REGULAMIN PRZETWARZANIA DANYCH OSOBOWYCH

DLA ZLECEBIOBIORCÓW I OFWCA

Multiagencja Conditor Sp. z o. o. S.K.A., w związku z zawarciem Umów Centralnych o Wykonywanie Czynności Agencyjnych oraz Umów Powierzenia Danych Osobowych niniejszym przekazuje do zapoznania i zobowiązuje do stosowania niniejszego Regulaminu Przetwarzania Danych Osobowych, zwanego dalej **Regulaminem.**

Niniejszy dokument opisuje reguły oraz procedury dotyczące sposobu przetwarzania oraz bezpieczeństwa przetwarzania Danych Osobowych,

Opisane reguły i procedury określają granice dopuszczalnego zachowania wszystkich osób przetwarzających Dane Osobowe współpracujących z Multiagencją Conditor. Dokument zwraca uwagę na konsekwencje, jakie mogą ponosić osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń w związku z naruszeniem bezpieczeństwa przetwarzania Danych Osobowych.

Regulamin obowiązuje wszystkie osoby przetwarzające dane osobowe (bez względu na formę współpracy) dokonujących jakichkolwiek operacji na Danych Osobowych. Realizacja postanowień tego dokumentu ma zapewnić ochronę Danych Osobowych, właściwą ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa przetwarzania oraz zapewnić właściwy tryb działania w celu przywrócenia bezpieczeństwa danych przetwarzanych w systemach informatycznych.

Celem niniejszego dokumentu oraz opisanych w nim reguł i procedur jest – zwłaszcza w odniesieniu do pracowników i współpracowników, którzy w toku pracy i współpracy przetwarzają lub mają styczność z danymi osobowymi – spełnienie następujących postulatów:

- spełnienie wymagań prawnych dotyczących przetwarzania Danych Osobowych jako cel podstawowy,

- zwiększenie świadomości co do wagi i wartości informacji wynikających z Danych Osobowych, w tym w szczególności Danych Osobowych szczególnie chronionych,
- konieczność ochrony Danych Osobowych oraz dóbr osobistych osób, których Dane dotyczą,
- ochrona informacji oraz zapewnienie prywatności i godności każdego pracownika, współpracownika, klienta oraz innych osób, których Dane dotyczą,
- ciągłe uczenie się i wyciąganie wniosków z błędów,
- stałe doskonalenie rozwiązań dostosowujących działania do nowych celów oraz potencjalnych zagrożeń związanych z przetwarzaniem Danych Osobowych,
- uświadomienie i zapewnienie, że wszyscy pracownicy i współpracownicy są zobowiązani do przestrzegania szczegółowych zasad postępowania wskazanych w niniejszym dokumencie.

§1

DEFINICJE

- **Zleceniobiorca** – osoba lub podmiot, z którym Multiagencja Conditor sp. z o. o. S.K.A zawarła Umowę Centralną; pomiot przetwarzający na podstawie Umowy Powierzenia Danych;
- **OFWCA**- osoba fizyczna wykonująca czynności agencyjne,
- **Sieć Telekomunikacyjna** - sieć telekomunikacyjna oraz publiczna sieć telekomunikacyjna w rozumieniu odpowiednio art. 2 pkt. 35 oraz art. 2 pkt 29 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (t. j.: Dz. U. z 2017 r., poz. 1907, ze zm.), w tym w szczególności Internet,
- **System Informatyczny** – zbiór powiązanych ze sobą elementów: serwerów z systemami operacyjnymi, systemu zarządzania Bazami Danych Osobowych, oprogramowania (programów użytkowych), urządzeń końcowych (komputerów, terminali, drukarek) oraz urządzeń służących do komunikacji między sprzętowymi elementami systemu,
- **Baza Danych Osobowych (Baza)** – każdy posiadający strukturę zbiór danych, które są lub mogą stanowić Dane Osobowe, dostępny według określonych kryteriów,
- **Dane Osobowe (Dane)** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
- **Hasło** – ciąg znaków literowych, cyfrowych lub innych pozwalający na dostęp do Systemu Informatycznego, znany jedynie osobie uprawnionej do pracy w Systemie Informatycznym,

- **Ustawa** – ustawa o ochronie danych osobowych,
- **Przetwarzanie Danych Osobowych** – jakiekolwiek operacje (zwłaszcza te, które wykonuje się w systemach informatycznych) wykonywane na Danych Osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, usuwanie i inne,
- **Podmiot przetwarzający** – podmiot, o którym mowa w art. 28 RODO, który dokonuje czynności przetwarzania Danych Osobowych na zlecenie Administratora Danych Osobowych.
- **Użytkownik (Użytkownicy)** - każda osoba upoważniona – Zleceniobiorcy i do bezpośredniego dostępu do Danych Osobowych.
- **PUODO** – Prezes Urzędu Ochrony Danych Osobowych, pełniący funkcję organu nadzorczego na terenie Rzeczpospolitej Polskiej w rozumieniu art. 4 pkt 21 w zw. z art. 51 ust. 1 RODO,
- **RODO** - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem Danych Osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne Rozporządzenie o Ochronie Danych Osobowych),

§2

PODSTAWA PRAWNA

Regulamin jest zgodny z następującymi aktami prawnymi:

a) Konstytucją Rzeczypospolitej Polskiej,
b) RODO,
c) Ustawą,
d) przepisami innych aktów prawnych powszechnie obowiązujących w zakresie, w jakim dotyczą ochrony danych osobowych.

§3

ZAKRES OBOWIĄZYWANIA

1. Ochrona Danych Osobowych obowiązuje wszystkie osoby, które mają dostęp do Danych Osobowych podlegających przetwarzaniu, bez względu na zajmowane stanowisko oraz miejsce wykonywania jak również charakter umowy lub stosunku pracy.

2. Zleceniobiorcy i OFWCA są zobligowani do stosowania niezbędnych środków zapobiegających ujawnieniu Danych Osobowych osobom nieupoważnionym, w tym w szczególności procedur i reguł wskazanych w niniejszej Polityce.
3. Zachowanie tajemnicy w zakresie Danych Osobowych obowiązuje zarówno podczas trwania współpracy z Conditor jak również po ustaniu tych stosunków.
4. Polecenia Conditor, Towarzystw Ubezpieczeniowych, a także innych osób delegowanych i wyznaczonych do działań związanych z ochroną Danych Osobowych oraz w zakresie ochrony informacji i bezpieczeństwa Systemu Informatycznego, muszą być bezwzględnie wykonywane.

§4

ZASADY PRZETWARZANIA ORAZ OCHRONY DANYCH OSOBOWYCH

1. Przetwarzanie Danych Osobowych może odbywać się wyłącznie zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której Dane dotyczą.
2. Dane Osobowe są zbierane tylko w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami.
3. Dane Osobowe mogą być przetwarzane przez użytkowników w sposób adekwatny, stosowny oraz ograniczony do tego, co niezbędne do celów, w których są przetwarzane.
4. Użytkownicy zobowiązani są do przetwarzania danych prawidłowych i w razie potrzeby ich uaktualniania - szczególnie na wniosek osoby, której Dane dotyczą.
5. Dane Osobowe są przechowywane w formie umożliwiającej identyfikację osoby, której Dane dotyczą, przez okres nie dłuższy niż jest to niezbędne do celów, w których Dane te są przetwarzane.
6. Dane Osobowe są przetwarzane w sposób zapewniający odpowiednie ich bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem za pomocą odpowiednich środków technicznych lub organizacyjnych.
7. Dostęp do pomieszczeń, w których przetwarzane są Dane Osobowe oraz do pomieszczeń, w których znajdują się serwery Baz Danych Osobowych lub przechowywane są kopie zapasowe

mogą mieć wyłącznie osoby, które posiadają do tego odpowiednie upoważnienie nadane przez Zleceniobiorcę.

8. Przetwarzania Danych Osobowych może dokonywać wyłącznie osoba posiadająca upoważnienie do ich przetwarzania, na podstawie nadanych upoważnień do wykonywania czynności agencyjnych oraz upoważnień do przetwarzania danych przez Zleceniobiorców.
9. Zleceniobiorcy zobowiązani są prowadzić ewidencję osób upoważnionych.
10. Zleceniobiorcy, na podstawie Umowy Powierzenia danych osobowych, zobowiązani są do pobrania od swoich pracowników i osób przy pomocy których wykonują czynności agencyjne stosowne oświadczenia dot. powierzenia danych, prawidłowego przetwarzania danych osobowych i zachowania poufności- wzór: Oświadczenie dla pracownika.
11. Zgodnie z postanowieniami Umowy Powierzenia Danych, Zleceniobiorca nie jest uprawniony do przekazywania danych osobowych osobom trzecim, z wyłączeniem osób współpracujących lub pracujących dla Zleceniobiorcy. W celu uniknięcia wątpliwości Strony ustalają, że w imieniu Podmiotu przetwarzającego powierzone dane osobowe mogą przetwarzać wyłącznie osoby, które uprzednio uzyskały od niego pisemne upoważnienie. Każde upoważnienie lub jego cofnięcie Podmiot przetwarzający zobowiązany jest wpisać do prowadzonej przez niego „Ewidencji osób upoważnionych do przetwarzania danych osobowych".
12. Wszystkich użytkowników przetwarzających Dane Osobowe obowiązuje zasada „czystego biurka", zabraniająca pozostawiania jakichkolwiek dokumentów z danymi osobowymi podczas nieobecności pracownika przy stanowisku pracy. Niedozwolone jest pozostawianie dokumentacji papierowej z danymi osobowymi na stanowisku pracy po jej zakończeniu, aby uniemożliwić zapoznanie się z danymi osobowymi osobom nieuprawnionym.
13. W przypadku opuszczenia stanowiska pracy, osoba przetwarzająca Dane Osobowe powinna wylogować się z Systemu lub zablokować dostęp do pulpitu stacji roboczej, z której korzysta przy przetwarzaniu Danych Osobowych. Ponadto w razie opuszczenia stanowiska pracy lub zakończenia pracy z Systemem Informatycznym, należy zamykać pliki zawierające Dane Osobowe. Uniemożliwi to dostęp do Danych Osobowych osobie nieupoważnionej (polityka czystego ekranu).

§5

PODSTAWA PRAWNA DO PRZETWARZANIA DANYCH OSOBOWYCH- ZGODA

1. Przetwarzanie Danych Osobowych przez Użytkownika możliwe jest pod warunkiem, że:
   a) osoba, której Dane dotyczą, wyraziła zgodę na przetwarzanie swoich Danych Osobowych w jednym lub większej liczbie określonych celów- wzór: oświadczenie klienta o wyrażeniu zgody na przetwarzanie danych osobowych. Pobranie pierwszej części zgody od klienta jest niezbędne do zwarcia umowy ubezpieczenia.
   b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której Dane dotyczą, lub do podjęcia działań na żądanie osoby, której Dane dotyczą, przed zawarciem umowy,
   c) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której Dane dotyczą, lub innej osoby fizycznej,
   d) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Użytkownika, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której Dane dotyczą, wymagające ochrony jej Danych Osobowych, w szczególności gdy osoba, której Dane dotyczą, jest dzieckiem.
2. Użytkownik zobowiązuje się nie przetwarzać Danych Osobowych jeżeli nie spełni przynajmniej jednej z przesłanek, o których mowa w punkcie poprzedzającym.
3. Użytkownicy zobowiązani są do pobierania, archiwizowania i ewidencjonowania zgód uzyskanych od klientów. Oświadczeń klienta o wyrażeniu zgody na przetwarzanie danych osobowych nie należy przesyłać do Conditor. Obowiązek archiwizacyjny spoczywa na Użytkowniku.

§6

REJESTR KATEGORII CZYNNOŚCI PRZETWARZANIA DANYCH PODMIOTU PRZETWARZAJĄCEGO

1. Zleceniobiorca zobowiązany jest do prowadzenia rejestru kategorii czynności przetwarzania danych Podmiotu przetwarzającego- wzór: Rejestr kategorii czynności przetwarzania danych podmiotów przetwarzających.

2. Rejestr kategorii czynności przetwarzania danych Podmiotu przetwarzającego zawiera informacje dotyczące:
    a) danych identyfikujących Podmiotu przetwarzającego oraz administratora, w imieniu którego działa Podmiot przetwarzający,
    b) kategorii przetwarzań dokonywanych w imieniu administratora wynikających z celu świadczonych usług lub zawartej umowy powierzenia,
    c) odnotowanie faktu przekazania Danych Osobowych do państwa trzeciego,
    d) ogólnego opisu technicznego i organizacyjnego środków bezpieczeństwa.

§7

ŚRODKI FIZYCZNE

1. Użytkownik jest zobowiązany do zastosowania środków technicznych i organizacyjnych zapewniających optymalną ochronę przetwarzanych Danych w Systemie Informatycznym, w tym w szczególności:
    a) zabezpieczenie Danych przed ich udostępnieniem osobom nieupoważnionym,
    b) zapobieganie pobraniu Danych przez osobę nieuprawnioną,
    c) zapobieganie zmianie, utracie, uszkodzeniu lub zniszczeniu Danych,
    d) zapewnianie przetwarzania Danych zgodnie z obowiązującymi przepisami prawa.
2. Zadania określone w punkcie poprzedzającym wykonują lub nadzorują ich wykonanie w imieniu Zleceniobiorcy, Conditor i Towarzystw Ubezpieczeniowych.
3. Zabezpieczenia pomieszczeń, w których przetwarzane są Dane Osobowe:
    a) dostęp do pomieszczeń, w których przetwarzane są Dane Osobowe jest ograniczony wyłącznie do osób mających odpowiednie upoważnienie nadane przez Zleceniobiorcę
    b) pomieszczenia, w których przetwarza się Dane Osobowe, zamykane są na klucz,
    c) w przypadku opuszczenia pomieszczenia przez ostatniego pracownika upoważnionego do przetwarzania Danych Osobowych - także w godzinach pracy - Dane Osobowe przechowywane w wersji tradycyjnej (papierowej) lub elektronicznej (na zewnętrznych nośnikach, np. pendrive, płyta CD/DVD, dyskietka) po zakończeniu pracy są przechowywane w miejscach zabezpieczonych przed dostępem nieupoważnionych osób trzecich; dodatkowo pracownik w razie opuszczania swojego stanowiska pracy

zobowiązany jest do wylogowania się ze swojego komputera stacjonarnego/laptopa lub innego urządzenia mającego dostęp do Systemu Informatycznego,

d) nieaktualne lub błędne wydruki zawierające Dane Osobowe niszczone są w sposób uniemożliwiający odczyt danych, np. w niszczarkach,

§8

ŚRODKI TECHNICZNE

1. Zabezpieczenia przed nieautoryzowanym dostępem do Bazy Danych Osobowych następuje poprzez:
   a) podłączenie urządzenia końcowego (komputera, terminala, drukarki) do Sieci Telekomunikacyjnej dokonywane jest przez osobę upoważnioną, Administratora Systemu lub inną osobę upoważnioną przez Zleceniobiorcę.
   b) udostępnianie każdemu Użytkownikowi zasobów programów i Bazy Danych Osobowych następuje na podstawie upoważnienia do przetwarzania Danych Osobowych,
   c) identyfikacja każdego Użytkownika w Systemie Informatycznym następuje poprzez zastosowanie uwierzytelnienia (tj. działania, którego celem jest weryfikacja deklarowanej tożsamości podmiotu korzystającego z Systemu Informatycznego),
   d) każdemu Użytkownikowi przysługuje przydzielenie indywidualnego Identyfikatora do korzystania z Systemu Informatycznego, np. osobiste konto w komputerze,
   e) udostępnianie kluczy od centrum przetwarzania Danych tylko upoważnionym pracownikom,
   f) stosowanie programu antywirusowego z zaporą antywłamaniową na wszystkich urządzeniach, na których dochodzi do przetwarzania Danych Osobowych,
   g) zabezpieczenie Hasłami kont na urządzeniach wskazanych w literze poprzedzającej oraz używanie kont z ograniczonymi uprawnieniami do ciągłej pracy,
   h) ustawienie monitorów stanowisk przetwarzania Danych Osobowych w sposób uniemożliwiający wgląd w Dane osobom nieupoważnionym.
2. Zabezpieczenia przed nieautoryzowanym dostępem do Bazy Danych Osobowych poprzez Sieć Telekomunikacyjną:

a) logiczne oddzielenie sieci lokalnej uniemożliwiające uzyskanie połączenia z Bazą Danych Osobowych spoza Systemu Informatycznego, jak również uzyskanie dostępu z Systemu Informatycznego do Sieci Telekomunikacyjnej publicznej,

b) zastosowanie zabezpieczenia Sieci Telekomunikacyjnej lokalnej poprzez instalację systemu typu firewall z funkcją analizy charakteru ruchu sieciowego, uniemożliwiającego nawiązanie połączenia do chronionych urządzeń i blokującego ruch o charakterystyce niepożądanej lub mogącej zostać uznanej za szkodliwą.

3. Zabezpieczenia przed utratą Danych Osobowych w wyniku awarii:
   a) ochrona sprzętu komputerowego przed zanikiem zasilania poprzez stosowanie listw przepięciowych,
   b) ochrona przed utratą zgromadzonych Danych poprzez cykliczne wykonywanie kopii zapasowych, z których w przypadku awarii odtwarzane są Dane i system operacyjny (tzw. backupy),
   c) zapewnienie właściwej temperatury i wilgotności powietrza dla pracy sprzętu komputerowego,
   d) zwiększenie niezawodności serwerów i urządzeń sieciowych poprzez ich logiczne rozmieszczenie.

§9

PROCEDURY NADAWANIA I ZMIANY UPRAWNIEŃ DO PRZETWARZANIA DANYCH

1. Każdy Użytkownik przed przystąpieniem do przetwarzania Danych Osobowych musi zapoznać się z niniejszym Regulaminem oraz zobowiązuje się go bezwzględnie stosować.
2. Zapoznanie się z niniejszym Regulaminem Użytkownik potwierdza własnoręcznym podpisem na oświadczeniu, który otrzyma od Zleceniobiorcy.
3. Zleceniobiorcy zobowiązują się do przestrzegania niniejszego Regulaminu zgodnie z zawartą Umową Powierzenia Danych Osobowych.
4. Zleceniobiorca lub osoba przez niego upoważniona zakładają konto Użytkownika w Systemie Informatycznym o odpowiednim Identyfikatorze i zabezpieczone Hasłem.
5. Hasło uprawniające do korzystania z Systemu Informatycznego Użytkownik wpisuje osobiście.
6. Konto zostaje zablokowane lub usunięte przez Zleceniobiorcę lub osobę przez niego upoważnioną.

7. Hasła dostępu Użytkownika do Systemu Informatycznego stanowią tajemnice służbową.
8. Hasła, w stosunku do których zaistniało podejrzenie o ich ujawnieniu osobie nieuprawnionej, podlegają bezzwłocznej zmianie.
9. W celu zabezpieczenia awaryjnego dostępu do Systemu Informatycznego przetwarzającego Dane Osobowe, aktualne hasło Administratora Systemu posiada Zleceniobiorca.
10. Pełne prawa Administratora Systemu posiada tylko Zleceniobiorca lub osoba przez niego upoważniona.

§10

ZASADY POSŁUGIWANIA SIĘ HASŁAMI

1. Bezpośredni dostęp do Systemu Informatycznego może mieć miejsce wyłącznie po podaniu Identyfikatora Użytkownika i właściwego Hasła.
2. Zmiana Haseł Użytkowników w Systemie Informatycznym powinna być wymuszana przez wspomniany System w odpowiednich odstępach czasu, nie rzadziej niż co 30 dni.
3. Hasło Użytkownika powinno być zmieniane, szczególnie w sytuacjach, kiedy zaistnieje podejrzenie, iż jest ono znane osobom nieupoważnionym.
4. Identyfikator Użytkownika nie może być zmieniany bez wyraźnej przyczyny, a po wyrejestrowaniu Użytkownika z Systemu Informatycznego nie może on zostać przydzielony innej osobie.
5. Użytkownicy, w tym w szczególności pracownicy, są odpowiedzialni za zachowanie Poufności swoich Identyfikatorów i Haseł.
6. Hasła Użytkowników utrzymuje się w tajemnicy również po upływie ich ważności.
7. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie. W sytuacji, kiedy zachodzi podejrzenie, że osoba nieupoważniona poznała Hasło w sposób nieuprawniony, Użytkownik zobowiązany jest do natychmiastowej zmiany Hasła i poinformowania o zaistniałym fakcie Zleceniobiorcę i Conditor.
8. Przy wyborze Hasła obowiązują następujące zasady:
    a) minimalna długość Hasła to 6 znaków, zaleca się jednak, aby hasła składały się z większej ilości znaków
    b) zakazuje się stosować:
        - Haseł, które Użytkownik stosował uprzednio,

- swojego Identyfikatora w jakiejkolwiek formie,
- swojego imienia, drugiego imienia, nazwiska, przezwiska, pseudonimu w jakiejkolwiek formie, imion (w szczególności imion osób z najbliższej rodziny),
- ogólnie dostępnych informacji o Użytkowniku (numer telefonu, numer rejestracyjny samochodu, numer PESEL itp.),

c) należy stosować:

- Podpowiedzi do haseł,
- Hasła zwierające kombinacje liter (małych i dużych) i cyfr arabskich,
- Hasła zawierające znaki specjalne: (. , ( ) ; ’ @ # & itp.), o ile System Informatyczny i oprogramowanie na to pozwala;
- kombinacji danych, znanych jedynie osobie, której dane dotyczą, np. może to być 2,5,7 cyfra Pesel + kilka cyfr z nr telefonu.

d) zmiany Hasła nie wolno zlecać innym osobom.

9. Jeżeli nie jest możliwym zastosowanie podpowiedzi do hasła, należy je przekazywać innym kanałem dystrybucji. Przykład: plik wysyłamy w wiadomości e-mail, a hasło przesyłamy w wiadomości sms.

§11

PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY W SYSTEMIE INFORMATYCZNYM

1. Rozpoczęcie pracy w Systemie Informatycznym na komputerach Użytkowników wymaga zalogowania przy użyciu indywidualnego Identyfikatora oraz Hasła.
2. Przed opuszczeniem stanowiska pracy należy zablokować stację roboczą lub wylogować się z oprogramowania i Systemu Informatycznego.
3. Przed wyłączeniem komputera należy bezwzględnie zakończyć prace uruchomionych programów i wylogować się z Systemu Informatycznego.
4. Niedopuszczalne jest wyłączanie komputera przed zamknięciem oprogramowania.
5. Na każdym stanowisku komputerowym musi być zainstalowane oprogramowanie antywirusowe z włączoną ochroną antywirusową.
6. Każdy e-mail wpływający na konta pocztowe musi być sprawdzony pod kątem występowania wirusów przez oprogramowanie antywirusowe.

7. Bezwzględnie zabrania się używania nośników niewiadomego pochodzenia.
8. Bezwzględnie zabrania się pobierania z Sieci Telekomunikacyjnej plików niewiadomego pochodzenia.
9. Administrator Systemu przeprowadza cykliczne kontrole antywirusowe na wszystkich komputerach, na których przetwarzane są Dane Osobowe, w tym co najmniej raz na jeden miesiąc.
10. Kontrola antywirusowa przeprowadzana jest również na wybranym komputerze w przypadku zgłoszenia nieprawidłowości w funkcjonowaniu sprzętu komputerowego lub oprogramowania. W przypadku wykrycia wirusów komputerowych sprawdzane jest stanowisko komputerowe, na którym wirusa wykryto oraz wszystkie posiadane przez Użytkownika nośniki.

§12

ROZDZIAŁ VIII POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. W przypadku stwierdzenia naruszenia:
    a) zabezpieczenia Systemu Informatycznego,
    b) technicznego stanu urządzeń,
    c) zawartości zbiorów Danych Osobowych,
    d) jakości transmisji danych w Sieci Telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych Danych,
    e) innych zdarzeń mogących mieć wpływ na naruszenie ochrony Danych Osobowych, np.:
        - ✓ kradzież laptopa,
        - ✓ zgubienie teczki z dokumentami klientów,
        - ✓ przypadkowe wykasowanie danych klientów z systemu,
        - ✓ wysłanie dokumentów na niewłaściwy adres email
        - ✓ ujawnienie danych uwierzytelniających (loginu, hasła) do systemu sprzedażowego,
        - ✓ nieuprawnione zniszczenie oryginałów przechowywanej dokumentacji,

- ✓ atak hakerski skutkujący zniszczeniem, utratą dostępu, zmodyfikowaniem, lub ujawnieniem danych osobowych; włamanie do pomieszczenia, w którym przechowywane są dane osobowe
- ✓ udostępnienie danych osobowych osobom niepowołanym.
- ✓ zalanie
- ✓ pożar
- ✓ kradzież dokumentów

2. Zleceniobiorca i każda osoba zatrudniona lub współpracująca ze Zleceniobiorcą zobowiązana jest do niezwłocznego powiadomienia o tym fakcie Conditor, nie później jednak niż w ciągu **24 godzin.**
3. W sytuacji dowiedzenia się o potencjalnym naruszeniu ochrony danych powierzonych Zleceniobiorcy, Zleceniobiorca natychmiast przeprowadza wewnętrzne postępowanie w celu ustalenia okoliczności naruszenia oraz jego skutków, a także podejmuje niezwłoczne działania w celu naprawienia lub zapobieżenia skutkom naruszenia.
4. Zleceniobiorca w terminie 24 godzin od dowiedzenia się o potencjalnym naruszeniu informuje CONDITOR o wystąpieniu potencjalnego naruszenia ochrony danych, przekazując następujące informacje:
    a) data i czas wystąpienia incydentu prowadzącego do naruszenia;
    b) data i czas dowiedzenia się o incydencie prowadzącym do naruszenia;
    c) opis incydentu, charakter naruszenia oraz opis ustalonych lub potencjalnych skutków naruszenia;
    d) przyczyna powstania incydentu
    e) kategorie osób, których danych osobowych dotyczy naruszenie;
    f) przybliżona liczba osób, których danych osobowych dotyczy naruszenie;
    g) kategorie danych osobowych, których dotyczy naruszenie;
    h) przybliżona liczba wpisów (rekordów) danych osobowych, których dotyczy naruszenie;
    i) opis środków zaradczych lub naprawczych podjętych przez Usługodawcę, o ile zostały podjęte.
5. W przypadku, gdy Zleceniobiorca nie ustalił wszystkich informacji określonych w ust. 4, przekazuje CONDITOR pozostałe, nieustalone wcześniej informacje niezwłocznie, nie później niż w terminie kolejnych 24 godzin.
6. Po wykryciu zdarzeń określonych w punktach poprzedzających, należy:

a) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców,

b) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,

c) zaniechać - o ile to możliwe - dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę zdarzenia,

d) podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji Systemu Informatycznego, aplikacji użytkowej lub innym właściwym dokumencie,

e) zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku,

7. Zleceniobiorca lub osoba upoważniona dokumentuje zaistniały przypadek naruszenia sporządzając stosową notatkę w oparciu o przeprowadzone bezpośrednio czynności lub w oparciu o uzyskane informacje i przekazuje ją niezwłocznie do Conditor.
8. Zaistniałe naruszenie może stać się przedmiotem szczegółowej analizy prowadzonej przez Conditor, IODO lub Administratora.
9. Analiza, o której mowa w ust. 8 powyżej, powinna zawierać wszechstronną ocenę zaistniałego naruszenia, wskazanie osób odpowiedzialnych, wnioski co do ewentualnych przedsięwzięć proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.
10. Wobec osoby, która w przypadku naruszenia zabezpieczeń Systemu Informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym
11. Regulaminie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, możliwe jest wszczęcie postępowania dyscyplinarnego.
12. Zleceniobiorca powinien prowadzić Dokumentację/rejestr naruszeń ochrony danych osobowych.

§13

MOŻLIWE ZAGROŻENIA DOTYCZĄCE NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Podział zagrożeń:
    a) zagrożenia losowe zewnętrzne – ich występowanie może prowadzić do utraty Integralności Danych, ich zniszczenia i uszkodzenia infrastruktury technicznej Systemu

    Informatycznego, a zatem ciągłość Systemu Informatycznego zostaje zakłócona, ale w przypadku takich zagrożeń nie dochodzi do naruszenia Poufności Danych, np. klęski żywiołowe, przerwy w zasilaniu itp.,

    b) zagrożenia losowe wewnętrzne – ich występowanie może prowadzić do zniszczenia Danych, zakłócenia ciągłości pracy Systemu Informatycznego oraz do naruszenia Poufności Danych, np. niezamierzone pomyłki użytkowników, Podmiotu przetwarzającego, awarie sprzętowe, błędy oprogramowania, pogorszenie jakości sprzętu i oprogramowania,

    c) zagrożenia zamierzone – świadome i celowe działania powodujące naruszenie Poufności Danych, zazwyczaj nie skutkujące uszkodzeniem infrastruktury technicznej i zakłóceniem ciągłości pracy; zagrożenia te można podzielić na:
        - nieuprawniony dostęp do Systemu Informatycznego z zewnątrz (włamanie do wskazanych Systemów),
        - nieuprawniony dostęp do Systemu Informatycznego z jego wnętrza,
        - nieuprawnione przekazanie Danych,
        - bezpośrednie zagrożenie materialnych składników Systemu Informatycznego (np. kradzież sprzętu).
2. Naruszenie lub podejrzenie naruszenia Systemu informatycznego, w którym przetwarzane są Dane Osobowe, następuje w sytuacji:
    a) losowego lub nieprzewidzianego oddziaływania czynników zewnętrznych na zasoby Systemu, jak np. wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne itp.,

b) niewłaściwych parametrów środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,
c) awarii sprzętu lub oprogramowania, która wyraźnie wskazuje na umyślne działanie w kierunku naruszenia ochrony Danych,
d) pojawienia się odpowiedniego komunikatu alarmowego,
e) podejrzenia nieuprawnionej modyfikacji Danych w Systemie lub innego odstępstwa od stanu oczekiwanego,
f) naruszenia lub próby naruszenia Integralności Systemu lub Bazy w tym Systemie,
g) pracy w Systemie wykazującej odstępstwa uzasadniające podejrzenie przełamania lub zaniechania ochrony Danych Osobowych, jak np. praca osoby, która nie jest formalnie dopuszczona do obsługi Systemie,
h) ujawnienia nieautoryzowanych kont dostępu do Systemu,
i) naruszenia dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (np. nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie Danych Osobowych w drukarce itp.).

3. Za naruszenie ochrony Danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia fizycznego miejsc przechowywania i przetwarzania Danych Osobowych, jak np.:
    a) niezabezpieczone pomieszczenia,
    b) niezabezpieczone urządzenia archiwizujące,
    c) pozostawianie Danych w nieodpowiednich miejscach (m.in. w koszach na śmieci czy w miejscach publicznie dostępnych),
    d) pozostawienie niezabezpieczonych dokumentów zawierających Dane Osobowe na stanowisku pracy w razie jego opuszczenia przez osobę przetwarzającą Dane w imieniu Administratora.