REGULAMIN OCHRONY DANYCH OSOBOWYCH

.....	.....	.....
administrator danych osobowych	podpis w imieniu administratora danych osobowych	data

Wstęp

Niniejszy Regulamin pomaga w ujednoliceniu i wdrożeniu najistotniejszych zapisów zawartych w dokumentacji ochrony danych osobowych, a które są jednocześnie wymagane prawem. Obowiązuje on pracowników etatowych oraz współpracowników, posiadających ważne upoważnienia do przetwarzania danych osobowych nadane przez administratora danych. Regulamin został utworzony w związku z wymaganiami zawartymi w ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000, 1669, z 2019 r. poz. 730.), oraz Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. oraz w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024) w związku z art. 68 i 69 ust.1 pkt 3 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (tekst jednolity: Dz.U.2013, poz. 885).

1. Nadawanie upoważnień i uprawnień

1. Administrator danych pełniący równocześnie funkcję administratora systemu informatycznego nadaje wszelkie upoważnienia dostępu do systemu.
2. Każdy zanim zostanie uprawniony do przetwarzania danych osobowych musi:
   a) zapoznać się z niniejszym Regulaminem,
   b) odbyć niezbędne szkolenie,
   c) podpisać oświadczenie o poufności i być świadomym obowiązków z tym związanych.
3. Upoważnienie nadawane jest do przetwarzania danych osobowych w wersji papierowej w następujących celach:

   a) Przetwarzanie danych osobowych do celów związanych z działalnością administratora danych jest zgodne z prawem w sytuacji, gdy dane te zostały uzyskane od osoby której dotyczą i dopuszczalne wtedy, gdy jest to niezbędne dla realizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa.

   b) W sytuacji, gdy dane osobowe nie zostały uzyskane od osoby której dotyczą, ich przetwarzanie jest zgodne z prawem, gdy przepis szczególny tak stanowi.

   c) Ocena niezbędności przetwarzania danych osobowych do wypełnienia usprawiedliwionych celów administratora danych powinna być dokonywana indywidualnie w każdej sytuacji.

   d) Przetwarzanie danych w celu innym niż ten, dla którego zostały zebrane, jest dopuszczalne jeżeli nie narusza praw i wolności osoby której dane dotyczą oraz następuje w celu realizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa.

4. W przypadku gdy upoważnienie udzielane jest do zbioru w systemie informatycznym, administrator tego systemu nadaje osobie indywidualny i unikalny identyfikator w systemie.
5. W przypadku odebrania upoważnienia do przetwarzania danych osobowych z jakiejkolwiek przyczyny, uprawnienia przydzielone w systemie informatycznym danej osoby są blokowane.
6. Administrator systemu odpowiada osobiście za rejestrowanie przydzielonych uprawnień w systemie informatycznym i zobowiązany jest do pilnowania i nadzorowania ich zgodności ze stanem rzeczywistym.
7. Należy mieć świadomość, że każdy, kto ma dostęp do pomieszczenia, w którym zainstalowano sprzęt systemu informatycznego może spowodować jego uszkodzenie lub może mieć dostęp do informacji wyświetlanych na monitorze lub wydruków. Zagrożenia w stosunku do systemu mogą pochodzić również od każdej innej osoby np. personelu pomocniczego, technicznego, konsultanta itp., posiadającej wystarczające umiejętności i wiedzę, aby uzyskać dostęp do sieci.
8. Pomieszczenia, w których znajdują się stanowiska komputerowe są: a) zamknięte, jeśli nikt w nich nie przebywa; b) wyposażone w sejfy lub inne pojemniki umożliwiające przechowywanie dokumentów. Instalacja urządzeń systemu i sieci teleinformatycznej odbywa się za wiedzą i pod kontrolą Administratora bezpieczeństwa informacji, który jest również odpowiedzialny za warunki wprowadzania do użycia, przechowywania, eksploatacji oraz wycofywania z użycia każdego urządzenia.

2. Polityka haseł

1. Hasło dostępu do systemu informatycznego składa się z co najmniej 8 znaków (dużych i małych liter oraz z cyfr lub znaków specjalnych).
2. Zmiana hasła dostępowego do systemu informatycznego następuje nie rzadziej niż co 30 dni oraz niezwłocznie w przypadku podejrzenia, że hasło mogło zostać ujawnione.
3. Użytkownik systemu w trakcie pracy w aplikacji jeśli zajdzie taka potrzeba może zmienić swoje hasło.
4. Zmiana hasła dokonywana jest przez użytkownika automatycznie.
5. Hasła nie mogą być powszechnie używanymi słowami, w szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów.
6. Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności, w szczególności zabronione jest zapisywanie haseł w sposób jawny w miejscach nieprzeznaczonych do tego oraz przekazywanie ich innym osobom.

3. Użytkowanie systemu informatycznego

1. Sprzęt informatyczny składa się z komputerów stacjonarnych, sieciowego sprzętu drukującego oraz stacji serwerowych.
2. Użytkownik systemu wykonuje wszelkie prace niezbędne do efektywnej oraz bezpiecznej pracy na stanowisku pracy /również z wykorzystaniem stacji roboczej/. Jest zobowiązany do utrzymania niezbędnych warunków bezpieczeństwa w szczególności do przestrzegania

procedur dostępu do systemu i ochrony danych osobowych. Osoba korzystająca z systemu informatycznego:

a) ma obowiązek używania sprzętu w sposób: zgodny z jego przeznaczeniem, w sposób zgodny z załączoną do niego instrukcją obsługi oraz do ochrony sprzętu przed zniszczeniem, utratą lub uszkodzeniem,
b) jest zobowiązana do niezwłocznego informowania administratora tego systemu o każdej sytuacji zniszczenia, utraty lub uszkodzenia powierzonego sprzętu,
c) nie może instalować i korzystać samowolnie z żadnego oprogramowania w systemie informatycznym, którego nie zaaprobował wcześniej ASI, ani próbować złamać lub uzyskać uprawnień administracyjnych w tym systemie, zabrania się również zgrywania na dysk twardy komputera oraz uruchamiania jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła (nielegalne źródło pochodzenia). Pliki takie powinny być ściągane tylko za każdorazową zgodą Administratora Danych Osobowych i tylko w uzasadnionych przypadkach, pod warunkiem, że nie doprowadzi to do złamania prawa.
d) nie może samowolnie ingerować, przenosić, otwierać (demontować) sprzętu, instalować dodatkowych urządzeń (np. twardych dysków, pamięci) lub podłączać jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego (w tym prywatnych urządzeń, nawet jedynie w celu ładowania baterii tych urządzeń).

3. Polityka antywirusowa W zakresie ochrony antywirusowej wprowadza się następujące zalecenia: a) nie należy używać oprogramowania na stacji roboczej innego niż zaleca administrator systemu; b) nie wolno instalować oprogramowania typu freeware czy shareware; c) regularnie uaktualniać bazę wirusów zainstalowanego oprogramowania antywirusowego; d) przed użyciem nośnika danych sprawdzić czy nie jest zainfekowany wirusem komputerowym.

4. Polityka czystego ekranu

1. Polityka **czystego ekranu**, tj. podjęcie wszelkich działań aby osoby nieupoważnione nie miały wglądu w treści wyświetlane na monitorach ekranowych lub ekranach komputerów przenośnych na których są przechowywane dane Klientów.
2. Osoba uprawniona do korzystania z systemu informatycznego przy każdym odejściu od stanowiska pracy jest zobowiązana do manualnego uruchamiania wygaszacza ekranu chronionego hasłem również w sytuacji gdy pozostawia system informatyczny bez nadzoru nawet na chwilę.
3. Zrzutów ekranów z systemu informatycznego gdzie są wyświetlane dane, jak i wysyłanie takich informacji poza organizację bez zgody administratora tego systemu jest zabronione.
4. Każdy kto jest uprawniony do korzystania z systemu informatycznego jest zobowiązany do:
   a) ustawiania monitorów i ekranów komputerów przenośnych w taki sposób, by nie można było podejrzeć wyświetlanych na nich treści zarówno względem okien jak i drzwi wejściowych do pomieszczeń w których się znajdują,

b) zapewnienia w sytuacji uruchamiania komputerów przenośnych poza obszarem przetwarzania np. lotniska, dworce, sale konferencyjne i w każdym innym miejscu publicznym, dyskrecji i ochrony wyświetlanych tam danych,
c) nadzorowania osób nieupoważnionych pozostających w obszarze przetwarzania danych.

5. Polityka czystego biurka i czystego druku

1. **Polityka czystego biurka**, tj. dbanie aby po zakończonej pracy wszelkie dokumenty na których znajdują się dane osób znajdowały się poza zasięgiem nieuprawnianego wzroku i dłoni.
2. Jeżeli pomieszczenie jest zaopatrzone w meble bądź szafkę zamykaną na klucz, to należy zamykać szafy przed zakończeniem pracy, wcześniej umieszczając w nich wszystkie wrażliwe dane i dokumenty, a klucze umieszczać w bezpiecznym miejscu aby osoby nieuprawnione nie miały do nich dostępu.
3. Każdy kto ostatni upuszcza miejsce przetwarzania danych powinien sprawdzić, czy wszystkie okna są zamknięte oraz czy wszelkie inne zabezpieczenia są uruchomione np. system alarmowy. Należy go uzbroić, drzwi należy zamknąć oraz uruchomić wszelkie inne systemy bezpieczeństwa.
4. Zabrania się pozostawiania dokumentów i wydruków zawierających dane osobowe w miejscach gdzie znajdują się urządzenia typu drukarki, kserokopiarki, skanery, bez nadzoru. Wszelkie dokumenty błędnie wydrukowane lub które przeznaczone są do wyrzucenia, należy niezwłocznie niszczyć z wykorzystaniem niszczarek lub pojemników do utylizacji dokumentacji poufnej.
5. Jeśli jest to konieczne i dochodzi do sytuacji przewozu dokumentów w wersji papierowej danych osobowych poza obszar ich przetwarzania, musi odbywać się to w sposób zapewniający ich poufność, tj. dokumenty muszą być zakryte i zabezpieczone przed przypadkową utratą i wglądem dla osób do tego nieuprawnionych.

6. Udostępnianie danych osobowych

1. Osoba przetwarzająca dane osobowe, gdy przekazuje dane drogą telefoniczną musi mieć pewność co do tożsamości swojego rozmówcy, w razie wątpliwości co do tożsamości należy zawiadomić administratora o problemie w ustaleniu tożsamości rozmówcy. Jeżeli ustne przekazanie danych nie gwarantuje poufności, należy skorzystać z udostępnienia w wersji pisemnej (do wglądu).
2. Dane osobowe można udostępnić tylko osobie, której dane dotyczą, lub innej osobie za jej zgodą przechowywaną w celach dowodowych przy zachowaniu procedury przewidzianej w punkcie powyższym.
3. Udostępniając dane osobowe poza siedzibą, gdzie nie mogą one być należycie chronione (np. w miejscach publicznie dostępnych), należy zagwarantować maksymalną poufność tych danych.
4. Ryzyko ujawnienia osobom nieuprawnionym danych osobowych lub innych informacji o stosowanych zabezpieczeniach należy niwelować przez podejmowanie różnych adekwatnych do tego celu środków. Sytuacje ryzykowne to takie jak:

a) żądanie danych o zastosowanych zabezpieczeniach przez osoby podszywające się (kradzież tożsamości),
b) żądanie udostępnienia informacji o poprzednio stosowanych hasłach dostępowych do systemów informatycznych (socjotechnika telefoniczna),
c) wszelkie inne podejrzane żądania udostępnienia niejawnych informacji, w szczególności drogą telefoniczną.

7. Korzystanie z dostępu do Internetu

1. Każdy kto przetwarza dane jest zobowiązany do korzystania z Internetu tylko w celu niezbędnym dla realizacji funkcji, które powierza mu administrator. Jest kategoryczny zakaz odwiedzania podczas pracy stron internetowych w celach prywatnych.
2. Przy korzystaniu z Internetu osoby przetwarzające dane mają obowiązek przestrzegać prawa, a zwłaszcza przestrzegać własności przemysłowej i praw autorskich.
3. Osoby przetwarzające dane mają kategoryczny zakaz korzystać z Internetu w celu przeglądania treści o charakterze niezwiązanym z ich funkcją, pracą a zwłaszcza o treści obraźliwej, niemoralnej lub niestosownej wobec powszechnie obowiązujących zasad postępowania, a także grać w gry komputerowe w Internecie lub w systemie informatycznym, oglądać filmy, lub korzystać z innej szeroko pojętej rozrywki.
4. W zakresie dozwolonym przepisami prawa administrator danych zastrzega sobie prawo do wglądu i kontrolowania sposobu korzystania przez osoby przetwarzające dane z Internetu, pod kątem wyżej opisanych zasad.

8. Korzystanie z poczty elektronicznej

1. Poczta elektroniczna jest przeznaczona i może być wykorzystywana wyłącznie do wykonywania obowiązków na zajmowanym stanowisku, każde inne wykorzystanie jest niedozwolone i może być przyczyną do pociągnięcia do odpowiedzialności.
2. Przy korzystaniu z poczty elektronicznej osoby przetwarzające dane mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego.
3. Osoby przetwarzające dane powinny zachować szczególną uwagę, by przez nieuwagę nie wysłać za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej wiadomości zawierających informacji określanych jako poufne osobom nieuprawnionym, dotyczące np. administratora danych, jego pracowników, klientów, dostawców lub kontrahentów.
4. Osoby przetwarzające dane powinny wykazać szczególną rozwagę i nie powinny otwierać wiadomości przesłanych drogą elektroniczną od nieznanych sobie nadawców, gdy tytuł nie sugeruje związku z wypełnianymi przez nie obowiązkami na zajmowanym stanowisku powinny takie wiadomości zgłosić administratorowi i wykasować ze swojej skrzynki pocztowej.
5. W przypadku przesyłania plików drogą elektroniczną, zawierających dane osobowe do podmiotów zewnętrznych, które są do tego uprawnione, osoba przetwarzająca dane zobowiązana jest do ich spakowania i opatrzenia hasłem. Hasło należy przesłać odrębnym środkiem komunikacji tak aby w razie błędnego wysłania bądź nieautoryzowanego przejęcia nie doszło do ryzyka otwarcia pliku z danymi.

9. Elektroniczne nośniki danych

1. Elektroniczne nośniki danych to np. wymienne twarde dyski, pen-drive, płyty CD, DVD, pamięci typu Flash.
2. Osoby przetwarzające dane nie mogą wynosić poza obszar przetwarzania wymiennych elektronicznych nośników zarówno prywatnych jak i udostępnionych w przypadku przegrania na nie informacji z danymi osobowymi bez zgody administratora danych i bez jego wiedzy w każdorazowym przypadku.
3. W przypadku uszkodzenia, zużycia lub zaprzestania korzystania z danego nośnika zawierającego dane osobowe należy fizycznie go zniszczyć przez spalenie lub rozdrobnienie tak aby zawarte na nich informacje nie mogły być ponownie odczytane bądź wykorzystane.

10. Instrukcja alarmowa

1. Osoba przetwarzająca dane zobowiązana jest do powiadomienia administratora danych w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych.
2. Administrator systemów informatycznych po stwierdzeniu naruszenia systemu informatycznego ma obowiązek, zabezpieczyć ślady pozwalające na określenie przyczyn naruszenia systemu informatycznego, przeanalizować i określić skutki naruszenia systemu informatycznego, określić czynniki, które spowodowały naruszenie systemu informatycznego, dokonać niezbędnych korekt w systemie informatycznym polegających na zabezpieczeniu systemu przed ponownym jego naruszeniem. Administrator podejmuje podobne środki w sytuacji gdy stwierdzi, że:

a) ślady na drzwiach, oknach i szafach wskazują na próbę włamania,
b) dokumentacja z danymi jest niszczona bez użycia niszczarki bądź nie niszczona wcale,
c) drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe, pozostają otwarte,
d) ustawienie monitorów nie zapewnia bezpieczeństwa przed wglądem osób nieupoważnionych,
e) ma miejsce nieautoryzowane kopiowanie i wynoszenie danych osobowych w wersji bądź to papierowej i/lub elektronicznej poza obszar przetwarzania bez zgody i poinformowania admina,
f) występują telefoniczne próby wyłudzenia danych osobowych bądź haseł dostępowych,
g) nastąpiła kradzież komputerów lub elektronicznych nośników danych,
h) pojawia się zagrożenie notyfikowane przez program antywirusowy,
i) hasła do systemów nie są należycie zabezpieczone bądź przechowywane są w pobliżu komputera.

11. Postępowanie dyscyplinarne

1. Wszelkie przypadki nieuzasadnionego niedopełnienia wytycznych co do ochrony danych wynikających z niniejszego Regulaminu mogą zostać potraktowane jako ciężkie naruszenie podstawowych obowiązków pracowniczych lub zobowiązań umownych, które nakładają na dana osobę przymus określonego zachowania się w danej sytuacji.

Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego podejrzenia takiego naruszenia nie podjęła działania określonego w niniejszym Regulaminie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, można wszcząć postępowanie dyscyplinarne co nie wyklucza pociągnięcia jej co do odpowiedzialności na podstawie odpowiednich przepisów prawa, za powstałą szkodę bądź ryzyko jej powstania.

2. Kara dyscyplinarna gdy zostanie zastosowana wobec osoby uchylającej się od powiadomienia administratora o niebezpieczeństwie, nie wyklucza pociągnięcia jej do dodatkowej odpowiedzialności karnej zgodnie w ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000, 1669, z 2019 r. poz. 730.), oraz Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego o zrekompensowanie poniesionych strat.