POLITYKA BEZPIECZEŃSTWA

1) POSTANOWIENIA OGÓLNE

Opracowana dokumentacja określa reguły dotyczące bezpieczeństwa przetwarzania danych osobowych zarówno w zbiorach tradycyjnych tj. papierowych, jak i w zbiorach elektronicznych - przetwarzanych w systemach informatycznych. Wprowadzenie odpowiednich zabezpieczeń, ochrona przetwarzania danych osobowych oraz niezawodność funkcjonowania, są podstawowymi wymogami stawianymi współczesnym systemom informatycznym. Poniższy dokument prezentuje szczegółowo mechanizmy ochrony danych, jak również zwraca uwagę na konsekwencje, jakie mogą ponieść osoby przekraczające określone granice. Zawiera także procedury postępowania służące zapobieganiu i minimalizowaniu skutków zagrożeń.

Celem Polityki Bezpieczeństwa przetwarzania danych osobowych, zwanej dalej Polityką Bezpieczeństwa, jest określenie kierunków działań oraz wsparcia dla zapewnienia bezpieczeństwa przetwarzania zbiorów danych osobowych zarządzanych przez NAWITEL SP. Z O.O. SP.K. z siedzibą w Bielanach Wrocławskich, przy ul. Atramentowej 10, 55-040 Kobierzyce, zwaną dalej NAWITEL SP. Z O.O. SP.K.

Polityka Bezpieczeństwa jest w NAWITEL SP. Z O.O. SP.K. najważniejszym dokumentem określającym zasady bezpieczeństwa przetwarzania danych, a wszystkie instrukcje i zalecenia muszą być z nią zgodne. Ma ona zastosowanie w stosunku do wszystkich pracowników, współpracowników, osób zatrudnionych na innej podstawie niż umowa o pracę, zleceniobiorców, wykonawców, konsultantów, praktykantów, stażystów i innych pracowników, którzy wykonują powierzane im zadania związane z przetwarzaniem danych osobowych.

Administrator Danych Osobowych zarządza bezpieczeństwem danych osobowych poprzez wykorzystanie danych tylko w określonym celu, który jest niezbędny do sprawnego wykonywania obowiązków wynikających z przepisów prawa. Ponadto jest on konieczny do realizacji umowy lub działań zmierzających do jej zawarcia, a przetwarzanie nie narusza praw i wolności osoby, której dotyczą, także w momencie wyrażenia przez nią zgody.

Polityka Bezpieczeństwa jest zgodna z obowiązującymi przepisami prawa, w szczególności z ustawą z dnia 29 sierpnia 1997r., o ochronie danych osobowych z późniejszymi zmianami oraz z wydanymi na jej podstawie aktami wykonawczymi.

Utrzymanie bezpieczeństwa przetwarzanych przez NAWITEL SP. Z O.O. SP.K. informacji, rozumiane jest, jako zapewnienie ich poufności, integralności i dostępności na odpowiednim poziomie, rozliczalności, autentyczności oraz niezaprzeczalności. Poziom procedur wpływających na bezpieczeństwo danych dostosowany jest do wielkości ryzyka. W odniesieniu do informacji i aplikacji wymienione pojęcia definiowane są w sposób następujący:

1) poufność – zapewnienie, że informacja nie jest udostępniona lub ujawniona nieupoważnionym osobom, podmiotom lub procesom,
2) integralność (danych, systemu) – zapewnienie, że dane nie zostały zmienione lub zniszczone
3) w sposób nieautoryzowany, a system informatyczny funkcjonuje w sposób nienaruszony, wolny od nieautoryzowanej manipulacji celowej bądź przypadkowej,

4) dostępność - zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne,

5) rozliczalności – zapewnienie, że wszystkie działania istotne dla przetwarzania informacji zostały zarejestrowane w systemie i możliwym jest zidentyfikowanie użytkownika, który działania dokonał,

6) autentyczność – zapewnienie, że tożsamość podmiotu lub zasobu jest taka jak deklarowana (dotyczy użytkowników, procesów, systemów i informacji),

7) niezaprzeczalności odbioru – zapewnienie, że w momencie wymiany danych system jest w stanie udowodnić, kiedy oraz kto uczestniczył w całości lub w części tej wymiany,

8) zarządzanie ryzykiem – rozumiane jako skoordynowane działania kierowania i zarządzania organizacją w procesie identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych.

2) DEFINICJE, STRUKTURA DOKUMENTÓW POLITYKI BEZPIECZEŃSTWA

Pojęcia użyte w Polityce Bezpieczeństwa oznaczają:

1) dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.

2) przetwarzanie danych osobowych – to jakiekolwiek operacje wykonywane na danych osobowych takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie danych osobowych, zwłaszcza w systemach informatycznych,

3) system informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,

4) zabezpieczenie danych w systemie informatycznym – rozumie się jako wdrożenie stosowanych środków administracyjnych, technicznych zapewniających ochronę danych przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem, a także nieuprawnionym przetwarzaniem,

5) zbiór danych – jest to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony (jego części znajdują się w różnych miejscach) lub podzielony funkcjonalnie (przetwarzany za pomocą programów realizujących różne funkcje),

6) Administrator Danych Osobowych (ADO) – organ, jednostka organizacyjna, podmiot decydujący o celach i środkach przetwarzania danych osobowych. Administratorem danych jest NAWITEL SP. Z O.O. SP.K., która ponosi pełnię odpowiedzialności wynikającej z przepisów ustawy o ochronie danych osobowych w odniesieniu do zbiorów danych osobowych znajdujących się w jego dyspozycji,

7) Pełnomocnik ADO – osoba pełniąca funkcje decyzyjne, która w świetle obowiązujących przepisów posiada prawny i faktyczny wpływ na przetwarzanie danych osobowych i działa w imieniu ADO,

8) Koordynator Ochrony Danych Osobowych (KODO) – należy przez to rozumieć osobę wyznaczoną przez Administratora Danych Osobowych do nadzorowania przestrzegania zasad ochrony oraz wymagań w zakresie ochrony, wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych,

9) Administrator Systemu Informatycznego (ASI) – osoba upoważniona do zarządzania systemem informatycznym,

10) Użytkownik – pracownik lub osoba współpracująca na podstawie umowy cywilno-prawnej upoważniona do przetwarzania danych osobowych.

Zakres przedmiotowy stosowania niniejszej Polityki Bezpieczeństwa obejmuje wszystkie zbiory danych osobowych przetwarzane w NAWITEL SP. Z O.O. SP.K., zarówno w formie elektronicznej, jak i tradycyjnej (papierowej).

W zakresie podmiotowym Polityka Bezpieczeństwa obowiązuje wszystkich pracowników w NAWITEL SP. Z O.O. SP.K., oraz inne osoby mające dostęp do danych osobowych, w tym stażystów, osób zatrudnionych na umowę zlecenia lub umowę o dzieło itp.

Informacje niejawne nie są objęte zakresem niniejszej Polityki.

Polityka Bezpieczeństwa wprowadza metody zarządzania oraz określa niezbędne wymagania do zapewnienia skutecznej i spójnej ochrony przetwarzanych informacji.

3) DOSTĘP DO INFORMACJI

1. ADO stosuje ograniczenia dostępu do danych osobowych: prawne (zobowiązania do poufności, zakresy upoważnień), fizyczne (strefy dostępu, zamykanie pomieszczeń) i logiczne (ograniczenia uprawnień do systemów przetwarzających dane osobowe i zasobów sieciowych, w których rezydują dane osobowe).
2. Każda osoba, która ma dostęp do danych osobowych, przed przystąpieniem do pracy, musi się zapoznać z przepisami prawa dotyczącymi ochrony danych osobowych oraz obowiązującymi w NAWITEL SP. Z O.O. SP.K. zasadami ochrony danych osobowych wynikających z Polityki Bezpieczeństwa.
3. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez Administratora Danych Osobowych. KODO prowadzi ewidencje osób upoważnionych do przetwarzania danych osobowych.
4. ADO upoważnia osobę do przetwarzania danych osobowych. W ramach tego upoważnienia osoba otrzymuje unikalny Identyfikator pozwalający na przetwarzanie danych w systemie informatycznym.
5. Wszystkie osoby dopuszczone do przetwarzania danych zobowiązane są do zapoznania się i stosowania wprowadzonych przez ADO procedur i środków określających zasady bezpiecznego przetwarzania.
6. Wszystkie osoby dopuszczone do przetwarzania danych zobowiązane są podpisać oświadczenie o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych i o zachowaniu poufności.
7. Odpowiedzialność osoby upoważnionej do przetwarzania danych w danym zbiorze powinna być odpowiednia do określonych zadań wykonywanych przy przetwarzaniu tych danych.
8. Przebywanie osób nieuprawnionych w obszarze przetwarzania danych osobowych dopuszczalne jest wyłącznie w obecności Użytkownika.
9. Udostępnianie danych osobowych podmiotom upoważnionym do ich otrzymania, na podstawie przepisów prawa, powinno odbywać się według określonych odrębnymi przepisami procedur postępowania.
10. Wraz z ustaniem stosunku pracy, umowy zlecenia / o dzieło następuje wygaśnięcie upoważnienia użytkownika do przetwarzania danych osobowych.

4) ZARZĄDZANIE DANYMI OSOBOWYMI

Za bezpieczeństwo przetwarzania danych osobowych w NAWITEL SP. Z O.O. SP.K. odpowiadają:

a) Pełnomocnik ADO (Administratora Danych Osobowych) – Prezes Zarządu
b) Koordynator Ochrony Danych Osobowych (KODO),

c) Administrator Systemu Informatycznego (ASI),
d) Użytkownicy.

Pełnomocnik ADO wyznacza Koordynatora Ochrony Danych Osobowych (KODO) oraz osobę upoważnioną do zastępowania KODO. Osoba zastępująca realizuje zadania z zakresu KODO tylko w momencie jego nieobecności. W takim przypadku w momencie powrotu KODO składa mu relację z podejmowanych działań w czasie tego zastępstwa.

Koordynator Ochrony Danych Osobowych w NAWITEL SP. Z O.O. SP.K. realizując Politykę Bezpieczeństwa ma prawo określać procedury i wydawać instrukcje regulujące kwestie ochrony danych osobowych w NAWITEL SP. Z O.O. SP.K.

Umowy zawierane przez NAWITEL SP. Z O.O. SP.K. na podstawie, których dane osobowe mogą zostać udostępnione i przetwarzane muszą zawierać zobowiązanie podmiotu zewnętrznego do zachowania reguł bezpieczeństwa danych zgodnie z obowiązującymi przepisami i zasadami określonymi w niniejszym dokumencie. Osoba odpowiedzialna za umowę zgłasza fakt powierzenia danych KODO oraz uzupełnia raport. Zasady prowadzenia projektów i inwestycji przez ADO odwołują się do zasad bezpieczeństwa danych osobowych oraz minimalizacji ich przetwarzania.

Nadzór nad przestrzeganiem zasad ochrony danych osobowych wynikających z ustawy o ochronie danych osobowych, a także innych powiązanych aktów prawnych oraz zasad ustanowionych w Polityce Bezpieczeństwa i Instrukcji zarządzania systemem informatycznym sprawuje Koordynator Ochrony Danych Osobowych.

KODO zobowiązany jest do zapoznania podległych pracowników z treścią ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, ze zmianami), Polityką Bezpieczeństwa w zakresie przetwarzania danych osobowych, Instrukcją zarządzania systemem informatycznym, służącymi do przetwarzania danych osobowych oraz Instrukcją postępowania w sytuacji naruszenia ochrony danych osobowych.

Zapoznanie się z dokumentami określonymi powyżej, pracownicy w NAWITEL SP. Z O.O. SP.K. potwierdzają podpisem na „Oświadczeniu" i przekazują Koordynatorowi Ochrony Danych Osobowych.

Ochrona zasobów danych osobowych NAWITEL SP. Z O.O. SP.K. jako całości przed ich nieuprawnionym użyciem lub zniszczeniem jest jednym z podstawowych obowiązków pracowników. Obowiązek zachowania tajemnicy danych osobowych spoczywa na wszystkich pracownikach, którzy mają do nich dostęp, także po ustaniu stosunku pracy.

5) ZAKRESY ODPOWIEDZIALNOŚCI

<u>Koordynator Ochrony Danych Osobowych:</u>

1. Odpowiada za przestrzeganie ustawy o ochronie danych osobowych w zakresie dotyczącym Koordynatora Ochrony Danych Osobowych;
2. Odpowiada na zapoznanie się Użytkowników z treścią „Polityki Bezpieczeństwa";
3. Wdraża i nadzoruje przestrzeganie „Polityki Bezpieczeństwa";
4. Monitoruje, a w razie zmiany obowiązujących przepisów prawa z zakresu ochrony danych osobowych dostosowuje do nich Politykę Bezpieczeństwa;
5. Z pomocą ASI:
    a) określa strategię zabezpieczania systemów informatycznych;

b) identyfikuje i analizuje zagrożenia oraz ryzyko, na które narażone może być przetwarzanie danych osobowych w systemach informatycznych;

6. Monitoruje działanie zabezpieczeń wdrożonych w celu ochrony danych osobowych w systemach informatycznych;
7. Sprawuje nadzór nad bezpieczeństwem danych zawartych w komputerach przenośnych, dyskach wymiennych, pamięciach przenośnych i innych nośnikach, przy pomocy, których przetwarzane są dane osobowe;
8. Sprawuje nadzór nad obiegiem oraz przechowywaniem dokumentów i wydawnictw zawierających dane osobowe;
9. Określa indywidualne obowiązki i odpowiedzialność osób zatrudnionych przy przetwarzaniu danych osobowych. W przypadku zatrudnienia nowego pracownika, zmiany stanowiska, zmiany zakresów obowiązków pracowniczych, utworzenia nowego zbioru danych osobowych, zmiany sposobu przetwarzania danych jest zobowiązany do wydania lub cofnięcia upoważnienia Użytkownikowi
10. Powiadamia ASI o konieczności utworzenia identyfikatora użytkownika w systemie oraz zmianie lub nadaniu uprawnień dostępu użytkownika do systemu i prowadzi ewidencję zmianę haseł;
11. Sprawuje nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników · w systemie informatycznym przetwarzającym dane oraz kontrolą dostępu do danych;
12. Odbiera od Użytkowników oświadczenia o zapoznaniu się z Polityką Bezpieczeństwa i Instrukcjami;
13. Prowadzi wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania danych;;
14. Stwarza warunki organizacyjno-techniczne umożliwiające spełnienie wymogów wynikających z obowiązywania ustawy o ochronie danych osobowych;
15. Ewidencjonuje wydane zgody na przetwarzanie danych osobowych poza wyznaczonym obszarem;
16. Ewidencjonuje raporty powierzenia danych osobowych;
17. Prowadzi rejestr raportów serwisowych;
18. Prowadzi rejestr z wykonania kopii zapasowych;
19. Prowadzi rejestr ze zniszczenia kopii zapasowych;
20. Działa zgodnie z „Instrukcją postępowania w sytuacji naruszenia ochrony danych osobowych”.

<u>Administrator Systemu Informatycznego</u>

1. Odpowiada za instalacje i konfiguracje oprogramowania systemowego, sieciowego, oprogramowania bazodanowego;
2. Monitoruje i zapewnia ciągłość działania systemu informatycznego oraz baz danych;
3. Optymalizuje wydajność systemu informatycznego baz danych;
4. Zarządza kopiami awaryjnymi danych, w tym danych osobowych oraz zasobów umożliwiających ich przetwarzanie;
5. Sprawuje nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych;
6. Sprawuje nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe;
7. Wspólnie z KODO identyfikuje i analizuje zagrożenia oraz ryzyko, na które narażone może być przetwarzanie danych osobowych w systemach informatycznych;
8. Określa i informuje KODO o potrzebach w zakresie zabezpieczenia systemów informatycznych, w których przetwarzane są dane osobowe;
9. Prowadzi profilaktykę antywirusową;

10. Przeciwdziała próbom naruszenia bezpieczeństwa informacji,
    10.1.1 Przyznaje ściśle określone prawa dostępu do informacji w danym systemie,
    10.1.2 Wnioskuje do KODO w sprawie procedur bezpieczeństwa i standardów zabezpieczeń,
    10.1.3 Zarządza licencjami i procedurami ich dotyczącymi;
11. Wykonuje polecenia KODO z zakresu stosowania Polityki Bezpieczeństwa.

Użytkownik

1. Zobowiązuje się do stosowania określonych przez ADO zasad, procedur oraz wytycznych mających na celu właściwe i adekwatne przetwarzanie danych;
2. Zobowiązuje się do zachowania w tajemnicy treści danych osobowych in. tajemnic prawnie chronionych;
3. Odpowiada za poprawność merytoryczną danych gromadzonych w systemach informatycznych oraz w formie papierowej;
4. Informuje KODO o wszelkich naruszeniach zasad bezpieczeństwa oraz ochrony danych osobowych
5. Zwraca się do KODO o wyjaśnienie wątpliwości z zakresu przepisów prawnych dotyczących ochrony danych osobowych;
6. Wykonuje polecenia KODO z zakresu stosowania Polityki Bezpieczeństwa;

6) REALIZOWANIE PRAW OSÓB, KTÓRYCH DANE DOTYCZĄ

ADO podejmuje odpowiednie środki, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem udzielić osobie, której dane dotyczą, wszelkich informacji, o których mowa w art.13 i 14 RODO oraz prowadzić z nią wszelką komunikację na mocy art. 15-22 i 34 RODO w sprawie przetwarzania.

Informacji udziela się na piśmie lub w inny sposób, w tym w stosownych przypadkach elektronicznie. Jeżeli osoba, której dane dotyczą, tego żąda, informacji można udzielić ustnie.

ADO bez zbędnej zwłoki, jednakże nie dłużej niż miesiąc od otrzymania żądania udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku z żądaniem na podstawie art. 15-22 RODO. W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. O takim przedłużeniu ADO informuje osobę, której dane dotyczą, wraz z podaniem przyczyn opóźnienia, w terminie miesiąca od otrzymania żądania.

Jeżeli administrator nie podejmie działań w związku z żądaniem osoby, której dane dotyczą, to niezwłocznie – najpóźniej w terminie od miesiąca otrzymania żądania – informuje osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

Osoba, której dane dotyczą ma prawo do:

1. uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz informacji wymienionych w art.15 ust.1
2. żądania niezwłocznego sprostowania nieprawidłowych danych i uzupełnienia niekompletnych danych osobowych
3. żądania niezwłocznego usunięcia danych osobowych, a ADO ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeśli zachodzi jedna z okoliczności określonych w art.17 RODO
4. żądania ograniczenia przetwarzania w przypadkach i na zasadach określonych w art.18 RODO
5. otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła ADO, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony ADO, któremu dostarczono te dane w przypadkach i na zasadach określonych w art.20 RODO.
6. W dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych opartego na art. 6 ust.1 lit.e) lub f) RODO. ADO nie wolno już przetwarzać danych osobowych, chyba, że wykaże on istnienie ważnych prawnie

uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

7. ADO informuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, których dokonał zgodnie z art. 16, art.17 ust.1 i art.18 RODO, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. ADO informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

7) UDOSTĘPNIANIE DANYCH

ADO udostępnia dane osobowe osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa

ADO lub osoba przez niego upoważniona udostępnia dane osobowe ze zbiorów zgodnie z powszechnie obowiązującymi w tym zakresie przepisami.

ADO może odmówić udostępniania danych osobowych, jeżeli spowodowałoby to istotne naruszenie praw i wolności osób, których dane dotyczą lub innych osób.

W umowach zawieranych przez komórki organizacyjne ADO, w przypadku, gdy do realizacji przedmiotu umowy niezbędne jest powierzenie danych osobowych podmiotowi zewnętrznemu, każdorazowo wymagane są postanowienia o powierzeniu danych osobowych. Fakt ten wymaga uzupełnienia przez osobę odpowiedzialną za umowę raportu z powierzenia danych osobowych i przekazania go KODO.

8) CHARAKTERYSTYKA ZAGROŻEŃ NARUSZAJĄCYCH OCHRONĘ DANYCH OSOBOWYCH

Zidentyfikowanie zagrożeń, które mogą naruszyć ochronę danych osobowych, pozwoli określić, a następnie wprowadzić i monitorować procedury zmierzające do ochrony danych osobowych.

1. Podział zagrożeń:
   a) zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych,
   b) zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora systemu informatycznego, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych,
   c) zagrożenia zamierzone, świadome i celowe – najpoważniejsze zagrożenia naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na:
      - nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu),
      - nieuprawniony dostęp do systemu z jego wnętrza,
      - pogorszenie, jakości sprzętu i oprogramowania,
      - nieuprawniony przekaz danych,
      - bezpośrednie zagrożenie materialnych składników systemu.
2. Przypadki zakwalifikowane, jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczeń zbiorów w formie papierowej oraz systemu informatycznego, w którym przetwarzane są dane osobowe to głównie:
   a) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.,
   b) niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie silnego pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,
   c) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a także fakt pozostawienia serwisantów bez nadzoru,

d) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,
e) jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenie systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
f) nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,
g) stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
h) nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie,
i) ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń np. login użytkownika i jego hasło,
j) praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych – np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.,
k) ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. „bocznej furtki" (backdoor), itp.,
l) podmieniono, lub zniszczono nośniki z danymi osobowymi bez odpowiedniego upoważnienia lub w inny sposób niedozwolony skasowano lub skopiowano dane osobowe,
m) rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowano się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, prace na danych osobowych w celach prywatnych, itp.).

3. Za naruszenie ochrony uważa się również stwierdzone nieprawidłowości w zakresie bezpieczeństwa miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, dyskietkach w formie niezabezpieczonej itp.

9) PRZETWARZANIE DANYCH OSOBOWYCH

Systemy informatyczne, służące do przetwarzania danych osobowych, muszą spełniać wymogi obowiązujących aktów prawnych regulujących zasady gromadzenia i przetwarzania danych osobowych.

Do tworzenia kopii bezpieczeństwa danych osobowych w postaci elektronicznej służą indywidualne systemy archiwizowania dla poszczególnych systemów przetwarzania.

Kopie bezpieczeństwa oraz dokumenty papierowe zawierające dane osobowe przechowuje się w warunkach uniemożliwiających dostęp do nich osobom nieuprawnionym.

Pozostałe informacje dotyczące przetwarzania danych osobowych zawarte są w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

10) SYSTEM ZABEZPIECZEŃ DANYCH OSOBOWYCH

Przez ochronę zbiorów danych rozumie się takie zabezpieczenie informacji zarówno podczas wprowadzania, przetwarzania w zbiorach papierowych jak i przesyłania w systemie informatycznym oraz na nośnikach informacji, aby uchronić ją przed nielegalnym ujawnieniem, kradzieżą oraz nieuprawnioną modyfikacją lub usunięciem. W tym celu należy wykorzystywać wchodzące w skład systemów informatycznych mechanizmy zarówno sprzętowe jak i programowe, a także opracowane procedury zwiększające bezpieczeństwo danych.

Procedury zwiększające bezpieczeństwo danych:

1. Dane osobowe mogą być przetwarzane wyłącznie przez osoby posiadające upoważnienia do przetwarzania danych osobowych. Osoby upoważnione do przetwarzania danych mają obowiązek zachować w tajemnicy dane, które przetwarzają, oraz sposoby ich zabezpieczenia.
2. Osoba odpowiedzialna za dokonanie modyfikacji zbioru danych: struktury, lokalizacji, a także utworzenia zbioru ma obowiązek zgłosić ten fakt Koordynatorowi Ochrony Danych Osobowych.
3. Dane osobowe mogą być przetwarzane w pomieszczeniach do tego przeznaczonych.
4. Osoby nieupoważnione do przetwarzania danych osobowych mogą przebywać w obszarach przetwarzania danych osobowych jedynie za zgodą Koordynatora Ochrony Danych Osobowych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.
5. Wszystkie pomieszczenia, w których przetwarza się dane osobowe są zamykane na klucz, w przypadku opuszczenia pomieszczenia przez ostatniego pracownika upoważnionego do przetwarzania danych osobowych – zasada ta obowiązuje zarówno w momencie kończenia pracy jak również w godzinach pracy.
6. Klucze do pomieszczeń służbowych mogą pobierać tylko te osoby, które są umieszczone w „wykazie kluczy do pomieszczeń służbowych" .
7. Dane osobowe w wersji tradycyjnej (papierowej) są przechowywane po zakończeniu pracy w zamykanych na klucz pomieszczeniach i meblach biurowych.
8. Klucze od szaf należy zabezpieczyć przed dostępem osób nieupoważnionych do przetwarzania danych osobowych.
9. Szafy z danymi powinny być otwarte tylko na czas potrzebny na dostęp do danych, a następnie powinny być zamykane.
10. Dane osobowe w formie papierowej mogą znajdować się na biurkach tylko na czas niezbędny na dokonanie czynności służbowych, a następnie muszą być chowane do szaf.
11. Dokumenty zawierające dane osobowe, w wyjątkowych sytuacjach za zgodą KODO i po zapewnieniu odpowiedniej ochrony mogą być wynoszone poza miejsce przetwarzania. Odpowiedzialność za dokumentację ponosi pracownik, który otrzymał zgodę. Zgodę przechowuje KODO oraz udziela instruktażu odnośnie bezpieczeństwa informacji.
12. Dane osobowe w wersji papierowej, wydruki i kopie a także, w wersji elektronicznej na nośnikach typu płyty CD, DVD, dyskach przenośnych należy niszczyć w niszczarkach (lub w inny sposób uniemożliwiający odczytanie) lub przekazywać do zniszczenia wynajętej do tego celu firmie.
13. Sprzątanie pomieszczeń gdzie przetwarzane są dane osobowe odbywa się po godzinach pracy przez personel sprzątający lub wytypowane do tego celu osoby, które zostały zapoznane z procedurami Polityki Bezpieczeństwa w zakresie ich dotyczących. Sprzątanie odbywa się tylko z założeniem, że zostaną zachowane przez pracowników przetwarzających dane osobowe zasady „czystego biurka". Zasada „czystego biurka", sprowadza się do zabezpieczenia w czasie i po pracy danych osobowych w formie papierowej w taki sposób, aby uniemożliwiało ich odczyt przez osoby nieuprawnione.
14. Przy przetwarzaniu danych osobowych w systemach teleinformatycznych stosuje się zasady „czystego biurka" oraz: wygaszacz ekranu z indywidualnym hasłem, ustawianie monitorów w taki sposób, aby nie była widoczna informacja dla osób postronnych.
15. Odchodząc od komputera należy się wylogować z używanego Systemu Informatycznego, a na koniec pracy wyłączyć komputer.
16. Do pomieszczeń gdzie znajduje się serwer oraz archiwum mają dostęp jedynie osoby do tego upoważnione, zwłaszcza osoby sprawujące bezpośredni nadzór nad serwerem (ASI). Pomieszczenia powinny być zabezpieczone poprzez drzwi zamykane na klucz.
17. W pobliżu wejścia do serwerowni, archiwum powinna znajdować się gaśnica, która jest okresowo napełniana.
18. Pomieszczenie, w którym znajdują się serwery powinny być odpowiednio chłodzone, zapewniając właściwą temperaturę i wilgotność powietrza dla sprzętu komputerowego.
19. Zabrania się udostępniania indywidualnego identyfikatora i haseł innym osobom.
20. Zabronione jest usuwanie danych przez wyrzucenie ich do kosza na odpadki.

21. Zabrania się korzystania z prywatnych nośników informacji w systemach przetwarzających dane osobowe.
22. Zabrania się korzystania z sieci publicznej (WWW) poprzez nieautoryzowane przeglądarki internetowe lub nieznajomego pochodzenia witryny internetowe, których treść wskazuje na duże ryzyko występowania oprogramowania szpiegowskiego, hakerskiego, spamerskiego oraz wirusowego.
23. W przypadku żądania udostępniania danych pracownicy w NAWITEL SP. Z O.O. SP.K. postępują zgodnie z przepisami ustawy o ochronie danych osobowych powiadamiając o tym Koordynatora Ochrony Danych Osobowych.
24. Udostępnianie danych jest odnotowywane w systemach informatycznych, a w przypadku zbiorów danych w formie tradycyjnej informacje o udostępnianiu przechowuje Koordynator Ochrony Danych Osobowych.
25. Szczegółowe procedury zarządzania systemem informatycznym reguluje „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych".
26. Procedury stosowane dla danych osobowych przetwarzanych w systemach informatycznych
    a) kontrola dostępu do zbiorów danych osobowych;
    b) indywidualne identyfikatory użytkowników (pracowników przetwarzających dane osobowe);
    c) uwierzytelnianie użytkowników (potwierdzanie ich tożsamości);
27. W celu zabezpieczenia danych osobowych przed ich utratą lub uszkodzeniem, stosuje się szereg zabezpieczeń fizycznych, informatycznych oraz organizacyjnych.
28. Użytkowników systemów przetwarzających dane osobowe obowiązuje następująca polityka haseł:
    - minimalna długość hasła wynosi 8 (osiem) znaków;
    - hasło zawiera małe i wielkie litery oraz cyfry lub znaki specjalne;
    - przechowywanie haseł w miejscu niedostępnym dla innych osób;
29. Użytkownik, który utracił hasło, zobowiązany jest zgłosić ten fakt bezzwłocznie Administratorowi Systemu Informatycznego, który ustali nowe hasło;
30. Zabezpieczanie danych przed ich utratą uszkodzeniem, lub nieupoważnionym przetworzeniem w pozostałych przypadkach:
    a) W przypadku naprawy, przekazania, likwidacji nośnika (papier, dysk twardy, płyta kompaktowa, pamięć przenośna, dyskietka, taśma magnetyczna itp.), który zawiera dane osobowe podmiotowi nieupoważnionemu do przetwarzania danych, należy zapewnić trwałe wymazanie informacji stanowiących dane osobowe;
    b) W przypadku korzystania z komputerów przenośnych zawierających dane osobowe należy zachować szczególną ostrożność podczas używania komputera poza obszarem przetwarzania danych;
       W szczególności należy stosować mechanizmy szyfrowania plików lub baz danych, wbudowanych w system operacyjny. Po ustaniu konieczności przetwarzania danych na komputerze przenośnym, należy je trwale usunąć z nośnika danych;
    c) Ekrany komputerów, na których przetwarzane są dane osobowe, są chronione wygaszaczami zabezpieczonymi hasłem. Monitory należy ustawić tak, aby ograniczyć dostęp do danych osobom nieupoważnionym do przetwarzania danych;
31. Zasady udostępniania danych osobowych pomiędzy działami oraz pracownikami:
    a) Informacje zawierające dane powszechnie dostępne mogą zostać udostępnione przez pracownika w formie bezpośredniej lub telefonicznej, po sprawdzeniu tożsamości w procedurze „ zwrotnej informacji telefonicznej";
    b) Natomiast udostępnienie danych osobowych w szerszym zakresie wymaga zgody KODO.
32. Upoważnienie do zbioru danych osobowych w ramach zastępstwa stanowiskowego: Upoważnienia do dostępu i przetwarzania danych osobowych są związane z zakresem wykonywanych czynności służbowych i zajmowanym stanowiskiem. W momencie nieobecności pracownika zostaje wyznaczona osoba zastępująca, która czasowo otrzymuje upoważnienie do dostępu i przetwarzania danych. Zasady upoważnienie w ramach zastępstwa stanowiskowego. Osoba zastępująca używa własnego loginu i hasła dostępu do systemu informatycznego.

11) PRZEGLĄDY I AKTUALIZACJE POLITYKI

Koordynator Ochrony Danych Osobowych przynajmniej raz w roku dokonuje analizy Polityki Bezpieczeństwa pod kątem jej przydatności, adekwatności i skuteczności.

Polityka Bezpieczeństwa podlega aktualizacji każdorazowo w przypadku:

1. likwidacji, utworzenia lub zmiany zawartości informacyjnej zbioru;
2. zmiany lokalizacji zbioru;
3. zmiany przepisów prawa dotyczącego ochrony danych osobowych, wymagającej aktualizacji Polityki Bezpieczeństwa;
4. innych znaczących zmian dotyczących danych osobowych w funkcjonowaniu NAWITEL SP. Z O.O. SP.K.;

Aktualizacji Polityki Bezpieczeństwa dokonuje Koordynator Ochrony Danych Osobowych – za zgodą i w porozumieniu z Administratorem Danych Osobowych.

12) POSTANOWIENIA KOŃCOWE

Niniejsza Polityka Ochrony Danych Osobowych zostaje ogłoszona w przedsiębiorstwie spółki i obowiązuje zarówno Jej pracowników, podmioty współpracujące, jak i postępowanie wobec kontrahentów.

W sprawach nieuregulowanych Polityką Bezpieczeństwa mają zastosowanie przepisy ustawy o ochronie danych osobowych, kodeksu pracy inne regulaminy wewnętrzne.

Polityka Bezpieczeństwa przechowywana jest przez KODO.