Polityka ochrony danych osobowych

Niniejsza polityka, zwana dalej „**Polityką**”, opisuje reguły i zasady ochrony danych osobowych przetwarzanych przez Elżbietę Szymańską zwanego dalej „**Administratorem**”.

Polityka ma za zadanie stanowić mapę wymogów, zasad i regulacji ochrony danych osobowych stosowanych przez administratora danych osobowych.

Polityka może podlegać aktualizacjom i modyfikacjom. Wszystkie zmiany w dokumencie muszą zostać odnotowane w poniższym rejestrze zmian.

Data modyfikacji	Autor modyfikacji	Opis zmian
20.04.2020	Elżbieta Szymańska	Wdrożenie pakietu RODO

Spis treści

§ 1 Postanowienia wstępne

1. Administrator prowadzi działalność gospodarczą w zakresie usług medycznych oraz edukacyjną
2. W związku z prowadzoną przez Administratora działalnością gospodarczą dochodzi do przetwarzania danych osobowych.
3. Dane osobowe przetwarzane są zarówno w formie elektronicznej, jak i papierowej.
4. Celem Polityki jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych sposobu przetwarzania informacji zawierających dane osobowe, w tym zapewnienie ochrony danych osobowych przed wszelakiego rodzaju zagrożeniami, tak wewnętrznymi jak i zewnętrznymi, świadomymi lub nieświadomymi.
5. Polityka opisuje również zasady zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych
6. Polityka została wdrożona w związku z treścią art. 24 ust. 2 RODO jako dowód dołożenia należytej staranności w zakresie ochrony danych osobowych.
7. Ochrona danych osobowych realizowana jest poprzez zabezpieczenia fizyczne, organizacyjne, oprogramowanie systemowe, aplikacje oraz samych użytkowników.
8. Polityka stanowi element dokumentacji ochrony danych osobowych wdrożonej przez Administratora, która to dokumentacja obejmuje, poza Polityką, również inne dokumenty. Dokumentacja ochrony danych osobowych jest przez Administratora przechowywana w formie elektronicznej.

§ 2 Zakres zastosowania

1. Polityka zawiera informacje dotyczące zasad przetwarzania danych osobowych, do którego dochodzi w związku z prowadzoną przez Administratora działalnością gospodarczą.
2. Politykę stosuje się w szczególności do:
    1) danych osobowych przetwarzanych w formie papierowej i elektronicznej,
    2) danych osobowych przetwarzanych w systemach informatycznych,
    3) informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych,
    4) rejestru osób dopuszczonych do przetwarzania danych osobowych,
    5) wszelkich innych dokumentów zawierających dane osobowe.
3. Zasady ochrony danych osobowych określone przez Politykę mają zastosowanie do wszystkich systemów informatycznych, w których przetwarzane są dane osobowe, wszystkich lokalizacji, w których przetwarzane są dane osobowe oraz wszystkich osób mających dostęp do danych osobowych z upoważnienia Administratora, a w szczególności:
    1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych, w których przetwarzane są dane osobowe podlegające ochronie,
    2) wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,
    3) wszystkich pracowników, zleceniobiorców, wykonawców umów o dzieło, wykonawców umów o świadczenie usług, praktykantów, stażystów i innych osób mających dostęp do informacji podlegających ochronie.
4. Polityka nie dotyczy podmiotów zewnętrznych, które przetwarzają dane osobowe powierzone im do przetwarzania przez administratora danych osobowych na podstawie stosownych umów powierzenia. Podmioty te stosują własne procedury i środki bezpieczeństwa związane z ochroną danych osobowych wymagane przez przepisy prawa, do czego zobowiązały się w ramach zawartych umów powierzenia przetwarzania danych osobowych. Niemniej jednak, część z podmiotów związanych z Administratorem umowami powierzenia może być zobowiązana do przestrzegania postanowień Polityki oraz pozostałych dokumentów wewnętrznych Administratora – chodzi tutaj o osoby, z którymi umowy powierzenia zostały zawarte z uwagi na współpracę w modelu B2B, nad którymi to jednak osobami Administrator posiada pewnego rodzaju kontrolę, w przeciwieństwie do podmiotów całkowicie zewnętrznych.

§ 3 Bezpieczeństwo danych osobowych

1. Utrzymanie bezpieczeństwa przetwarzanych danych osobowych rozumiane jest jako zapewnienie ich poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z ochroną danych osobowych.
2. Zastosowane zabezpieczenia mają służyć zapewnieniu bezpieczeństwa danych osobowych i zapewnić:
    1) poufność danych – rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom,
    2) integralność danych – rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany
    3) rozliczalność danych – rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie
    4) integralność systemu – rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej
    5) dostępność informacji – rozumianą jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne
    6) zarządzanie ryzykiem – rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych służących do przetwarzania danych osobowych.
3. Bezpieczeństwo danych osobowych opiera się o filary ochrony danych osobowych stosowane przez Administratora:
    1) legalność – Administrator dba o ochronę prywatności i przetwarzane dane zgodnie z prawem,
    2) bezpieczeństwo – Administrator zapewnia odpowiedni poziom bezpieczeństwa danych, podejmując stale działania w tym zakresie,
    3) prawa jednostki – Administrator umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje,
    4) rozliczalność – Administrator dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność.

§ 4 Administrator danych osobowych (ADO)

1. Administratorem danych osobowych jest Elżbieta Szymańska
2. Do najważniejszych zadań Administratora należy:
   1) wdrożenie, utrzymywanie i aktualizowanie Polityki,
   2) organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami obowiązujących przepisów prawa,
   3) zapewnienie przetwarzania danych zgodnie z uregulowaniami Polityki,
   4) wydawanie i anulowanie upoważnień do przetwarzania danych osobowych,
   5) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,
   6) weryfikacja podmiotów przetwarzających i zawieranie umów powierzenia,
   7) prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych i zgłoszenie faktu naruszenia organowi nadzorczemu oraz zawiadomienie o tym osoby, której dane dotyczą,
   8) nadzór nad bezpieczeństwem danych osobowych,
   9) inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych,
   10) przeprowadzanie szkoleń użytkowników przed przystąpieniem przez nich do przetwarzania danych osobowych,
   11) pozbawianie urządzeń i innych nośników informacji przeznaczonych do likwidacji zapisu danych lub – gdy nie jest to możliwe – uszkadzanie je trwale w sposób uniemożliwiający odczytanie danych,
   12) nadzorowanie usuwania awarii sprzętu komputerowego w sposób zapewniający bezpieczeństwo przetwarzanych danych osobowych,
   13) nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których przetwarzane są dane osobowe,
   14) nadzór nad czynnościami związanymi z ochroną przeciwwirusową, czynnościami serwisowymi dotyczącymi komputerów oraz systemów operacyjnych, przy wykorzystaniu których przetwarzane są dane osobowe,
   15) podejmowanie i nadzorowanie wszelkich innych działań zmierzających do zapewnienia bezpieczeństwa przetwarzanych w systemie informatycznym danych osobowych.
3. Za realizację i koordynację zadań związanych z ochroną danych osobowych odpowiedzialny jest Elżbieta Szymańska W razie nieobecności lub niedostępności, wyznaczy on swojego zastępcę.

§ 5 Inspektor ochrony danych osobowych (IODO)

Administrator nie wyznaczył inspektora ochrony danych osobowych świadomie, stwierdzając, że nie ciąży na nim taki obowiązek na podstawie art. 37 RODO ze względu na fakt, że:

1) nie jest organem ani podmiotem publicznym,
2) jego główna działalność nie polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę,
3) jego główna działalność nie polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych ani danych osobowych dotyczących wyroków skazujących i czynów zabronionych (administrator w ogóle nie przetwarza tego rodzaju danych osobowych).

§ 6 Obsługa informatyczna

1. Czynności w zakresie obsługi informatycznej wykonywane i koordynowane są przez Elżbietę Szymańską W razie nieobecności lub niedostępności Krzysztofa Wesołowskiego, wyznaczy on zastępcę.
2. Do czynności, o których mowa powyżej, należy:
   1) bieżący monitoring i zapewnienie ciągłości działania komputerów i innych urządzeń wykorzystywanych do przetwarzania danych osobowych oraz systemów operacyjnych,
   2) optymalizację wydajności komputerów i innych urządzeń wykorzystywanych do przetwarzania danych osobowych oraz systemów operacyjnych,
   3) instalację i konfiguracje sprzętu sieciowego i serwerowego,
   4) instalację i konfigurację oprogramowania systemowego, sieciowego,
   5) konfigurację i administrowanie oprogramowaniem systemowym, sieciowym oraz zabezpieczającym dane chronione przed nieupoważnionym dostępem,
   6) nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych,
   7) współpracę z dostawcami usług oraz sprzętu sieciowego i serwerowego,
   8) zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego,
   9) zarządzanie kopiami awaryjnymi danych osobowych oraz zasobów umożliwiających ich przetwarzanie,
   10) przeciwdziałanie próbom naruszenia bezpieczeństwa informacji,
   11) przyznawanie określonych praw dostępu do informacji w danym systemie,
   12) zarządzanie licencjami, procedurami ich dotyczącymi,
   13) prowadzenie profilaktyki antywirusowej.

§ 7 Obszar przetwarzania danych

1. Podstawowym obszarem przetwarzania danych osobowych jest siedziba Administratora znajdująca się pod następującym adresem: ul. Rejtana 10/14 Bydgoszcz
2. Siedziba Administratora to lokal o powierzchni ok. 70 m^2 znajdujący się na pierwszym piętrze w budynku, w którym znajdują się również inne lokale. Wejście do siedziby zabezpieczone jest dwoma parami drzwi, które wyposażone są w zamki antywłamaniowe. W siedzibie Administratora znajdują się trzy oddzielne pokoje oraz korytarz i przestrzeń socjalna. Pokoje wyposażone są w drzwi zwykłe zamykane na zamek.
3. Wejście do siedziby zabezpieczone jest drzwiami. Dostęp do siedziby kontrolowany jest z wykorzystaniem systemu elektronicznego. Fakt otworzenia drzwi z wykorzystaniem specjalnego klucza odnotowywany jest w systemie stosowanym przez Administratora. Lista osób posiadających klucz pozwalający na dostęp do siedziby stanowi załącznik nr 1 do Polityki.
4. Siedziba Administratora wyposażona jest w system alarmowy przeciwwłamaniowy oraz objęta monitoringiem.
5. W obrębie siedziby Administratora dochodzi do przetwarzania danych w formie papierowej oraz elektronicznej.
6. W siedzibie Administratora znajduje się szafa biurowa klasy A, w której przechowywane są wszystkie dokumenty zawierające dane osobowe.
7. Dane osobowe są również przetwarzane poza siedzibą Administratora z uwagi na wykorzystywanie do pracy urządzeń mobilnych pozwalających przetwarzać dane w dowolnym czasie i z dowolnego miejsca. Dane te są przetwarzane na komputerach oraz telefonach. W tym zakresie stosowane są środki ostrożności takie jak m.in.: aktywowanie dwuskładnikowego logowania wszędzie tam, gdzie jest to możliwe, stosowanie polityki czystego pulpitu, posługiwanie się silnymi hasłami składającym się co najmniej z 8 znaków, w tym liter i cyfr, szyfrowanie dysków, korzystanie z szyfrowanej teletransmisji, a także aktywowanie wygaszaczy ekranów na urządzeniach wykorzystywanych do przetwarzania danych osobowych po określonym czasie nieaktywności użytkownika. Wszystkie czynności podejmowane w związku z przetwarzaniem danych osobowych poza siedzibą Administratora muszą być wykonywane z należytą dbałością o zabezpieczenie danych osobowych i zapewnienie ich poufności.
8. W obrębie siedziby Administratora mogą przebywać osoby upoważnione do przetwarzania danych osobowych, a także osoby przebywające tam w związku z realizacją zawartych z nimi umów. Obecność innych osób jest dopuszczalna, ale tylko pod nadzorem osób upoważnionych do przetwarzania danych osobowych i z zachowaniem zasad bezpieczeństwa mających na celu uniemożliwienie uzyskanie dostępu do danych osobowych przez osoby do tego nieuprawnione. W szczególności, na czas obecności osób nieupoważnionych, dokumenty zawierające dane osobowe chowane są w miejsca uniemożliwiające zapoznanie się z nimi, a ekrany komputerów są wygaszane lub tak ustawiane by uniemożliwić wgląd w dane osobowe.
9. Ponieważ Administrator powierza przetwarzanie danych osobowych podmiotom trzecim, do przetwarzania danych osobowych dochodzi również w innych lokalizacjach, ale w tym zakresie czynności przetwarzania dokonuje podmiot trzeci lub ewentualnie podmioty do

tego przez niego upoważnione. Administrator danych osobowych nie ma szczegółowej wiedzy na temat lokalizacji, w obrębie których dochodzi do przetwarzania danych przez podmioty, którym powierzył przetwarzanie danych osobowych, ale podmioty te zobowiązały się do stosowania odpowiednich środków ochrony i bezpieczeństwa danych osobowych wymaganych przez przepisy prawa. W zakresie lokalizacji przetwarzania danych przez podmioty przetwarzające, Administrator pozyskuje zawsze informację czy dane przetwarzane są w obrębie Europejskiego Obszaru Gospodarczego czy poza nim, a w sytuacji, gdy poza nim, weryfikuje czy dany podmiot zapewnia odpowiedni poziom ochrony danych osobowych poprzez korzystanie z mechanizmów zgodności takich jak Tarcza Prywatności, standardowe klauzule umowne.

§ 8 Sprzęt wykorzystywany do przetwarzania danych osobowych

1. Dane osobowe przetwarzane są z wykorzystaniem komputerów, smartfonów oraz dysków lub pamięci przenośnych.
2. Ponadto, dane osobowe przechowywane są na serwerach. Serwery te nie należą do Administratora, lecz zapewniane są przez podmioty trzecie, z którymi łączą Administratora umowy powierzenia przetwarzania danych osobowych. Do serwerów, na których przechowywane są dane w ramach oprogramowania zapewnionego przez zewnętrzne podmioty administrator ani osoby upoważnione w ogóle nie mają dostępu. Dostęp do plików i bazy danych przechowywanej na serwerze zapewnianej przez zewnętrznego hostingodawcę mają określone osoby wskazane w załączniku nr 9 do Polityki.
3. Osoby upoważnione do przetwarzania danych osobowych mogą przetwarzać dane z wykorzystaniem własnego, prywatnego sprzętu, po uprzednim uzyskaniu stosownej zgody od Administratora. W takiej sytuacji zobowiązane są do wdrożenia na swoim sprzęcie takich zabezpieczeń, by zapewnić pełną poufność przetwarzanych danych osobowych. Administrator ma prawo do kontroli zastosowanych zabezpieczeń. Ponadto, Administrator ogranicza logowanie do systemów wykorzystywanych do przetwarzania danych osobowych wyłącznie do zweryfikowanego wcześniej sprzętu. Oznacza to, że osoba upoważniona będzie mogła zalogować się do systemu tylko z uprzednio zdefiniowanego w systemie przez Administratora sprzętu.
4. Wykaz sprzętu wykorzystywanego do przetwarzania danych osobowych stanowi załącznik nr 3 do Polityki.
5. Na dyskach komputerów mogą być przechowywane pliki zawierające dane osobowe. W celu zapewniania poufności danych, dyski podlegają szyfrowaniu, a możliwość uzyskania dostępu do danych przechowywanych na dysku uzależniona jest od uprzedniego zalogowania się z wykorzystaniem nazwy użytkownika oraz hasła.
6. W pamięci smartfonów również mogą być przechowywane pliki zawierające dane osobowe. W celu zapewniania poufności danych, dane podlegają szyfrowaniu, a możliwość uzyskania dostępu do danych uzależniona jest od uprzedniego potwierdzenia swojej tożsamości poprzez mechanizm uwierzytelniania użytkownika funkcjonujący w ramach danego smartfona.
7. Jeżeli dane przechowywane są na dyskach lub w pamięciach przenośnych, dyski te lub pamięci podlegają szyfrowaniu. Administrator dąży jednak do minimalizacji wykorzystywania dysków lub pamięci przenośnych. Jeżeli dane przechowywane są na zewnętrznym dysku twardym, to w przypadku konieczności likwidacji dysku twardego, zostaje on w miarę możliwości poddany pełnemu formatowaniu.
8. Ekrany monitorów, na których możliwy jest dostęp do danych osobowych, są automatycznie wyłączane po upływie ustalonego czasu nieaktywności użytkownika.
9. Monitory komputerów są tak ustawione, aby uniemożliwić osobom postronnym wgląd do danych osobowych.

10. Urządzenia komputerowe, dyski twarde lub inne informatyczne nośniki danych przeznaczone do naprawy, pozbawia się przed tymi czynnościami zapisu zgromadzonych na nich danych osobowych.
11. Sprzętem pośrednio wykorzystywanym przy przetwarzaniu danych osobowych są również drukarki, które służą do drukowania dokumentów zawierających dane osobowe. Drukarki mogą funkcjonować w sieci bezprzewodowej, co oznacza, że z każdego komputera podłączonego do sieci WiFi zarządzanej przez Administratora możliwe jest połączenie się z drukarką i wykonanie wydruku. Wydrukowane dokumenty zabierane są niezwłocznie z tacy drukarki po wykonaniu wydruku. Postępowanie z dokumentami drukowanymi opisane jest szczegółowo w § 10 Polityki.
12. Komputery wykorzystywane do przetwarzania danych osobowych w obrębie siedziby Administratora mają połączenie z Internetem poprzez sieć WiFi funkcjonującą w obrębie siedziby Administratora. Dostęp do sieci zabezpieczony jest hasłem, które znane jest wyłącznie Administratorowi i osobom upoważnionym do przetwarzania danych osobowych.
13. Komputery wykorzystywane do przetwarzania danych osobowych wyposażone są w system antywirusowy oraz firewall służący zapewnieniu bezpieczeństwa podczas korzystania z urządzenia.

§ 9 Oprogramowanie wykorzystywane do przetwarzania danych osobowych

1. Dane osobowe przetwarzane są z wykorzystaniem zarówno oprogramowania lokalnie zainstalowanego na dysku komputera lub smartfona, jak również w postaci oprogramowania chmurowego. Wykaz oprogramowania wykorzystywanego do przetwarzania danych osobowych stanowi załącznik nr 8 do Polityki.
2. Oprogramowanie wykorzystywane do przetwarzania danych osobowych zostało wskazane również w ramach rejestru czynności przetwarzania z przyporządkowaniem do poszczególnych czynności przetwarzania.
3. Administrator dąży do tego, by każda osoba biorąca udział w przetwarzaniu danych osobowych posiadała swoje własne konto w ramach oprogramowania do przetwarzania danych, tak by wszystkie czynności dokonywane na danych osobowych mogły być przypisane konkretnym użytkownikom. Nie zawsze jest to jednak możliwe, w szczególności, gdy chodzi o oprogramowanie zainstalowane lokalnie na komputerze, takie jak oprogramowanie biurowe czy wręcz sam system operacyjny. W tym zakresie odrębne konto użytkownika dotyczy konta użytkownika w systemie operacyjnym.

§ 10 Dokumentacja papierowa

1. Dane osobowe mogą być przetwarzane w formie papierowej, gdy zachodzi konieczność dokonania bieżących wydruków określonych dokumentów w celach operacyjnych lub gdy określone dokumenty przechowywane są w dłuższych okresach czasu. Ponadto, część dokumentów może być dostarczana Administratorowi przez inne podmioty.
2. Dokumenty zawierające dane osobowe to, w szczególności:
    1) faktury,
    2) formularze zamówień,
    3) umowy,
    4) oświadczenia,
    5) reklamacje,
    6) oświadczenie o odstąpieniu od umowy,
    7) dokumentacja pracownicza,
    8) potwierdzenia przelewów,
    9) wyciągi bankowe,
    10) korespondencja papierowa.
3. Dokumenty drukowane z uwagi na bieżące cele operacyjne są niezwłocznie niszczone z wykorzystaniem niszczarki po zrealizowaniu zadania wymagającego uprzedniego wydruku.
4. Dokumenty zawierające dane osobowe nie mogą być pozostawiane w miejscach ogólnodostępnych bez opieki. Dokumenty mogą znajdować się na biurkach i innych tego typu powierzchniach podczas wykonywania określonych zadań wymagających dostępu do dokumentów. Po zakończeniu pracy dokument powinien zostać zniszczony z wykorzystaniem niszczarki lub włożony do szafy, o której mowa w ust. 7 poniżej.
5. Dokumenty dostarczane pocztą lub za pośrednictwem kuriera odbierane są przez Administratora lub przez osoby przez niego do tego upoważnione.
6. Postępowanie z dokumentacją papierową ma prowadzić do tego, by nikt nieupoważniony nie uzyskał wglądu do danych osobowych zawartych w treści dokumentów.
7. Administrator nie posiada oddzielnego pomieszczenia przeznaczonego na archiwum. Dokumenty, które przechowywane są w dłuższych okresach czasu, przechowywane są w szafie biurowej klasy A znajdującej się w siedzibie Administratora, do której dostęp posiadają wyłącznie osoby upoważnione do przetwarzania danych osobowych.
8. Dokumenty zawierające dane osobowe nie mogą być wynoszone poza obszar siedziby Administratora, chyba że Administrator wyrazi na to zgodę ze względu na konieczność realizacji określonych obowiązków poza siedzibą Administratora. W takiej sytuacji, muszą zostać podjęte wszelkie środki ostrożności mające na celu zapewnienie poufności dokumentów wynoszonych poza siedzibę Administratora.
9. Jeżeli zachodzi konieczność przesłania dokumentów zawierających dane osobowe, dopuszczalne jest wyłącznie korzystanie z pocztowych przesyłek rejestrowanych oraz usług kurierskich, tak by w razie ewentualnych problemów z doręczeniem możliwe było

sprawne przeprowadzenie postępowania reklamacyjnego. Dokumenty powinny być w odpowiedni sposób zapakowane, by ograniczyć ryzyko ich zniszczenia.

10. Szczególnym rodzajem dokumentacji zawierającej dane osobowe jest dokumentacja księgowa, która gromadzona jest przez zewnętrzne biuro rachunkowe, a po zakończeniu roku podatkowego wydawana Administratorowi i przechowywana w szafie biurowej klasy A.

§ 11 Monitoring

1. Administrator ma możliwość monitorowania korespondencji wymienianej w ramach poczty elektronicznej przez osoby, dla których zostały utworzone skrzynki pocztowe w ramach organizacji Administratora. Skrzynki zakładane są przez Administratora. Administrator może w każdej chwili dokonywać monitoringu skrzynek pocztowych, logując się do nich i przeglądać ich zawartość. Administrator może również blokować dostęp do skrzynek, zmieniać hasła itp. Osoby korzystające ze skrzynek zostały o tym poinformowane w ramach obowiązku informacyjnego.
2. Wykaz skrzynek e-mail stanowi załącznik nr 4 do Polityki.
3. W ramach oprogramowania chmurowego wykorzystywanego do przetwarzania danych osobowych, Administrator ma możliwość weryfikacji, który użytkownik i w jakim czasie logował się do swojego konta.
4. Formą monitoringu jest również rejestracja otwierania drzwi do siedziby z wykorzystaniem breloka przypisanego do konkretnych osób upoważnionych. Tworzony w ten sposób rejestr przechowywany jest w wersji elektronicznej.
5. Obszar siedziby Administratora objęty jest monitoringiem wizyjnym. Funkcjonują dwie kamery w obrębie siedziby oraz jedna przed wejściem do siedziby. Nagrania nadpisywane są w trybie tygodniowym. Może zaistnieć jednak potrzeba utrwalenia niektórych nagrań w celach dowodowych – w takiej sytuacji wybrane nagrania mogą być przechowywane dłużej. Nagrania przechowywane są na dysku komputera i dostępne są z poziomu dedykowanej aplikacji, do której dostęp posiadają wyłącznie osoby upoważnione do tego. Dane dostępowe znane są tylko osobom upoważnionym w tym celu. Wykaz osób posiadających dostęp do nagrań z monitoringu stanowi załącznik nr 2 do polityki.

§ 12 Kopie bezpieczeństwa

1. W stosunku do dokumentów zawierających dane osobowe nie są wykonywane ich kopie. Postępowanie z dokumentami opisane w § 10 Polityki jest zdaniem Administratora wystarczające, by zapewnić bezpieczeństwo dokumentów i nie ma konieczności wykonywania ich dodatkowych kopii.
2. Wykonywane są kopie zapasowe elektronicznych baz danych Administratora. Kopie wykonywane są cyklicznie, co 24 godziny. Kopie przechowywane są w formie zaszyfrowanej i skompresowanej na serwerze zapewnianym przez podmiot zewnętrzny. Kopie są nadpisywane, co oznacza, że wykonanie kolejnej kopii zapasowej powoduje trwałą niedostępność poprzednio wykonanej kopii zapasowej.
3. Jeżeli chodzi o dane osobowe przetwarzane w ramach plików elektronicznych przechowywanych na dysku komputerów, to pliki te są automatycznie synchronizowane z Dyskiem Google, co stanowi ich dodatkową kopię zapasową na wypadek utraty dostępu do danych z dysku komputera.
4. Ponadto, kopie zapasowe wykonywane są przez zewnętrznego hostingodawcę według procedur przez niego stosowanych, które to procedury, zgodnie ze zobowiązaniami wynikającymi z powierzenia przetwarzania danych, odpowiadają wymogom przepisów prawa.

§ 13 Ochrona antywirusowa

1. Ochrona antywirusowa jest realizowana poprzez zainstalowanie odpowiedniego oprogramowania antywirusowego.
2. W przypadku wykrycia wirusa komputerowego, użytkownik systemu zobowiązany jest do natychmiastowego poinformowania o tym fakcie Administratora.
3. System operacyjny podlega regularnej kontroli pod kątem obecności wirusów komputerowych.
4. Wykryte zagrożenia usuwa się niezwłocznie z systemu operacyjnego.
5. Przed przystąpieniem do unieszkodliwienia wirusa, należy zabezpieczyć dane zawarte w systemie przed ich utratą.
6. Osobą odpowiedzialną za powyższe działania jest .Elżbieta Szymańska

§ 14 Zasady dotyczące przetwarzania danych osobowych

1. Administrator przetwarza dane osobowe z poszanowaniem następujących zasad:
    1) w oparciu o podstawę prawną i zgodnie z prawem (legalizm),
    2) uczciwie i w sposób przejrzysty (rzetelność i transparentność),
    3) w konkretnych celach i nie „na zapas” (minimalizacja),
    4) nie więcej niż potrzeba (adekwatność),
    5) z dbałością o prawidłowość danych (prawidłowość),
    6) nie dłużej niż potrzeba (czasowość),
    7) zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo).
2. W celu przestrzegania zasady legalności, Administrator dokonał analizy wszystkich czynności przetwarzania danych osobowych i określił właściwe podstawy prawne, w oparciu, o które dane czynności przetwarzania mogą się odbywać. Informacje w tym zakresie zawarte są w rejestrze czynności przetwarzania.
3. W celu przestrzegania zasady rzetelności i transparentności, Administrator zadbał o to, by w każdej sytuacji pozyskiwania danych osobowych, w stosunku do osoby, której dane są pozyskiwane, realizowany był obowiązek informacyjny zgodnie z art. 13 RODO. Sposób realizacji obowiązku informacyjnego wskazany jest w rejestrze czynności przetwarzania w stosunku do każdej czynności przetwarzania.
4. W celu przestrzegania zasady minimalizacji, Administrator przemyślał, jakie dane potrzebne są mu do określonych celów, co znalazło odzwierciedlenie w rejestrze czynności przetwarzania. Administrator pouczył wszystkie osoby biorące udział w procesie przetwarzania danych osobowych, by nie pozyskiwały danych osobowych w zakresie przekraczającym uzasadnione potrzeby opisane w rejestrze czynności przetwarzania.
5. W celu przestrzegania zasady adekwatności, Administrator przemyślał, jakie dane są mu potrzebne do realizacji określonych celów i określił w stosunku do każdej czynności przetwarzania zakres niezbędnych danych. W związku z tym, zakazane jest pozyskiwanie danych osobowych ponad określony przez Administratora katalog danych niezbędnych do realizacji poszczególnych celów.
6. Nie wszystkie czynności przetwarzania pozwalają na z góry określenie sztywnego katalogu przetwarzanych danych. Szczególnie, gdy chodzi o obsługę klientów, zakres przetwarzanych danych nie jest możliwy do precyzyjnego określenia z uwagi na fakt, że zakres usługi będzie również determinował zakres przetwarzanych danych. Podobnie w przypadku wymiany korespondencji, nie jest możliwe jednoznaczne określenie, jakie dane druga strona przekaże administratorowi w ramach korespondencji.
7. W celu przestrzegania zasady prawidłowości, Administrator przyjął zasadę, zgodnie z którą w razie wątpliwości dotyczących prawidłowości danych osobowych mu przekazanych, podejmowane są działania mające na celu wyjaśnienie powstałych wątpliwości.
8. W celu przestrzegania zasady czasowości, Administrator przemyślał terminy, w jakich dane stają się mu zbędne i będą podlegać usunięciu, co znalazło odzwierciedlenie w

rejestrze czynności przetwarzania danych osobowych. Ponadto, Administrator przynajmniej raz w roku dokonuje przeglądu czy posiadane przez niego dane nie są już mu zbędne i w razie stwierdzenia zbędności, dokonuje ich trwałego usunięcia.

9. W celu przestrzegania zasady bezpieczeństwa, Administrator wdrożył odpowiednie środki techniczne i organizacyjne mające zapewnić należytą ochronę przetwarzanych danych osobowych. Decyzja o wyborze środków została poprzedzona przeprowadzeniem analizy ryzyka.

§ 15 Środki bezpieczeństwa, analiza ryzyka, ocena skutków

1. W celu zapewnienia odpowiedniego poziomu ochrony danych osobowych wprowadzono odpowiednie zabezpieczenia organizacyjne i techniczne.
2. Decyzja o wyborze zabezpieczeń organizacyjnych i technicznych została poprzedzona analizą ryzyka, która to analiza została spisana w postaci oddzielnego dokumentu.
3. Wykaz zastosowanych środków bezpieczeństwa stanowi załącznik nr 7 do Polityki.
4. Środki bezpieczeństwa zostały wymienione również w analizie ryzyka oraz rejestrze czynności przetwarzania.
5. Wymienione środki techniczne i organizacyjne zabezpieczenia danych dotyczą wyłącznie środków wdrożonych bezpośrednio przez administratora danych osobowych. W zakresie, w jakim administrator danych osobowych powierzył przetwarzanie danych osobowych innym podmiotom, podmioty te zobowiązały się utrzymywać odpowiednie środki ochrony danych osobowych wymagane przez przepisy prawa.
6. Administrator nie przeprowadził oceny skutków operacji przetwarzania dla ochrony danych osobowych, stwierdzając, że nie ciąży na nim taki obowiązek na podstawie art. 35 RODO. Rodzaje przetwarzania danych osobowych dokonywane przez Administratora nie powodują, zdaniem Administratora, wysokiego ryzyka naruszenia praw lub wolności osób fizycznych. Taki wniosek Administratora wynika z tego, że Administrator:
    1) przetwarza głównie podstawowe dane identyfikacyjne i kontaktowe,
    2) przetwarza wyłącznie dane osobowe zwykłe,
    3) nie stosuje narzędzi śledzących i profilujących wykorzystujących dane osobowe,
    4) nie przetwarza danych na dużą skalę.
7. Ponadto, Administrator zapoznał się z wykazem rodzajów operacji wymagających oceny skutków ogłoszonym przez Prezesa Urzędu Ochrony Danych Osobowych i pośród dokonywanych przez siebie operacji przetwarzania danych nie zidentyfikował żadnej, która znajdowałaby się w wykazie.

§ 16 Obsługa praw jednostki

1. Administrator spełnia obowiązki informacyjne wobec osób, których dane przetwarza oraz oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania.
2. Sposób realizacji obowiązków informacyjnych został wskazany w rejestrze czynności przetwarzania w odniesieniu do każdej czynności.
3. Obsługa żądań kierowanych do Administratora przez osoby, których dane są przetwarzane, odbywa się za pośrednictwem poczty elektronicznej z wykorzystaniem adresu e-mail dedykowanego obsłudze związanej z ochroną danych osobowych: zielinska.szymanska@gmail.com
4. Osobą odpowiedzialną za obsługę żądań dotyczących danych osobowych jest Elżbieta Szymańska W razie nieobecności lub niedostępności, wyznacza on swojego zastępcę. Jeżeli żądanie spływa na adres e-mail nieobsługiwany przez Szymona Szymańskiego, osoba obsługująca dany adres e-mail przekazuje żądanie na adres obsługiwany przez Szymona Szymańskiego
5. Obsługa żądań archiwizowana jest w ramach archiwum poczty elektronicznej. Ponadto, prowadzony jest rejestr obsługi żądań osób, których dane są przetwarzane, w którym odnotowywane są wszystkie żądania oraz sposób ich obsługi.
6. Realizując prawa osób, których dane dotyczą, Administrator wprowadza proceduralne gwarancje ochrony praw i wolności osób trzecich. W szczególności w przypadku powzięcia wiarygodnej wiadomości o tym, że wykonanie żądania osoby o wydanie kopii danych lub prawa do przeniesienia danych może niekorzystnie wpłynąć na prawa i wolności innych osób, Administrator może zwrócić się do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu.
7. Jeżeli żądanie zgłaszane jest przez osobę, której danych Administrator nie przetwarza, osoba obsługująca żądanie informuje tę osobę o tym, że Administrator nie przetwarza jej danych osobowych.
8. W sytuacji odmowy realizacji żądania kierowanego do Administratora, osoba obsługującą żądanie informuje osobę kierując żądanie o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych.
9. Na żądanie osoby dotyczące dostępu do jej danych, Administrator informuje osobę, czy przetwarza jej dane oraz informuje osobę o szczegółach przetwarzania, zgodnie z art. 15 RODO, a także udziela osobie dostępu do danych jej dotyczących. Dostęp do danych może być zrealizowany przez wydanie kopii danych, z zastrzeżeniem, że kopii danych wydanej w wykonaniu prawa dostępu do danych Administrator nie uzna za pierwszą nieodpłatną kopię danych dla potrzeb opłat za kopie danych.
10. Na żądanie, Administrator wydaje osobie kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych.
11. Administrator dokonuje sprostowania nieprawidłowych danych na żądanie osoby. Administrator ma prawo odmówić sprostowania danych, chyba, że osoba w rozsądny sposób wykaże nieprawidłowość danych, których sprostowania się domaga. W

przypadku sprostowania danych, Administrator informuje osobę o odbiorcach danych, na żądanie tej osoby.

12. Administrator uzupełnia i aktualizuje dane na żądanie osoby. Administrator ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych. Administrator może polegać na oświadczeniu osoby co do uzupełnianych danych, chyba że będzie to niewystarczające w świetle przyjętych przez Administratora procedur, prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.
13. Na żądanie osoby, Administrator usuwa dane, gdy:
    1) dane nie są niezbędne do celów, w których zostały zebrane, ani przetwarzane w innych zgodnych z prawem celach,
    2) zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania,
    3) osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,
    4) dane były przetwarzane niezgodnie z prawem,
    5) konieczność usunięcia danych wynika z obowiązku prawnego.
14. Administrator dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:
    1) osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość,
    2) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,
    3) Administrator nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,
    4) osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, czy po stronie Administratora zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.
15. Na żądanie osoby, Administrator wydaje w ustrukturyzowanym, powszechnie używam formacie nadającym się do odczytu maszynowego lub przekazuje innemu podmiotowi, jeśli jest to możliwe, dane dotyczące tej osoby, które dostarczyła ona Administratorowi, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej.
16. Jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, a dane przetwarzane są przez Administratora w oparciu o uzasadniony interes Administratora, Administrator uwzględni sprzeciw, o ile nie zachodzą po stronie Administratora ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.

17. Jeżeli osoba zgłosi sprzeciw względem przetwarzania jej danych przez Administratora na potrzeby marketingu bezpośredniego, Administrator uwzględni sprzeciw i zaprzestanie takiego przetwarzania.

§ 17 Retencja danych

1. W rejestrze czynności przetwarzania wskazane zostały okresy przez jakie dane są przechowywane w związku z poszczególnymi czynnościami przetwarzania.
2. W sytuacji, gdy zachodzi konieczność usunięcia lub zniszczenia danych osobowych, czy to z uwagi na upływ okresu przechowywania czy też ze względu na stosowne żądanie złożone w tym zakresie przez osobę, której dane dotyczą, dane zostaną usunięte lub zniszczone w taki sposób, by ich odtworzenie nie było możliwe.
3. W przypadku konieczności usunięcia danych osobowych, podejmowane są następujące kroki:
    1) identyfikacja dokumentów zawierających dane osobowe podlegające usunięciu, a następnie zniszczenie tych dokumentów z wykorzystaniem niszczarki; jeżeli zniszczenie dokumentów nie jest uzasadnione, można ograniczyć się do zamazania lub innego trwałego uczynienia nieczytelnymi danych osobowych zawartych w dokumencie,
    2) weryfikacja w ramach poszczególnego oprogramowania, czy przetwarzane są w nim dane podlegające usunięciu, a jeżeli tak, usunięcie tych danych,
    3) weryfikacja czy na dyskach komputerów oraz w chmurach synchronizowanych z komputerami są przechowywane pliki zawierające dane podlegające usunięciu, a jeżeli tak, usunięcie tych plików w sposób trwały.
4. Z uwagi na skalę przetwarzania danych osobowych, niewielkie ryzyko związane z przetwarzaniem danych osobowych oraz możliwości finansowe i organizacyjne, Administrator nie ma możliwości usunięcia danych z kopii zapasowych. Przy czym, biorąc pod uwagę, że kopie zapasowe są nadpisywane przy ich wykonywaniu, w ramach kopii zapasowych znajduje się zawsze aktualny stan bazy danych. Oznacza to, że jeżeli po usunięciu danych dojdzie do wykonania kopii zapasowych, w tej kopii zapasowej usunięte dane nie będą się już znajdować.

§ 18 Podmioty przetwarzające

1. W procesie przetwarzania danych osobowych biorą udział podmioty zewnętrzne.
2. Podmioty zewnętrzne biorą udział w procesie przetwarzania danych osobowych na podstawie zawartych z tymi podmiotami umów powierzenia danych osobowych.
3. Wszystkie podmioty biorące udział w procesie przetwarzania danych osobowych zostały wskazane w rejestrze czynności przetwarzania oraz w wykazie podmiotów przetwarzających stanowiącym załącznik nr 5 do Polityki.
4. Dokonując wyboru podmiotów przetwarzających, Administrator weryfikuje, czy określone podmioty spełniają wymogi dotyczące bezpieczeństwa ochrony danych osobowych na poziomie wymaganym przez RODO. W szczególności, administrator podejmuje następujące czynności w ramach procesu wyboru podmiotów przetwarzających:
    1) weryfikacja renomy podmiotu w środowisku branżowym,
    2) weryfikacja dokumentów dotyczących danych osobowych udostępnianych przez podmiot (regulaminy, polityki prywatności itp.),
    3) weryfikacja treści proponowanej umowy powierzenia przetwarzania danych osobowych,
    4) weryfikacja lokalizacji, w której będą przechowywane dane osobowe, w szczególności lokalizacji serwerów, a w sytuacji, gdy dane miałyby być przekazywane poza obszar EOG – weryfikacja czy odbywa się to na podstawie odpowiednich mechanizmów zgodności.
5. Ponadto, jeżeli jest to możliwe, administrator odbiera od podmiotu przetwarzającego stosowne oświadczenia w ramach ankiety dla podmiotu przetwarzającego. Oświadczenie te służą weryfikacji czy podmiot przetwarzający zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie danych spełniało wymogi prawa i chroniło prawa osób, których dane dotyczą.
6. W stosunku do każdego podmiotu przetwarzającego Administrator zebrał stosowne dokumenty związane z prywatnością, ochroną danych osobowych i przechowuje ja razem z dokumentacją ochrony danych osobowych.
7. W procesie przetwarzania danych osobowych mogą brać biorą udział współpracownicy administratora, pracujący zdalnie na odległość z wykorzystaniem własnego sprzętu. Administrator traktuje te osoby również jako podmioty przetwarzające i zawiera z nimi umowy powierzenia przetwarzania danych osobowych. Dla osób tych tworzone są oddzielne konta i dostępy w ramach oprogramowania wykorzystywanego do przetwarzania danych osobowych, a w tym zakresie stosowane są odpowiednio postanowienia § 19 ust. 5 – 9 Polityki. Osoby te znajdują się zarówno w wykazie powierzeń stanowiącym załącznik nr 5 do Polityki, jak również w wykazie osób upoważnionych i innych użytkowników stanowiącym załącznik nr 6 do Polityki.

§ 19 Osoby upoważnione

1. Osoby, które przetwarzają dane osobowe w ramach stosunku pracy lub na podstawie stosunku cywilnoprawnego, ale pozostając pod fizycznym nadzorem administratora, przetwarzają dane na podstawie upoważnienia do przetwarzania danych. Pozostałe osoby, w szczególności współpracownicy zdalni, przetwarzają dane na podstawie umów powierzenia przetwarzania danych.
2. Upoważnienie do przetwarzania danych osobowych dokonywane jest na piśmie.
3. Każda osoba upoważniona uwzględniana jest w ewidencji osób upoważnionych.
4. Ewidencję osób upoważnionych prowadzi Administrator. Ewidencja stanowi załącznik nr 6 do Polityki.
5. Każda osoba upoważniona posiada oddzielne konto użytkownika w systemach informatycznych wykorzystywanych do przetwarzania danych osobowych.
6. Nadawanie identyfikatorów i przydzielanie haseł:
   1) hasło składa się z co najmniej 8 znaków; zalecane jest, aby zawierało małe i wielkie litery oraz cyfry i znaki specjalne,
   2) identyfikator użytkownika powinien być inny dla każdego użytkownika, a po jego wyrejestrowaniu z systemu informatycznego, nie powinien być przydzielany innej osobie,
   3) identyfikatory użytkowników ujawnione są w wykazie osób upoważnionych do przetwarzania danych osobowych,
   4) hasła pozostają tajne, każdy użytkownik jest zobowiązany do zachowania w tajemnicy swego hasła, także po jego zmianie; obowiązek ten rozciąga się także na okres po upływie ważności hasła,
   5) hasło, co do którego zaistniało choćby podejrzenie ujawnienia powinno być niezwłocznie zmienione przez użytkownika,
   6) utrata upoważnienia do przetwarzania danych osobowych powoduje natychmiastowe usunięcie z grona użytkowników systemu informatycznego.
7. Przed rozpoczęciem pracy w systemie operacyjnym oraz w systemach informatycznych osoba upoważniona musi podjąć następujące kroki:
   1) zalogować się do systemu operacyjnego z wykorzystaniem zastrzeżonych tylko dla siebie identyfikatora i hasła w sposób uniemożliwiający ich ujawnienie osobom postronnym,
   2) sprawdzić prawidłowość funkcjonowania komputera i systemu operacyjnego,
   3) w razie stwierdzenia nieprawidłowości, powiadomić o tym administratora systemu informatycznego lub Administratora,
   4) zalogować się do systemu informatycznego z wykorzystaniem zastrzeżonych tylko dla siebie identyfikatora i hasła w sposób uniemożliwiający ich ujawnienie osobom postronnym,

5) w razie stwierdzenia naruszenia zabezpieczenia systemu operacyjnego lub informatycznego, lub stanu wskazującego na istnienie takiej możliwości, podjąć odpowiednie kroku stosownie do zasad postępowania w sytuacji naruszenia zabezpieczenia danych osobowych.

8. Przerywając przetwarzanie danych, osoba upoważniona powinna co najmniej aktywować wygaszasz ekranu lub w inny sposób zablokować możliwość korzystania ze swego konta użytkownika przez inne osoby.
9. Po zakończeniu przetwarzania danych osobowych, osoba upoważniona zobowiązana jest do zakończenia pracy w systemie informatycznym, wylogowania się z systemu operacyjnego i wyłącznie komputera.

§ 20 Odbiorcy danych

1. Odbiorcy danych osobowych zostali wskazani w rejestrze czynności przetwarzania w odniesieniu do poszczególnych czynności przetwarzania.

§ 21 Naruszenia ochrony danych osobowych

1. Każde naruszenie ochrony danych osobowych powinno być niezwłocznie zgłaszane przez użytkowników Administratorowi.
2. Typowe sytuacje, które należy postrzegać w kontekście naruszenia ochrony danych osobowych:
    1) naruszenie lub próby naruszenia integralności systemów informatycznych przeznaczonych do przetwarzania danych osobowych – przez osoby nieuprawnione do dostępu do sieci lub aplikacji ze zbiorem danych osobowych,
    2) naruszenie lub próba naruszenia integralności danych osobowych w systemie przetwarzania (wszelkie dokonane lub usiłowane modyfikacje, zniszczenia, usunięcia danych osobowych przez nieuprawnioną do tego osobę),
    3) celowe lub nieświadome przekazanie zbioru danych osobowych osobie nieuprawnionej do ich otrzymania,
    4) nieautoryzowane logowanie do systemu,
    5) nieuprawnione prace na koncie użytkownika dopuszczonego do przetwarzania danych osobowych przez osobę do tego nieuprawnioną,
    6) istnienie nieautoryzowanych kont dostępu do danych osobowych,
    7) włamanie lub jego usiłowanie z zewnątrz sieci,
    8) nieautoryzowane zmiany danych w systemach informatycznych,
    9) niezablokowanie dostępu do systemu informatycznego przez osobę uprawnioną do przetwarzania danych osobowych w czasie jej nieobecności,
    10) ujawnienie indywidualnych haseł dostępu użytkowników do systemów informatycznych,
    11) brak nadzoru nad serwisantami lub innymi pracownikami przebywającymi w pomieszczeniach, w których odbywa się przetwarzanie danych osobowych,
    12) nieuprawniony dostęp lub próba dostępu do pomieszczeń, w których odbywa się przetwarzanie danych osobowych,
    13) zniszczenie dokumentacji zawierającej dane osobowe bez użycia niszczarki,
    14) fizyczna obecność w budynku lub pomieszczeniach, w których dochodzi do przetwarzania danych osobowych, osób zachowujących się podejrzanie,
    15) otwarte drzwi do szaf, w których przechowywane są dane osobowe,
    16) ustawienie monitorów pozwalające na wgląd osób postronnych w dane osobowe,
    17) wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz firmy bez upoważnienia administratora danych osobowych,
    18) udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej i ustnej,
    19) telefoniczne próby wyłudzenia danych osobowych,

20) kradzież komputerów lub CD, twardych dysków, pendrive'a z danymi osobowymi,

21) e-maile zachęcające do ujawnienia identyfikatora i/lub hasła,

22) pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów,

23) przechowywanie haseł do systemów w pobliżu komputera.

3. W przypadkach, o których mowa powyżej, należy podjąć czynności zmierzające do zabezpieczenia miejsca zdarzenia, zabezpieczenia ewentualnych dowodów i minimalizacji zaistniałych szkód, w tym w szczególności:

   1) zapisać wszelkie informacje związane z danym zdarzeniem, a w szczególności:

      a) dokładny czas uzyskania informacji o naruszeniu zabezpieczenia danych osobowych i czas samodzielnego wykrycia tego faktu,

      b) dane osoby zgłaszającej,

      c) opis miejsca zdarzenia,

      d) opis przedstawiający stan techniczny sprzętu służącego do przetwarzania lub przechowywania danych osobowych,

      e) wszelkie ustalone okoliczności zdarzenia.

   2) na bieżąco wygenerować i wydrukować wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustaleniu okoliczności zdarzenia, opatrzyć je datą i podpisem,

   3) dokonać identyfikacji zaistniałego zdarzenia, poprzez ustalenie w szczególności:

      a) rozmiaru zniszczeń,

      b) sposobu, w jaki osoba niepowołana uzyskała dostęp do danych osobowych,

      c) rodzaju danych, których dotyczyło naruszenie,

      d) wyeliminować czynniki bezpośredniego zagrożenia utraty danych osobowych,

      e) sporządzić protokół z wyżej wymienionych czynności,

      f) poinformować właściwe organy ścigania w przypadku podejrzenia popełnienia przestępstwa.

4. Administrator obowiązany jest do niezwłocznego podjęcia działań mających na celu powstrzymanie lub ograniczenie osobom niepowołanym dostępu do danych osobowych w szczególności przez:

   1) zmianę hasła dla użytkownika,

   2) fizyczne odłączenie urządzeń i tych segmentów sieci, które mogły umożliwić dostęp do bazy danych osobie niepowołanej;

   3) wylogowanie użytkownika podejrzanego o naruszenie zabezpieczenia ochrony danych.

5. Po przeanalizowaniu przyczyn i skutków zdarzenia powodującego naruszenie bezpieczeństwa przetwarzanych danych osobowych, osoby odpowiedzialne za bezpieczeństwo danych osobowych obowiązane są podjąć wszelkie inne działania mające na celu wyeliminowanie podobnych naruszeń w przyszłości oraz zmniejszenie

ryzyka występowania ich negatywnych skutków. W szczególności, jeżeli przyczyną naruszenia są:

1) błąd osoby upoważnionej do przetwarzania danych osobowych związany z przetwarzaniem danych osobowych – należy przeprowadzić dodatkowe szkolenie, indywidualne lub grupowe,
2) uaktywnienie wirusa komputerowego – należy ustalić źródło jego pochodzenia oraz wykonać test zabezpieczenia antywirusowego,
3) zaniedbanie ze strony osoby upoważnionej do przetwarzania danych osobowych – należy wyciągnąć konsekwencje zgodnie z przepisami prawa,
4) włamanie – należy dokonać szczegółowej analizy wdrożonych środków zabezpieczających,
5) zły stan urządzenia lub sposób działania programu lub inne niedoskonałości informatycznego systemu przetwarzania danych osobowych – należy niezwłocznie przeprowadzić kontrolne czynności serwisowo – programowe.

6. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia, jego skutki oraz podjęte środki zaradcze. Dokumentacja odbywa się z wykorzystaniem zestawienia incydentów naruszenia ochrony danych osobowych.
7. W przypadku naruszenia ochrony danych osobowych, na Administratorze ciąży obowiązek przeprowadzenia oceny czy zachodzi konieczność zgłoszenia tego faktu do organu nadzorczego zgodnie z postanowieniami art. 33 RODO oraz zawiadomienia osoby, której dane dotyczą, zgodnie z postanowieniami art. 34 RODO.

§ 22 Administrator jako podmiot przetwarzający

1. Administrator w stosunku do niektórych z przetwarzanych danych osobowych, występuje w roli podmiotu przetwarzającego, któremu inne podmioty powierzają do przetwarzania dane osobowe na podstawie stosownej treści umów.
2. Szczegóły dotyczące przetwarzania powierzonych danych znajdują się w rejestrze kategorii czynności przetwarzania.
3. W stosunku do danych powierzonych do przetwarzania Administratorowi, mogą być podejmowane wyłącznie czynności odpowiadające zakresowi powierzenia.
4. W stosunku do danych powierzonych do przetwarzania Administratorowi stosuje się wszystkie zasady oraz środki bezpieczeństwa i ochrony danych osobowych opisane w Polityce i analizie ryzyka.

§ 23 Postanowienia końcowe

1. Niniejsza Polityka oraz pozostałe dokumenty związane z ochroną danych osobowych, ulegać będą przeglądom w celu weryfikacji aktualności informacji w nim zawartych w cyklu przynajmniej corocznym.
2. Każdy przegląd będzie podlegał raportowaniu z wykorzystaniem wzoru raportu wchodzącego w skład dokumentacji ochrony danych osobowych.
3. W przypadku aktualizacji któregoś z dokumentów, zmiany będą uwidaczniane w rejestrze zmian stanowiącym część dokumentu podlegającego aktualizacji.

Załączniki

Załącznik nr 1 - lista osób posiadających klucz pozwalający uzyskać dostęp do siedziby Administratora

- Elżbieta Szymańska.
- Szymon Szymański
- .....

Załącznik nr 2 – lista osób posiadających dostęp do nagrań z monitoringu

- Elżbieta Szymańska
- .....
- .....

Załącznik nr 3 – wykaz sprzętu wykorzystywanego do przetwarzania danych osobowych

- Laptop Asus
- Tablet Ipad
- .....

Załącznik nr 4 – wykaz skrzynek e-mail funkcjonujących w ramach organizacji Administratora

- zielinska.szymanska@gmail.com
- .....
- .....

Załącznik nr 5 – wykaz podmiotów przetwarzających

Podmiot przetwarzający	Świadczone usługi	Umowa powierzenia
OVH Sp. z o.o. ul. Swobodna 1, 50-088 Wrocław	Hosting	Zawarta w formie elektronicznej.
Google Ireland Limited Gordon House, Barrow Street, Dublin 4, Ireland	Usługi Google w ramach pakietu G-Suite	Zawarta w formie elektronicznej.
Biuro Rachunkowe Sp. z o.o. ul. Wapienna 145a, 54-123 Mury	Księgowość	Zawarta w formie pisemnej.
ManyChat, Inc. One International Place, 535 Everett Ave, Apt. 312, Palo Alto, CA 94301 United States of America	Narzędzie ManyChat	Zawarta w formie elektronicznej.
Rocket Science Group LLC The Rocket Science Group, LLC 675 Ponce de Leon Ave NE Suite 5000 Atlanta, GA 30308 USA	System mailingowy MailChimp	Zawarta w formie elektronicznej
CRM Sp. z o.o. ul. Migdałowa 40, 04-123 Koza Wola	System CRM	Zawarta w formie elektronicznej
IT MAX Jan Kowalski ul. Bohaterska 123c, 91-123 Wrocław	Obsługa IT	Zawarta w formie pisemnej
Slack Technologies, Inc. 500 Howard Street San Francisco, CA 94105 United States	Komunikator Slack	Zawarta w formie elektronicznej
Fakturownia Sp. z o.o. 00-389 Warszawa ul. Smulikowskiego 6/8	System do fakturowania	Zawarta w formie elektronicznej

Załącznik nr 6 – wykaz osób upoważnionych i innych użytkowników - nie dotyczy

Załącznik nr 7 – wykaz środków ochrony danych osobowych

- Kontrola dostępu do siedziby Administratora (drzwi z systemem breloków).
- Kontrola dostępu do sprzętu oraz oprogramowania wykorzystywanego do przetwarzania danych osobowych (logowanie z wykorzystaniem identyfikatora użytkownika oraz hasła lub autoryzacja czynnikiem biometrycznym).
- Ograniczenie dostępu do kluczowej infrastruktury do zawężonego kręgu osób
- Dwuskładnikowe logowanie aktywowane tam, gdzie jest to możliwe.
- Kopie zapasowe.
- Szafa biurowa klasy A dla dokumentów zawierających dane osobowe.
- Szyfrowanie dysków twardych i innych nośników danych.
- Szyfrowana transmisja przy przesyłaniu danych.
- Niszczarka dokumentów.
- Wygaszacze ekranów zabezpieczone hasłem.
- Blokada systemów po dłuższej nieaktywności.
- Ochrona antywirusowa.
- Polityka czystego biurka i czystego pulpitu.
- Bieżący monitoring operacji wykonywanych na danych osobowych.
- Różnicowanie dostępu do poszczególnych zasobów zawierających dane osobowe.
- Przeszkolenie osób biorących udział w przetwarzaniu danych.
- Procedura weryfikacji podmiotów przetwarzających oraz powierzenia danych.
- Procedura nadawania upoważnień do przetwarzania danych.
- Dokumentacja ochrony danych osobowych.

Załącznik nr 8 – wykaz oprogramowania wykorzystywanego do przetwarzania danych

- Google Docs i Google Sheets – oprogramowanie biurowe dostępne w chmurze Google, które przechowuje dane również w chmurze Google,
- Google Drive – chmura umożliwiające przechowywanie w niej plików zawierających dane osobowe,
- Slack – system do komunikacji wewnętrznej dostępne w modelu on-line,
- ManyChat – narzędzie do zarządzania chatbotem w serwisie Facebook dostępne w modelu on-line,
- Fakturownia – system do fakturowania dostępny w modelu on-line
- System CRM – system CRM dostępny w modelu on-line
- klient poczty zainstalowany lokalnie na komputerze – korespondencja przechowywana jest na serwerze zapewnianym przez zewnętrznego hostingodawcę,
- oprogramowanie biurowe zainstalowane lokalnie na komputerach wykorzystywanych do przetwarzania danych,
- system operacyjny komputera – w zakresie, w jakim dane przetwarzane są z wykorzystaniem standardowych funkcji i narzędzi dostępnych w ramach systemu, np. w postaci folderów zawierających w swojej nazwie dane osobowe.

Załącznik nr 9 – wykaz osób posiadających dostęp do serwera

- Elżbieta Szymańska.
- .....
- .....