Załącznik nr 3

do Polityki Ochrony Danych Osobowych

Toruń, dnia 25 maja 2018 r.

Zasady bezpieczeństwa w systemach informatycznych
służących do przetwarzania danych osobowych
DRIMER Sp. z o.o. sp.k. z siedzibą w Toruniu

I. ZAKRES ZASTOSOWANIA

1. Niniejszy dokument, stanowiący część Polityki Ochrony Danych Osobowych, określa zasady zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych, a w szczególności:
   a) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w Systemie Informatycznym;
   b) metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;
   c) procedury rozpoczęcia, zawieszenia i zakończenia pracy przez użytkowników Systemu;
   d) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;
   e) sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych;
   f) sposób zabezpieczenia Systemu Informatycznego przed działalnością wirusów komputerowych, nieuprawnionym dostępem oraz awariami zasilania;
   g) sposoby realizacji w Systemie wymogów dotyczących przetwarzania danych;
   h) procedury wykonywania przeglądów i konserwacji Systemu oraz nośników informacji służących do przetwarzania danych.
2. Ilekroć w niniejszym dokumencie jest mowa o:
   a. sieci lokalnej – należy przez to rozumieć połączenie systemów informatycznych Administratora wyłącznie dla własnych potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych,
   b. sieci rozległej – należy przez to rozumieć sieć publiczną w rozumieniu art. 1 ust. 1 pkt 29 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (t.j. – Dz. U. z 2017 r., poz. 1907).

II. REJESTROWANIE I WYREJESTROWANIE UŻYTKOWNIKA – NADAWANIE UPRAWNIEŃ

1. Użytkownikiem Systemu Informatycznego, mającym dostęp do danych osobowych może być osoba upoważniona przez Spółkę w dowolnej formie, zaś w przypadku Danych Szczególnych – działająca na podstawie pisemnego upoważnienia.
2. Uzyskanie uprawnień następuje na dwóch poziomach:
    1) Zarejestrowanie w systemie (założenie konta),
    2) Nadanie upoważnienia do przetwarzania danych osobowych.
3. Osoba odpowiedzialna za obsługę informatyczną tworzy oraz modyfikuje konta dostępowe/ pocztowe pracownika oraz ustawia dostęp do wybranych baz danych i aplikacji na podstawie informacji o nowym pracowniku oraz o wszelkich zmianach stanu zatrudnienia uzyskanych od osoby odpowiedzialnej.
4. W przypadku zakończenia pracy lub wygaśnięcia upoważnienia osoba odpowiedzialna za obsługę informatyczną likwiduje konto po uzyskaniu informacji od bezpośredniego przełożonego pracownika lub innej upoważnionej osoby informację o zakończeniu pracy w Spółce. Wyrejestrowanie Użytkownika (skasowanie konta dostępowego) jest jednoznaczne z uniemożliwieniem mu dostępu do systemu informatycznego (zablokowanie dostępu).
5. Uprawnienia osób upoważnionych do przetwarzania danych osobowych są rejestrowane w systemie informatycznym. Wszystkie formularze i inne dokumenty związane z rejestrowaniem i wyrejestrowaniem Użytkowników są archiwizowane i przechowywane przez Spółkę.

III. SPOSÓB UWIERZYTELNIANIA UŻYTKOWNIKA I POLITYKA HASEŁ

1. Każdorazowe uwierzytelnienie Użytkownika w systemie informatycznym następuje po podaniu identyfikatora i hasła.
2. W Spółce obowiązują następujące zasady korzystania z haseł:
    1) Hasło użytkownika:
        a) Składa się z co najmniej 8 znaków,
        b) Hasło musi zawierać co najmniej jedną małą literę, jedną wielką literę, jedną cyfrę oraz co najmniej jeden znak specjalny,
        c) Hasło do kont o uprawnieniach administratora systemu są kilkunastoznakowe i zawierają co najmniej jedną małą literę, jedną wielką literę, jedną cyfrę oraz jeden znak specjalny,
        d) Zmiana hasła następująca co 30 dni.
    2) Elementy systemu informatycznego związane z bezpieczeństwem dostępu są tak sparametryzowane, aby wymusić stosowanie podanych zasad.

3) Niezastosowanie przez użytkownika zasad wskazanych w punkcie 1 a.-c. powoduje odmowę dostępu do systemu informatycznego.

3. Prawidłowe wykonywanie obowiązków związanych z korzystaniem przez Użytkowników z haseł nadzoruje osoba odpowiedzialna za obsługę informatyczną. Nadzór ten w szczególności polega na okresowym monitorowaniu funkcjonowania mechanizmu uwierzytelniania.
4. Użytkownicy zobowiązani są do zachowania w tajemnicy swoich haseł i mogą je udostępnić innej osobie w zakresie, w jakim jest to niezbędne do wykonywania swoich obowiązków pracowniczych.
5. Wprowadzanie hasła powinno odbywać się w sposób, który uniemożliwia zapoznanie się z hasłem przez inne osoby.

IV. PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY

1. Przed przystąpieniem do pracy w systemie informatycznym Użytkownik zobowiązany jest sprawdzić urządzenie komputerowe i stanowisko pracy ze zwróceniem uwagi, czy nie zaszły okoliczności wskazujące na naruszenie ochrony danych osobowych.
2. Użytkownik rozpoczyna pracę w systemie informatycznym od następujących czynności:
    1) Włączenia komputera,
    2) Uwierzytelnienia się (logowania) w systemie informatycznym za pomocą swojego identyfikatora i hasła,
    3) Uwierzytelnienia się (logowania) w ramach dostępnej Użytkownikowi bazy danych.
3. Niedopuszczalne jest logowanie się z wykorzystaniem identyfikatora i hasła innego Użytkownika, jak również przekazywanie przez Użytkownika swego hasła innym Użytkownikom.
4. Przy opuszczaniu stanowiska pracy na odległość uniemożliwiającą jego obserwację należy uniemożliwić osobom nieuprawnionym dostęp do Systemu Informatycznego, np. poprzez zastosowanie wygaszacza ekranu wymagającego podania hasła lub poprzez wylogowanie się z Systemu. Najprostszym i zalecanym sposobem blokady dostępu do komputera jest użycie kombinacji klawisz z logo systemu Windows + L.
5. Zakończenie przez użytkownika pracy w systemie informatycznym następuje po wylogowaniu się z Systemu. Po zakończeniu pracy Użytkownik zobowiązany jest zabezpieczyć swoje stanowisko pracy, w szczególności informatyczne nośniki danych, dokumenty i wydruki zawierające dane osobowe, przed dostępem osób nieupoważnionych oraz wyłączyć komputer, bądź pozamykać wszystkie otwarte bazy danych, pliki i aplikacje i zablokować komputer.
6. W przypadku wystąpienia nieprawidłowości w mechanizmie uwierzytelniania się w systemie informatycznym oraz/lub bazie danych Użytkownik niezwłocznie powiadamia o nich pracownika odpowiedzialnego za obsługę informatyczną.

V. PROCEDURA TWORZENIA KOPII ZAPASOWYCH ZBIORÓW DANYCH ORAZ PROGRAMÓW I NARZĘDZI PROGRAMOWYCH SŁUŻĄCYCH DO ICH PRZETWARZANIA

1. Spółka odpowiada za okresowe wykonanie kopii bezpieczeństwa danych gromadzonych w Systemie Informatycznym, przy pomocy przewidzianych przez System Informatyczny narzędzi.
2. Kopia zbioru danych na każdym komputerze jest tworzona nie rzadziej niż co 7 (siedem) dni poprzez kopiowanie zbiorów danych na specjalnie wydzielony do tego celu obszar dysku na zewnętrznym serwerze.
3. Kopie zapasowe przechowuje się na serwerze odrębnym od tego, na którym zbiór danych eksploatowany jest na bieżąco. Regularnie, nie rzadziej niż co miesiąc, kopie zapasowe przechowywane na serwerze zewnętrznym powinny być kopiowane na dysk zewnętrzny, który jest przechowywany u osoby odpowiedzialnej w Spółce za obsługę informatyczną.
4. Kopie zapasowe przechowywane są w sposób uniemożliwiający nieuprawnione przejęcie, modyfikację, uszkodzenie lub zniszczenie.
5. Dostęp do nośników z kopiami zapasowymi Systemu Informatycznego oraz kopiami danych osobowych ma Zarząd Spółki oraz osoba odpowiedzialna za obsługę informatyczną.
6. Kopie zapasowe zbiorów danych są okresowo sprawdzane pod kątem ich przydatności do odtworzenia przez Spółkę Systemu Informatycznego.
7. Po ustaniu ich użyteczności, kopie zapasowe danych przetwarzanych w Systemie Informatycznym są niezwłocznie usuwane.
8. Kopie zapasowe danych przetwarzanych w Systemie Informatycznym, które uległy uszkodzeniu, podlegają natychmiastowemu zniszczeniu.
9. Nośniki z backupem są okresowo sprawdzane pod kątem ich przydatności do odtworzenia danych.

VI. SPOSÓB I CZAS PRZECHOWYWANIA NOŚNIKÓW INFORMACJI, W TYM KOPII INFORMATYCZNYCH ORAZ WYDRUKÓW

1. Za zewnętrzne nośniki danych uważa się:
    - dyski CD-R, CD-RW, DVD-R, DVD-RW itp.;
    - twarde dyski wymienne;
    - taśmy magnetyczne;
    - komputery przenośne;

- inne nośniki, służące do przechowywania danych i mogące być przenoszone niezależnie od sprzętu komputerowego.

2. Nieupoważnieni Użytkownicy nie mogą bez upoważnienia wykonywać kopii baz (zbiorów) danych oraz zapisywać – na informatycznych nośnikach danych – danych osobowych, w szczególności dokonywać kopii zapasowej całych zbiorów danych.
3. Dane osobowe w postaci elektronicznej, za wyjątkiem kopii bezpieczeństwa, mogą być wynoszone poza obszar przetwarzania danych osobowych tylko w przypadku zapisania ich na przeznaczonym do tego komputerze przenośnym i przez upoważnionych do tego pracowników lub współpracowników Spółki.
4. Wymienne elektroniczne nośniki informacji zawierające dane osobowe są przechowywane na terenie zakładu Spółki.
5. Po zakończeniu pracy przez Użytkowników Systemu Informatycznego wymienne elektroniczne nośniki informacji zawierające dane osobowe są przechowywane w zamykanych szafach biurowych lub kasetkach.
6. Urządzenia, dyski lub inne informatyczne nośniki zawierające dane osobowe, przeznaczone do likwidacji, są pozbawiane zapisu tych danych, a w przypadku, gdy nie jest to możliwe, są uszkadzane w sposób uniemożliwiający ich odczytanie.
7. Urządzenia, dyski lub inne informatyczne nośniki zawierające dane osobowe przeznaczone do naprawy są pozbawiane danych zapisu tych danych.
8. Fizycznej likwidacji zniszczonych lub niepotrzebnych informatycznych nośników danych z danymi osobowymi należy dokonywać w sposób uniemożliwiający odczyt danych osobowych.
9. Dopuszczalne jest zlecenie/powierzenie niszczenia wszelkich nośników danych osobowych wyspecjalizowanym podmiotom zewnętrznym. Podstawą przekazania danych do zniszczenia innemu podmiotowi powinna być w każdym przypadku umowa zawarta na piśmie.
10. Dostęp do wydruków z Systemu Informatycznego zawierających dane osobowe mają wyłącznie osoby do tego upoważnione.
11. Wydruki są przechowywane w miejscu uniemożliwiającym bezpośredni do nich dostęp osobom niepowołanym.

VII. PROCEDURA I SPOSÓB ZABEZPIECZENIA PRZED OPROGRAMOWANIEM, KTÓREGO CELEM JEST NIEUPRAWNIONY DOSTĘP DO ZASOBÓW SYSTEMU INFORMATYCZNEGO ORAZ POSTĘPOWANIE W PRZYPADKU AWARII ZASILANIA

1. Na wszystkich komputerach (w tym także komputerach przenośnych) oraz serwerach zostało zainstalowane oprogramowanie antywirusowe oraz oprogramowanie zapobiegające nieuprawnionemu dostępowi do Systemu Informatycznego.

2. Połączenie lokalnej sieci komputerowej z siecią rozległą jest dopuszczalne wyłącznie przy włączonym oprogramowaniu antywirusowym oraz po zainstalowaniu mechanizmów ochronnych (firewall).
3. Zabrania się:
    a. używania zewnętrznych nośników informacji bez wcześniejszego sprawdzenia ich programem antywirusowym, a w przypadku gdy pochodzenie nośnika nie jest możliwe, zabrania się w ogóle używania takiego nośnika,
    b. zabrania się pobierania z sieci rozległej plików co do których istnieje podejrzenie, że mogą zawierać złośliwe oprogramowanie/wirusa,
    c. otwierania/pobierania załączników do wiadomości elektronicznej bez wcześniejszego sprawdzenia ich programem antywirusowym.
4. Pracownik Spółki odpowiedzialny za obsługę informatyczną Spółki przeprowadza cykliczne, nie rzadziej niż co 3 (trzy) miesiące, kontrole antywirusowe na wszystkich komputerach w Spółce.
5. W przypadku stwierdzenia wystąpienia wirusa Zarząd Spółki, osoba odpowiedzialna za obsługę informatyczną lub inny upoważniony pracownik zobowiązany jest do podjęcia działań zmierzających do wykrycia źródła pojawienia się wirusa w Systemie Informatycznym, jego wyeliminowania, a jeśli jest to niemożliwe – do usunięcia zainfekowanego pliku.
6. Sprzęt komputerowy służący do przetwarzania danych osobowych jest wyposażony w urządzenia podtrzymujące zasilanie.
7. W przypadku wystąpienia przerw w dostawie energii elektrycznej osoba odpowiedzialna za obsługę informatyczną lub inny upoważniony pracownik zobowiązany jest do:
    - zakończenia trwających procesów;
    - zakończenia pracy sprzętu (np. komputera).
8. Po przywróceniu zasilania i upewnieniu się, że jest ono trwałe osoba odpowiedzialna za obsługę informatyczną lub inny upoważniony pracownik zobowiązany jest do:
    - włączenia sprzętu komputerowego;
    - kontroli poprawności jego funkcjonowania i działania Systemu Informatycznego.
9. W przypadku stwierdzenia nieprawidłowości działania Systemu Informatycznego osoba odpowiedzialna za obsługę informatyczną lub inny upoważniony pracownik zobowiązany jest do niezwłocznego podjęcia czynności, związanych z usunięciem awarii.

VIII. PROCEDURA USUWANIA AWARII SPRZĘTU LUB OPROGRAMOWANIA

1. W przypadku wystąpienia awarii Systemu Informatycznego pracownik lub współpracownik, który ją stwierdził zobowiązany jest do zgłoszenia faktu wystąpienia awarii Zarządowi Spółki, osobie odpowiedzialnej za obsługę informatyczną lub upoważnionemu pracownikowi.
2. Administrator danych, osoba odpowiedzialna za obsługę informatyczną lub upoważniony pracownik zobowiązany jest do niezwłocznego podjęcia czynności zmierzających do usunięcia awarii np. poprzez wezwanie serwisu.
3. Po usunięciu awarii administrator danych, osoba odpowiedzialna za obsługę informatyczną lub inny upoważniony pracownik zobowiązany jest do:
   - uruchomienia Systemu Informatycznego;
   - kontroli poprawności jego funkcjonowania;
   - kontroli integralności danych.
4. W przypadku stwierdzenia uszkodzenia danych zgromadzonych w Systemie, Zarząd Spółki, osoba odpowiedzialna za obsługę informatyczną lub inny upoważniony pracownik zobowiązany jest do otworzenia danych z ostatniej posiadanej kopii bezpieczeństwa (backup).
5. W przypadku gdy usunięcie awarii wymaga przekazania sprzętu komputerowego na zewnątrz, przed przekazaniem tego sprzętu osoba odpowiedzialna za obsługę informatyczną lub inny upoważniony pracownik zobowiązany jest do usunięcia z dysków twardych wszystkich danych, po ich uprzednim skopiowaniu na inny nośnik. Jeśli z przyczyn technicznych jest to niemożliwe, osoba przekazująca sprzęt ze strony Spółki zobowiązana jest uzyskać od serwisanta protokół przyjęcia danych i zobowiązanie do zachowania ich poufności.

IX. SPOSÓB REALIZACJI WYMOGU ZAPISANIA W SYSTEMIE INFORMATYCZNYM INFORMACJI O ODBIORCACH DANYCH

1. Dane osobowe zapisane w Systemie Informatycznym mogą być udostępniane partnerom Spółki, w tym w szczególności podmiotom kapitałowo lub osobowo powiązanym ze Spółką, które korzystają z tego samego Systemu Informatycznego co Spółka.
2. W przypadku udostępniania danych osobowych zapisanych w Systemie Informatycznym podmiotom innym, niż partnerzy Spółki korzystający z tego samego Systemu Informatycznego, co Spółka, możliwe jest sporządzenie i wydrukowanie raportu, zawierającym następujące informacje:
   - identyfikatora osoby, której dane dotyczą;
   - odbiorcy danych;
   - zakresu udostępnienia danych osobowych;

- daty operacji udostępnienia.

X. SPOSÓB REALIZACJI WYMOGU UDOSTĘPNIENIA DANYCH W INTEROPERACYJNYM FORMACIE DANYCH

Po wpływie oraz akceptacji wniosku osoby fizycznej, osoba obsługująca zgłoszenie przekazuje żądanie udostępnienia danych osobie odpowiedzialnej za obsługę informatyczną lub przy pomocy narzędzi dostępnych z poziomu oprogramowania dokonuje eksportu danych do formatu:

- PDF (Portable Document Format) lub
- ODF (Open Document Format)

XI. SPOSÓB I CZAS PRZECHOWYWANIA NOŚNIKÓW INFORMACJI, W TYM KOPII INFORMATYCZNYCH ORAZ WYDRUKÓW

1. Dokumenty papierowe zawierające dane osobowe przechowywane są wyłącznie w specjalnie do tego celu przeznaczonych segregatorach, w szafach zamykanych na klucz.
2. Nieupoważnieni Użytkownicy nie mogą wykonywać kopii baz danych oraz zapisywać - na informatycznych nośnikach danych - danych osobowych, w szczególności dokonywać kopii zapasowej całych zbiorów danych.
3. Fizycznej likwidacji zniszczonych lub niepotrzebnych informatycznych nośników danych z danymi osobowymi należy dokonywać w sposób uniemożliwiający odczyt danych osobowych.
4. Dopuszczalne jest zlecenie/powierzenie niszczenia wszelkich nośników danych osobowych wyspecjalizowanym podmiotom zewnętrznym. Podstawą przekazania danych do zniszczenia innemu podmiotowi powinna być w każdym przypadku umowa zawarta na piśmie.

XII. PROCEDURY WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMU INFORMATYCZNEGO ORAZ INFORMATYCZNYCH NOŚNIKÓW DANYCH

1. Przegląd i konserwacja Systemu Informatycznego oraz informatycznych nośników danych zawierających dane osobowe dokonywane są poprzez:
    a) sprawdzanie zgodności danych z dokumentami;
    b) analizę zgłaszanych uwag użytkowników.
2. Przeglądu i konserwacji Systemu Informatycznego dokonuje Zarząd Spółki, osoba odpowiedziana za obsługę informatyczną lub inny upoważniony pracownik. Dopuszczalne jest zlecenie/powierzenie przeglądów i konserwacji zbiorów danych wyspecjalizowanym podmiotom zewnętrznym na podstawie pisemnych umów.

3. Przekazywane na zewnątrz Informatyczne nośniki danych (komputery, dyski, laptopy), dla celów naprawy czy konserwacji, nie zawierają baz (zbiorów) danych osobowych.