POLITYKA BEZPIECZEŃSTWA

JACEK TURCZYNOWICZ
YACHTING JACEK TURCZYNOWICZ
ul. Gen. Józefa Zajączka 23/22, 01-505 Warszawa
NIP: 1231056768, REGON: 142763110

pieczęć firmowa podpis administratora danych osobowych data

Wstęp

Stosownie do art. 36 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. Nr 133, poz. 883, z późn, zm.), zwanej dalej ustawą, administrator danych osobowych jest zobowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. W tym celu administrator prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki ochrony.

Zgodnie z art. 38 ustawy administrator zobowiązany jest zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.

Polityka bezpieczeństwa stanowi wykonanie obowiązku, o którym mowa w § 4 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29.04.2004 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. Nr 100, poz. 1024, z późn. zm.).

Rozdział 1
Postanowienia ogólne

Ilekroć w Polityce bezpieczeństwa jest mowa o:

1. **ustawie** – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. Nr 133, poz. 883 z późn. zm.),
2. **danych osobowych** – rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej; osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne; informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań,
3. **zbiorze danych** – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
4. **przetwarzaniu danych** – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,

5. **systemie informatycznym** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,

6. **zabezpieczeniu danych w systemie informatycznym** – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,

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

1. **administratorze danych** – rozumie się przez to Jacka Turczynowicza, prowadzącego działalność gospodarczą pod firmą Yachting Jacek Turczynowicz, NIP: 1231056768, REGON: 142763110,

8. **zgodzie osoby, której dane dotyczą** – rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści; zgoda może być odwołana w każdym czasie,

9. **odbiorcy danych** – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem osoby, której dane dotyczą, osoby upoważnionej do przetwarzania danych, przedstawiciela, o którym mowa w art. 31a ustawy, podmiotu, o którym mowa w art. 31 ustawy, organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem,

10. **państwie trzecim** – rozumie się przez to państwo nienależące do Europejskiego Obszaru Gospodarczego,

11. **obszarze przetwarzania danych** – należy przez to rozumieć wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe,

12. **wykazie zbiorów** – należy przez to rozumieć wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych,

13. **opisie struktury zbiorów** – należy przez to rozumieć opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi,

14. **opisie przepływu danych** – należy przez to rozumieć opis sposobu przepływu danych pomiędzy poszczególnymi systemami informatycznymi,

15. **środkach technicznych i organizacyjnych** – należy przez to rozumieć środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych.

Rozdział 2
Administrator danych

1. Administrator danych jest zobowiązany w szczególności do:

a) opracowania i wdrożenia Polityki bezpieczeństwa oraz Instrukcji zarządzania systemem informatycznym przetwarzającym dane osobowe,

b) stały nadzór nad treścią Polityki bezpieczeństwa, Instrukcji zarządzania systemem informatycznym,

c) wydawania i anulowania upoważnienia do przetwarzania danych osobowych osobom, które mają te dane przetwarzać (załącznik nr 1),

d) prowadzenia wykazu osób upoważnionych do przetwarzania danych osobowych (załącznik nr 2),

e) prowadzenia wykazu obszarów przetwarzania (załącznik nr 3),

f) prowadzenia wykazu zbiorów danych osobowych (załącznik nr 4),

g) prowadzenia opisu struktury zbiorów (załącznik nr 5),

h) prowadzenia opisu sposobu przepływu danych (załącznik nr 6),

i) dokonywania aktualizacji dokumentów wymienionych powyżej pod lit. a-h,

j) zgłaszania Generalnemu Inspektorowi Danych Osobowych (GIODO) zbiorów danych podlegających rejestracji.

2. Administratorem danych jest Jacek Turczynowicz prowadzący działalność gospodarczą pod firmą Yachting Jacek Turczynowicz, NIP: 1231056768, REGON: 142763110.

Rozdział 3

Zbieranie danych osobowych

W przypadku zbierania danych dokonujący tej czynności zobowiązany jest do poinformowania osoby, której dane dotyczą o:

a) adresie swojej siedziby i pełnej nazwie,

b) celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych,

c) prawie dostępu do treści swoich danych oraz ich poprawiania,

d) dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

Rozdział 4

Środki techniczne i organizacyjne

1. W celu ochrony danych spełniono wymogi, o których mowa w art. 36–39 ustawy:

a) administrator danych sam wykonuje czynności administratora bezpieczeństwa informacji,

b) do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych,

c) prowadzona jest ewidencja osób upoważnionych do przetwarzania danych,

d) została opracowana i wdrożona Polityka bezpieczeństwa,

e) została opracowana i wdrożona Instrukcja zarządzania systemem informatycznym.

2. W celu ochrony danych osobowych stosuje się następujące środki ochrony fizycznej danych osobowych:

a) zbiory danych osobowych przechowywane są w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi),

b) pomieszczenia, w których przetwarzane są zbiory danych osobowych, zabezpieczone są przed skutkami pożaru za pomocą wolnostojącej gaśnicy,

c) niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe musi odbywać się w sposób uniemożliwiający odczytanie zawartej w nich w szczególności w sposób mechaniczny za pomocą niszczarek dokumentów.

3. W celu ochrony danych osobowych stosuje się następujące środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej:

a) zbiory danych osobowych przetwarzane są przy pomocy komputerów przenośnych,

b) komputery służące do przetwarzania danych nie są połączone z lokalną siecią komputerową,

c) dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe, zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła,

d) zastosowano środki uniemożliwiające wykonanie nieautoryzowanych kopii danych osobowych przetwarzanych za pomocą systemu teleinformatycznego,

e) zastosowano systemowe mechanizmy wymuszające okresową zmianę haseł,

f) zastosowano środki ochrony przed szkodliwym oprogramowaniem,

4. W celu ochrony danych osobowych stosuje się następujące środki ochrony w ramach narzędzi programowych i baz danych:

a) wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych,

b) dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła,

c) zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe,

d) zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

5. W celu ochrony danych osobowych stosuje się następujące środki organizacyjne:

a) osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych,

b) przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego,

c) osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy,

d) monitory komputerów, na których przetwarzane są dane osobowe, ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane,

e) niedopuszczalne jest wynoszenie materiałów zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych, a za bezpieczeństwo i zwrot materiałów zawierających dane osobowe odpowiada w tym przypadku osoba dokonująca ich wyniesienia,

f) 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 dostępem,

g) w miejscu przetwarzania danych osobowych utrwalonych w formie papierowej pracownicy zobowiązani są do stosowania zasady tzw. „czystego biurka", co oznacza nie pozostawianie materiałów zawierających dane osobowe w miejscu umożliwiającym fizyczny dostęp do nich osobom nieuprawnionym,

h) pracownicy i współpracownicy zobowiązani są do zamykania na klucz wszelkich pomieszczeń 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 i współpracownicy zobowiązani są do dołożenia należytej staranności w celu zabezpieczenia posiadanych kluczy przed nieuprawnionym dostępem.

Rozdział 5

Tryb postępowania w sytuacji naruszenia ochrony danych osobowych

1. Każda osoba, która poweźmie wiadomość w zakresie naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe bądź posiada informacje mogące mieć wpływ na bezpieczeństwo danych osobowych, jest zobowiązana fakt ten niezwłocznie zgłosić administratorowi danych.

2. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych administratora danych lub upoważnionej przez niego osoby, osoba powiadamiająca powinna:

a) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków, a następnie ustalić przyczyny lub sprawców zaistniałego zdarzenia, jeżeli jest to możliwe,

b) zaniechać dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić jego udokumentowanie i analizę,

c) udokumentować wstępnie zaistniałe naruszenie,

d) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia administratora danych lub osoby upoważnionej.

3. Po przybyciu na miejsce naruszenia ochrony danych osobowych, administrator danych lub osoba go zastępująca:

a) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metod dalszego postępowania,

b) wysłuchuje relacji osoby zgłaszającej z zaistniałego naruszenia, jak również relacji każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem.

4. Administrator danych dokumentuje zaistniały przypadek naruszenia oraz sporządza notatkę lub sprawozdanie.

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

Rozdział 6
Postanowienia końcowe

1. Wszelkie zasady opisane w Polityce bezpieczeństwa są przestrzegane przez osoby upoważnione do przetwarzania danych osobowych ze szczególnym uwzględnieniem dobra osób, których dane te dotyczą.

2. Administrator danych może powierzyć przetwarzanie danych innemu podmiotowi, w drodze umowy zawartej na piśmie. Podmiot ten może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie oraz jest obowiązany przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające zbiór danych, o których mowa w art. 36–39 ustawy, oraz spełnić wymagania określone w przepisach, o których mowa w art. 39a ustawy. W zakresie przestrzegania tych przepisów taki podmiot ponosi odpowiedzialność jak administrator danych. W przypadkach, o których mowa powyżej, odpowiedzialność za przestrzeganie przepisów ustawy spoczywa na administratorze danych, co nie wyłącza odpowiedzialności podmiotu, który zawarł umowę, za przetwarzanie danych niezgodnie z tą umową.

3. Polityka bezpieczeństwa obowiązuje od dnia jej zatwierdzenia przez administratora danych.

Załącznik nr 1

UPOWAŻNIENIE

do przetwarzania danych osobowych

w systemie informatycznym lub w zbiorze w wersji papierowej

Niniejszym, jako Administrator Danych Osobowych, na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. Nr 133, poz. 883, z późn, zm.), dniem ..... upoważniam:

1. Imię i nazwisko: ……..
2. Zbiory danych objęte zakresem upoważnienia: klienci (w tym uczestnicy szkoleń, kursów i wykładów), potencjalni klienci (w tym osoby kontaktujący się poprzez formularz kontaktowy i livechat – narzędzia do kontaktu ze Sprzedawcą, z których można skorzystać na stronie internetowej sklepu internetowego www.yachting.edu.pl), podwykonawcy (kontrahenci i partnerzy Administratora).

Osoba upoważniona obowiązana jest przetwarzać dane osobowe zawarte w ww. zbiorach danych osobowych w zakresie i w sposób wymagany do wypełnienia obowiązków służbowych względem Administratora Danych.

Osoba upoważniania jest obowiązana do przestrzegania przepisów dotyczących ochrony danych osobowych oraz wprowadzonych i wdrożonych do stosowania przez Administratora Danych Osobowych Polityki Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym.

Niniejsze upoważnienie jest ważne do odwołania, rozwiązania lub wygaśnięcia umowy o pracę, umowy zlecenia, umowy o dzieło lub innego stosunku prawnego.

miejscowość, data *podpis administratora danych*

OŚWIADCZENIE

Oświadczam, iż zostałam/em zapoznana/y z przepisami dotyczącymi ochrony danych osobowych, w szczególności ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. Nr 133, poz. 883, z późn. zm.), wydanymi na jej podstawie aktami wykonawczymi oraz wprowadzonymi i wdrożonymi do stosowania przez Administratora Danych Osobowych Polityki Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym.

Zobowiązuję się do:

- zachowania w tajemnicy danych osobowych, do których mam lub będę miał/a dostęp w związku z wykonywaniem zobowiązań umownych lub obowiązków pracowniczych,
- niewykorzystywania danych osobowych w celach pozasłużbowych i pozaumownych o ile nie są one jawne,
- zachowania w tajemnicy sposobów zabezpieczenia danych osobowych, o ile nie są one jawne,
- korzystania ze sprzętu komputerowego oraz oprogramowania wyłącznie w związku z wykonywaniem obowiązków pracowniczych lub zobowiązań umownych,
- wykorzystywania jedynie legalnego oprogramowania pochodzącego od administratora danych osobowych,
- należytej dbałości o sprzęt i oprogramowanie zgodnie z dokumentacją ochrony danych osobowych,
- korzystania z urządzeń przenośnych zgodnie z dokumentacją ochrony danych osobowych.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższym może być uznane przez Administratora Danych Osobowych za ciężkie naruszenie obowiązków pracowniczych lub zobowiązań umownych w rozumieniu przepisów prawa lub za naruszenie przepisów karnych ustawy o ochronie danych osobowych.

podpis osoby upoważnionej

Załącznik nr 2

WYKAZ OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Lp.	**Nazwisko i imię osoby upoważnionej**	**Identyfikator w systemie informatycznym**	**Wersja papierowa**	**Wersja elektroniczna**	**Data nadania upoważnienia**	**Data odebrania upoważnienia**	**Lokalizacja** *(proszę podać stanowisko i/lub miejsce pracy - adres)*
1.			Tak / Nie	Tak / Nie			
2.			Tak / Nie	Tak / Nie			
3.			Tak / Nie	Tak / Nie			
4.			Tak / Nie	Tak / Nie			

Dane aktualne na dzień: Podpis administratora danych:

Załącznik nr 3

WYKAZ OBSZARÓW PRZETWARZANIA DANYCH OSOBOWYCH

Lp.	Lokalizacja	Środki ochrony fizycznej danych	Środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej	Środki ochrony w ramach narzędzi programowych i baz danych	Środki organizacyjne
1.	ul. Gen. Józefa Zajączka 23/22, 01-505 Warszawa	DZ, SM, PPOŻ, NIS	IH, AUT, ANW	PIH, WYG, BLOK,	OZ, SZ, OP, PE, KZ
2.					
3.					

Legenda:

Skróty oznaczenia środków ochrony fizycznej danych:

DZ – drzwi zwykłe (niewzmacniane, nieprzeciwpożarowe)

DO – drzwi o podwyższonej odporności ogniowej >= 30 min.

DW – drzwi o podwyższonej odporności na włamanie – drzwi klasy C

KR – okna zabezpieczone są za pomocą krat, rolet lub folii antywłamaniowej

SA – system alarmowy przeciwwłamaniowy

SK – system kontroli dostępu

SM – system monitoringu z zastosowaniem kamer przemysłowych

SO – obszar nadzorowany przez służbę ochrony

SC – obszar nadzorowany przez służbę ochrony (całodobowo)

ZS – zamknięta niemetalowa szafa

ZM – zamknięta metalowa szafa

KP – zamknięty sejf lub kasa pancerna

KZS – kopia zapasowa przechowywana w zamkniętej niemetalowej szafie

KZM – kopia zapasowa przechowywana w zamkniętej metalowej szafie

KZP – kopia zapasowa przechowywana w zamkniętym sejfie lub kasie pancernej

KT – dane przechowywane w kancelarii tajnej

PPOŻ – system przeciwpożarowy i/lub wolno stojąca gaśnica

NIS – niszczarki do dokumentów

Skróty oznaczenia środków sprzętowych infrastruktury informatycznej i telekomunikacyjnej:

SL – komputery połączone z lokalną siecią komputerową

UPS – zastosowano UPS, generator prądu i/lub wydzieloną sieć elektroenergetyczną

BIOS – zastosowano hasło BIOS

IH – zastosowano identyfikator użytkownika oraz hasło

TOK – zastosowano karty procesorowe oraz kod PIN lub token

BIO – zastosowano uwierzytelnienie z wykorzystaniem technologii biometrycznej

AUT – zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii

HZ – zastosowano systemowe mechanizmy wymuszające okresową zmianę haseł

RD – zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych

KRT – zastosowano środki kryptograficznej ochrony danych w teletransmisji

UT – zastosowano mechanizm uwierzytelnienia przy dostępie do środków teletransmisji

CALL – zastosowano procedurę oddzwonienia (callback) przy transmisji za pośrednictwem modemu

MD – zastosowano macierz dyskową

ANW – zastosowano program antywirusowy

FW – zastosowano system Firewall przy dostępie do sieci komputerowej

IDS – zastosowano system IDS/IPS

Skróty oznaczenia środków ochrony w ramach narzędzi programowych i baz danych:

REJ – zastosowano rejestrację zmian wykonywanych na poszczególnych elementach zbioru

DOS – określono prawa dostępu do wskazanego zakresu danych

PIH – zastosowano identyfikator użytkownika oraz hasła

PTOK – zastosowano karty procesorowe oraz kod PIN lub token

PBIO – zastosowano technologię biometryczną

PRD – zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych

PZH – zastosowano okresową zmianę haseł dostępu

PKRY – zastosowano kryptograficzne środki ochrony danych

WYG – zainstalowano wygaszacze ekranów

BLOK – zastosowano automatyczną blokadę dostępu w przypadku dłuższej nieaktywności pracy użytkownika

Skróty oznaczenia środków organizacyjnych:

OZ – osoby upoważnione zostały zaznajomione z przepisami o ochronie danych

SZ – osoby upoważnione zostały przeszkolone z zabezpieczeń systemu informatycznego

OP – osoby upoważnione zostały zobowiązane do zachowania danych w poufności

PE – zastosowano politykę czystego ekranu

KZ – kopia zapasowa danych jest przechowywana w innym pomieszczeniu niż oryginał

Dane aktualne na dzień: Podpis administratora danych:

Załącznik nr 4

WYKAZ ZBIORÓW DANYCH OSOBOWYCH

Lp.	**Nazwa zbioru danych**	**Program przetwarzający**	**Rejestracja w GIODO**	**Lokalizacja**	**Podstawa prawna przetwarzania danych w zbiorze**
1.	Klienci (w tym uczestnicy szkoleń, kursów, wykładów)	Wersja papierowa z wykorzystaniem komputera, wersja elektroniczna,	Tak	*u. Gen. Józefa Zajączka 23/22, 01-505 Warszawa*	art. 23 ust. 1 pkt 1, 3 i 5 ustawy o ochronie danych osobowych
2.	Potencjalni klienci	Wersja papierowa z wykorzystaniem komputera, wersja elektroniczna	Tak	*ul. Gen. Józefa Zajączka 23/22, 01-505 Warszawa*	art. 23 ust. 1 pkt 1, 3 i 5 ustawy o ochronie danych osobowych
3.	Podwykonawcy	Wersja papierowa z wykorzystaniem komputera, wersja elektroniczna	Tak	*ul. Gen. Józefa Zajączka 23/22, 01-505 Warszawa*	art. 23 ust. 1 pkt 1, 3 i 5 ustawy o ochronie danych osobowych

Dane aktualne na dzień: Podpis w imieniu administratora danych:

Załącznik nr 5

OPIS STRUKTURY ZBIORÓW

Nazwa zbioru danych	**Wersja papierowa**	**System informatyczny**	**Zawartość pól informacyjnych i powiązania pomiędzy nimi**
Klienci	Tak	Tak	imię, nazwisko, adres (kod pocztowy, miejscowość, ulica, nr domu/mieszkania), adres e-mail, telefon, nazwa i siedziba firmy, numer identyfikacji podatkowej (NIP), data urodzenia
Potencjalni klienci	Nie	Tak	imię, nazwisko, nazwa firmy, adres e-mail, numer telefonu, + treść wiadomości
Podwykonawcy	Tak	Tak	imię, nazwisko, adres (kod pocztowy, miejscowość, ulica, nr domu/mieszkania), adres e-mail, telefon, nazwa i siedziba firmy, numer identyfikacji podatkowej (NIP), REGON, KRS, PESEL

Dane aktualne na dzień: Podpis w imieniu administratora danych:

Załącznik nr 6

OPIS SPOSOBU PRZEPŁYWU DANYCH

Zbiór danych osobowych	**Rodzaj systemu/programu**	**Sposób przesyłania danych osobowych**
Klienci	Manualny oraz półautomatyczny lub automatyczny (Fachowcy.pl – hosting, dane księgowe →biuro rachunkowe – Fiscoplan Sp. z o.o. → ZUS, Urząd Skarbowy)	Nie istnieje bezpośredni przepływ danych
Potencjalni klienci	Manualny oraz półautomatyczny lub automatyczny (Fachowcy.pl – hosting)	Nie istnieje bezpośredni przepływ danych
Podwykonawcy (dane księgowe)	Manualny oraz półautomatyczny lub automatyczny (biuro rachunkowe – Fiscoplan Sp. z o.o.--> ZUS, Urząd Skarbowy)	Nie istnieje bezpośredni przepływ danych

Dane aktualne na dzień: Podpis w imieniu administratora danych……