REGULAMIN
OCHRONY DANYCH

Niniejszy Regulamin stanowi doprecyzowanie zapisów zawartych w dokumentacji ochrony danych osobowych spółki DGD AGENCY sp. z o.o. Obowiązuje pracowników oraz współpracowników, posiadających ważne upoważnienia do przetwarzania danych osobowych nadane przez administratora danych osobowych.

Rozdział I
[nadawanie upoważnień i uprawnień]

1. Za nadawanie upoważnień do przetwarzania danych osobowych odpowiada Administrator Danych Osobowych.
2. Każda osoba przed nadaniem upoważnienia do przetwarzania danych osobowych jest zobowiązana do:
   a) zapoznania się z niniejszym regulaminem;
   b) odbycia szkolenia z zasad ochrony danych osobowych;
   c) podpisania oświadczenia o poufności.
3. Upoważnienie do przetwarzania danych osobowych nadawane jest w wersji papierowej.
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, uprawnienia przydzielone w systemie informatycznym osoby są blokowane.
6. Administrator systemów informatycznych odpowiada za rejestrowanie przydzielonych uprawnień w systemie informatycznym.

Rozdział II

[polityka haseł]

1. Hasła użytkowników powinny składać się z minimum 12 znaków.
2. Hasła użytkowników powinny zawierać duże litery + małe litery + cyfry i znaki specjalne.
3. Hasła użytkowników nie mogą być łatwe do odgadnięcia. Nie powinny być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion i nazwisk osób bliskich, imion zwierząt, popularnych dat, popularnych słów, typowych zestawów: 123456, qwerty, admin itp.
4. Hasła użytkowników nie powinny być ujawnianie innym osobom. Nie należy zapisywać haseł na kartkach i w notesach, nie naklejać na monitorze komputera, nie trzymać pod klawiaturą lub w szufladzie.
5. W przypadku ujawnienia hasła – należy natychmiast zgłosić ten fakt administratorowi systemów informatycznych lub dokonać zmiany.
6. Hasła muszą być zmieniane co 30 dni.
7. Jeżeli system informatyczny nie wymusza zmiany haseł, użytkownik zobowiązany jest do samodzielnej zmiany hasła.
8. Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności.
9. Zabrania się używania w innych miejscach i do celów prywatnych takich samych lub podobnych haseł jak w systemie informatycznym firmy.
10. Zabrania się stosowania tego samego hasła jako zabezpieczenia w dostępie do różnych systemów informatycznych.

Rozdział III

[procedura pracy]

1. Każdy użytkownik systemu informatycznego musi posiadać swój własny indywidualny identyfikator (login) i hasło.
2. Użytkownik nie może samodzielnie zmieniać swoich uprawnień.
3. Każdy użytkownik musi posiadać indywidualny identyfikator. Zabronione jest umożliwianie innym osobom pracy na koncie innego użytkownika.
4. Zabrania się pracy wielu użytkowników na wspólnym koncie.
5. Użytkownik rozpoczyna pracę z użyciem identyfikatora i hasła.

6. Użytkownik jest zobowiązany do powiadomienia administratora systemów informatycznych o próbach logowania się do systemu osoby nieupoważnionej, jeśli system to sygnalizuje.
7. W przypadku, gdy użytkownik podczas próby zalogowania się zablokuje system, zobowiązany jest powiadomić o tym administratora systemów informatycznych.
8. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest zablokować ekran komputera wygaszaczem ekranu, blokadą ekranu lub wylogować się z systemu.
9. 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.

Rozdział IV
[użytkowanie systemu informatycznego]

1. Sprzęt informatyczny służący do przetwarzania danych osobowych składa się w szczególności z:
   a) komputerów stacjonarnych,
   b) komputerów przenośnych,
   c) telefonów komórkowych (smartfonów),
   d) tabletów,
   e) sprzętu sieciowego,
   f) sprzętu drukującego,
   g) nośników danych,
   h) routera,
   i) switchy,
   j) access pointów.
2. Osoba korzystająca z systemu informatycznego:
   a) jest zobowiązana do użytku sprzętu w sposób zgodny z jego przeznaczeniem oraz do ochrony sprzętu przed zniszczeniem, utratą lub uszkodzeniem,
   b) jest zobowiązana do informowania administratora tego systemu o każdej sytuacji zniszczenia, utraty lub uszkodzenia powierzonego sprzętu,

c) nie może instalować samowolnie żadnego oprogramowania w systemie informatycznym, ani próbować złamać lub uzyskać uprawnienia administracyjne w tym systemie,
d) nie może samowolnie 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),
e) jest zobowiązana do usuwania plików z nośników/dysków do których mają dostęp inni użytkownicy nieupoważnieni do dostępu do takich plików,
f) nie może samodzielnie podłączać jakichkolwiek urządzeń do portów komputera, w szczególności portów USB.

Rozdział V
[polityka czystego ekranu]

1. Osoba korzystająca z systemu informatycznego jest zobowiązana do zachowania polityki czystego ekranu, tj. zapewnienia, by osoby nieupoważnione nie miały wglądu w treści wyświetlane na monitorach ekranowych lub ekranach komputerów.
2. Osoba korzystająca z systemu informatycznego jest zobowiązana do manualnego uruchamiania wygaszacza ekranu chronionego hasłem w każdej sytuacji, gdy pozostawia system informatyczny bez nadzoru.
3. Zabronione jest gromadzenie danych osobowych w postaci tzw. zrzutów ekranów z systemu informatycznego, jak i wysyłanie takich informacji bez zgody administratora tego systemu.
4. Osoby korzystające z systemu informatycznego powinny zwracać szczególną uwagę na:
   a) ustawienie monitorów lub ekranów komputerów w obszarze przetwarzania względem okien (w przypadku blisko siebie sąsiadujących budynków) oraz drzwi wejściowych, przez które mogą wejść osoby nieupoważnione,
   b) uruchamianie komputerów przenośnych poza obszarem przetwarzania w miejscach publicznie dostępnych (np. lotniska, dworce, sale konferencyjne, itp.),
   c) osoby nieupoważnione pozostające w obszarze przetwarzania danych bez nadzoru osób upoważnionych.

Rozdział VI

[polityka czystego biurka i czystego druku]

1. Osoba przetwarzająca dane osobowe jest zobowiązana do zachowania polityki czystego biurka, tj. zapewnienia, by po zakończeniu pracy wszelkie dane osobowe zarówno w wersji papierowej, jak i na elektronicznych nośnikach znajdowały się poza zasięgiem wzroku i dłoni.
2. Osoba przetwarzająca dane osobowe jest zobowiązana do stosowania wszelkich zabezpieczeń danych udostępnionych przez administratora danych, tj. jeżeli pomieszczenie jest zaopatrzone w meble zamykane na klucz, to należy zamykać szafy przed zakończeniem pracy, a klucze umieszczać w bezpiecznym miejscu.
3. Ostatnia osoba opuszczająca obszar przetwarzania jest zobowiązana do sprawdzenia, czy wszystkie okna są zamknięte (ryzyko zalania pomieszczeń lub włamania) oraz czy wszelkie inne zabezpieczenia są uruchomione.
4. Niedozwolone jest pozostawianie wydruków zawierających dane osobowe w pobliżu urządzeń drukujących bez nadzoru. Dokumenty błędnie wydrukowane należy niezwłocznie zniszczyć z wykorzystaniem niszczarek lub pojemników do utylizacji .
5. Przewożenie poza obszarem przetwarzania wersji papierowej danych osobowych musi odbywać się w sposób zapewniający ich poufność, tj. dokumenty muszą być zakryte i zabezpieczone przed przypadkową utratą.

Rozdział VII

[udostępnianie danych osobowych]

1. Osoba przetwarzająca dane osobowe może udostępniać dane osobowe drogą telefoniczną jedynie wtedy, gdy ma pewność co do tożsamości swojego rozmówcy (w razie wątpliwości należy weryfikować tożsamość np. poprzez żądanie podania fragmentu informacji znanej tylko osobie właściwej).
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 ust. 1 powyżej.
3. Udostępniając dane osobowe w miejscach publicznie dostępnych, należy zagwarantować poufność danych. Jeżeli ustne przekazanie danych nie gwarantuje poufności, należy skorzystać z udostępnienia w wersji pisemnej (do wglądu).

4. Należy zwracać uwagę na sytuacje mogące stanowić ryzyko ujawnienia danych osobowych lub informacji o stosowanych zabezpieczeniach osobie nieupoważnionej, takie jak:

a) żądanie udostępnienia danych przez osoby podszywające się (kradzież tożsamości),
b) żądanie udostępnienia informacji o stosowanych zabezpieczeniach, w tym w szczególności udostępnienia obecnych, jak i poprzednio stosowanych haseł dostępowych do systemów informatycznych (socjotechnika telefoniczna),
c) wszelkie inne nieuzasadnione i podejrzane żądania udostępnienia informacji, w szczególności drogą telefoniczną.

Rozdział VIII
[korzystanie z sieci www]

1. Osoby przetwarzające dane są uprawnione do korzystania z dostępu do sieci Internet jedynie w celu wykonywania obowiązków służbowych.
2. Podczas korzystania z Internetu osoby przetwarzające dane są zobowiązane do przestrzegania przepisów prawa dotyczących ochrony własności intelektualnej oraz ochrony prawa autorskiego i praw pokrewnych.
3. Korzystanie z sieci Internet przez osoby przetwarzające dane w celu przeglądania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania, jak również używanie internetowych gier komputerowych lub gier znajdujących się w systemie informatycznym jest niedozwolone.
4. W zakresie dozwolonym powszechnie obowiązującymi przepisami prawa, administrator danych zastrzega sobie prawo do kontrolowania sposobu korzystania z sieci Internet przez osoby przetwarzające dane. Kontrola ma na celu sprawdzenie przestrzegania zasad bezpieczeństwa w sferze przetwarzania danych osobowych.
5. Zabrania się pobierania na dysk twardy komputera oraz instalowania i uruchamia jakichkolwiek plików programów.
6. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu.
7. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.
8. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na bezpieczne połączenie oraz adresu www rozpoczynającego się od https.

9. Należy zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku, portalu społecznościowego, e-sklepu, poczty mailowej) lub podania naszych loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet.

Rozdział IX
[korzystanie ze skrzynek poczty elektronicznej]

1. Poczta elektroniczna jest przeznaczona wyłącznie do wykonywania obowiązków służbowych.
2. Podczas korzystania z poczty elektronicznej osoby przetwarzające dane są zobowiązane do przestrzegania przepisów prawa dotyczących ochrony własności intelektualnej oraz ochrony prawa autorskiego i praw pokrewnych.
3. Wysyłanie wiadomości zawierających informacje określone jako poufne, dotyczące administratora danych, jego pracowników, klientów, dostawców lub kontrahentów za pośrednictwem sieci internet, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej, przez osoby przetwarzające dane jest niedozwolone.
4. Osoby przetwarzające dane nie powinny otwierać wiadomości przesłanych drogą elektroniczną od nieznanych sobie nadawców w szczególności, gdy tytuł nie wskazuje na istnienie związku z obowiązkami służbowymi.
5. Użytkownicy nie powinni uruchamiać wykonywalnych załączników dołączonych do wiadomości przesyłanych pocztą elektroniczną.
6. W przypadku przesyłania plików zawierających dane osobowe do podmiotów zewnętrznych, osoba przetwarzająca dane zobowiązana jest do ich spakowania i opatrzenia hasłem. Hasło należy przesłać odrębnym środkiem komunikacji (np. SMS).
7. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
8. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.
9. Podczas wysyłania wiadomości email do wielu adresatów jednocześnie, należy użyć metody: ukryte do wiadomości – UDW. Zabronione jest przesyłanie wiadomości email do wielu adresatów z użyciem metody: do wiadomości – DW.

10. Zabronione jest przesyłanie korespondencji służbowej na prywatne skrzynki pocztowe użytkownika lub innych osób.
11. Zabroniona jest zmiana konfiguracji poczty lub programu pocztowego do automatycznego przekierowywania wiadomości email na adres zewnętrzny.
12. Zabronione jest wysyłanie wiadomości zawierających dane osobowe lub inne informacje firmowe za pośrednictwem prywatnej poczty email.

Rozdział X
[aktualizacja oprogramowania]

1. Użytkownicy zobowiązani są do niezwłocznego poinformowania administratora systemów informatycznych o każdym przypadku powiadomienia o konieczności aktualizacji oprogramowania.
2. Użytkownicy zobowiązani są do skanowania plików wprowadzanych z zewnętrznych nośników programem antywirusowym, jeśli system antywirusowy taką funkcje posiada.
3. Zabronione jest wyłączanie oprogramowania antywirusowego lub zapory w systemie informatycznym.

Rozdział XI
[Elektroniczne nośniki danych]

1. Elektroniczne nośniki danych to np. wymienne twarde dyski, pendrive, płyty CD, DVD, Blue-Ray pamięć typu Flash.
2. Osoby przetwarzające dane nie mogą wynosić poza obszar przetwarzania wymiennych elektronicznych nośników informacji z zapisanymi danymi osobowymi bez zgody administratora danych.
3. Dane osobowe wynoszone na nośnikach elektronicznych poza obszar przetwarzania muszą być zaszyfrowane, pliki powinny być zabezpieczone hasłem.
4. W przypadku uszkodzenia lub zużycia nośnika zawierającego dane osobowe należy fizycznie zniszczyć nośnik przez spalenie lub rozdrobnienie.
5. Należy zapewnić bezpieczne przewożenie dokumentacji papierowej w plecakach, teczkach.

6. W przypadku, gdy dokumentację papierową lub nośniki elektroniczne przewozi pracownik, zobowiązany jest do zabezpieczenia przewożonych dokumentów przed zagubieniem i kradzieżą
7. W przypadku konieczności wysyłki dokumentacji papierowej lub nośników elektronicznych należy korzystać ze sprawdzonych firm kurierskich.

Rozdział XII

[elektroniczne nośniki danych]

1. Elektroniczne nośniki danych to np. wymienne twarde dyski, pendrive, płyty CD, DVD, Blue-Ray pamięć typu Flash.
2. Osoby przetwarzające dane nie mogą wynosić poza obszar przetwarzania wymiennych elektronicznych nośników informacji z zapisanymi danymi osobowymi bez zgody administratora danych.
3. Dane osobowe wynoszone na nośnikach elektronicznych poza obszar przetwarzania muszą być zaszyfrowane, pliki powinny być zabezpieczone hasłem.
4. W przypadku uszkodzenia lub zużycia nośnika zawierającego dane osobowe należy fizycznie zniszczyć nośnik przez spalenie lub rozdrobnienie.
5. Należy zapewnić bezpieczne przewożenie dokumentacji papierowej w plecakach, teczkach.
6. W przypadku, gdy dokumentację papierową lub nośniki elektroniczne przewozi pracownik, zobowiązany jest do zabezpieczenia przewożonych dokumentów przed zagubieniem i kradzieżą
7. W przypadku konieczności wysyłki dokumentacji papierowej lub nośników elektronicznych należy korzystać ze sprawdzonych firm kurierskich.

Rozdział XIII

[instrukcja alarmowa]

1. Osoba przetwarzająca dane zobowiązana jest do powiadomienia administratora danych w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych, w szczególności gdy:
   a) ślady na drzwiach, oknach i szafach wskazują na próbę włamania,
   b) dokumentacja jest niszczona bez użycia niszczarki,

c) drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe, pozostają otwarte,
d) ustawienie monitorów pozwala na wgląd osób nieupoważnionych,
e) ma miejsce nieautoryzowane wynoszenie danych osobowych w wersji papierowej i/lub elektronicznej poza obszar przetwarzania,
f) występują telefoniczne próby wyłudzenia danych osobowych,
g) nastąpiła kradzież komputerów lub elektronicznych nośników danych,
h) pojawia się zagrożenie notyfikowane przez program antywirusowy,
i) hasła do systemów przechowywane są w pobliżu komputera.

Rozdział XIV

[zachowanie poufności]

1. Każda z osób dopuszczona do przetwarzania danych osobowych jest zobowiązana do:
   a) przetwarzania danych osobowych wyłącznie w zakresie i celu określonym w upoważnieniu,
   b) zachowania w tajemnicy danych osobowych do których ma dostęp w związku z wykonywaniem zadań,
   c) niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem określonym w upoważnieniu,
   d) zachowania w tajemnicy sposobów zabezpieczenia danych osobowych i systemów informatycznych,
   e) ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem.
2. Jeśli jest to przewidziane, osoba dopuszczona do przetwarzania odbywa szkolenie z zasad ochrony danych osobowych.
3. Zabrania się przekazywania lub ujawniania danych osobowych osobom lub instytucjom, które nie mogą wykazać się jasną podstawą prawną do dostępu do takich danych.

4. Zabrania się ujawniania na grupach dyskusyjnych, forach internetowych, blogach itp. jakichkolwiek szczegółów dotyczących funkcjonowania firmy, w tym informacji na temat

sprzętu i oprogramowania, z jakiego korzysta firma, oraz informacji kontaktowych innych, niż ogólnodostępne w materiałach zewnętrznych.

Rozdział XV

[postępowanie dyscyplinarne]

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego Regulaminu mogą zostać potraktowane jako ciężkie naruszenie obowiązków pracowniczych lub zobowiązań umownych. 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, może zostać wszczęte postępowanie dyscyplinarne.
2. Kara dyscyplinarna zastosowana wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby, na podstawie ustawy o ochronie danych osobowych oraz możliwości wniesienia przez administratora powództwa cywilnego o odszkodowanie.

wprowadzono dnia 07.08.2024 r..