niezwłocznie po zakończeniu pracy, po uprzednim ich przesłaniu na służbową pocztę elektroniczną.

§5
ZAKAZ WYKONYWANIA OBOWIĄZKÓW SŁUŻBOWYCH POZA SIEDZIBĄ DDC PRZY UŻYCIU PRYWATNEGO SPRZĘTU KOMPUTEROWEGO

1. Wykonywanie obowiązków służbowych, w ramach którego dochodzi do przetwarzania danych osobowych, poza siedzibą DDC przy użyciu prywatnego sprzętu komputerowego (komputera, laptopa, tabletu) jest zabronione, z zastrzeżeniem ust. 2 poniżej.
2. W wypadkach nagłych i wyjątkowych, dopuszcza się wykonanie obowiązków służbowych w sposób, o którym mowa w ust. 1 powyżej, przy czym członek Personelu DDC obowiązany jest do usunięcia z prywatnego sprzętu komputerowego (także z poczty elektronicznej i kosza) dokumentów elektronicznych i innych plików wytworzonych lub zmodyfikowanych w celach służbowych, w szczególności tych zawierających dane osobowy, niezwłocznie po zakończeniu pracy, po uprzednim ich przesłaniu na służbową pocztę elektroniczną.

3. O każdym przypadku wykonania obowiązków służbowych w sposób, o którym mowa w ust. 1 powyżej, członek Personelu DDC zobowiązany jest niezwłocznie poinformować ADO.

§6
KORZYSTANIE PRZEZ UŻYTKOWNIKÓW Z POCZTY ELEKTRONICZNEJ

1. Członkowie Personelu DDC uprawnieni są do korzystania ze służbowej poczty elektronicznej wyłącznie w celach służbowych.
2. Korzystanie przez członków Personelu DDC z prywatnej poczty elektronicznej w celach służbowych, w szczególności polegające na przesyłaniu ze służbowego komputera lub serwera na prywatną pocztę elektroniczną dokumentów elektronicznych i innych plików, w tym tych zawierających dane osobowe, jest bezwzględnie zabronione.

§7
KORZYSTANIE PRZEZ UŻYTKOWNIKÓW Z SIECI PUBLICZNEJ INTERNET

Członkowie Personelu DDC uprawnieni są do korzystania z Internetu w celach służbowych, przy czym dopuszcza się możliwość przeglądania stron internetowych w celach prywatnych w trybie prywatnych (trybie incognito), za wyjątkiem pobierania prywatnych plików z niesprawdzonych źródeł; dokonywania zakupów, pobierania utworów muzycznych, tapet i innych plików, które nie służą celom służbowym.

§8
PROCEDURA POSTĘPOWANIA W PRZYPADKU NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

1. Naruszeniem bezpieczeństwa danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawniania danych osobowych, udostępniania lub umożliwiania dostępu do nich osobom nieupoważnionym, zabrania danych osobowych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego, a w szczególności:
   1) nieautoryzowany dostęp do danych osobowych;
   2) utrata nośników zawierających dane osobowe;
   3) nieautoryzowane modyfikacje lub zniszczenie danych osobowych;
   4) udostępnianie danych osobowych nieautoryzowanym podmiotom;

5) nielegalne ujawnianie danych osobowych;

6) pozyskiwanie danych osobowych z nielegalnych źródeł.

2. W przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego lub zaistnienia sytuacji, które mogą wskazywać na naruszenie zabezpieczenia danych osobowych, każdy członek personelu DDC jest zobowiązany przerwać przetwarzanie danych osobowych i niezwłocznie powiadomić o tym fakcie ABI lub ASI oraz bezpośredniego przełożonego, a następnie stosować się do podjętych przez niego decyzji.

3. Powiadomienie o naruszeniu ochrony danych osobowych powinno obejmować:

1) opis stwierdzonego naruszenia ochrony danych osobowych;

2) określenie sytuacji, miejsca i czasu, w jakim stwierdzono naruszenie ochrony danych osobowych;

3) określenie wszelkich istotnych informacji mogących wskazywać na przyczynę tego naruszenia;

4) określenie znanych danej osobie sposobów zabezpieczenia systemu oraz wszelkich kroków podjętych po ujawnieniu zdarzenia.

4. W celu realizacji procedury postępowania w przypadku naruszenia bezpieczeństwa danych osobowych, każdy członek Personelu DDC zobowiązany jest stosować się do poleceń i instrukcji ABI lub innej upoważniona przez niego osoby, a w szczególności zobowiązany jest do udzielania wszelkich wyjaśnień i informacji.

§9
ODPOWIEDZIALNOŚĆ ZA NARUSZENIE REGULAMINU

Naruszenie postanowień Regulaminu może stanowić ciężkie naruszenie podstawowych obowiązków pracowniczych lub poważne naruszenie zobowiązań umownych, a w konsekwencji stanowić podstawę do podjęcia przez ADO przysługujących mu środków prawnych, a w szczególności może stanowić przyczynę uzasadniającą:

1) zastosowanie kary porządkowej;

2) wypowiedzenie umowy o pracę albo innej umowy będącej podstawą świadczenia pracy na rzecz ADO;

3) rozwiązanie umowy o pracę albo innej umowy będącej podstawą świadczenia pracy na rzecz ADO bez wypowiedzenia z winy osoby odpowiedzialnej za naruszenie.