POLITYKA BEZPIECZEŃSTWA OCHRONY DANYCH OSOBOWYCH

SPIS TREŚCI

WSTĘP ………………………………………………………………………………………………………………..….3

CEL POWSTANIA DOKUMENTU ………………………………………………………………………………4

PODSTWA PRAWNA ORAZ ZAKRES OBOWIĄZYWANIA……………………………......................5

ZAKRES INFORMACJI OBJĘTYCH POLITYKĄ BEZPIECZEŃSTWA OCHRONY DANYCH OSOBOWYCH………………………………………………………………………………………………………….6

WYJAŚNIENIE TERMINÓW UŻYWANYCH W DOKUMENCIE ……………………………………..7

ZASADY PRZECHOWYWANIA DANYCH OSOBOWYCH……………………………………………10

ZAKRES PRZETWARZANIA DANYCH OSOBOWYCH ……………………………………………….11

OSOBY ODPOWIEDZIALNE ZA OCHRONĘ DANYCH OSOBOWYCH ………………………….12

SPOSÓB PRZECHOWYWANIA ……………………………………………………………………………….13

PODSTWOWE ZASADY PRZETWARZANIA……………………………………………………………..14

OBOWIĄZKI WOBEC OSÓB, KTÓRYCH DANE SĄ PRZETWARZANE………………………….15

OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH……………………16

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH…………………………..….17

OGÓLNE ZASADY BEZPIECZEŃSTWA…………………………………………………………………….18

ZASADY BEZPIECZEŃSTWA W POMIESZCZENIU …………………………………………………..20

OBSZAR ……………………………………………………………………………………………………………….21

KLUCZE………………………………………………………………………………………………………………..23

WYKAZ ZBIORÓW DANYCH…………………………………………………………………………………. 24

ZASADY PRZECHOWYWANIA DOKUMENTÓW……………………………………………………….25

NISZCZENIE DOKUMENTÓW……………………………………………………………………..………….26

ZASADY OBIEGU KORESPONDENCJI ……………………………………………………………………..26

ZASADY PRZEWOZU DOKUMENTÓW…………………………………………………………………….27

ZASADY UDOSTĘPNIANIA DOKUMENTÓW…………………………………………………………….27

ZASADY ZAWIERANIA UMOWY PODPOWIERZENIA……………………………………………….29

INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA……………………….……………..30

ZAWIADOMIENIE OSOBY………………………………………………………………………………………31

ZNAJOMOŚĆ POLITYKI…………………………………………………………………………………………..32

ZASADY PRZETWARZANIA DANYCH OSOBOWYCH…………………………..……………………32

PRAWO DO BYCIA ZAPOMNIANYM………………………………………………………………………..32

REJESTR PRZETWARZANIA DANYCH………………………………………………………..…………….33

LISTY PRACOWNICZE…………………………………………………………………………………………….33

ŚRODKI TECHNICZNE I ORGANIZACYJNE NIEZBĘDNE DLA ZAPEWNIENIA POUFNOŚCI, INTERGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH…………………………………………………………………………………………………………34

OBOWIĄZKI PRACOWNIKÓW…………………………………………………………………………………36

INSTRUKCJA ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI ……………..……………….37

WSTĘP

Polityka Bezpieczeństwa Ochrony Danych Osobowych została sporządzona na rzecz i obowiązuje w firmie Mariusz Gołdyn Mash Korek z siedziba ul. Agrestowa 37 b/2, 55-093 Kiełczów, który zwany jest dalej „Administratorem Danych Osobowych”.

Niniejsza Polityka Ochrony Bezpieczeństwa Danych Osobowych opisuje szczegółowe zasady ochrony i nadzoru nad przetwarzaniem danych osobowych, zwana dalej „Polityką”.

Każde naruszenie zasad Polityki Ochrony Bezpieczeństwa Danych Osobowych może być uznane za poważne naruszenie podstawowych obowiązków pracowniczych lub obowiązków wynikających z umów cywilno-prawnych o współpracy i może skutkować daleko idącymi konsekwencjami.

CEL POWSTANIA DOKUMENTU

Celem powstania niniejszej polityki jest realizacja obowiązków wynikających z przepisów Rozporządzenia 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) - (Dz.Urz.UE.L Nr 119, str. 1).

Przedmiotem Polityki Bezpieczeństwa Ochrony Danych Osobowych jest określenie, opisanie i zawarcie, w tym i załączonych dokumentach, zastosowanych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych osobowych objętych ochroną, a w szczególności zabezpieczeń danych osobowych przez ich udostępnianiem osobą nieupoważnionym, zbieraniem przez osoby nieuprawnione, przetwarzaniem z naruszeniem obowiązujących przepisów prawa oraz przed zmianą, utratą, uszkodzeniem lub zniszczeniem.

PODSTWA PRAWNA ORAZ ZAKRES OBOWIĄZYWANIA

I. Polityka Bezpieczeństwa Ochrony Danych Osobowych została przygotowana, aby spełniać wymogi:

1. 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) - (Dz.Urz.UE.L Nr 119, str. 1).

2. Ustawy o ochronie danych osobowych z dnia 10 maja 2018 r. (Dz.U. z 2018 r. poz. 1000) i aktów wykonawczych do ustawy.

II. Polityka Bezpieczeństwa Ochrony Danych Osobowych obowiązuje przy przetwarzaniu wszelkich danych osobowych w firmie Mariusz Gołdyn Mash Korek.

ZAKRES INFORMACJI OBJĘTYCH POLITYKĄ BEZPIECZEŃSTWA OCHRONY DANYCH OSOBOWYCH

I. Na Politykę Bezpieczeństwa Ochrony Danych Osobowych składają się następujące informacje:

1. w jaki sposób przetwarzane są dane osobowe,

2. wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych,

3. opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi,

4. sposób przepływu danych osobowych,

5.wykaz pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane lub przechowywane są dane osobowe,

6. określenie środków technicznych niezbędnych do zachowania poufności,

WYJAŚNIENIE TERMINÓW UŻYWANYCH W DOKUMENCIE

I. Terminy i pojęcia zawarte w niniejszym dokumencie:

1. Administrator Danych Osobowych – organ, jednostka organizacyjna, podmiot lub osoba, która w sposób zautomatyzowany lub niezautomatyzowany, zbiera, utrwala, organizuje, porządkuje, przechowuje, adaptuje lub modyfikuje, pobiera, przegląda, wykorzystuje, ujawnia poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie dane osobowe.

2. Ustawa – ustawa o ochronie danych osobowych z dnia 10 maja 2018 r. (Dz.U. z 2018 r. poz. 1000).

3. Dane osobowe – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię̨ i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź́ kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczna tożsamość osoby fizycznej.

4. Przetwarzanie - oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie .

5. Zbiór danych - oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

6. Zgoda - zgoda osoby, której dane dotyczą̨ oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

7. Poufność danych - należy rozumieć zapewnienie ich poufności, integralności, dostępności, rozliczalności, autentyczności, niezaprzeczalności oraz niezawodności na odpowiednim poziomie.

Poufność – oznacza zapewnienie, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom.

Integralność – oznacza zapewnienie, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany.

Dostępność – oznacza zapewnienie osiągalności lub możliwości do wykorzystania na żądanie, w założonym czasie przez uprawniony podmiot.

Rozliczalność – oznacza zapewnienie, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

Autentyczność – oznacza zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana (autentyczność dotyczy użytkowników, procesów, systemów).

Niezaprzeczalność – oznacza zapewnienie braku możliwości wyparcia się swojego uczestnictwa w całości lub w części przetwarzania danych przez jeden z podmiotów uczestniczących w przetwarzaniu

8. Dokument - przez dokument rozumie się nośnik informacji umożliwiający jej odtworzenie.

9. Przesyłka - oznacza towary lub dokumenty jakiegokolwiek rodzaju, którą przyjmuje się do przewozu od określonego adresu do drugiego, zarówno za listem przewozowym jak i bez takiego listu.

10. Rozporządzenie - 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) - (Dz.Urz.UE.L Nr 119, str. 1).

ZASADY PRZECHOWYWANIA DANYCH

I. Dane osobowe muszą być:

1. przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”);
2. zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami.

3.  adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”);

1. prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość́”);

4.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; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym.

5. przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność”).

ZAKRES PRZETWARZANIA DANYCH OSOBOWYCH

1. W niniejszej polityce przetwarzane są dane osobowe niezbędne do prawidłowej realizacji świadczeń.
2. Przetwarzane Dane Osobowe zbierane są w konkretnie prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami.
3. Jeżeli przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym, prawo Unii lub Państwa członkowskiego mogą określać i precyzować zadania i cele, w których dalsze przetwarzanie powinno być uznawane za zgodne z prawem i pierwotnymi celami.

OSOBY ODPOWIEDZIALNE ZA OCHRONĘ DANYCH OSOBOWYCH

I. Osobą odpowiedzialną za przetwarzanie danych osobowych oraz ich ochronę zgodnie z postanowieniami Rozporządzenia Parlamentu Europejskiego i Rady EU 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 oraz Ustawy, Polityki Ochrony Bezpieczeństwa Ochrony Danych Osobowych oraz Instrukcji Zarzadzania Systemami Informatycznymi jest:

a) Administrator Danych Osobowych, tj. Mariusz Gołdyn prowadzący działalność gospodarczą pod firmą Mariusz Gołdyn Mash Korek z siedzibą ul. Agrestowa 37b/2, 55-093 Kiełczów.

b) Osoby fizyczne lub osoby prawne wykonujące pracę bądź świadczące usługi cywilnoprawne na rzecz Administratora Danych Osobowych, które uzyskały upoważnienie do przetwarzania danych osobowych.

SPOSÓB PRZECHOWYWANIA

I. Polityka została zatwierdzona przez firmę Mariusz Gołdyn Mash Korek z siedzibą ul. Argestowa 37b/2, 55-093 Kiełczów.

jako dokument obowiązujący w niniejszej jednostce organizacyjnej.

II. Niniejszy dokument jest przechowywany i aktualizowany w wersji elektronicznej ze względu na czytelność i różnorodność obszarów, w których przetwarzane są dane osobowe. Jest on regularnie przeglądany i aktualizowany przez Administratora Danych Osobowych.

Zmiany w dokumencie Polityki oraz załącznikach wprowadzane są w chwili pojawienia się ważnych okoliczności lub nowego przepisu, istotnego dla spójności i aktualności Polityki Bezpieczeństwa Danych Osobowych, bądź aktualizacji dotychczasowych przepisów dotyczących ochrony lub przetwarzania danych osobowych. Zmiany zatwierdzane są przez Administratora Danych Osobowych.

III. Informacje o zmianach podawane są do wiadomości osób uczestniczących w przetwarzaniu danych osobowych poprzez sposób ustalony wewnętrznie, zwyczajowy dla jednostki.

IV. W przypadku zatwierdzenia nowej wersji Polityki Ochrony Bezpieczeństwa Danych Osobowych jest ona drukowana, a wydruk dołączany jest do prowadzonej dokumentacji ochrony danych osobowych.

V. Załączniki są przechowywane w formie papierowej.

VI. Dokument Polityki, wraz z załącznikami, stanowi tajemnicę przedsiębiorstwa Administratora Danych Osobowych i jest klasyfikowany jako dokument wewnętrzny.

PODSTAWOWE ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

I. Przetwarzanie danych osobowych może następować tylko w uzasadnionych przypadkach, na warunkach określonych niniejszą Polityką oraz Rozporządzeniem Parlamentu Europejskiego i rady UE z dnia 27 kwietnia 2016r., w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, przepisami ustawy o ochronie danych osobowych wraz z przepisami wykonawczymi.

II. Przetwarzanie danych osobowych jest dopuszczalne, gdy:

1. osoba, której dane dotyczą wyrazi na to zgodę.

Zgoda powinna wyraźnie obejmować pozwolenie dla Administratora Danych Osobowych na przetwarzanie danych osobowych w określonym celu,

2. zezwalają na to przepisy prawa ,

3. jest to niezbędne w celu wywiązania się z umowy, gdy osoba, której dane dotyczą jest jej stroną lub w celu podjęcia niezbędnych działań przed zawarciem umowy,

4. jest niezbędne do wykonania określonych prawem zadań publicznych,

5. jest niezbędne do wypełnienia prawnie usprawiedliwionych celów administratorów danych lub osób trzecich, którym przekazywane są dane, do których należą, a w szczególności:

1. marketing bezpośredni usług lub własnych produktów,
2. dochodzenie roszczeń z tytułu prowadzonej działalności gospodarczej.

OBOWIĄZKI WOBEC OSÓB KTÓRYCH DANE OSOBOWE SĄ PRZETWARZANE

I. W razie przetwarzania danych osobowych obowiązkiem Administratora Danych Osobowych jest poinformowanie osoby, której dane osobowe dotyczą, w szczególności o:

1. celu zbierania danych osobowych,

2. celu wykorzystywania danych osobowych,

3. uprawnieniach osoby do wglądu do swoich danych osobowych oraz ich poprawiania.

II. Na żądanie osoby, której dane osobowe są przetwarzane, należy udzielić jej
w ciągu 30 dni informacji na temat wykorzystywania jej danych osobowych
(celu, zakresu i sposobu przetwarzania danych oraz źródła uzyskania danych).

III. Na żądanie osoby, której dane osobowe są przetwarzane, jej dane mogą zostać uzupełnione, uaktualnione, sprostowane, względnie czasowo lub w sposób trwały może zostać wstrzymane ich przetwarzanie. O ile dane zostały udostępnione innym Administratorom Danych należy ich bez zbędnej zwłoki powiadomić o dokonanym uaktualnieniu, sprostowaniu lub zastrzeżeniu.

Odpowiedzialność za bezpieczeństwo danych osobowych, obowiązki użytkownika systemu oraz administratora bezpieczeństwa informacji

*Za bezpieczeństwo danych osobowych odpowiedzialna jest każda osoba
przetwarzająca dane osobowe włącznie z Administratorem Danych Osobowych jak i osoby które na jego zlecenie je przetwarzają.*

OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH

I. Nadzór nad przetwarzaniem danych osobowych w jednostce organizacyjnej sprawuje osoba kierująca prowadzoną działalnością gospodarczą (Administrator Ochrony Danych). Administrator Danych Osobowych może upoważnić osobę przez siebie wskazaną do określonych czynności związanych z przetwarzaniem danych lub jeżeli zachodzi taka potrzeba lub wymagają tego przepisy prawa wyznaczyć Inspektora do spraw ochrony danych osobowych do którego zadań będzie należało bezpośrednie nadzorowanie stanu realizacji procedur związanych z ochroną danych osobowych, a w razie potrzeby także bezpośrednia realizacja procedur w imieniu osoby kierującej działalnością jednostki organizacyjnej.

II. Każda osoba, która uzyskała upoważnienie do przetwarzania danych osobowych zobowiązana jest do ich ochrony w sposób zgodny z przepisami Rozporządzenia Parlamentu Europejskiego i rady UE z dnia 27 kwietnia 2016r., w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, Ustawy, Polityki Bezpieczeństwa Ochrony Danych Osobowych oraz Instrukcji zarządzania systemem informatycznym.

III. Osoba upoważniona zobowiązana jest do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje, także po ustaniu zatrudnienia lub wygaśnięciu łączącej strony umowy cywilno – prawnej.

UPOWARZNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

I. Upoważnienie do przetwarzania danych osobowych nadaje Administrator Ochrony Danych Osobowych, a także każda osoba przez niego upoważniona w tym zakresie, która jest także zobowiązana do przeprowadzania analizy ryzyka związanego z zagrożeniami związanymi z przetwarzaniem danych osobowych w jednostce organizacyjnej.

II. Administrator Danych Osobowych prowadzi również następujące wykazy:

1. ewidencję osób, którym nadano upoważnienia do przetwarzania danych osobowych (załącznik nr 1 do niniejszego dokumentu);

2.wykaz pomieszczeń, w których przetwarzane są dane osobowe, stanowiących obszar przetwarzania (załącznik nr 2 do niniejszego dokumentu)

3. wykaz podmiotów, z którymi zawarto umowy powierzenia przetwarzania danych osobowych (załącznik nr 3 do niniejszego dokumentu)

III. Administrator Danych Osobowych może czynności z zakresu prowadzenia rejestrów powierzyć w drodze upoważnienia innej osobie. Wykaz osób uprawnionych do prowadzenia rzeczonego rejestru stanowi załącznik nr 4 do niniejszego dokumentu.

IV. Wzór upoważnienia do przetwarzania danych osobowych stanowi załącznik nr 5 do niniejszej Polityki Ochrony Bezpieczeństwa Danych Osobowych.

OGÓLNE ZASADY BEZPIECZEŃSTWA OBOWIĄZUJĄCE PRZY PRZETWARZANIU DANYCH OSOBOWYCH

I. Wprowadzenie odpowiednich ze względu na charakter organizacji pracy Administratora Danych Osobowych ogólnych zasad bezpieczeństwa przetwarzania danych - zgodnie z wymaganiami przepisów prawnych z zakresu ochrony danych osobowych – pozwoli na prawidłowe przetwarzanie danych osobowych.

II. Za bezpieczeństwo przetwarzania danych osobowych w określonym zbiorze, odpowiada każdy pracownik lub osoba fizyczna lub prawna upoważniona do dostępu do danych osobowych.

III. Pracownicy mający dostęp do danych osobowych nie mogą̨ ich ujawnić́ zarówno w miejscu pracy, jak i poza nim, w sposób wykraczający poza czynności związane z ich przetwarzaniem w zakresie obowiązków służbowych, w ramach udzielonego upoważnienia do przetwarzania danych.

IV.W miejscu przetwarzania danych osobowych utrwalonych w formie papierowej pracownicy zobowiązani są do stosowania zasady tzw. „czystego biurka”. Zasada ta oznacza nie pozostawianie materiałów zawierających dane osobowe w miejscu umożliwiającym fizyczny dostęp do nich osobom nieuprawnionym. Za realizację powyższej zasady odpowiedzialny jest na swym stanowisku każdy z pracowników, zaś nieprzestrzeganie tej zasady może rodzić konsekwencje pracownicze polegające na udzieleniu kary pracowniczej osobie niestosującej się do niniejszej zasady, a nawet rozwiązaniem umowy o pracę lub umowy cywilno-prawnej.

V. Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe musi odbywać się w sposób uniemożliwiający odczytanie zawartej w nich treści.

VI. Niedopuszczalne jest wynoszenie materiałów zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych. Za bezpieczeństwo i zwrot materiałów zawierających dane osobowe odpowiada w tym przypadku osoba dokonująca ich wyniesienia.

VII. Przebywanie osób nieuprawnionych w pomieszczeniu, w którym przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych osobowych, chyba że dane te są w odpowiedni sposób zabezpieczone przed nieuprawnionym dostępem.

VIII. Pracownicy zobowiązani są do zamykania na klucz wszelkich pomieszczeń lub budynków wchodzących w skład obszarów, w których przetwarzane są dane osobowe w czasie ich chwilowej nieobecności w pomieszczeniu pracy, jak i po jej zakończeniu, a klucze nie mogą być pozostawione w zamku w drzwiach. Pracownicy zobowiązani są do dołożenia należytej staranności w celu zabezpieczenia posiadanych kluczy przed nieuprawnionym dostępem.

ZASADY BEZPIECZEŃSTWA W POMIESZCZENIU

I. Zasady bezpieczeństwa w pomieszczeniu, w którym przetwarzane są dane osobowe:

1.Osoby przebywające w pomieszczeniach w których przetwarzane są dane osobowe zobowiązani są do przestrzegania podstawowych przepisów bezpieczeństwa przeciwpożarowego co poczytuje się jako:

a) nie wrzucania niedopałków lub innych łatwopalnych materiałów w pobliżu miejsca gdzie przechowywane lub przetwarzane są dane osobowe.

b) wyłączenia odbiorników energii elektrycznej lub innych urządzeń obarczonych wysokim ryzkiem zapłonu po zakończeniu pracy.

c) bezwzględnie zabrania się z korzystania niesprawnych lub uszkodzonych urządzeń elektrycznych.

d) wszelkie materiały zawierające dane osobowe należy przechowywać w zamkniętych i osłoniętych szafkach jak najdalej od źródeł ciepła.

II. Po każdym dniu na zakończenie pracy pomieszczenia lub ich części w których przetwarzane są dane osobowe należy sprawdzić pod względem zachowania procedur bezpieczeństwa.

OBSZAR PRZETWARZANIA DANYCH OSOBOWYCH

1. Obszar w którym przetwarzane są dane osobowe stanowi wykaz pomieszczeń oraz części pomieszczeń tworzących obszar w którym przetwarzane są dane osobowe jest treścią osobnego dokumentu i stanowi załącznik nr 6 .
2. Wydzielona część pomieszczenia w której przechowywana jest dokumentacja i inne nośniki, na których przechowywane są dane osobowe może być wykorzystywana tylko i wyłącznie w tym celu. Szczegółowy opis urządzeń i innych rzeczy wykorzystywanych w celu przechowywania lub przetwarzania danych stanowi załącznik nr 7.

1. Z pomieszczeń lub ich części w których przetwarzane lub przechowywane są dane osobowe lub inne dokumenty może korzystać wyłącznie Administrator Danych Osobowych oraz osoby przez niego upoważnione.
2. Kluczami do szafek biurowych w których przechowywane są dane osobowe lub w pomieszczeniu lub miejscu gdzie są przetwarzane dysponuje Administrator Danych Osobowych oraz osoby przez niego upoważnione. Szczegółowy wykaz osób posiadających upoważnienie do dostępu do kluczy stanowi załącznik nr 8.
3. W pomieszczeniach lub ich częściach, w których przechowywane są dane osobowe dokonywane są wyłącznie takie działania które nie stwarzają zagrożenia dla przechowywanych lub przetwarzanych danych osobowych.
4. Każda osoba przebywająca w miejscu przetwarzania danych osobowych zobowiązana jest do przestrzegania zasad niniejszej polityki oraz innych zasad dotyczących:
5. zasad higieny pracy;
6. zachowania porządku i czystości;
7. pozostawiania wyposażenia biurowego i innych rzeczy niezbędnych do przechowywania i przetwarzania danych osobowych w pierwotnej bezpiecznej, konfiguracji.
8. W pomieszczeniach lub ich częściach, w których przechowywane lub przetwarzane są dane osobowe nie organizuje się spotkań, szkoleń oraz nie organizuje się innych czynności które mogłoby w sposób istotny zagrozić bezpieczeństwu przechowywanych tam dokumentacji.
9. Zgodę (pisemną) na udostępnienie pomieszczeń lub miejsc w których przechowywane lub przetwarzane są dane osobowe wyraża każdorazowo Administrator Danych Osobowych.

KLUCZE

1. Klucz do szafy biurowej jest w posiadaniu Administratora Danych Osobowych lub pracownika lub osoby podejmującej na rzecz Administratora Danych Osobowych czynności z zakresu prowadzonej przez niego działalności gospodarczej (pełnomocnik) przez Administratora Danych Osobowych upoważnionych, na wypadek nieobecności Administratora Danych Osobowych w miejscu przetwarzania danych osobowych.
2. Duplikaty kluczy, będące kluczami zapasowymi do pomieszczeń, w których przechowywane lub przetwarzane są dane osobowe znajdują sie zamkniętej kasetce, do której dostęp posiada wyłącznie Administrator Danych Osobowych.
3. Wydawanie kluczy zapasowych pracownikom może odbywać się tylko w uzasadnionych sytuacjach oraz w przypadkach awaryjnych za pokwitowaniem. Klucze zapasowe po ich wykorzystaniu należy niezwłocznie zwrócić do depozytu.

WYKAZY ZBIORÓW DANYCH

1. Wykaz zbiorów danych osobowych wraz z bazami danych, w których przetwarzane są dane osobowe oraz listą programów i narzędzi zastosowanych do ich przetwarzania jest treścią osobnego dokumentu i stanowi załącznik nr 9.

EWAKUACJA

1. W przypadku wystąpienia zdarzeń siły wyższej, jeżeli jest to możliwe Administrator Danych Osobowych przeprowadza ewakuację.
2. Zasady postępowania w przypadku ogłoszenia ewakuacji
3. zastosowanie do poleceń wydawanych przez Administratora Danych Osobowych lub inne uprawnione służby
4. Jeżeli to możliwe zakończenie pracy sprzętu komputerowego oraz wykonać niezbędne czynności mające na celu zabezpieczenie danych przed dostępem osób nieuprawnionych.
5. Jeżeli jest to możliwe przygotować do ewakuacji dokumentacje oraz sprzęt informatyczny
6. Nie zamykać drzwi
7. Udać się do wyznaczonego rejonu ewakuacji
8. Powiadomić Administratora Danych Osobowych lub właściwe służby o zakończonej akcji ewakuacyjnej.
9. W rejonie ewakuacji przebywać do czasu otrzymania informacji co do powrotu i kontynuacji pracy lub jej zakończenia.

III. Ewakuacja mienia lub jego zabezpieczenie nie może sią odbywać z narażeniem osób.

ZASADY PRZECHOWYWANIA DOKUMENTACJI

1. Dokumenty zawierające dane osobowe przechowuje się w wyznaczonym do tego miejscu osłoniętym przed czynnikami szkodliwymi.
2. Dokumenty segregowane są i kategoryzowane wg struktury, oraz przechowywane i archiwizowane przez czas prawem wymagany.
3. Dokumentację podatkową przechowuje się i archiwizuje przez łączny okres 5 lat licząc od końca roku kalendarzowego w którym upłyną termin płatności podatku.
4. Dokumentację pracowniczą przechowuje się i archiwizuje przez łączny okres 10 lat liczony od daty zakończenia stosunku prac przez pracownika lub osobę zatrudnioną w oparciu o umowę cywilno-prawną.
5. Dokumentacja zawierająca dane osobowe osób fizycznych jest zbierana, utrwalana, organizowana, porządkowana, przechowywana w sposób gwarantujący jej pełne bezpieczeństwo.

NISZCZENIE DOKUMENTACJI

1. Niszczenie dokumentacji zawierającej dane osobowe osób fizycznych, której termin przechowywania upłynął lub dokumentacji wybrakowanej następuje w sposób uniemożliwiający odtworzenie jej treści.
2. Do niszczenia dokumentacji stosuje się profesjonalną niszczarkę, zaś pozostałości Administrator Danych Osobowych utylizuje.
3. Raz w roku kalendarzowym Administrator Danych Osobowych lub osoba przez niego upoważniona dokonuje przeglądu zgromadzonej dokumentacji pod kątem:
4. ustaleniu dalszego obowiązywania celu przetwarzania danych osobowych;
5. wydzielania do zniszczenia dokumentacji zawierającej dane osobowe osób fizycznych, której okres przechowywania upłynął,
6. weryfikacji bezpieczeństwa dokumentacji.
7. Z czynności których przedmiotem jest zniszczenie dokumentacji zawierającej dane osobowe osób fizycznych sporządza się raport, którego wzór stanowi załącznik nr 10.

ZASADY PRZYJMOWANIA KORESPONDENCJI

Korespondencja przychodząca zawierająca dane osobowe osób fizycznych przechowywana jest w miejscu, w który przetwarzane lub archiwizowane są dane osobowe i podlega procedurze wskazanej w treści Polityki Ochrony Bezpieczeństwa Danych Osobowych.

ZASADY PRZEWOZU DOKUMENTÓW

1. W przypadku gdy transportowana jest dokumentacja zawierająca dane osobowe osób fizycznych należy ją zabezpieczyć przed dostępem osób nieupoważnionych, w sposób uniemożliwiający ich odczytanie przez osoby nieuprawnione.
2. W szczególności zabrania się przewożenia dokumentacji zawierającej dane osobowe osób fizycznych na fotelach wewnątrz pojazdów mechanicznych.
3. Dokumentacja zawierająca dane osobowe osób fizycznych w trakcie transportu każdorazowo musi być przechowywana w pojemniku do przechowywania i przenoszenia przedmiotów wymagających ostrożnego obchodzenia się z nim.
4. Doręczenie przesyłki potwierdzane jest przez odbiorcę w sposób zwyczajowo przyjęty i może to nastąpić w sposób:
5. elektroniczny;
6. pokwitowanie.
7. Jeżeli doręczenie przesyłki następuje na papierowym formularzu potwierdzenia, formularz ten zabezpiecza się w sposób uniemożliwiający jego odczytanie przez osoby nieupoważnione.
8. Przesyłka zawierająca dane osobowe osób fizycznych jest przygotowana do przewozu w bezpiecznym miejscu, bezpośrednio przez Administratora Danych lub osoby przez niego upoważnione.
9. Administrator Danych Osobowych zabezpiecza wszelkie informacje oraz oświadczenia związane z przesyłką zawierającą dane osobowe osób fizycznych, które związane są z transportem przesyłki w sposób uniemożliwiający ich odczytanie przez osoby nieuprawnione.
10. Pracownik lub osoba upoważniona przez Administratora Danych Osobowych przewożąca przesyłkę zobowiązana jest do przestrzegania wszelkich zasad bezpieczeństwa oraz nienarażania na utratę lub udostępnienie danych osobowych osób fizycznych. W tym celu zabrania się opuszczania pojazdu bez jego zamknięcia, gdzie pozostawione będą dane osobowe osób fizycznych.

ZASADY UDOSTĘPNIANIA DOKUMENTACJI

1. Administrator Danych Osobowych na wniosek osoby, której dane osobowe dotyczą udostępnia wszelkie żądane informacje. Rejestr udostępnionych danych osobowych stanowi załącznik nr 11.
2. Administrator Danych Osobowych udostępnia dokumenty zawierające dane osobowe osób fizycznych na żądanie organów kontrolnych, organów ścigania i wymiaru sprawiedliwości oraz innych podmiotów, wobec których obowiązek udostępnienia wynika z obowiązujących przepisów prawa.
3. Nie dopuszcza się wypożyczania dokumentacji poza obręb jednostki organizacyjnej z wyjątkiem podmiotów, wobec których występuje taki obowiązek.

ZASADY ZAWIERANIA UMOWY POWIERZANIA DANYCH OSOBOWYCH OSÓB FIZYCZNYCH

1. Rozporządzenie Parlamentu Europejskiego i Rady EU 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 przewiduje możliwość powierzenie przetwarzania danych osobowych przez Administratora Danych Osobowych zewnętrznym podmiotom. Powierzenie danych osobowych osób fizycznych jest dopuszczalne wyłącznie w drodze umowy powierzenia, w której należy określić zbiór, który zostanie przekazany, cel tego przekazania oraz zakres i czas planowanego przetwarzania danych przez inny podmiot.
2. Wzór umowy powierzenia stanowi załącznik nr 12.
3. Zawarte umowy powierzenia są przechowywaniu zgodnie z zasadami Polityki Ochrony Bezpieczeństwa Danych Osobowych oraz wymogami prawem przewidzianymi.
4. Wykaz zawartych przez Administratora Danych Osobowych umów powierzenia danych osobowych stanowi załącznik nr 13.

INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH

I. Administrator Danych Osobowych w sytuacja co najmniej podejrzenia naruszenia ochrony danych osobowych podejmuje następujące działania:

1) niezwłocznie podejmuje czynności niezbędne dla powstrzymania niepożądanych skutków, a następnie ustala przyczyny, lub sprawców zaistniałego zdarzenia, o ile jest to możliwe,

2) wstrzymuje wykonanie dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić jego udokumentowanie i analizę,

3) dokumentuje zaistniałe naruszenie, i nie opuszcza bez uzasadnionej potrzeby miejsca zdarzenia.

4) dokonuje wybór metody dalszego postępowania.

II. Procedury postępowania w przypadku stwierdzenia naruszenia ochrony danych osobowych pozwalają na wypracowanie generalnych reguł dotyczących zachowania pracowników Administratora Danych Osobowych w przypadku wystąpienia naruszenia zasad ochrony danych osobowych.

III. Administrator Danych Osobowych zobowiązany jest do stworzenia ogólnego trybu postępowania w wyżej wskazanej sytuacji, który będzie odpowiadać bądź organizacji pracy pracowników lub też specjalizacji prowadzonej działalności.

IV. W przypadku, gdy nastąpi naruszenie danych osobowych należy stosować poniższą instrukcję postepowania w sytuacji naruszenia danych osobowych:

a) Każda osoba, która poweźmie informację w zakresie naruszenia ochrony bezpieczeństwa danych osobowych osób fizycznych przez osobę przetwarzającą dane osobowe bądź posiada informacje mogące mieć wpływ na ochronę bezpieczeństwo danych osobowych osób fizycznych, jest zobowiązana fakt ten niezwłocznie zgłosić Admininistratorowi Danych Osobowych

b) Administrator Danych Osobowych wysłuchuje relacji osoby zgłaszającej z zaistniałego naruszenia, jak również relacji każdej innej osoby, która może posiadać informacje związane z naruszeniem, po czym sporządza notatkę, którą podpisuje Administrator Danych Osobowych oraz osoba zgłaszająca naruszenie.

c) Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu, Administrator Danych Osobowych, zasięga niezbędnych opinii i proponuje postępowanie naprawcze (w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń) i zarządza termin wznowienia przetwarzania danych osobowych.

d) Jeżeli naruszenie obarczone jest wysokim ryzykiem naruszenia praw i wolności osób fizycznych Administrator Danych Osobowych w terminie 72 godzin po stwierdzeniu naruszenia zgłasza je organowi kontrolnemu

e) Zgłoszenie do organu kontrolnego zawiera:

- opis naruszenia (kategorie danych, liczbę osób dotkniętych naruszeniem);

- oznaczenie danych kontaktowych Administratora Danych Osobowych;

- opis możliwych konsekwencji naruszenia ochrony danych osobowych;

ZAWIADOMIENIE OSOBY KTÓREJ DANE DOTYCZĄ

1. Administrator Danych osobowych bez zbędnej zwłoki powiadamia osobę której ochrona danych osobowych została naruszona.
2. Powiadomienie następuje za pomocą dostępnych Administratorowi Danych Osobowych narzędzi, np. e – mail., nr tel. Lub pisemnie;
3. Powiadomienie następuje bez zbędnej zwłoki.

ZNAJOMOŚĆ POLITYKI

1. Do zapoznania się z Polityką Ochrony Bezpieczeństwa Danych Osobowych oraz stosowania zawartych w niej zasad zobowiązane są wszystkie osoby przetwarzające dane osobowe z upoważnienia Administratora Danych Osobowych.
2. Administrator Danych Osobowych zobowiązuje się do podnoszenia kwalifikacji swoich pracowników lub osób zatrudnionych w oparciu o umowy cywilno-prawne w zakresie ochrony danych osobowych co rozumiane jest przez podnoszenie wiedzy stosownie do zajmowanego stanowiska w obrębie jednostki organizacyjnej.

ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

1. Administrator Danych Osobowych każdorazowo pobiera zgodę na przetwarzanie danych osobowych od osoby, której dane będą przetwarzane. Administrator pobiera zgodę na przetwarzanie danych osobowych w formie pisemnego oświadczenia.
2. Administrator Danych Osobowych informuje o uprawnieniach osoby, której dane osobowe będą przetwarzane.

PRAWO DO BYCIA ZAPOMNIANYM

1. Administrator Danych Osobowych usuwa na żądanie osoby, której dane są przetwarzane jej dane osobowe jeżeli nie są one niezbędne do celów, w których zostały zebrane oraz nie służą zabezpieczeniu wzajemnych roszczeń.
2. Administrator Danych Osobowych informuje osobę której dane osobowe są przetwarzane o ich usunięciu lub ograniczeniu przetwarzania.

REJESTR PRZETWARZANIA DANYCH

I. Administrator Danych osobowych prowadzi rejestr wszystkich kategorii czynności przetwarzania danych osobowych. Rejestr prowadzony jest w formie papierowej oraz formie elektronicznej.

II. Administrator Danych osobowych wypełnia rejestr na bieżąco.

LISTY PRACOWNICZE

Wszelkie dokumenty wewnętrzne służące do ewidencji czasu pracowników, konstruowane są w sposób umożliwiający zachowanie poufności w stosunku między pracownikami.

ŚRODKI TECHNICZNE I ORGANIZACYJNE NIEZBĘDNE DLA ZAPEWNIENIA POUFNOŚCI, INTERGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

I. Wykaz środków technicznych i organizacyjnych, które zostały zastosowane przez Administratora Danych Osobowych w celu zapewnienia odpowiedniego poziomu bezpieczeństwa przetwarzania danych osobowych osób fizycznych, a także dla zagwarantowania poufności, integralności i rozliczalności przetwarzanych danych osobowych wskazane są poniżej:

1) Klucze do pomieszczeń w których przechowywane są dane osobowe znajdują się z zamykanej kasetce.

2) Stacje robocze i inne urządzenia elektroniczne zabezpieczone są systemem antywirusowych oraz firewall. Stacje robocze oraz inne urządzenia na których przechowywane są dane osobowe wyposażone są w oprogramowanie wymuszające sezonową zmianę hasła.

3. Sieć internetowa zabezpieczona jest hasłem dostępu.

4. Wybrakowane dokumenty lub których cel przetwarzania odpadł lub termin przechowywania minął niszczone są przy pomocy niszczarki, a następnie szczątki są utylizowane.

OBOWIĄZKI PRACOWNIKÓW

Administrator Danych Osobowych zobowiązuje pracowników do:

1) zwracania uwagi na osoby wchodzące do siedziby jednostki organizacyjnej;

2) reagowania na próby niszczenia, wynoszenia lub wywożenia przedmiotów z jednostki organizacyjnej w szczególności dokumentacji zawierającej dane osobowe osób fizycznych;

3) natychmiastowego reagowania przez powiadomienie odpowiednich służb w przypadku zagrożenia zdrowia i życia osób przebywających w jednostce, lub zaobserwowanych próbach stworzenia zagrożenia również w przypadku gdy mogło by to narazić na utratę zniszczenie lub rozpowszechnienie dokumentacji objętej z mocy przepisów prawa ochrona.

4) sprawdzenia stanu zastosowanych zabezpieczeń sprzętu biurowego i komputerowego, dokumentacji i innego wposażenia przed przystąpieniem do pracy.

**5)** powiadomienia Administratora Danych Osobowcy w przypadku stwierdzenia nieprawidłowości lub naruszenia stanu zabezpieczeń

.

INSTRUKCJA ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYM

1. **Postanowienia ogólne.**
2. Niniejsza Instrukcja stanowi załącznik do obowiązującej **Polityki Bezpieczeństwa Ochrony Danych Osobowych.**
3. Celem instrukcji jest określenie sposobu zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych zawartych w przetwarzanych zbiorach danych,
ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji.
4. Osobą odpowiedzialną za bezpieczeństwo danych osobowych w systemach służących do przetwarzania danych osobowych w firmie Mariusz Gołdyn Mash Korek z siedzibą ul. Agrestowa 37b, Wrocław jest Mariusz Gołdyn zwany dalej „Administratorem Danych Osobowych”.
5. Dane osobowe przetwarzane są w systemach własnych Administratora Danych.
6. Na czas odzyskania bazy danych z kopii zapasowych/awaryjnych dopuszcza się przechowanie danych osobowych na innym serwerze lub w innym systemie niż dedykowany do ich przetwarzania.
7. Dostęp do baz danych oraz systemów informatycznych przetwarzających dane osobowe mają wyłącznie osoby posiadające stosowne upoważnienia wydane przez Administratora Danych na zasadach określonych w Polityce Bezpieczeństwa Ochrony Danych Osobowych.
8. Każda upoważniona osoba przed przystąpieniem do pracy przy przetwarzaniu danych osobowych zobowiązany jest zapoznać się z:
	1. Polityką Bezpieczeństwa Ochrony Danych Osobowych
	2. Obowiązującą Instrukcją postępowania w sytuacji naruszenia ochrony przetwarzania danych osobowych,
	3. Niniejszą instrukcją.
9. Fakt zapoznania się z przepisami, osoba upoważniona do przetwarzania danych zobowiązany jest potwierdzić własnoręcznym podpisem we właściwym dokumencie, przedstawionym mu do podpisania przez Administratora Danych.
10. Teksty wszystkich wymienionych dokumentów i aktów prawnych znajdują się do wglądu w siedzibie firmy.
11. **Obszar przetwarzania danych.**
	1. Dane osobowe przetwarzane są przez Administratora Danych w następujących budynkach, pomieszczeniach, tworzących obszar przetwarzania danych osobowych i omówione są w załączniku do Polityki Bezpieczeństwa Ochrony Danych Osobowych.
	2. Dostęp do pomieszczeń oraz zasady ich udostępniania, w których przetwarzane są dane osobowe, zawarte w zbiorach administrowanych przez Administratora Danych Osobowych zostały omówione w Polityce Bezpieczeństwa Ochrony Danych Osobowych.
	3. W przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych, lub podejrzenia takiego naruszenia, każda osoba posiadająca taką wiedzę zobowiązana jest postępować zgodnie z Polityką Bezpieczeństwa Ochrony danych Osobowych („Instrukcja postępowania w sytuacjach naruszenia ochrony danych osobowych”).
	4. Do przesłanek wskazujących na naruszenie bezpieczeństwa ochrony danych należą m. in.:
	5. Próby błędnych logowań do systemów przetwarzających dane osobowe
	6. Próby nieautoryzowanego dostępu do baz danych
	7. Próby wynoszenia danych na nośnikach pamięci masowych
	8. Pozostawienie wydruków danych osobowych na drukarkach, kserokopiarkach lub innych urządzeniach poligraficznych lub w miejscach niechronionych
	9. Wysyłanie, przez osoby nieupoważnione, dokumentów lub informacji zawierających dane osobowe za pośrednictwem poczty elektronicznej lub konwencjonalnej oraz urządzeń teletransmisyjnych
12. **Procedura przydziału i zmiany haseł oraz rejestracji i wyrejestrowania w systemach informatycznych, w których przetwarzane są dane osobowe; stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem**
13. Warunkiem uzyskania dostępu do systemów jest posiadanie przez użytkownika systemu stosownego upoważnienia oraz własnego identyfikatora i hasła do aplikacji.
14. Administrator Danych, przyznając upoważnienia do przetwarzania danych osobowych, stosuje zasadę przyznawania uprawnień w minimalnym zakresie, niezbędnym do wykonania czynności służbowych przez danego użytkownika
15. Identyfikatory, hasła lub inne mechanizmy uwierzytelniające użytkownika przydzielane są przez Administratora Danych
16. Administrator Danych ewidencjonuje identyfikatory użytkowników mających uprawnienia dostępu do systemów związanych z przetwarzaniem danych osobowych.
17. Każda osoba posiada własny identyfikator (lub identyfikatory w przypadku braku możliwości korzystania z tego samego identyfikatora w różnych systemach) i ma ściśle określony zakres praw dostępu do zasobów systemów informatycznych w których przetwarzane są dane osobowe
18. Do identyfikatora, uprawniającego do korzystania z systemu operacyjnego komputera, przypisane są prawa dostępu do zasobów z których korzysta przetwarzając dane osobowe.
19. Stosowane są następujące rodzaje haseł:
	1. Hasła logowania do systemu operacyjnego komputera lub serwera, na którym przetwarzane są dane osobowe
	2. Hasła do wygaszacza ekranu, o ile jest dostępny
	3. Hasła dostępu do systemów informatycznych lub aplikacji służących do przetwarzania danych osobowych
	4. Hasła dostępu do baz danych

O ile to możliwe, wszystkie wyżej wymienione hasła powinny być różne.

1. Zasady postępowania z hasłami użytkowników:
	1. Hasła użytkowników muszą się składać z co najmniej 8 znaków i muszą zawierać duże i małe litery, cyfry oraz znaki specjalne. Powinny być zmieniane co 30 dni.

(kategoria D – systemy przetwarzające dane osobowe),

|  |  |
| --- | --- |
|  | Kategoria |
| Parametr jakości hasła | D |
| Ilość znaków | 8 |
| Wymagane znaki wg zasady 2 z 3 wymienionych warunków | Duże i małe litery | 1 |
| Cyfry | 1 |
| Znaki specjalne (?><{}][\*&^%$#@!) | 1 |
| Ważność [dni] | 30 |

* 1. Hasła nie powinny zawierać imion, nazwisk, nazw własnych ani żadnych innych popularnych lub możliwych do odgadnięcia słów,
	2. Haseł nie wolno udostępniać ani dopuścić do ich ujawnienia,
	3. W sytuacji możliwego naruszenia bezpieczeństwa danych osobowych lub podejrzenia ujawnienia hasła obowiązuje konieczność niezwłocznej zmiany wszystkich stosowanych przez użytkownika haseł,
	4. Zarówno obecne, jak i wszystkie nieaktualne hasła objęte są ścisłą tajemnicą.
1. W przypadku cofnięcia prawa do przetwarzania danych osobowych osobie do tego upoważnionej (np. w związku ze zmianą zakresu obowiązków lub stanowiska, rozwiązaniem umowy o pracę lub zakończeniem współpracy) obowiązują następujące zasady:
	1. Zobowiązania do nierozpowszechniania i niewykorzystywania poufnych informacji zdobytych w trakcie wykonywania powierzonych prac zachowują ważność także po cofnięciu uprawnień,
	2. Osoba, której upoważnienie cofnięto musi zwrócić wszelkie dokumenty i inne materiały dotyczące zbiorów i baz danych osobowych, przetwarzanych danych osobowych lub stosowanych zabezpieczeń,
	3. Z chwilą cofnięcia uprawnienia do przetwarzania danych osobowych wszystkie identyfikatory wykorzystywane zostają, we współpracy z Administratorem Danych, zablokowane i wyrejestrowane z systemów, a wszystkie hasła z nimi powiązane tracą ważność,
2. **Procedury rozpoczęcia, zakończenia pracy i obsługi komputera.**
3. Każdorazowo przy rozpoczęciu pracy osoby upoważnione mają obowiązek podać hasło startowe komputera, a następnie zalogować się do systemu informatycznego (system operacyjny lub aplikacja) w którym przetwarzane są dane osobowe.
4. Osoba upoważniona rozpoczynająca pracę zobowiązany jest dopilnować, czy załadowało się programowanie antywirusowe monitorujące komputer, jeśli takowe jest dostępne.
5. Wszelkie zauważone okoliczności wskazujące na możliwość naruszenia bezpieczeństwa danych osobowych muszą zostać bezzwłocznie zgłoszone do Administratora Danych.
6. Jeśli istnieje taka możliwość, to muszą być stosowane wygaszacze ekranu zabezpieczone hasłem. Wygaszacz powinien się włączyć automatycznie po maks. 10 minutach bezczynności, dodatkowo osoby upoważnione powinny mieć możliwość ręcznego włączenia wygaszacza.
7. Wyłączenie wygaszacza ekranu wymaga podania hasła.
8. Po zakończeniu pracy osoba upoważniona oraz administrator jest zobowiązany wylogować się
z aplikacji/systemu oraz zabezpieczyć komputer przed dostępem do danych przez osoby nieuprawnione.
9. **Komputery przenośne wykorzystywane do przetwarzania danych osobowych.**

1. Osoba użytkująca komputer przenośny, służący do przetwarzania danych osobowych, zobowiązana jest zachować szczególną ostrożność podczas transportu oraz używania komputera poza siedzibą firmy, w celu zapobieżenia dostępowi do zgromadzonych
i przetwarzanych na nim danych przez osoby nieupoważnione, a w szczególności:

* 1. Nie zezwalać na korzystanie komputera osobom nie posiadającym upoważnienia do przetwarzania danych osobowych wydanego przez Administratora Danych Osobowych
	2. Przewozić lub przenosić komputer z zachowaniem koniecznych wymogów bezpieczeństwa, w szczególny sposób chroniąc go przed utratą
	3. W przypadku zgubienia lub kradzieży komputera użytkownik zobowiązany jest niezwłocznie powiadomić o tym fakcie Administratora Danych Osobowych
1. Komputer musi zostać skonfigurowany tak, aby do jego uruchomienia wymagane było podanie hasła startowego, a start systemu operacyjnego możliwy był jedynie z wewnętrznego dysku.
2. O ile to możliwe należy uruchomić mechanizmy kryptograficzne (sprzętowe lub programowe) pozwalające na szyfrowanie danych znajdujących się na wewnętrznym dysku.
3. Na wszystkich kartach sieciowych (Ethernet, WiFi, IR, Bluetooth, FireWire, modem, itp) należy skonfigurować i uruchomić oprogramowanie firewall, ograniczając do niezbędnego minimum możliwość inicjowania połączeń sieciowych z zewnątrz komputera.
4. **Metody tworzenia i przechowywania kopii awaryjnych oraz innych nośników danych związanych z danymi osobowymi.**
5. Kopie awaryjne powinny być wykonywane regularnie i zgodnie z przyjętym harmonogramem przez Administratora Danych Osobowych lub inna upoważniona osobę. Po sporządzeniu powinno się sprawdzić wykonaną kopię pod kątem jej prawidłowości i możliwości odtworzenia danych.
6. Kopie awaryjne są okresowo sprawdzane pod kątem przydatności do odtworzenia danych
w przypadku awarii systemu.
7. Kopie danych przechowywane są na dyskach lokalnych lub macierzach serwerów wykonujących backup lub magazynujących dane.
8. W przypadku konieczności oddania dysku lub innego nośnika danych osobowych do serwisu, Administrator Danych lub inna upoważniona osoba pod jego nadzorem, wymazuje zawartość nośnika tak, by nie dało sie jej potem odzyskać. Jeśli skasowanie danych jest niemożliwe lub nie daje pewności usunięcia, nośnik taki powinien być zniszczony, a nie serwisowany.
9. W uzasadnionych przypadkach (np. wysoka cena nośnika który powinien być, zniszczony) istnieje możliwość wykonania naprawy nośnika danych na którym znajdują się nieusunięte dane osobowe, ale czynność taka musi odbywać pod nadzorem Administratora Danych, lub na mocy osobnego porozumienia z wykonującym serwis. Porozumienie takie musi zawierać zapisy związane z ochroną danych osobowych przetwarzanych przez Administratora Danych. Jeśli to możliwe powinna to być „Umowa powierzenia przetwarzania danych osobowych”, zapewniająca ochronę danych.
10. Wszelkie nośniki, które podlegają niszczeniu, w tym uszkodzone dyski twarde, muszą zostać zniszczone komisyjnie przy udziale Administratora Danych lub jego przedstawiciela tak, by nie dało sie w żaden sposób odzyskać tych danych.
11. **Metody i częstotliwość sprawdzania obecności niebezpiecznego oprogramowania na stanowiskach operatorów danych oraz sposoby ich usuwania.**
	1. Wszystkie komputery i stacje robocze, na których operatorzy danych przetwarzają dane osobowe, należy wyposażyć w, aktualizowane automatycznie, oprogramowanie antywirusowe sprawdzające aktywnie funkcjonowanie systemów operacyjnych, przetwarzanych plików danych oraz podłączanych nośników danych, w celu wykrycia obecności lub identyfikacji podatności na działanie „złośliwego oprogramowania (malware)”.
	2. W przypadku wykrycia nieprawidłowości w zakresie opisanym w punkcie 1, należy niezwłocznie powiadomić Administratora Danych oraz podjąć niezbędne działania mające na celu weryfikację zidentyfikowanych nieprawidłowości oraz, jeśli potwierdzono zagrożenie dla przetwarzanych danych osobowych, przywrócenie bezpieczeństwa komputera lub stacji roboczej.
12. **Metody i częstotliwość aktualizacji i instalacji oprogramowania systemowego oraz aplikacji na stanowiskach operatorów danych.**
	1. Na wszystkich komputerach i stacjach roboczych, na których operatorzy danych przetwarzają dane osobowe, obowiązują następujące zasady:
13. System operacyjny instaluje i konfiguruje osoba upoważniona przez Administratora Danych Osobowych,
14. Tylko osoby upoważnione przez Administratora Danych Osobowych mogą samodzielnie instalować na swoich stanowiskach aplikacje i oprogramowanie użytkowe.
15. Aktualizacja aplikacji i oprogramowania użytkowego odbywa się w trybie automatycznym lub manualnym, pod nadzorem osoby upoważnionej przez Administratora Danych.
	1. Tylko Administrator Danych Osobowych posiada uprawnienia administracyjne komputerów lub stacji roboczych.

1. **Sposób dokonywania przeglądów i konserwacji systemów przetwarzania danych osobowych.**
	1. Operacje związane z dokonywaniem przeglądów i konserwacji systemów przetwarzających dane osobowe wykonywane są pod nadzorem Administratora Danych.
	2. Administrator Danych Osobowych zobowiązany jest do wyznaczenia osób upoważnionych do dokonywania przynajmniej raz na sześć miesięcy, pod nadzorem, całościowego przeglądu
	i konserwacji systemów, wykorzystywanych w firmie nośników informacji i zbiorów danych osobowych.
	3. W przypadku wykrycia nieprawidłowości w działaniu systemów, związanych z naruszeniem mechanizmów ochrony, niezwłocznie podejmowane są działania określone w Instrukcji postepowania w przypadku naruszenia ochrony danych osobowych.
2. **Sposoby postępowania w zakresie komunikacji w sieci komputerowej.**
	1. Dane osobowe przetwarzane powinny być przesyłane za pośrednictwem sieci komputerowych w postaci zaszyfrowanej lub przy użyciu transmisji kodowanej.
	2. Dostęp do sieci wewnętrznych (biurowej) i wszystkich urządzeń je obsługujących mają jedynie uprawnione osoby posiadające Upoważnienie nadane przez Administratora Danych Osobowych.
	3. Bazy danych w których przetwarzane są dane osobowe powinny być skonfigurowana tak, by pozwalać na połączenia tylko z wcześniej określonych komputerów.
3. **Zabezpieczenie zasilania systemów przetwarzających dane osobowe.**
	1. O ile to możliwe urządzenia powinny być podłączone do dwóch niezależnych, gwarantowanych źródeł zasilania.
	2. Nadzór nad funkcjonowaniem systemu zasilania urządzeń sprawuje Administrator Danych Osobowych w zakresie sprzętu biurowego.
4. **Rejestracja i monitoring dostępu do systemów przetwarzania danych osobowych.**
	1. Każdorazowy dostęp do baz danych osobowych oraz serwerów, na których przetwarzane są dane osobowe jest odnotowywany w logach/rejestrach. System rejestracji w pełni pozwala na identyfikację tożsamości operatora danych, aplikacji lub administratora, który w danym czasie uzyskał dostęp do systemów przetwarzających dane osobowe i/lub dokonał operacji na danych.

.

1. **Zasady ogólne.**
	1. Wszystkie czynności związane z przetwarzaniem w firmie danych osobowych, które nie zostały opisane w niniejszej Instrukcji, są nadzorowane przez Administratora Danych Osobowych.
	2. Administrator Danych posiada uprawnienia do zmian regulacji wynikających z niniejszego dokumentu.
	3. Administrator Danych Osobowych może powierzyć całość lub część czynności związanych z nadzorem nad funkcjonowaniem części lub całości systemów i procesów związanych z przetwarzaniem danych osobowych
	w ramach prowadzonej działalności. W każdym przypadku na Administratorze Danych Osobowych lub osobie przez nią upoważnionej ciąży obowiązek kontrolowania właściwego wykonywania czynności związanych z przetwarzaniem danych osobowych.