POLITYKA BEZPIECZEŃSTWA
OCHRONY I PRZETWARZANIA DANYCH OSOBOWYCH
WRAZ Z INSTRUKCJĄ ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM
W WAIKIKI.PL – TOMASZ ISALSKI Z SIEDZIBĄ W BYTOMIU
I ODDZIAŁEM W PIEKARACH ŚLASKICH
wydana w dniu 25.05.2018

Spis treści:

Celem niniejszej Polityki Bezpieczeństwa jest zapewnienie ochrony DANYCH OSOBOWYCH przetwarzanych w celach określonych w ROZPORZĄDZENIU 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), przetwarzanych przez „Waikiki – Tomasz Isalski", przed wszelkiego rodzaju zagrożeniami, tak wewnętrznymi jak i zewnętrznymi, świadomymi lub nieświadomymi. Polityka obowiązuje wszystkich pracowników „Waikiki – Tomasz Isalski"

oraz dostawców, podmiotów współpracujących na podstawie umów cywilnoprawnych, mających jakikolwiek kontakt z danymi osobowymi objętymi ochroną.
Przetwarzanie danych osobowych w „Waikiki – Tomasz Isalski" odbywa się za pomocą systemów informatycznych. Administratorem danych w „Waikiki – Tomasz Isalski" jest właściciel firmy w osobie Tomasza Isalskiego

1. Słownik pojęć użytych w dokumencie:

a) „Waikiki – Tomasz Isalski" z siedzibą w Bytomiu, ul.Orzegowska 9 NIP: 626 246 57 08
b) 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 imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
c) Administrator – „Waikiki – Tomasz Isalski"
d) ASI - administrator systemu informatycznego- osoba odpowiedzialna za funkcjonowanie systemu informatycznego, którą jest właściciel Tomasz Isalski
e) Identyfikator - należy przez to rozumieć elektroniczne, indywidualne oznaczenie pracowników w systemie informatycznym tzw. login.
f) Pracownik - należy przez to rozumieć osobę zatrudnioną w formie umowy o pracę lub umowy cywilno-prawnej.
g) Użytkownik systemu - należy przez to rozumieć osobę pisemnie upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
h) Rozporządzenie - należy przez to rozumieć 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)

2. Wykaz zbiorów danych przetwarzanych w placówce.

Wykaz zbiorów danych przetwarzanych w placówce wymieniony jest w załączniku nr 1 do niniejszej polityki bezpieczeństwa, będący jej integralną częścią.

3. Zakres danych osobowych przetwarzanych w placówce.

W Globtel Internet Szymon Hersztek ul. Matecznikowa 2/1 80-126 Gdańsk (operator serwerów, na których jest zlokalizowana baza danych kontrahentów firmy: „Waikiki-Tomasz Isalski" utworzono i wydzielono następujące zbiory danych osobowych: Baza kontrahentów - „Waikiki-Tomasz Isalski" w których przetwarzane są następujące dane: Imię, telefon, e-mail, lista transakcji przeprowadzonych w sklepie internetowym zlokalizowanym pod adresem waikiki.pl, informacje o rodzaju treści otrzymywanych wiadomości marketingowych za pośrednictwem środków komunikacji elektronicznej.

Niniejsza część musi być powiązana z **załącznikiem nr 1** do niniejszej polityki bezpieczeństwa tzn. nazwy zbiorów muszą być tożsame z nazwami wymienionymi w załączniku nr 1

4. Wykaz budynków, pomieszczeń lub części pomieszczeń, w których przetwarzane są dane osobowe.

Przetwarzanie danych osobowych w zakresie bazy danych odbywa się zdalnie z siedziby firmy Waikiki-Tomasz Isalski na serwerach będących własnością Globtel Internet Szymon Hersztek ul. Matecznikowa 2/1 80-126 Gdańsk i zlokalizowanych na terenie unii europejskiej

5. Procedury nadawania i zmiany uprawnień do przetwarzania danych osobowych

Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się z następującymi dokumentami:

- ROZPORZĄDZENIEM 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);
- rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100 poz. 1024);
- niniejszą polityką bezpieczeństwa i instrukcją zarządzania systemem informatycznym.
- Zapoznanie się z powyższymi dokumentami użytkownik systemu potwierdza własnoręcznym podpisem na oświadczeniu, którego wzór stanowi **Załącznik nr 2.**
- Przetwarzania danych osobowych może dokonywać jedynie użytkownik systemu upoważniony przez administratora danych osobowych. Wzór upoważnienia stanowi **Załącznik nr 3.**
- Przyznanie uprawnień w zakresie dostępu do systemu informatycznego polega na wprowadzeniudo systemu przez ASI dla każdego użytkownika systemu unikalnego identyfikatora hasła zewskazaniem zakresu dostępnych danych i operacji.
- Hasło pierwszego logowania w systemie ustanawia ASI.

6. Odpowiedzialność

- Użytkownik systemu ma prawo do wykonywania tylko tych czynności, do których został upoważniony.
- Użytkownik systemu ponosi wszelką odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu z wyjątkiem sytuacji, kiedy Administrator użyje hasła użytkownika podczas jego nieobecności. Administrator ma obowiązek sporządzić z tego zdarzenia protokół, z którym zostaje zapoznany użytkownik systemu, którego

hasło zostało użyte. Po zapoznaniu się z protokołem, użytkownik systemu ma obowiązek dokonać natychmiastowej zmiany hasła dostępu i przekazać je Administratorowi.

- Wszelkie przekroczenia lub jakiekolwiek próby przekroczenia przyznanych uprawnień, traktowane będą jako naruszenie podstawowych obowiązków pracowniczych.
- W uzasadnionym przypadku Administrator może odebrać uprawnienia pracownikowi z podaniem daty oraz przyczyny odebrania uprawnień. W uzasadnionej sytuacji Administrator może odebrać uprawnienia w sposób natychmiastowy. Z takiego postępowania ma on sporządzić notatkę służbową do wiadomości użytkownika systemu, którego sprawa dotyczy.
- Hasło oraz uprawnienia użytkownika systemu, który je utracił, należy niezwłocznie wyrejestrować z systemu informatycznego. Wyrejestrowania z systemu dokonuje ASI.
- Użytkownik systemu zatrudniony przy przetwarzaniu danych osobowych zobowiązany jest do zachowania ich w poufności oraz dołożenia wszelkich starań, aby dane osobowe nie zostały przekazane osobom nieuprawnionym.

7. Rejestr użytkowników

- Administrator jest zobowiązany do prowadzenia i ochrony rejestru użytkowników i ich uprawnień w systemie informatycznym.
- Rejestr musi odzwierciedlać aktualny stan systemu w zakresie użytkowników i ich uprawnień oraz umożliwić przeglądanie historii zmian w systemie informatycznym,
- Rejestr, którego wzór stanowi **Załącznik nr 4** zawiera:
- imię i nazwisko użytkownika,
- identyfikator użytkownika zgodny z indywidualnie przydzielonym adresem email;
- zakres uprawnienia,
- datę nadania uprawnień,
- datę odebrania uprawnień,
- przyczynę odebrania uprawnień,
- podpis Administratora.

8. Instrukcja dotycząca sposobu zarządzania systemem informatycznym.

a)Procedura rozpoczęcia i zakończenia pracy

- Przy wejściu do systemu przetwarzającego dane osobowe wprowadza indywidualny kod nadany przez administratora
- Zakończenie pracy związanej z przetwarzaniem danych odpowiadać winno wszystkim regułom bezpieczeństwa informacji.

b) Zabezpieczenie systemu przed nieuprawnionym dostępem

- Dopuszcza się możliwość przyłączenia sieci internetowej do systemu, w którym przetwarzane są dane osobowe pod następującymi warunkami:
- na każdym stanowisku komputerowym oraz serwerze musi być zainstalowane oprogramowanie antywirusowe,
- każdy e-mail wpływający do jednostki musi być sprawdzony pod kątem występowania wirusów,
- aktualizacje programów antywirusowych muszą być dokonywane nie rzadziej niż raz w tygodniu,
- zabrania się używania nośników niewiadomego pochodzenia bez wcześniejszego sprawdzenia ich programem antywirusowym, którego dokonuje użytkownik zamierzający go użyć,
- zabrania się pobierania z Internetu plików niewiadomego pochodzenia oraz odczytywania załączników poczty elektronicznej bez wcześniejszego sprawdzenia ich programem antywirusowym.
- Każdy użytkownik systemu musi zostać przeszkolony z obsługi programu antywirusowego, co poświadcza stosownym podpisem, zgodnie z **załącznikiem 5** do niniejszej polityki bezpieczeństwa.
- Administrator przeprowadza cykliczne kontrole antywirusowe na wszystkich komputerach systemu nie rzadziej niż raz na rok kalendarzowy. Z kontroli tych sporządza się protokół zgodnie z **załącznikiem 6** do niniejszej polityki bezpieczeństwa, stanowiącym jej integralną cześć.
- Użytkownicy systemu są odpowiedzialni za nieudostępnianie stanowisk pracy osobom postronnym

- W drodze wyjątku udostępnienie może się odbyć tylko pod stałą kontrolą uprawnionego użytkownika stanowiska
- Po zakończeniu udostępniania stanowiska należy niezwłocznie sprawdzić stan zabezpieczeń i profilaktycznie uruchomić pełne skanowanie system pod kątem niepożądanych aplikacji i zagrożeń.

c) Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych

Procedury naprawy sprzętu komputerowego:
- naprawa sprzętu komputerowego użytkowanego w systemie może odbywać się w siedzibie biura i dokonywać jej może jedynie wyspecjalizowana firma informatyczna lub uprawniony pracownik.
Czynności te muszą być wykonywane w obecności Administratora lub ASI lub innego upoważnionego przez nich użytkownika systemu,
- naprawa sprzętu komputerowego użytkowanego w systemie poza siedzibą biura
musi zostać poprzedzona usunięciem z twardego dysku wszelkich aplikacji przetwarzających i zawierających dane o charakterze osobowym. ASI odpowiedzialny jest za stworzenie kopii tej bazy, która jest przechowywana przez Administratora na dysku wspólnym. Po powrocie z serwisu sprzętu komputerowego, ASI ponownie instaluje bazę danych.

Procedura przeglądu systemu:
- przeglądu systemu dokonuje pracownik „Waikiki-Tomasz Isalski" lub firma informatyczna obsługująca jednostkę pod względem informatycznym, czynności przeglądowe muszą odbywać się w obecności ASI lub Administratora lub innego upoważnionego przez nich pracownika.

9. Zasady udostępniania danych

- Dane osobowe przetwarzane zgodnie z art. 9 ust. 2 lit. h rozporządzenia mogą być wydane jedynie na pisemny wniosek osoby, której dotyczą lub pisemny wniosek osoby upoważnionej na piśmie przez zainteresowanego.
- Dopuszcza się przekazywanie danych osobowych, o których mowa w art. 9 ust. 2 lit. h

rozporządzenia podmiotom i organom upoważnionym na podstawie odrębnych przepisów, wskazanym w art. 26 ustawy z dnia 6 listopada 2008r.

- Każda osoba przetwarzająca dane osobowe, w przypadku podejrzenia naruszenia zabezpieczenia danych osobowych, zobowiązana jest niezwłocznie powiadomić o tym Administratora lub inną upoważnioną osobę.
- Administrator (lub upoważniona osoba) w porozumieniu z ASI po otrzymaniu powiadomienia:
- sprawdza stan urządzeń wykorzystywanych do przetwarzania danych osobowych,
- sprawdza sposób działania programów (w tym obecność wirusów komputerowych),
- sprawdza jakość komunikacji w sieci telekomunikacyjnej,
- sprawdza zawartość zbioru danych osobowych,
- poddaje analizie metody pracy osób upoważnionych do przetwarzania danych osobowych,

10. W przypadku stwierdzenia naruszenia zabezpieczeń danych administrator:

- podejmuje niezbędne działania mające na celu uniemożliwienie dalszego ich naruszenia (odłączenie wadliwych urządzeń, zablokowanie dostępu do sieci telekomunikacyjnej, programów oraz zbiorów danych itp.),
- w celu powstrzymania lub ograniczenia dostępu do danych osoby niepowołanej podejmuje odpowiednie kroki poprzez: fizyczne odłączenie urządzeń i segmentów sieci, które mogłyby umożliwić dostęp do bazy danych osoby nieupoważnionej, wylogowanie użytkownika podejrzewanego o naruszenie zabezpieczenia ochrony danych, zmianę hasła na koncie administratora i użytkownika, poprzez które uzyskano nielegalny dostęp w celu uniknięcia ponownej próby włamania,
- zabezpiecza, utrwala wszelkie informacje i dokumenty mogące stanowić pomoc przy ustaleniu przyczyn naruszenia,
- niezwłocznie przywraca prawidłowy stan działania systemu,
- dokonuje analizy stanu zabezpieczeń wraz z oszacowaniem rozmiaru szkód powstałych na skutek naruszenia,
- sporządza szczegółowy raport zawierający w szczególności: datę i godzinę otrzymania informacji o naruszeniu, opis jego przebiegu, przyczyny oraz wnioski ze zdarzenia.

Administrator podejmuje niezbędne działania w celu wyeliminowania naruszeń zabezpieczeń danych w przyszłości, a w szczególności:

- jeżeli przyczyną zdarzenia był stan techniczny urządzenia, sposób działania programu, uaktywnienie się wirusa komputerowego lub jakość komunikacji w sieci telekomunikacyjnej, niezwłocznie przeprowadza przeglądy oraz konserwacje urządzeń i programów, ustala źródło pochodzenia wirusa oraz wdraża skuteczniejsze zabezpieczenia antywirusowe, a w miarę potrzeby kontaktuje się z dostawcą usług telekomunikacyjnych,
- jeżeli przyczyną zdarzenia były wadliwe metody pracy, błędy i zaniedbania osób zatrudnionych przy przetwarzaniu danych osobowych, przeprowadza się dodatkowe kursy i szkolenia osób biorących udział przy przetwarzaniu danych, a wobec osób winnych zaniedbań wnioskuje do administratora danych osobowych o wyciągnięcie konsekwencji przewidzianych prawem,
- jeżeli przyczyną zdarzenia jest sprzeczny z prawem czyn lub zachodzi takie podejrzenie, zawiadamia organy ścigania.

Załącznik 1 Wykaz zbiorów danych osobowych.

Zbiory danych osobowych przetwarzane w sposób tradycyjny.

Zbiór	**Zawartość pól informacyjnych**	**Użytkownicy przetwarzający dany zbiór lub część zbioru**
Ewidencja klientów	Imię, nazwisko, nazwa firmy, miejsce prow. Działalności, nip, telefon, e-mail, lista transakcji z datą. uwagi	Właściciel i uprawnieni pracownicy.
Formularze osób zapisanych na newsletter	Imię, telefon, e-mial, wybrany zakres interesujących tematów newslettera. Częstotliwość wysyłki, zgoda na przetwarzanie danych, data rejestracji zgody	Właściciel i uprawnieni pracownicy.
Kadrowe	Imię i nazwisko pracownika, miejsce zamieszkania, zameldowania, imiona i nazwiska, daty i miejsca urodzenia współmałżonków, dzieci, nazwiska rodowe, imiona i nazwiska rodziców pracownika, PESEL, numer NIP, numery telefonów stacjonarnych, numery telefonów komórkowych, numer konta bankowego, świadectwa pracy, odpisy dyplomów ukończenia studiów wyższych magisterskich, licencjackich, podyplomowych lub ich uwierzytelnione kopie, odpisy aktów zawarcia związku małżeńskiego, odpisy aktów urodzenia dzieci, kopie ukończenia kursów udoskonalających,	Właściciel Firmy, Księgowa
Ewidencja Pracy	Imię, nazwisko, czas pracy, dni wolnych i l4	Właściciel, Księgowa
Dokumentacja ZUS	Imię, nazwisko, wynagrodzenie i informacje zusowskie	Właściciel, Księgowa

Zbiory danych osobowych przetwarzane w systemie informatycznym.

Zbiór	**Zawartość pól informacyjnych**	**Użytkownicy systemu informatycznego przetwarzający dany zbiór lub część zbioru**
Trello	Imię, nazwisko, mail, telefon, specyfikacja zamówienia	Właściciel i pracownicy
Newsletter	Imię, mail, telefon, zgoda na otrzymywanie treści o charakterze informacyjnym i marketingowym , zakres otrzymywanych treści	Właściciel i pracownicy
DGCS	Imię, nazwisko, nazwa firmy, dane adresowe firmy, nip, lista transakcji wraz z datami	Właściciel i pracownicy
WEBD	Imię, Nazwisko, Adres, Telefon, E-mial, specyfikacje zamówień, formy płatności, dane firmowe	Właściciel i pracownicy

Załącznik nr 2

. . . . . , dn. . . . . r.
[data sporządzenia]

. . . . . .
imię i nazwisko osoby upoważnionej
. . . . . .
stanowisko
. . . . . .
miejsce pracy

OŚWIADCZENIE

Oświadczam, że – w związku z wykonywaniem przeze mnie prac na rzecz Waikiki-Tomasz Isalski z siedzibą w Bytomiu, Orzegowska 9 i oddziałem w Piekarach Śląskich, Leśna 22 i upoważnieniem mnie do Przetwarzania danych osobowych – zostałem/łam zapoznany/a ze stosownymi przepisami i standardami ochrony danych osobowych, zobowiązuję się do przestrzegania:

- Przepisów o ochronie danych osobowych, w tym Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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

- Polityki Bezpieczeństwa informacji w Waikiki-Tomasz Isalski

- Instrukcji zarządzania systemem Informatycznym w Waikiki-Tomasz Isalski

W związku z powyższym zobowiązuję się do:

a. zapewnienia ochrony danych osobowych przetwarzanych w zbiorach administratora, a w szczególności zapewnienia ich bezpieczeństwa przed udostępnianiem osobom trzecim i nieuprawnionym, zabraniem, uszkodzeniem oraz nieuzasadnioną modyfikacją lub zniszczeniem,
b. zachowania w tajemnicy, także po zaprzestaniu wykonywania prac, wszelkich informacji dotyczących funkcjonowania systemów służących do przetwarza nia danych osobowych w zbiorach . . . . . .
c. natychmiastowego zgłaszania do Administratora Danych zaobserwowania próby lub faktu naruszenia zabezpieczenia fizycznego pomieszczenia, bezpieczeństwa zbioru/zbiorów lub systemów informatycznych.

. . . . . .
[podpis pracownika/współpracownika]

Załacznik nr 3

. . . . . , dn. . . . . r.
[data sporządzenia]

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Działając w imieniu Waikiki-Tomasz Isalski niniejszym upoważniam:
Panią/Pana … . . . . . .

do przetwarzania danych osobowych w Waikiki-Tomasz Isalski w następującym zakresie*:

A. Okres upoważnienia:
☐ na okres zatrudnienia / współpracy z Waikiki – Tomasz Isalski do momentu ustania umowy zatrudnienia włącznie lub wcześniejszego cofnięcia upoważnienia.
B. Zakres upoważnienia obejmuje:
☐ dane przetwarzane na nośnikach papierowych,
☐ system informatyczny,
☐ dane osobowe objęte zbiorem:
Trello, Newsletter, DGCS, oraz: ……..

* bez ograniczeń, podgląd danych, wprowadzanie danych, opracowywanie danych, zmienianie danych, usuwanie danych, na komputerach przenośnych) [należy pozo stawić właściwe]

. . . . . .
[administrator danych]

Załącznik nr 4

Ewidencja osób upoważnionych do przetwarzania danych osobowych

Lp	Numer upoważnienia	Nazwa zbioru danych	Nazwisko i imię osoby upoważnionej	Data nadania upoważnienia	Zakres upoważnienia	Data wygaśnięcia/cofnięcia upoważnienia	Uwagi) przyczyna cofnięcia upoważnienia

Załącznik 5

……..

Miejscowość, dnia

Oświadczenie

Oświadczam, że zostałem/am zapoznany/a z obsługą programu anty-wirusowego, oraz z zakresu zachowania higieny informatycznej jak również aktywnych sposobów zapobiegania infekcji i nieautoryzowanego dostępu do administrowanych danych oraz zasobów komputerowych.

……..

Podpis

Załącznik nr 6

Protokół kontroli zabezpieczeń antyvirusowych systemów informatycznych zarządzanych przez Waikiki-Tomasz Isalski

Data	Stanowisko	Użytkownik	Zastosowane zabezpieczenia	wykryte nieprawidłowości	zastosowane rozwiązanie i zalecenia	końcowa ocena zabezpieczenia

.....

Podpis administratora

Załącznik nr 7

Obszary przetwarzania danych osobowych wraz ze wskazaniem przetwarzanych zbiorów oraz sposobu zabezpieczenia.

Obszary oraz zbiory danych osobowych przetwarzane w sposób tradycyjny.

Budynek	Zabezpieczenie budynku	Pomieszczenie	Zabezpieczenie zbioru danych	Nazwa zbioru danych
Orzegowska 9, 41-907 Bytom. Parter 100 letniej Kamienicy.	Żaluzje antywłamaniowe w oknach i drzwiach, System alarmowy z powiadomieniem GSM. Zamki patentowe. Monitoring całodobowy wnętrza i zewnętrznej elewacji budynku	Dział obsługi klienta Pomieszczenie produkcyjne	Kontrola dostępu, przez wzajemne monitorowanie się pracowników. Zbiory przechowywane w sejfie zabezpieczonym hasłem. Lokalizacja sejfu i kod znany jest wyłącznie uprawnionym pracownikom.	Formularze zapisu/zgody na otrzymywanie newslettera i informacji handlowych. Dokumenty handlowe (faktury VAT) Wypełnione druki zamówień (zawierające nazwisko i dane telefoniczne i e-mailowe klientów.)
Leśna 22, 41-943 Piekary Śląskie, 1 piętro budynku spółdzielni mieszkaniowej	Monitoring całodobowy i czasowy obchód stróża nocnego. Zamki Patentowe	Dział obsługi klienta Pomieszczenie produkcyjne	Kontrola dostępu, przez wzajemne monitorowanie się pracowników. Zbiory przechowywane są w zamkniętej szafce w gabinecie właściciela firmy.	Formularze zapisu/zgody na otrzymywanie newslettera i informacji handlowych. Dokumenty handlowe (faktury VAT) Wypełnione druki zamówień (zawierające nazwisko i dane telefoniczne i e-mailowe klientów.)

Załącznik nr 8

Obszary oraz zbiory danych osobowych przetwarzane w systemie informatycznym.

Budynek, Piętro, Pomieszczenie	Dostęp do pomieszczenia	Typ urządzenia, system, identyfikacja i logowanie	Urządzenia należą do sieci	Zbiory danych osobowych przetwarzane za pomocą urządzenia	Programy wykorzystywane do przetwarzania zbiorów danych
Orzegowska 9, 41-907 Bytom. Parter, Obsługa klienta	Dostęp posiadają zarówno pracownicy jak i klienci pod stałą kontrolą uprawnionych pracowników	Komputery stacjonarne, Windows 7, Logowanie użytkownika, brak konta gościa,	Sieć lan lokalna kablowa, z dostępem do internetu prze router z sprzętowym firewallem i dodatkowo na każdym komputerzefirewall programowy oraz program antyvirusowy i zestaw programów antyszpiegowskich.	Projekty klientów dane adresowe (e-mail i telefon, imię i nazwisko klientów) informacje o zamówieniach klientów lista klientów zapisanych na newsletter	Corel Draw Libre office DGCS Mmagazyn przeglądarka www, szyfrowane połączenie ssl Thunderbird połaczenie szyfrowane ssl
Leśna 22, 41-943 Piekary Śląskie, 1 piętro, Obsługa klienta	Dostęp posiadają zarówno pracownicy jak i klienci pod stałą kontrolą uprawnionych pracowników	Komputery stacjonarne, Windows 7, Logowanie użytkownika, brak konta gościa,	Sieć lan lokalna kablowa, z dostępem do internetu prze router z sprzętowym firewallem i dodatkowo na każdym komputerzefirewall programowy oraz program antyvirusowy i zestaw programów antyszpiegowskich.	Projekty klientów dane adresowe (e-mail i telefon, imię i nazwisko klientów) informacje o zamówieniach klientów lista klientów zapisanych na newsletter	Corel Draw Libre office DGCS Mmagazyn szyfrowane połączenie ssl Thunderbird połaczenie szyfrowane ssl

Załącznik nr 9

. . . . . , dn. . . . . r.
[data sporządzenia]

Prezes Urzędu Ochrony Danych Osobowych
. . . . . .

ZGŁOSZENIE INCYDENTU NARUSZENIA
OCHRONY DANYCH OSOBOWYCH

Działając na podstawie art. 33 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fzycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego prze pływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), niniejszym zgłaszam zajście incydentu naruszenia ochrony danych osobowych.

Dane Administratora Danych Osobowych	
Miejsce i dzień naruszenia	
Kategoria i przybliżona liczba osób, których dane dotyczą	
Kategorie i przybliżona liczba wpisów danych oso bowych, których dotyczy naruszenie	
Opis charakteru naruszenia ochrony danych	
Możliwe konsekwencje naruszenia ochrony danych	
Środki zastosowane w celu zminimalizowania ewentualnych negatywnych skutków naruszenia ochrony danych	

. . . . . .
[podpis osoby uprawnionej
do reprezentowania Administratora Danych]