POLITYKA

BEZPIECZEŃSTWA DANYCH OSOBOWYCH W GREEN DOOR EDYTA ZIĘBA, EWA SPAŁEK S.C.

Łódź, czerwiec 2019r

Dokument wprowadzony zarządzeniem z dnia …..

Spis treści (rozdziałów);

Rozdział 1 . Strategia bezpieczeństwa

Administrator - Preambuła

1. Administrator mając na uwadze konieczność zapewnienia odpowiedniej ochrony wszelkich przetwarzanych danych osobowych wdraża niezbędne mechanizmy zabezpieczające zarówno o charakterze technicznym, organizacyjnym, osobowym

2. Działania wspierane przez Administratora obejmować będą ochronę danych osobowych przetwarzanych w każdej postaci, tj. elektronicznej, i papierowej. Działania te realizowane będą w sposób zapewniający zgodność z wymaganiami prawnymi zawartymi w 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, w Ustawie z 10 maja 2018 r. o ochronie danych osobowych jak również wewnętrznymi zapisami Firmy.

3. Wsparcie Administratora przejawiać się będzie zarówno poprzez zapewnienie organizacji pracy pozwalającej na zagwarantowanie wymaganej ochrony danych jak również alokację środków finansowych i pozafinansowych, niezbędnych do realizacji przedmiotowych działań.

Rozdział 2 . Polityka bezpieczeństwa

Niniejszy dokument zwany dalej Polityką, został opracowany przez Administratora Danych. Polityka określa zasady i wymagania w zakresie bezpieczeństwa danych osobowych przetwarzanych w całej Firmie, niezależnie od formy przetwarzania (w sposób tradycyjny czy w systemach informatycznych w tym także w sposób zautomatyzowany).

Polityka określa sposoby ochrony danych osobowych, sposoby bezpiecznego przetwarzania danych, zawiera rozwiązania organizacyjne i środki techniczne zapewniające ochronę przetwarzanych danych, odpowiednie do występujących lub mogących wystąpić zagrożeń.

Celem Polityki jest zapewnienie ochrony danych osobowych przetwarzanych w Firmie przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów rozporządzenia (w szczególności jeśli chodzi o aspekt legalności i innych przesłanek przetwarzania) przed zmianą, utratą, ich uszkodzeniem lub zniszczeniem. Dokument określa prawa dostępu osób do swoich danych, zasady przenoszenia danych pomiędzy administratorami. Stosowane rozwiązania techniczne jak pseudonimizacja i szyfrowanie danych w przypadku przetwarzania danych osobowych.

Powyższy cel jest realizowany poprzez wdrożenie rozwiązań organizacyjnych i zabezpieczeń technicznych mających służyć osiągnięciu poniższych cech przetwarzania danych osobowych:

- Poufność danych – rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom;
- Przejrzystość, zgodność z prawem danych – rozumiana jako właściwość zapewniająca zrozumiały, łatwy w dostępie przekaz (komunikat, informacje) związany z przetwarzaniem danych (np. obowiązek informacyjny)
- Integralność danych – rozumianą, jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
- Rozliczalność danych – rozumianą, jako właściwość zapewniającą, że działania podmiotu w zakresie przetwarzania danych mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi
- Dostępność danych – rozumianą jako właściwość bycia osiągalnym i możliwym do wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot,
- Rzetelność danych – rozumiana jako właściwość przejrzystości przetwarzania danych w stosunku do osób, których prawa dotyczą

- Adekwatność danych – rozumiana jako właściwość ograniczonego okresu przetwarzania danych do niezbędnego minimum.
- Minimalizm danych – rozumiana jako zbieranie , przetwarzanie danych tylko w niezbędnym zakresie adekwatnym do celu przetwarzania
- Ograniczenie przetwarzania danych – rozumiana jako ograniczenie przetwarzania danych w obrębie celu w jakim zostały zebrane

Istotnymi elementami niniejszej Polityki są jej następujące załączniki – zatwierdzane i na bieżąco aktualizowane przez ADO

1. Wykaz zbiorów danych osobowych wraz z programami zastosowanymi do przetwarzania danych osobowych
2. Rejestr czynności przetwarzania danych
3. Rejestr umów powierzenia ochrony danych
4. Rejestr incydentów wraz z procedurą
5. Wniosek zgłoszenia incydentu/naruszenia
6. Upoważnienie do przetwarzania danych
7. Polecenie przetwarzania danych
8. Wniosek dotyczący usunięcia zbioru
9. Ewidencja udostępnienia danych
10. Ewidencja osób uprawnionych

Oznaczenie treści i pojęć wskazanych w dokumencie

Ilekroć w Polityce jest mowa o:

1. Administratorze Danych Osobowych (ADO, FIRMA, Podmiot) – rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, decydującą o celach i środkach przetwarzania danych osobowych.

2. Green Door Edyta Zięba, Ewa Spałek s.c. – rozumie się przez to całość firmy (pracownicy, klienci i mienie).

3. Ciągłość działania – rozumie się przez to zdolność firmy do prowadzenia działalności w sposób nieprzerwany w zakresie określonym przez prawo zewnętrzne i wewnętrzne.

4. Danych archiwalnych – rozumie się przez nie dane osobowe, które Podmiot może lub musi przechowywać przez czas określony w przepisach szczególnych ustaw, mimo ustania celu, dla którego były zbierane lub podmiot danych osobowych wyraził zgodę na ich archiwizację.

5. Danych osobowych – rozumie się przez nie 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, dane o lokalizacji, identyfikator internetowy albo jeden lub kilka specyficznych czynników

określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.

6. Szczególnej kategorii danych zw. Danymi wrażliwymi – rozumie się przez to dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne, światopoglądowe lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również dane o stanie zdrowia, dane biometryczne, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

7. Incydent bezpieczeństwa informacji - pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń, które związane są z naruszeniem przyjętych zasad bezpieczeństwa i zagrażają bezpieczeństwu informacji, w tym danych osobowych.

8. Naruszenie ochrony danych – oznacz naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przetwarzanych w jakiejkolwiek formie.

9. Kopiowaniu danych – rozumie się przez to każde powielenie danych.

10. Odbiorcy danych – rozumie się przez to każdego (osoba fizyczna, prawna, organ publiczny) komu udostępnia się dane osobowe, z wyłączeniem:

a) Osoby, której dane dotyczą;
b) Organów publicznych, którym dane są udostępniane na podstawie przepisów prawa ale zgodnie z przepisami o ochronie danych.

11. Opracowywaniu danych – rozumie się przez to w szczególności takie czynności na danych jak ich zestawianie, sortowanie, kompilowanie, szyfrowanie lub odczytywanie ich treści.

12. Polityka – rozumie się przez to Politykę Bezpieczeństwa Danych Osobowych w firmie.

13. Powierzeniu przetwarzania danych – rozumie się przez to zlecenie wykonania czynności przetwarzania danych innemu podmiotowi w drodze odrębnej umowy zawartej na piśmie lub stosownego pisemnego zapisu do umowy wyłącznie w zakresie i celu w nich przewidzianym.

14. Przechowywaniu danych – rozumie się przez to przetwarzanie danych tylko w celu określonym przez przepisy szczególnych ustaw.

15. Przetwarzaniu danych – rozumie się przez to jakiekolwiek operacje lub zestaw operacji wykonywane na danych osobowych w sposób zautomatyzowany i niezautomatyzowany takie jak zbieranie, utrwalanie, przechowywanie,

opracowywanie, zmienianie, kopiowanie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

16. Rozporządzeniu (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.

17. System informatyczny – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

18. Sytuacja kryzysowa – rozumie się przez to sytuację nadzwyczajną, która wystąpiła w wyniku zaistnienia zagrożenia, pozbawiająca firmę możliwości normalnego wykonywania swoich funkcji lub znacznie ogranicza tę możliwość.

19. Udostępnianiu danych – rozumienie się przez to w szczególności takie czynności na danych jak ich przekazywanie, rozpowszechnianie lub ujawnienie odbiorcy danych lub podmiotowi danych osobowych, w sposób tradycyjny lub poprzez teletransmisję poza struktury organizacyjne firmy.

20. Ustawie – rozumie się przez to Ustawę z dnia 10 maja 2018r. o ochronie danych osobowych (Dz.U. 2018 poz.1000).

21. Usuwaniu danych – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.

22. Utrwalaniu danych – rozumie się przez to zapisywanie danych w sposób trwały na wszelkiego rodzaju nośnikach analogowych, w szczególności w formie skorowidzów, ksiąg, wykazów, kartotek lub na elektronicznych nośnikach informacji, w szczególności takich jak: dyskietka, płyta CD lub DVD, dysk twardy, pamięć przenośna typu pen-drive.

23. Pseudonimizacja – oznacza przetworzenia danych osobowych w taki sposób aby nie można było ich przypisać konkretnej osobie, której dane dotyczą bez użycia dodatkowej informacji, pod warunkiem, że takie dodatkowe informacje sa przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie.

24. Zabezpieczeniu danych w systemie informatycznym – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem, modyfikacją lub zniszczeniem.

25. Podmiot Przetwarzający oznacza osobę fizyczną lub prawną, organ publiczny lub inny podmiot który przetwarza dane osobowe w imieniu Administratora.

26. Zbieraniu danych – rozumie się przez to pozyskiwanie danych od osoby, której one dotyczą lub pozyskiwanie danych od osób trzecich.

27. Zbiorze danych – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

28. Profilowanie danych – oznacza zautomatyzowany proces przetwarzania danych. Zautomatyzowany proces przetwarzania danych to np. przetwarzania danych przez program informatyczny bez udziału czynnika ludzkiego.

29. Zgodzie osoby, której dane dotyczą – rozumie się przez to dobrowolne, konkretne, świadome, jednoznaczne oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych, tego, kto składa oświadczenie. Zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści. Zgoda obejmuje jeden cel przetwarzania danych. Dla celów dowodowych winna być przyjęta w formie pisemnej choć dopuszcza się inne wyraźne potwierdzenia takiego działania.

30. Zmienianiu danych – rozumie się przez to w szczególności takie czynności na danych jak uzupełnianie lub poprawianie treści danych osobowych, którymi dysponuje ADO

31. UODO(organ nadzorujący) – Urząd Ochrony Danych Osobowych na czele z Prezesem Urzędu Ochrony Danych Osobowych PUODO.

Za powyższe założenia strategii i założeń bezpieczeństwa danych w Firmie

odpowiadają:

- Administrator Danych;
- Każdy pracownik firmy, który uzyskał upoważnienie do przetwarzania danych osobowych.

Administrator Danych Osobowych.
Administratorem Danych jest Green Door Edyta Zięba, Ewa Spałek s.c.

Do jego obowiązków należy:

- Ustanowienie i bieżąca aktualizacja odpowiednio do celów i zakresu przetwarzanych danych osobowych – polityki bezpieczeństwa i procedur zarządzania tym bezpieczeństwem;
- Wdrażanie i stosowanie odpowiednich kodeksów postępowania lub korzystanie z mechanizmów certyfikacji;
- Nadzorowanie wdrożenia i stosowania środków przewidzianych w ustanowionej Polityce Bezpieczeństwa Danych Osobowych;

- Organizowanie systematycznego szkolenia pracowników w zakresie zgodnego z prawem przetwarzania danych osobowych, w tym odpowiedzialności za jego naruszenie;
- Zapewnienie odpowiednich relacji z podmiotem, któremu powierzono przetwarzanie danych lub innym administratorem danych.

Pracownik firmy upoważniony do przetwarzania danych osobowych – użytkownik systemu informatycznego.

- Każdy pracownik firmy, który uzyskał upoważnienie do przetwarzania danych osobowych zobowiązany jest do ich ochrony w sposób zgodny z przepisami Rozporządzenia, Ustawy i Polityki. Dostęp do określonego zbioru danych osobowych pracownik firmy uzyskuje na podstawie pisemnego upoważnienia. Dodatkowo zgodnie z art. 29 Rozporządzenia każda osoba dopuszczona posiada polecenie administratora do przetwarzania danych.
- Pracownicy zatrudnieni przy przetwarzaniu danych osobowych zobowiązani są do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu zatrudnienia.
- Naruszenie obowiązku ochrony danych osobowych, a w szczególności obowiązku zachowania danych osobowych w tajemnicy skutkuje poniesieniem odpowiedzialności karnej na podstawie przepisów Ustawy oraz stanowi ciężkie naruszenie obowiązków pracowniczych i może być podstawą rozwiązania stosunku pracy w trybie art. 52 Kodeksu Pracy.
- W przypadku zmiany stanowiska pracy lub długotrwałej nieobecności w jej wykonywaniu,(powyżej 30 dni) przez pracownika należy dokonać powołania innej osoby na jej miejsce. ADO dokonuje cofnięcia lub zawieszenia uprawnień
- Poprzez zmianę stanowiska pracy bądź jego utratę należy rozumieć zmianę stanowiska pracy w ramach firmy, jak i całkowite rozwiązanie stosunku pracy. Poprzez długotrwałą nieobecność w wykonywaniu pracy należy rozumieć przebywanie pracownika na zwolnieniu lekarskim, urlopie bezpłatnym lub macierzyńskim przez okres powyżej 30 dni.

Zasady przetwarzania danych osobowych

1. Uprawnienie do podejmowania decyzji w sprawie zbierania danych osobowych i tworzenia ich nowego zbioru przysługuje wyłącznie Administratorowi Danych i powinien mieć formę pisemną. Zasady dotyczące zbierania, przetwarzania danych osobowych, prognozowania długości okresu przetwarzania danych określone w tym rozdziale obowiązują dla wszystkich pracowników firmy. Postanowienia w zakresie zbierania danych, dotyczą zarówno zbierania danych bezpośrednio od osób, których dane dotyczą, jak i od osób trzecich w drodze pozyskania od nich danych do nowego zbioru lub zbioru już prowadzonego w firmie.

Pracownik wnisokuje do Administratora Danych o zbieranie danych i tworzenie nowego zbioru danych osobowych, w terminie minimum 30 dni przed rozpoczęciem

procesu zbierania danych osobowych i utworzeniu nowego zbioru zgłaszają swój zamiar ADO, podając jednocześnie informacje dotyczące:

- Podstawy prawnej zbierania danych i ich przetwarzania;
- Zakresu i struktury danych;
- Celu zbierania danych;
- Prognozowanego okresu przetwarzania danych;
- Zamiaru udostępniania lub powierzania przetwarzania danych na zewnątrz;
- Formy prowadzenia zbioru (papierowa czy elektroniczna);
- Wykazu stosowanych środków i mechanizmów zabezpieczeń;
- Infrastruktury systemu informatycznego służącego do przetwarzania danych osobowych;
- Obszaru przetwarzania danych osobowych;

Na podstawie art. 13, 14 RODO Administrator Danych jest zobowiązany do spełnienia **obowiązku informacyjnego** względem każdej z osób fizycznych, której dane przetwarza. Obowiązek ten należy realizować niezwłocznie po utrwaleniu danych osobowych. Zgodnie z art. 13 RODO w przypadku danych zbieranych bezpośrednio od osoby , której dane dotyczą koniecznym jest podanie następujących informacji:

1. Danych dotyczących Administratora Danych Osobowych w szczególności o adresie swojej siedziby i jej pełnej nazwie.
2. Celu i zakresie zbierania danych.
3. Znanych mu lub przewidywanych odbiorców danych.
4. O przekazaniu danych do państwa trzeciego.
5. Prawie żądania dostępu do treści swoich danych oraz ich poprawiania, ograniczenia przetwarzania, usunięcia, prawie do wniesienia sprzeciwu wobec przetwarzania a także prawie do przenoszenia danych.
6. Prawie do cofnięcia zgody na każdym etapie przetwarzania.
7. Dobrowolności albo obowiązku podania danych, jeśli taki obowiązek istnieje – jego podstawie prawnej.
8. Okresie przechowywania danych.
9. Informacji o możliwości wniesienia skargi do organu nadzorującego.
10. Informacji o zautomatyzowanym przetwarzaniu danych w szczególności profilowaniu danych.

Zgodnie z art. 14 RODO w przypadku danych zbieranych nie od osoby , której dane dotyczą koniecznym jest podanie następujących informacji. Obowiązek ten ADO podaje w odpowiednim terminie najpóźniej w ciągu miesiąca mając na uwadze konkretne okoliczności przetwarzania danych. W przypadku danych które mają być stosowane do komunikacji z osobą, której dane dotyczą (np. email, telefon) – najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą. W przypadku chęci ujawnienia tych danych innemu odbiorcy – najpóźniej przy pierwszym ujawnieniu. Na powyższy obowiązek składają się następujące informacje:

- Dane Administratora Danych Osobowych w szczególności o adresie swojej siedziby i jej pełnej nazwie.
- Celu i zakresie zbierania danych.
- Kategorii danych osobowych.
- Informacji o odbiorcach danych.
- Informacji o zamiarze przekazania danych osobowych do państwa trzeciego.
- Okresie przechowywania danych.
- Prawie żądania dostępu do treści swoich danych oraz ich poprawiania, ograniczenia przetwarzania, usunięcia, prawie do wniesienia sprzeciwu wobec przetwarzania a także prawie do przenoszenia danych.
- Prawie do cofnięcia zgody na każdym etapie przetwarzania.
- Informacji o możliwości wniesienia skargi do organu nadzorującego.
- Informacji o zautomatyzowanym przetwarzaniu danych w szczególności profilowaniu danych.

Przetwarzanie każdej informacji stanowiącej dane osobowe musi być zawsze oparte na poniższych zasadach:

- Przestrzegania zasady legalności – przetwarzanie danych zgodnie z prawem;
- Przestrzegania zasady celowości – zbieranie i przetwarzanie danych dla oznaczonych i zgodnych z prawem celów zgodnie z zasadą jeden cel jedna zgoda;
- Przestrzegania zasady adekwatności i merytorycznej poprawności, przejrzystości – dane powinny być merytorycznie poprawne i w minimalnym zakresie zbierane w stosunku do celu w jakich są przetwarzane;
- Przestrzegania zasady czasowości – przechowywanie i przetwarzanie danych w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż to jest konieczne do osiągnięcia celu przetwarzania.
- Przestrzegania zasady minimalizacji danych – zbierania i przetwarzania danych w minimalnym zakresie potrzebnym do osiągnięcia celu przetwarzania danych
- Przestrzeganie i stosowania zasady prognozowanego okresu przechowywania danych – przetwarzania danych przez okres wynikający z przepisów szczególnych bądź oparciu o zastosowany mechanizm wewnętrzny długości przetwarzania danych

Zasady bezpieczeństwa osobowego obowiązujące w procesie powierzenia przetwarzania danych osobowych obejmują:

W Green Door Edyta Zięba, Ewa Spałek s.c. może występować sytuacja powierzania danych osobowych podmiotom zewnętrznym. W związku z tym zasady opisane w poniższych punktach mogą wymagać stosowania zawartych w nich działań**.**

W procesie powierzenia przetwarzania danych osobowych występuje Administrator Danych oraz przetwarzający, któremu administrator powierzył dane do przetwarzania. Podstawą powierzenia przetwarzania danych jest pisemna umowa pomiędzy administratorem a przetwarzającym zgodnie z art. 28 RODO

Treść takiej umowy musi zawierać przynajmniej:

- Obowiązek ochrony tych danych (zabezpieczenia ich przed dostępem do nich osób trzecich),
- Właściwego doboru przetwarzającego biorąc pod uwagę bezpieczeństwo danych stosowanych przez ten podmiot (w tym poufności danych, zapewnienie inspekcji, audytów przez Administratora)
- Określenie przedmiotu umowy, celu , charakteru danych
- Określenie zasad anonimizacji, usunięcia danych po ustaniu umowy
- Wskazania możliwości dalszego podpowierzania ale za zgodą Administratora danych wyrażoną w treści umowy.

ADO prowadzi rejestr podmiotów którym powierzono dane, zgodnie z **Załącznikiem nr 3.**

Zasady bezpieczeństwa obowiązujące przy przetwarzaniu danych osobowych

1. Administrator Danych Osobowych jest zobowiązany do zapewnienia stosownych, specjalistycznych i okresowych szkoleń z zakresu ochrony danych osobowych dla pracowników, których udział jest konieczny w skutecznej realizacji wymagań prawnych, organizacyjnych lub technicznych dotyczących ochrony danych osobowych w firmie.
2. W przypadku braku powołania Inspektora Ochrony Danych ADO podejmuje decyzję o czasowych audytach z udziałem zewnętrznych podmiotów.
3. Każda osoba, przed dopuszczeniem do przetwarzania danych osobowych i uzyskaniem upoważnienia a następnie polecenie zostaje zapoznana z zasadami ochrony danych osobowych. Polega to na zapoznaniu osoby z Polityką oraz innymi przepisami, regulaminami itp. Fakt zapoznania z ww. dokumentami i przyjęcie na siebie obowiązku ich stosowania potwierdza podpis pracownika na upoważnieniu do przetwarzania danych osobowych a następnie wydaniu polecenia.
4. Szkolenia okresowe (weryfikujące) pracowników, organizowane są w przypadku:
   - istotnych zmian w przepisach dotyczących ochrony danych osobowych lub zasadach ich ochrony określonych w Polityce;
   - w przypadku stwierdzenia w wyniku kontroli wewnętrznej lub zewnętrznej istotnych uchybień w dziedzinie ochrony danych osobowych celem podniesienia wiedzy przez wszystkich pracowników firmy

5. Przetwarzanie i przechowywanie danych osobowych odbywa się w pomieszczeniach biurowych o ograniczonym i kontrolowanym dostępie.
6. Ustalenie i przestrzeganie zasad gospodarki kluczami do pomieszczeń, szaf i regałów biurowych jak i samych pomieszczeń. Każdy pracownik odpowiada za swoje stanowisko pracy.
7. Zabezpieczenie materiałów zawierających dane w sposób uniemożliwiający dostęp do nich osobom nieuprawnionym. Dane osobowe zebrane i przetwarzane w formie papierowej muszą być przechowywane, co najmniej w meblach biurowych zamykanych na klucz. Klucze należy przechowywać w sposób bezpieczny, bez możliwości dostępu do nich osób nieuprawnionych.
8. Przechowywanie danych wrażliwych oraz nośników wymiennych i nośników kopii zapasowych, w miejscach zabezpieczonych kluczem.
9. Odpowiednie do zagrożeń wyposażenie i zabezpieczenie pomieszczeń specjalnych takich jak np. archiwum.
10. Zastosowanie programów antywirusowych.
11. Zastosowanie zapory sieciowej (firewall)
12. Stosowanie pseudonimizacji i szyfrowania danych
13. Regularne tworzenie kopii zapasowych zbiorów danych osobowych przetwarzanych w programach informatycznych.
14. Zastosowanie ochrony zasilania przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.
15. Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe w sposób bezpieczny uniemożliwiający odczytanie zawartej w nich treści.
16. Obowiązuje zakaz udzielania informacji dotyczących danych osobowych na podstawie prośby o takie dane w formie zapytania telefonicznego, za wyjątkiem spraw związanych z wykonywaniem obowiązków służbowych z zastrzeżeniem potwierdzenia uprawnienia rozmówcy do otrzymania takich informacji.
19. Przebywanie osób nieuprawnionych w obszarze przetwarzania danych osobowych jest dopuszczalne jedynie w obecności osoby upoważnionej do przetwarzania danych osobowych.
20. Obowiązuje polityka „czystego biurka” i „czystego ekranu” - w przypadku zawieszenia pracy z systemem informatycznym użytkownik zobowiązany jest do zablokowania dostępu do komputera.
21. Zapewnia się bezpieczeństwo nośników informacji zawierających dane osobowe w przypadku, gdy zachodzi konieczność naprawy sprzętu, w którym te nośniki są zamontowane (wymontowanie w przypadku naprawy poza siedzibą firmy lub nadzór nad serwisem w siedzibie firmy)

Zasady obowiązujące przy kopiowaniu danych osobowych w ramach obszaru przetwarzania.

1. Kopiowanie danych osobowych w ramach Podmiotu może odbywać się wyłącznie przez osobę w ramach posiadanego upoważnienia do przetwarzania danych i może być dokonywane wyłącznie na potrzeby związane z realizacją zadań Firmy.
2. Kopia danych osobowych podlega zniszczeniu niezwłocznie po realizacji celu, dla którego została wykonana, chyba że co innego wynika z postanowień umów, regulacji wewnętrznych firmy lub powszechnie obowiązujących przepisów prawa.

Archiwizacja zbiorów danych osobowych

Dane osobowe mogą podlegać archiwizacji, stając się przez to Danymi Archiwalnymi, jedynie w przypadku, gdy wynika to z powszechnie obowiązujących przepisów prawa lub z indywidualnej wyraźnej zgody osoby, której archiwizowane dane dotyczą.
Dokumentacja przechowywana jest na podstawie przepisów prawa i zgodnie z odpowiednimi okresami.
W przypadku, gdy regulacje wymienione w powyższym punkcie nie określają innych kwestii związanych z archiwizacją danych osobowych, stosowne decyzje w tym zakresie podejmuje ADO.

Usuwanie danych osobowych , ograniczenie przetwarzania, usunięcie zbioru danych

Usuwanie danych ze zbioru lub usunięcie całego zbioru następuje przy spełnieniu przynajmniej jednego z poniższych warunków:

1. Gdy cel, dla którego dane zebrano został osiągnięty lub dane są już zbędne dla osiągnięcia tego celu;
2. Na mocy wniosku osoby zainteresowanej (o ile nie zachodzą szczególne sytuacje przewidziane prawem)

Ograniczenie zakresu przetwarzania określonych danych podyktowane wnioskiem osoby której dane są przetwarzane występuje przy spełnieniu jednego z poniższych warunków:

1. Osoba kwestionuje prawidłowość danych;
2. Przetwarzanie jest niezgodne z prawem;
3. Ustał cel przetwarzania;
4. Wniesienie sprzeciwu wobec dalszego przetwarzania danych.

Usunięcia zbioru należy dokonywać w sytuacji kiedy ustał cel w którym dany zbiór powstał. Decyzję w tym zakresie podejmuje ADO. Z czynności tej sporządza się w dwóch egzemplarzach protokół zniszczenia całego zbioru podpisany przez co najmniej dwie osoby. Protokół z w/w czynności pozostaje w zasobach ADO - **Załącznik nr 8.**

Zbiory wyodrębnione oraz obszary przetwarzania danych

W firmie wyodrębniono zbiory danych. Ich zakres, przedmiot określa **Załącznik nr 1**.

Zidentyfikowane zbiory zawierające dane osobowe w wersji papierowej i elektronicznej są przetwarzane i przechowywane w budynkach dzierżawionych znajdujących się w Łodzi Al. Kościuszki 40a Z uwagi na niewielki organizacyjnie i strukturalnie podmiot dane te mieszczą się pod jednym adres w trzech pomieszczeniach firmy.

Udostępnianie i przeniesienie danych osobowych

Dane osobowe udostępnia się:
1. Osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa;
2. Pozostałym osobom lub podmiotom, jeżeli w sposób wiarygodny uzasadnią potrzebę posiadania tych danych, a ich udostępnienie nie naruszy praw i wolności osób, których dane dotyczą;

Zgody na udostępnienie danych udziela ADO. Odnotowanie informacji o udostępnieniu danych (komu, zakresie, dacie) powinno nastąpić niezwłocznie po udostępnieniu danych w postaci ewidencji udostępniania danych. IOD odpowiada za udostępnienie danych osobowych w sposób zgodny z ich przeznaczeniem. **Załącznik nr 9**.

Przeniesienie danych osobowych

Zgodnie z art. 20 RODO wszelkie dane osobowe dotyczące osoby na jej wyraźny wniosek muszą zostać przesłane innemu (wskazanemu) administratorowi danych w formacie nadającym się do odczytu maszynowego z zachowaniem odpowiednich środków bezpieczeństwa. Powyższe prawo obejmuje sytuacje przewidziane prawem tj.

- fizyczna zgoda osoby na przetwarzania danych (zwykle, wrażliwe),
- sytuacji przetwarzania danych potrzebnych do zawarcia umowy (dotyczy danych zwykłych),
- lub zautomatyzowanego przetwarzania danych.

Rozdział 3. Rejestr operacji przetwarzania danych osobowych

Zgodnie z art. 30 RODO każdy ADO , który spełnia określone kryteria musi prowadzić rejestr czynności przetwarzania. Administrator Danych na podstawie art. 30 ust 2 lit 5 zwolniony jest z prowadzenia takiego rejestru. Jednocześnie ADO świadomy zmian jakie mogą zachodzić w Podmiocie będzie analizował zasadność prowadzenia takiego

rejestru. W momencie konieczności prowadzenia RCP będzie on prowadzony w oparciu o **załącznik nr 2**

Rozdział 4. Polityka monitorowania i reagowania na naruszenia ochrony danych

Administrator Danych podejmuje wszelkie środki techniczne, organizacyjne i osobowe celem odpowiedniego bezpieczeństwa i zabezpieczania przetwarzanych danych osobowych.
Środki osobowe (szkolenia, świadomość pracowników, upoważnienia, klauzule poufności)
Środki organizacyjne (zabezpieczenie pomieszczeń , dokumentów, wdrożenie polityki ochrony danych, stosowanie umów powierzenia etc)
Środki techniczne (ograniczony dostęp do przetwarzania danych, zabezpieczenia i wykonywania kopii danych, pseudonimizacja, szyfrowanie danych, realizacja kopii danych, testowanie i ocena skuteczności środków technicznych).
Na podstawie art. 25 RODO , i zgodnie z założeniami Administrator Danych Osobowych podejmuje następujące kroki:

- na wstępnym etapie prognozuje i projektuje środki potrzebne do stosowania przy zapewnieniu atrybutu bezpieczeństwa danych, uwzględniając stan wiedzy i możliwości techniczne, charakter, zakres przetwarzanych danych, cel i ich ryzyka,
- stosuje bezwzględnie zasadę minimalizacji przetwarzanych danych już na etapie ich zbierania, prognozowanego okresu przetwarzania danych,
- określa zasadność ich przetwarzania adekwatnie do celu.

Taka praktyka pozwala uniknąć sytuacji rozpoczęcia procesu przetwarzania bez ich wstępnej kontroli. Prognozowanie okresu przetwarzania danych może odbywać się poprzez odwołanie do przepisów szczególnych regulujących obowiązek przechowywania i archiwizacji poszczególnych dokumentów i danych lub stworzenie pewnego mechanizmu weryfikacyjnego np. poprzez zawieranie umów terminowych, zawierających dane, tak aby mieć kontrole nad zasadnością dalszego przetwarzania w sytuacji wygaśnięcia umowy.

Rozdział 5. Rejestr incydentów

Postępowanie w przypadku powstania incydentu

Celem procedury jest określenie zasad zgłaszania, analizowania i postępowania z incydentami związanymi z bezpieczeństwem danych osobowych w Firmie

Opis postępowania

1. Pracownik firmy zobowiązany jest do powstrzymania się od kontynuowania jakiejkolwiek czynności mogącej spowodować zatarcie śladów bądź dowodów naruszenia ochrony danych osobowych.
2. Pracownik firmy podejmuje, stosownie do zaistniałej sytuacji, inne niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować dalszym naruszeniom bezpieczeństwa danych osobowych.
3. Pracownik firmy zgłasza incydent związany z bezpieczeństwem informacji do ADO.
4. Pracownik firmy zgłasza incydenty za pośrednictwem formularza zgłoszenia incydentu- **Załącznik nr 5**, poczty e-mail lub w przypadku konieczności natychmiastowej reakcji – telefonicznie lub osobiście.
5. Po zgłoszeniu ustnym lub telefonicznym pracownik zobowiązany jest wysłać uzupełniające zgłoszenie lub złożyć wniosek w formie papierowej w najbliższym możliwym czasie.

Rejestrowanie incydentów

6. ADO prowadzi Rejestr incydentów naruszenia bezpieczeństwa danych osobowych **Załącznik nr 4**, w którym odnotowuje dane: data zgłoszenia, zgłaszający, przyjmujący zgłoszenie, nazwa incydentu, miejsce wystąpienia incydentu, opis (przyczyna), podjęte działania.
7. ADO klasyfikuje, czy zgłoszenie jest incydentem bezpieczeństwa danych osobowych w rozumieniu art. 33 RODO.
8. ADO weryfikuje czy zagrożenie jest naruszeniem ochrony danych.
9. ADO zabezpiecza wszelkie materiały dowodowe np. miejsca włamania, pliki elektroniczne itp.
10. ADO podejmuje działania niezbędne do usunięcia skutków zgłoszonego incydentu bezpieczeństwa.
11. Po uzupełnieniu informacji w odniesieniu do naruszenia ochrony danych na temat usunięcia skutków oraz podjętych działań ADO zamyka zgłoszenie tego faktu.
12. Pracownik firmy może kontynuować pracę przerwaną incydentem bezpieczeństwa informacji po uzyskaniu zgody od ADO.
13. W przypadku naruszenia kwalifikującego się na określenie mianem – incydentu - ADO przekazuje najpóźniej w ciągu 72 godzin informację do Urzędu Ochrony Danych o powstałym naruszeniu, jego zakresie, ilości osób których naruszenie dotyczyło, środków powziętych celem minimalizacji powstałego zagrożenie. Sam fakt powstania incydentu powoduje obowiązek ADO poinformowania osób

których naruszenie dotknęło lub jeżeli wymagałoby to niewspółmiernie dużego wysiłki podaje w/w informacje w formie publicznego komunikatu.

Analiza i przegląd incydentów

14. ADO przegląda Rejestr incydentów regularnie przynajmniej raz na kwartał. Przegląd obejmuje:

- określenie liczby incydentów bądź naruszeń,
- określenie incydentów powtarzających się,
- określenie trendów(te same błędy) związanych z incydentami bezpieczeństwa,
- określenie kosztów (straty oraz nakłady finansowe) związanych z incydentami bezpieczeństwa'
- formułowanie wniosków z przeprowadzonego przeglądu i zastosowanie ich w Podmiocie

15. Na podstawie tych danych ADO określa czy jest wymagane zastosowanie dodatkowych środków bezpieczeństwa. Wdraża rozwiązania aby do dalszych takich naruszeń nie dochodziło.

Rozdział 6. Polityka zarządzania ryzykiem utraty prywatności (Privacy Impact Assessment)

Wartościami, na jakie RODO kładzie szczególny nacisk w zakresie szacowania ryzyka, są prawa i wolności osób, których dane dotyczą i te wartości należy mieć przede wszystkim na uwadze, oceniając ryzyko związane z przetwarzaniem danych osobowych. ADO spełniając powyższe, podejmuje kroki celem analizy zagrożeń w obszarze przetwarzanych danych. Mówiąc o ryzyku naruszenia praw i wolności osób fizycznych na gruncie RODO, konieczne jest uwzględnienie:

- prawdopodobieństwa wystąpienia określonego zdarzenia będącego naruszeniem,
- powagi tego zdarzenia, tj. wielkości szkody, jakie zdarzenie to może spowodować w odniesieniu do osoby, której dane dotyczą.

Aby zapobiegać tego typu ryzykom Administrator Danych Osobowych w sposób ciągły analizuje wszelkie procesy przetwarzania danych, biorąc pod uwagę ryzyka związane z przetwarzaniem danych osobowych. Powyższa zasada, podejścia opartego na ryzyku, wymusza na Administratorze Danych Osobowych, ale również o ile zachodzi taka przesłanka, podmiocie przetwarzającym dbanie odpowiednią ochronę na wszystkich etapach przetwarzania danych osobowych, tj. podczas całego cyklu życia informacji, od momentu zbierania danych aż do ich usunięcia. Zgodnie z art. 35 RODO obligatoryjność stosowania analizy ryzyka w obecnym kształcie nie występuje w firmie nie mniej jednak Administrator Danych będzie śledził konieczność zastosowania takiej analizy o ile powstaną skuteczne przesłanki do jej prowadzenia. Obecnie

przetwarzanie danych odbywa się na podstawie przepisów prawa i w niewielkim zakresie przetwarzania danych innych osób. Pojęcie przetwarzania danych na dużą skalę nie znajduje uzasadnienia, biorąc pod uwagę wytyczne grupy roboczej art. 29 jak i wytycznych PUODO określających pojęcia przetwarzania danych na dużą skalę tj, zakres przetwarzanych danych, okres, zakres geograficzny przetwarzania danych osobowych oraz liczbę osób w kontekście procentowego ujęcia względem całego społeczeństwa. Pojawianie się okoliczności dokonania analizy ryzyka zostanie potwierdzone raportem, który będzie stanowił integralną cześć polityki.

Rozdział 7. Procedura zarządzania zmianą / zarządzania projektami (Privacy by Design)

Administrator Danych Osobowych stosownie do art. 25 RODO podejmuje i stosuje odpowiednie środki celem przeciwdziałania wystąpieniu potencjalnego niebezpieczeństwa naruszenia danych. Jednym z nich, choć nie jedynym, jest planowanie procesu przetwarzania danych już na samym początku jego rozpoczęcia(zbierania danych). Zatem spełnienie tego wymogu będzie realizowane poprzez regularny przegląd funkcjonowania procesu przetwarzania danych oraz jego składowych elementów (systemów informatycznych, sposobu zbierania zgód, wypełniania obowiązków informacyjnych itp.). W Green Door Edyta Zięba, Ewa Spałek S.c. powyższe będzie realizowane biorąc m.in. pod uwagę;

- Ocenę zasadności, legalności przetwarzanych danych.
- Prywatność i bezpieczeństwo na każdym etapie przetwarzania.
- Przejrzystość postępowania.
- Minimalizm zbieranych i przetwarzanych danych.

Aby spełnić powyższe kryteria w obszarze firmy, każda zebrana informacja podlega już na wstępnym etapie analizie przez upoważnionego pracownika pod względem legalności przetwarzania danych, zakresu ich zbierania (biorąc pod uwagę cel i przypisaną do niego adekwatność zbieranych danych). Zbieranie danych zgodnie z wymogami prawa podlega obowiązkowi informacyjnemu w tym również przejrzystości postępowania tj. możliwości sprostowania, dostępu do swoich danych ich usunięcia, przeniesienia etc.) Każdorazowo przy podjęciu decyzji o zebraniu danych jak i ich przetwarzaniu na dalszym etapie niezależnie od formy (papierowej czy elektronicznej) zapewnia się ten sam wolumen prywatności. Osoby odpowiedzialne za przetwarzanie danych niezależnie od formy przetwarzania danych są szkolone w tym zakresie aby

spełnić zadość przepisom Rozporządzenia. Przekazywanie danych poza siedzibą Administratora w formie papierowej odbywa się w sposób zapewniający poufność i bezpieczeństwo , korespondencja wysyłana jest listami poleconymi. Przekazywanie danych drogą komunikacji elektronicznej, poza siedzibę Administratora danych odbywa się w formie szyfrowanej komunikacji, bądź stosując inne techniki anonimizacji danych np. pseudonimizację czy hasłowanie plików. Udostępnienie danych odbywa się z zachowaniem zasady legalności, a powierzenie w oparciu o stosowanie umów powierzenia. Funkcjonalność systemów informatycznych zapewnia dostęp do danych tylko upoważnionym pracownikom firmy bez szkody dla prywatności i poufności zebranych danych. W firmie nie stosuje się profilowania danych.

Rozdział 8. Plan awaryjny / polityka zarządzania kopiami zapasowymi

Procedura ma zastosowanie do programów informatycznych ADO, w których przetwarzane są dane osobowe, wymagające zabezpieczenia atrybutu dostępności w wymaganym czasie.

Odpowiedzialność

Za przestrzeganie zasad wymienionych w niniejszej procedurze odpowiada każdy pracownik. Za nadzór nad realizacją zasad wymienionych w niniejszej procedurze odpowiada ADO.

Zasady bezpieczeństwa

Zasady bezpieczeństwa dotyczą wszystkich ważnych dla działania firmy systemów/programów informatycznych. W celu zabezpieczenia danych każdy pracownik wykonuje samodzielnie codzienne kopie folderów w których znajdują się kopie zapasowe.
Za przestrzeganie realizacji tego obowiązku ADO . Kopia tworzy się na nośniku zewnętrznym ewentualnie w folderze lokalnym użytkownika.
Na każdym pracowniku spoczywa obowiązek każdorazowego weryfikowania poprawności wykonania kopii zapasowej. W przypadku niepoprawnego zapisu kopii zapasowej obowiązkowo sprawdzany jest stan techniczny nośnika, na którym zapisywana jest kopia oraz ponownie przeprowadzany jest proces wykonywania kopii zapasowej na nieuszkodzonym nośniku.
ADO sprawdza okresowo operację testowego odzyskiwania z kopii zapasowych losowo wybranych danych w celu weryfikacji możliwości odzyskania danych. Nośniki

informacji należy przechowywać w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem
W przypadku transportowania nośników z kopiami zapasowymi poza obszar firmy, należy zapewnić bezpieczne warunki transportu poprzez:

- Zapewnienie poufności danych przez zaszyfrowanie informacji na nośniku.
- Przewożenie kopii bezpieczeństwa w postaci niezaszyfrowanej wyłącznie w obecności dwóch pracowników firmy.
- Nie pozostawianie kopii zapasowych bez nadzoru.
- Umieszczanie nośników w bezpiecznych pojemnikach zabezpieczających je przed zniszczeniem lub skopiowaniem.

Nośniki kopii zapasowych, które zawierają nieaktualne dane, są uszkodzone lub których nie można ponownie wykorzystać, muszą być niezwłocznie zniszczone przez ADO w sposób uniemożliwiający odtworzenie zapisanych na nich danych.

Rozdział 9. Procedura zarządzania użytkownikami i prawem dostępu.

W celu zapewnienia odpowiedniego poziomu bezpieczeństwa wprowadzono następujące środki;

- W programach informatycznych służących do przetwarzania danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych;
- Uwierzytelnione hasło dostępu do logowania się na stanowisko pracy
- W przypadku dostępu do danych przetwarzanych w programie informatycznym, przez co najmniej dwie osoby zapewnia się, aby w systemie dla każdego użytkownika rejestrowany był oddzielny identyfikator i hasło
- Dostęp do danych przetwarzanych w tym systemie jest możliwy tylko i wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia;
- W celu ochrony systemów informatycznych służących do przetwarzania danych osobowych przed zakłóceniami pochodzącymi z sieci energetycznej, których skutkiem mogłoby być zakłócenie lub przerwanie ich pracy zastosowano zasilacze awaryjne UPS;
- Dane osobowe przetwarzane w systemach informatycznych zabezpiecza się poprzez wykonywanie kopii zapasowych . Dane osobowe przetwarzane w plikach ms office powinny dodatkowo zabezpieczone hasłem.
- Osoby użytkujące komputery przenośne stanowiące własność Firmy. zawierające dane osobowe, zachowują szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych osobowych oraz stosują środki ochrony kryptograficznej wobec przetwarzanych

danych osobowych. Pracownicy maja dostęp jedynie do własnej poczty elektronicznej;

- Urządzenia, dyski lub inne elektroniczne nośniki informacji stanowiące własność firmy, zawierające dane osobowe, przeznaczone do likwidacji pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
- Urządzenia, dyski lub inne elektroniczne nośniki informacji stanowiące własność firmy, zawierające dane osobowe, przeznaczone do przekazania podmiotowi nieuprawnionemu do przetwarzania danych pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
- Urządzenia, dyski lub inne elektroniczne nośniki informacji stanowiące własność firmy, zawierające dane osobowe, przeznaczone do naprawy pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych;
- Hasła użytkowników wykorzystywane do uwierzytelniania składają się, z co najmniej 8 znaków, zawierają małe i wielkie litery oraz cyfry, z okresowym trybem ich zmiany. Urządzenia i nośniki zawierające dane osobowe wrażliwe społecznie, przekazywane poza obszar przetwarzania danych osobowych, zabezpiecza się w sposób zapewniający poufność i integralność tych danych;
- Systemy informatyczne służące do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej z wykorzystaniem firewalla
- Wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane za pomocą sieci publicznej stosuje się środki kryptograficznej ochrony jak szyfrowanie danych, psedonimizacja danych etc.

W firmie Podmiotu wprowadzono następujące rozwiązania nadawania uprawnień w systemach w których przetwarza się dane osobowe.

- Dostęp do danych osobowych i programów informatycznych posiadają jedynie pracownicy, którym nadano w sposób formalny uprawnienia i posiadają polecenia wydane przez Administratora
- Nadawanie uprawnień /poleceń użytkownikom do korzystania z systemów informatycznych opiera się o zasadę „wiedzy koniecznej” i zasadę „minimalnych uprawnień”. Użytkownik ma dostęp tylko do tych danych osobowych, które są mu potrzebne do realizacji zadań zgodnych z zakresem czynności.
- Zarządzanie uprawnieniami wykonuje się w oparciu o zakresy czynności dla każdego rodzaju użytkownika opisujące jego uprawnienia do korzystania z systemu informatycznego w procesie przetwarzania danych osobowych.
- Za określenie uprawnień adekwatnych do zakresów czynności użytkowników odpowiedzialny jest ADO
- Formalne nadawanie, zmiana i odbieranie uprawnień użytkownikom leży w gestii ADO

Opis postępowania

Podstawowe zasady nadawania uprawnień w systemie:

1. Przed dopuszczeniem do pracy przy przetwarzaniu danych osobowych każdy pracownik podmiotu z którego zakresu obowiązków (czynności, ustalonej roli) wynika konieczność przetwarzania danych osobowych, powinien zostać zapoznany przez ADO z przepisami dotyczącymi ochrony danych osobowych.
2. ADO włącza do indywidualnych zakresów obowiązków służbowych każdego pracownika zatrudnionego przy przetwarzaniu danych osobowych, obowiązku ochrony danych osobowych oraz odpowiedzialności za nieuzasadnioną ich modyfikację, zniszczenie bądź nielegalne ujawnienie lub pozyskanie.

Sposoby nadawania uprawnień:

3. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające nadane upoważnienie i w kolejnym etapie polecenia działania wyłącznie na polecenie Administratora. Upoważnienia wydawane są indywidualnie, odrębnie do każdego zbioru danych osobowych przed rozpoczęciem przez pracownika przetwarzania danych osobowych w danym zbiorze. Jeżeli pracownik Firmy musi posiadać dostęp do więcej niż jednego zbioru danych osobowych, możliwe jest nadanie upoważnienia do przetwarzania danych osobowych kilku zbiorów jednocześnie.
4. Administrator Danych Osobowych nadaje upoważnienia do każdego zbioru, do którego podmiot wniosku ma uzyskać dostęp. Wzór upoważnienia stanowi **Załącznik nr 6.**
3. Adekwatnie do zakresu czynności i konieczności uzyskania dostępu do określonego zbioru danych w Podmiocie każdy pracownik po zapoznaniu się z zakresem bezpieczeństwa danych, których znajomość jest niezbędna do przetwarzania danych w zakresie udzielonego mu upoważnienia, uzyskuje upoważnienie do przetwarzania danych, które przygotowuje ADO. Dodatkowo osoba uzyskuje polecenie przetwarzania w imieniu Administratora, zgodnie z **Załącznikiem nr 7.**Zapoznanie się z zakresem bezpieczeństwa danych odbywa się w formie szkolenia wstępnego realizowanego przez ADO.
4. Zakres nadanych pracownikowi uprawnień a następnie poleceń może ulegać zmianie (rozszerzeniu bądź zawężeniu) w związku z pełnieniem przez niego zadań w określonym przedziale czasu. W takim przypadku tryb wskazany do nadawania uprawnień określony w niniejszej polityce jest właściwy również w razie zmiany zakresu uprawnień pracownika w związku z jego dostępem do określonego zbioru danych osobowych. Wszelkie uprawnienia w tym zakresie posiada ADO.
6. Utrata prawa do przetwarzania danych osobowych określonych w upoważnieniu następuje w szczególności w przypadku;

- zmiany stanowiska pracy w Firmie, na którym nie ma konieczności posiadania dostępu do danych osobowych,
- gdy ustaje zasadność i celowość dalszego wykonywania prawa do przetwarzania danych w związku ze zmianą realizowanych przez pracownika zadań wynikających z jego indywidualnego zakresu czynności,

- umyślnego naruszenia zasad ochrony danych osobowych określonych w Rozporządzeniu, Polityce, innych dokumentach związanych z bezpieczeństwem danych osobowych,
- rozwiązania stosunku pracy.

7. W przypadkach cofnięcia upoważnienia decyzje podejmuje ADO. Wszelkie zmiany w tym zakresie prowadzone są w ewidencji osób dopuszczonych do przetwarzania danych osobowych- **Załącznik nr 10**.
9. Centralną „Ewidencję osób upoważnionych do przetwarzania danych osobowych Podmiocie prowadzi ADO.
10. Modyfikację uprawnień prowadzi ADO. W miejsce „starego" wystawia nowy zakres upoważnienie.
11. W przypadku utraty przez użytkownika upoważnienia do przetwarzania danych osobowych (np. rozwiązanie stosunku pracy, nie obsługiwanie systemu z powodu zmiany stanowiska pracy, nieobecności powyżej 30 dni) ADO cofa nadane upoważnienia jednocześnie dokonuje aktualizacji „Ewidencji osób upoważnionych do przetwarzania danych osobowych.

Zakres obowiązywania polityki zarządzania uprawnieniami

Procedura obowiązuje wszystkich użytkowników przetwarzających dane osobowe w Green Door Edyta Zięba, Ewa Spałek S.c.

Odpowiedzialność

- Każdy Użytkownik systemu informatycznego jest odpowiedzialni za przestrzeganie zasad bezpieczeństwa przy stosowaniu haseł.

Zasady bezpieczeństwa

- Wszystkie osoby posiadające dostęp do danych osobowych w szczególności przetwarzanych w systemach informatycznych są zobowiązane uwierzytelniać się (logować) do nich przy użyciu identyfikatora i hasła. Jedna zasada jeden użytkownik jedno konto użytkownika
- Szczegółowe wymagania dotyczące budowy oraz ochrony haseł (hasła muszą zawierać litery, cyfry, znak specjalny).

- Hasła użytkownika są poufne – użytkownikowi nie wolno przekazywać własnego hasła innym osobom.

- Hasło użytkownika składa się, co najmniej z 8 znaków, przy czym zwiera duże i małe litery, cyfry. Hasło nie może kojarzyć się w łatwy sposób z innymi danymi pracownika.
- Pracownik obligatoryjnie wprowadza nowe hasła nie **rzadziej niż raz w miesiącu.**

Hasło stanowiące element uwierzytelniający użytkownika powinno być przechowywane w sposób bezpieczny i wprowadzane w sposób uniemożliwiający

osobom trzecim poznanie jego treści. Jeśli zachodzi jakiekolwiek podejrzenie, że hasło zostało ujawnione, należy bezzwłocznie dokonać jego zmiany.

Rozdział 10. Standardy zabezpieczeń

Procedura rozpoczynania i zakończenia pracy użytkowników systemu.

Zakres obowiązywania

Procedura obowiązuje wszystkich użytkowników przetwarzających dane osobowe w Firmie

Odpowiedzialność

- Za wykonanie czynności zawartych w niniejszej instrukcji odpowiadają wszyscy użytkownicy
- Nadzór nad właściwą i terminową realizacją postanowień niniejszej procedury pełni ADO.

Zasady bezpieczeństwa

- Przed rozpoczęciem pracy użytkownik zobowiązany jest sprawdzić czy urządzenie komputerowe nie nosi śladów uszkodzeń lub ingerencji osób trzecich. W przypadku stwierdzenia nieprawidłowości użytkownik zgłasza sprawę ADO.
- Logowanie do systemu powinno być przeprowadzone w sposób zapewniający poufność wprowadzanego hasła użytkownika (tj. uniemożliwić jego podejrzenie etc.). W przypadku domniemania, że hasło utraciło atrybut poufności należy dokonać jego zmiany.

  Zawieszenie pracy:
  - W momencie pozostawiania komputera bez nadzoru lub opuszczaniu pomieszczania biurowego, w którym jest komputer, osoba za niego odpowiedzialna zobowiązana jest do zablokowania urządzenia komputerowego.
  - Wymaga się stosowania opcji blokowania komputera.
  - Po poprawnym zakończeniu pracy w systemie informatycznym, użytkownik ma obowiązek wylogować się z systemu oraz upewnić się, że urządzenie komputerowe zostało wyłączone. Wylogowanie nie jest jednoznaczne z zamknięciem programu np. poprzez czerwony krzyżyk na aplikacji.
- Wszystkie zasoby informatyczne – sprzęt, oprogramowanie i usługi informatyczne, wykorzystywane są w celach służbowych i nie mogą być używane w celach prywatnych.
- Urządzenie komputerowe (stacja robocza, urządzenia peryferyjne) przydzielane jest użytkownikowi wyłącznie:
  - w celach związanych z realizacją zadań o charakterze służbowym.

- w zakresie przyznanych uprawnień.

- Zapewnienie właściwej ochrony informacjom przetwarzanym na urządzeniu komputerowym.
- Ograniczenie dostępu do oprogramowania zainstalowanego na urządzeniu komputerowym.

Użytkownikom korzystającym z urządzeń komputerowych zabrania się:

- Używania modemów na stanowiskach komputerowych podłączonych do sieci LAN, bez pisemnego zezwolenia ADO.
- Udostępniania osobom trzecim haseł oraz szczegółów technicznych dotyczących konfiguracji posiadanych usług (np. dane konfiguracyjne zdalnego dostępu).
- Samodzielnej instalacji, wymiany i usuwania jakichkolwiek komponentów oraz wyposażenia urządzenia komputerowego (napędy i nagrywarki CD i DVD, FDD, dodatkowe dyski twarde, rozszerzenia pamięci operacyjnej, itp.) bez zgody ADO.
- Przechowywania danych osobowych na prywatnych komputerach lub prywatnych przenośnych nośnikach informacji.
- Podłączania urządzenia prywatnych do urządzeń i sieci Firmy.
- Zakazuje się także przenoszenia pomiędzy nimi danych (np. na kartach pamięci czy samoistnej konfiguracji służbowej poczty elektronicznej np. na smartfonie czy innym urządzeniu przenośnym. Powyższe zasady bezpieczeństwa dotyczą również telefonów, smartfonów, które ze względu na rozbudowaną funkcjonalność mogą zawierać, przetwarzać dane osobowe a nie posiadają właściwej ochrony. Telefony zabezpiecza się hasłem uwierzytelniającym jak również programem antywirusowym
- Dokonywania prób obejścia zabezpieczeń narzucanych przez systemy informatyczne.

Korzystanie z sieci Internet dozwolone jest wyłącznie do celów związanych z wykonywanymi czynnościami służbowymi.
Korzystanie z sieci ograniczone jest tylko dla pracowników Podmiotu
Konserwacja i serwisowanie urządzeń ma na celu zapewnienie nieprzerwanej i bezpiecznej pracy systemów, zapobieganie utratom, uszkodzeniom lub innym naruszeniom bezpieczeństwa informacji. Decyzje w tym zakresie podejmuje ADO.
Sprzęt przekazywany do naprawy poza siedzibę Firmy powinien być transportowany w sposób minimalizujący ryzyko kradzieży, uszkodzenia, zniszczenia lub kompromitacji danych na nim zapisanych.
Przeglądy, konserwacje i serwis sprzętu wymagające zaangażowania firm zewnętrznych powinny być wykonywane pod nadzorem ADO. Niedopuszczalny jest samodzielny serwis urządzenia komputerowego lub jego rozmontowywanie przez użytkownika

Ochrona przed złośliwy oprogramowaniem

1. Za złośliwe oprogramowanie, którego celem jest nieuprawniony dostęp zniszczenie w systemach informatycznych, uważa się:

a. Wirusy, kody trojańskie, robaki internetowe;
b. Programy mające na celu nieautoryzowane zdobycie, modyfikację lub destrukcję danych komputerowych;
c. Programy umożliwiające zdobycie lub podniesienie uprawnień w systemach komputerowych;
d. Programy, które mogą wpłynąć niekorzystnie na pracę systemów komputerowych poprzez utrudnienie lub sparaliżowanie ich pracy;
e. Inne, które może spowodować destabilizację działania i fałszowanie danych(podsłuchy, fałszywa tożsamość, kompromitacja danych wskutek fałszywych programów).

2. Ochrona przed złośliwym oprogramowaniem jest realizowana poprzez zapobieganie, wykrywanie i usuwanie tego typu programów oraz uświadamianie użytkowników w zakresie zasad bezpiecznego korzystania z zasobów systemów informatycznych oraz bieżących zagrożeń występujących w sieci zewnętrznej.

3. W Firmie wdrożono system ochrony antywirusowej. O ile jest to możliwe technicznie, wszystkie aktywa informatyczne objęte są ochroną przed złośliwym oprogramowaniem w czasie rzeczywistym, w sposób umożliwiający automatyzację wszystkich niezbędnych czynności, w tym np. umożliwiający automatyczne aktualizowanie baz wirusów dla oprogramowania antywirusowego.

4. Podmiot prowadzi edukację użytkowników w zakresie ochrony przed szkodliwym oprogramowaniem.

5. Za zarządzanie aplikacjami zabezpieczającymi przed złośliwym oprogramowaniem (w tym antywirusowym, filtrami i zaporami sieciowymi) odpowiada ADO.

6. W przypadku uszkodzenia danych lub oprogramowania należy przywrócić sprawność systemu wykorzystując kopie zapasowe.

Ochrona przed nieautoryzowanym dostępem do sieci

Systemy informatyczne służące do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej z wykorzystaniem firewalla, który realizuje następujące zadania:

a. Filtrowanie danych;
b. Filtrowanie URL;
c. Wykrywanie i blokowanie prób wykorzystania słabych punktów aplikacji;
d. Ochrona przed wirusami, oprogramowaniem spyware oraz robakami.

Załączniki (10 osobych) stanowią integralną i spójną całość polityki ochrony danych obowiązującej w Green Door Edyta Ziętek, Ewa Spałek s.c Dokument zawiera 27 kolejno ponumerowanych stron.