POLITYKA OCHRONY DANYCH
BGT Sp. z o. o.

25 MAJ 2018

Metryka dokumentu	
Tytuł	POLITYKA OCHRONY DANYCH BGT Sp. z o. o.
Wersja bieżąca	1.0
Data ostatniej modyfikacji	25-05-2018
Opracował	Jarosław Rudawski, FORMICA Szerszenowicz Sp. J., 15-706 Białystok, ul. Gruntowa 9/1 lok. 102
Ostatni modyfikował	Dylewicz Marek – Administrator systemów informatycznych w BGT Sp. z o.o., 15-080 Białystok, ul. Elektryczna 1
Zaakceptował	Aliaksandr Bokhan – Prezes Zarządu BGT Sp. z o.o., 15-080 Białystok, ul. Elektryczna 1

Historia zmian dokumentu

Wersja	Data wersji	Uwagi
1.0	25-05-2018	Wersja pierwsza

Polityka Ochrony Danych określa sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.

Oświadczenie zarządcze

W pełni świadomi znaczenia informacji i systemów informacyjnych dla realizacji misji i celów BGT Sp. z o.o. zapewniamy, że podejmowane przez BGT Sp. z o.o. działania dążą do zapewnienia bezpieczeństwa zasobów informacyjnych i są zgodne z wymogami obowiązującego prawa.

W celu udokumentowania realizacji Systemu Bezpieczeństwa Informacji przyjmujemy Politykę Ochrony Danych. Zasady, działania, kompetencje i zakresy odpowiedzialności opisane w dokumentach Polityki Ochrony Danych obowiązują wszystkich pracowników BGT Sp. z o.o. i osób współpracujących.

Funkcjonujący System Bezpieczeństwa Informacji jest w pełni zgodny z wymaganiami obowiązującego prawa i będzie nieustannie nadzorowany i doskonalony.

Podstawy prawne

BGT Sp. z o.o. wprowadzając Politykę Ochrony Danych kieruje się obowiązkiem spełnienia wymagań płynących z następujących aktów prawnych i innych dokumentów regulacyjnych:

1. Konstytucja Rzeczypospolitej Polskiej art. 47, 51;
2. Ustawa ochronie danych osobowych;
3. 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), w skrócie „RODO” lub z angielskiego GDPR.

Definicje

- **Dane osobowe** - to wszelkie informacje związane ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną. Osoba jest uznawana za osobę bezpośrednio lub pośrednio identyfikowalną poprzez odniesienie do identyfikatora, takiego jak nazwa, numer identyfikacyjny, dane dotyczące lokalizacji, identyfikator internetowy lub jeden lub więcej czynników specyficznych dla fizycznego, fizjologicznego, genetycznego, umysłowego, ekonomicznego, kulturowego lub społecznego.

- **Podmiotem danych** jest każda osoba fizyczna, która dane osobowe są przetwarzane.

- **Administrator (danych)** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.

- **Administrator Systemów Informatycznych** (ASI) to osoba, której Administrator Danych Osobowych powierzył pełnienie obowiązków Administratora Systemów Informatycznych w odniesieniu do systemu nadzoru nad informacją (aktywami) funkcjonującą w systemach informatycznych.

- **Inspektor Ochrony Danych (IOD) -** to osoba formalnie wyznaczona przez Administratora w celu informowania i doradzania Administratorowi/Podmiotowi przetwarzającemu/pracownikom w zakresie obowiązującego prawa o ochronie danych i niniejszej Polityki oraz w celu monitorowania ich przestrzegania oraz działania jako punkt kontaktowy dla osób przetwarzanych i organu nadzorczego.

- **Odbiorca** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią.

- **Podmiot przetwarzający** (**Procesor)** to osoba fizyczna lub prawna, organ publiczny, agencja lub jakikolwiek inny organ przetwarzający dane osobowe w imieniu administratora.

- **RODO** – rozporządzenie parlamentu europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46 z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016)

- **Przetwarzanie danych osobowych** to dowolna zautomatyzowana lub niezautomatyzowana operacja lub zestaw operacji wykonywanych na danych osobowych lub w zestawach danych osobowych i obejmuje zbieranie, rejestrowanie, organizowanie, strukturyzowanie, przechowywanie, adaptację lub zmianę, wyszukiwanie, konsultacje, wykorzystanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, wyrównanie lub połączenie, ograniczenie, usunięcie lub zniszczenie danych osobowych.

- **Ograniczenie przetwarzania** - polega na oznaczeniu przetwarzanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania

- **Anonimizacja**- zmiana danych osobowych w wyniku której dane te tracą charakter danych osobowych

- **Pseudonimizacja -** oznacza przetwarzanie danych osobowych w taki sposób (np. poprzez zastępowanie nazw liczbami), że danych osobowych nie można już przypisać do określonego podmiotu danych bez użycia dodatkowych informacji (np. Listy referencyjnej nazwisk i numerów), pod warunkiem, że takie dodatkowe informacje są przechowywane oddzielnie i podlegają środkom technicznym i organizacyjnym w celu zapewnienia, że dane osobowe nie są przypisane do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

- **Szczególne kategorie danych osobowych** - ujawniają pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, członkostwo w związkach zawodowych i obejmują przetwarzanie danych genetycznych, dane biometryczne w celu jednoznacznej identyfikacji osoby fizycznej, dane dotyczące zdrowia, dane dotyczące naturalnego życia seksualnego osoby lub orientacji seksualnej. W zależności od obowiązującego prawa, specjalne kategorie danych osobowych mogą również zawierać informacje o środkach zabezpieczenia społecznego lub postępowaniach administracyjnych i karnych oraz o sankcjach.

- **Ocena skutków w ochronie danych -** to proces przeprowadzany przez Administratora, jeśli jest wymagany przez obowiązujące prawo i, jeśli to konieczne, z uczestnictwem Inspektora Ochrony Danych, przed przetwarzaniem, w przypadku, gdy istnieje prawdopodobieństwo wysokiego ryzyka dla praw i wolności osób fizycz-

nych, jako rodzaju przetwarzania danych osobowych i zachodzi wraz z wykorzystaniem nowych technologii, biorąc pod uwagę charakter, zakres, kontekst i cele przetwarzania. Proces ten musi ocenić wpływ planowanych operacji przetwarzania na ochronę danych osobowych.

- **Profilowanie** – jest dowolną forma zautomatyzowanego przetwarzania danych osobowych, która polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

- **Naruszenie ochrony danych osobowych -** jest to przypadkowy lub niezgodny z prawem incydent prowadzący do zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych,
- **Informacja –** treść wszelkiego rodzaju dokumentów przechowywanych na dowolnym nośniku informacji. Informacja może być wyrażona za pomocą mowy, pisma, obrazu, rysunku, znaku, kodu, dźwięku lub w jakikolwiek inny sposób,
- **Poufność informacji -** zapewnienie, że tylko uprawnieni pracownicy mają dostęp do informacji,
- **Integralność informacji -** zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania,
- **Dostępność informacji -** zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne,
- **Bezpieczeństwo informacji -** rozumiane, jako odpowiedni poziom poufności, integralności i dostępności informacji, ochrona informacji przed nieautoryzowanym dostępem, modyfikacją, zatajeniem, kradzieżą i zniszczeniem,
- **Zarządzanie ryzykiem -** proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych,
- **Administrator Systemów Informatycznych (ASI**) – należy przez to rozumieć pracownika lub pracowników Informatyki odpowiedzialnych za stosowanie technicznych i organizacyjnych środków ochrony danych osobowych,
- **Hasło –** ciąg znaków literowych cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,
- **Zalogowanie** –uwierzytelnienie, czyli działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu,

Cel i strategia bezpieczeństwa

Cele BGT Sp. z o.o. w dziedzinie bezpieczeństwa informacji:

- ochrona zasobów informacyjnych BGT Sp. z o.o. i zapewnienie ciągłości działania procesów,
- ochrona wizerunku BGT Sp. z o.o.,
- zapewnienie zgodności z prawem podejmowanych działań,
- uzyskanie i utrzymanie odpowiednio wysokiego poziomu bezpieczeństwa zasobów BGT Sp. z o.o. rozumiane, jako zapewnienie poufności, integralności i dostępności zasobów oraz zapewnienie rozliczalności podejmowanych działań,
- wyznaczenie ogólnych kierunków rozwoju systemu informacyjnego,
- podnoszenie kultury informatycznej i tworzenie bezpiecznego społeczeństwa informacyjnego.

Cele osiągane są przez realizowane strategie:

- zapewnienie wsparcia kierujących BGT Sp. z o.o. dla Systemu Zarządzania Bezpieczeństwa Informacji,
- zarządzanie ryzykiem w celu ograniczania go do akceptowanego poziomu,
- właściwa ochrona informacji, a w szczególności informacji prawnie chronionych,
- zapewnienie odpowiedniego poziomu dostępności informacji i niezawodności systemów informatycznych,
- właściwa ochrona informacji związanych z zawartymi umowami,
- wdrażanie i rozwój systemów informacyjnych z zachowaniem zasad bezpieczeństwa,
- eksploatowanie systemów informacyjnych zgodnie z zasadami bezpieczeństwa,
- stała edukacja użytkowników systemu informacyjnego.

Obowiązki ADO, IOD, ASI

Administrator Danych Osobowych

Administrator Danych Osobowych (ADO) jest nim BGT Sp. z o.o reprezentowany przez Zarząd, pełniący nadzór nad realizacją obowiązków wynikających z zarządzania bezpieczeństwem informacji.

Administrator Danych Osobowych (ADO) jest odpowiedzialny za:

1. Dostosowanie sposobu przetwarzania danych osobowych do RODO,
2. Realizację ustawy o ochronie danych, w tym danych osobowych w zakresie dotyczącym Administratora Danych,
3. Zgłoszenie do organu nadzorczego powołania i odwołania Inspektora Ochrony Danych;
4. Pełnienie zwierzchnictwa nad działaniami IOD,
5. Zapewnienie środków i organizacyjnej odrębności Inspektora Ochrony Danych niezbędnego do niezależnego wykonywania przez niego zadań.
6. Zgłaszanie incydentów do organu nadzorczego.

Inspektor Ochrony Danych

Inspektor Ochrony Danych (IOD) odpowiedzialny jest za:

1. Informowanie Administratora oraz pracowników o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów,
2. Monitorowanie przestrzegania RODO oraz innych przepisów Unii i państw członkowskich oraz polityk administratora lub procesora,
3. Szkolenie personelu uczestniczącego w operacjach przetwarzania
4. Przeprowadzania systematycznych audytów w organizacji, w której został powołany,
5. Udzielania wskazówek administratorowi w przedmiocie wdrożenia odpowiednich i skutecznych środków technicznych jak również organizacyjnych mających zabezpieczyć dane osobowe oraz wykazać przestrzeganie prawa przez administratora lub podmiot przetwarzający dane w szczególności, jeżeli chodzi o identyfikowanie ryzyka związanego z przetwarzaniem, o jego ocenę pod katem źródła, charakteru,

prawdopodobieństwa i wagi zagrożenia oraz o najlepsze praktyki pozwalające zminimalizować to ryzyko,
6. Udzielania na żądanie zaleceń, co do oceny skutków oraz monitorowanie ich wykonania w przypadku, gdy administrator danych przed rozpoczęciem przetwarzania zobowiązany jest do przeprowadzenia oceny skutków planowanych operacji przetwarzania dla ochrony danych.
7. Nadzorowanie opracowywania i aktualizowania Polityki Ochrony Danych,
8. Weryfikację dopuszczenia użytkowników do przetwarzania danych,
9. Powiadomienie ASI o konieczności utworzenia identyfikatora użytkownika w systemie,
10. Powiadomienie ASI o zmianie uprawnień dostępu Użytkownika do systemu,
11. Prowadzenie rejestru osób upoważnionych do przetwarzania danych osobowych,

Administrator Systemów Informatycznych

Administrator Systemu Informatycznego (ASI) jest odpowiedzialny za:
1. Bieżący monitoring oraz zapewnianie ciągłości działania systemu informatycznego,
2. Optymalizację wydajności systemu informatycznego,
3. Instalację i konfigurację sprzętu sieciowego i serwerowego,
4. Instalację i konfigurację oprogramowania systemowego i sieciowego,
5. Konfigurację i administrację oprogramowaniem systemowym i sieciowym zabezpieczającym dane chronione przed nieupoważnionym dostępem,
6. Konfigurację i administrację systemem pocztowym,
7. Współpracę z dostawcami usług sprzętu sieciowego i serwerowego,
8. Zarządzanie kopiami awaryjnymi danych, w tym danych osobowych oraz zasobów umożliwiających ich przetwarzanie,
9. Bieżący monitoring oraz zapewnianie ciągłość działania systemów baz danych,

Podstawowe zasady ochrony danych osobowych.

Ze względu na fakt, iż BGT Sp. z o.o. jest Administratorem Danych Osobowych, została opracowana i wdrożona Polityka Ochrony Danych. Dotyczy ona wszystkich osób biorących udział w przetwarzaniu danych osobowych zarówno w systemie informatycznym jak również w formie papierowej.

Celem niniejszej polityki jest określenie podstawowych zasad bezpiecznego przetwarzania danych osobowych w systemie informatycznym BGT Sp. z o.o. Wszelkie dokumenty określające zasady przetwarzania danych osobowych w systemie informatycznym winny być zgodne z niniejszą polityką.

BGT Sp. z o. o., rozumiejąc konieczność zabezpieczenia danych, w tym osobowych wynikającą z obowiązujących w Polsce przepisów prawa, deklaruje pełne wsparcie dla podejmowanych działań uzasadnionych realizacją celów zabezpieczenia danych, w tym osobowych przetwarzanych w systemie informatycznym.

BGT Sp. z o.o., pełniąc rolę Administratora Danych, może lecz nie musi wyznaczyć Inspektora Ochrony Danych w celu sprawowania nadzoru nad przestrzeganiem obowiązujących zasad bezpieczeństwa danych osobowych, koordynacji procesów związanych z zarządzaniem systemem informatycznym przetwarzającym dane osobowe w aspekcie ich bezpieczeństwa oraz bezpośredniego reprezentowania go wobec Administratora Systemu Informatycznego. W sytuacji jeśli IOD nie zostanie wyznaczony, jego obowiązki wykonuje ADO. BGT SP. z o.o. z uwagi na zakres przetwarzanych danych nie wyznaczył Inspektora Ochrony Danych.

1. Zabezpieczenie przetwarzanych danych

Wszystkie osoby biorące bezpośredni lub pośredni udział w procesie przetwarzania danych, w tym osobowych w systemie informatycznym, są odpowiedzialne za właściwe zabezpieczenie tych danych.
Zabezpieczenie danych, w tym osobowych przetwarzanych w systemie informatycznym, obejmuje:

- ochronę poufności rozumianej, jako zabezpieczenie informacji przed dostępem do niej osób nieuprawnionych,
- ochronę integralności rozumianej, jako zabezpieczenie informacji przed wprowadzeniem przypadkowych lub celowych zmian powodujących jej zafałszowanie,
- ochronę dostępności rozumianej, jako zabezpieczenie informacji przed jej zniszczeniem, jak również zapewnienie takiego działania systemu informatycznego, aby dane osobowe były dostępne dla osób upoważnionych do ich przetwarzania.

Zabezpieczenia są określane na podstawie obowiązujących wymagań prawnych i wyników procesu analizy ryzyka. Za koordynację procesu analizy ryzyka odpowiedzialny jest IOD.

Proces przetwarzania danych

W celu należytej ochrony ADO zinwentaryzował przetwarzane dane osobowe. Wyniki inwentaryzacji przedstawione są w Załączniku nr 3a do Polityki Ochrony Danych – Rejestrze czynności przetwarzania – dla danych których jest Administratorem oraz w Załączniku nr 3b do Polityki Ochrony Danych - Rejestrze kategorii czynności - dla danych które przetwarza jako podmiot przetwarzający.

ADO zobowiązany jest do spełnienia obowiązków prawnych wobec przetwarzanych danych W szczególności zapewnia, że:

- dane te są legalnie przetwarzane (na podstawie art. 6, 9 RODO),
- dane te są adekwatne w stosunku do celów przetwarzania,
- dane te są przetwarzane przez określony czas (określono retencję danych),
- opracowano klauzule informacyjne dla powyższych osób (Wzór klauzuli informacyjnej zawiera Załącznik nr 7 do Polityki Ochrony Danych) oraz wykonano względem nich obowiązek informacyjny (art. 12, 13 i 14 RODO)
- istnieją umowy powierzenia z podmiotami przetwarzającymi (art. 28 RODO). Załącznik nr 8 do Polityki Ochrony Danych zawiera wzór umowy powierzenia, natomiast Załącznik nr 9 do Polityki Ochrony Danych zawiera wzór Rejestru umów powierzenia.
- potwierdzenie spełnienia powyższych wymagań prawnych RODO znajduje się w Załączniku nr 3a - Rejestr czynności przetwarzania.

Za ochronę danych osobowych odpowiedzialni są wszystkie pracownicy. Systemy informatyczne przetwarzające dane, w tym dane osobowe, umieszczone są w kontrolowanych przez odpowiedzialnego za dany sprzęt pracownika. Szczególną ochroną otacza się pomieszczenie serwerowni będące pod nadzorem ASI.

Pracownicy upoważnieni i zarazem odpowiedzialni za ochronę danych przetwarzanych na będącym w ich użytkowaniu komputerze są zobowiązani do stosowania procedur wynikających z niniejszej instrukcji.
Dane, w tym dane osobowe, przetwarzane w systemie informatycznym i przesyłane za pośrednictwem sieci informatycznych są zabezpieczone przy użyciu mechanizmów kryptograficznych.

Kontrola dostępu

Dostęp użytkowników do systemu informatycznego przetwarzającego dane, w tym dane osobowe, jest kontrolowany za pomocą mechanizmów uwierzytelnienia, autoryzacji. Podstawą uwierzytelnienia użytkownika jest wykorzystanie unikalnego dla użytkownika identyfikatora i hasła. Autoryzacja użytkownika odbywa się na podstawie nadanych przez IOD, a wprowadzonych przez ASI zakresu indywidualnych uprawnień. System informatyczny przetwarzający dane, w tym dane osobowe, jest wyposażony w mechanizmy pozwalające w sposób jednoznaczny przypisać wykonanie określonych operacji na danych osobowych konkretnemu użytkownikowi.

Wszelkiego rodzaju nośniki danych osobowych, które są przekazywane osobom lub podmiotom nieupoważnionym do otrzymania tych danych lub też, gdy istnieje podejrzenie, że mogą się one znaleźć w rękach osób nieupoważnionych do otrzymania danych, w tym danych osobowych (na przykład w procesie likwidacji), pozbawia się danych lub też doprowadza do stanu uniemożliwiającego ich odczytanie.
Za pozbawienie zapisu odpowiada ASI.

W razie, gdy przekazanie nośnika osobie niebędącej pracownikiem BGT Sp. z o.o. jest związane z jego naprawą lub konserwacją albo naprawą lub konserwacją urządzenia, którego składową jest nośnik, dopuszczalne jest pozostawienie zapisanych danych pod warunkiem sprawowania nadzoru przez IOD lub ASI w trakcie trwania naprawy lub konserwacji.

4. Środki techniczne i organizacyjne

Część ta zawiera opis środków technicznych, organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych.

Środki organizacyjne

1. Dostęp do danych osobowych mogą mieć tylko i wyłącznie pracownicy posiadający pisemne, imienne upoważnienia podpisane przez ADO. Wzór upoważnienia stanowi Załącznik nr 1b do Polityki Ochrony Danych. Wszystkie osoby upoważnione odnotowane są w ewidencji osób upoważnionych do przetwarzania danych osobowych stanowiącej Załącznik nr 2 do Polityki Ochrony Danych.
2. Każdy z pracowników powinien zachować szczególną ostrożność przy przetwarzaniu danych osobowych.
3. Należy chronić dane przed dostępem do nich osób nieupoważnionych.
4. Pomieszczenia, w których są przetwarzane dane osobowe, muszą być zamykane na klucz.
5. Dostęp do kluczy powinni posiadać tylko upoważnieni pracownicy.
6. Dostęp do pomieszczeń, w których są przetwarzane dane osobowe mogą mieć tylko upoważnieni pracownicy BGT Sp. z o.o.
7. W przypadku pomieszczeń do których dostęp mają również osoby nieupoważnione, mogą przebywać w tych pomieszczeniach tylko w obecności osób upoważnionych, i tylko w czasie wymaganym na wykonanie niezbędnych czynności.
8. Szafy, w których przechowywane są dane osobowe muszą być zamykane na klucz.
9. Klucze do tych szaf powinni posiadać tylko upoważnieni pracownicy.
10. Szafy z danymi powinny być otwarte tylko na czas potrzebny na dostęp do danych, a następnie powinny być zamykane.
11. Dane osobowe w formie papierowej mogą znajdować się na biurkach tylko na czas niezbędny na dokonanie czynności służbowych, a następnie muszą być chowane do szaf.

4.2 Środki techniczne

1. Dostęp do komputerów, na których są przetwarzane dane osobowe mogą mieć tylko upoważnieni pracownicy BGT Sp. z o.o..
2. Stacje komputerowe, na których przetwarzane są dane osobowe powinny mieć tak ustawione monitory, aby nie miały wglądu w dane osoby nieupoważnione.
3. W przypadku przetwarzania danych osobowych na komputerach przenośnych (notebook) należy zachować szczególną ostrożność przy ich przewożeniu.
4. Nie należy udostępniać osobom nieupoważnionym komputerów przenośnych.
5. W przypadku potrzeby przeniesienia danych osobowych pomiędzy komputerami należy dokonać tego z zachowaniem szczególnej ostrożności.
6. Nośniki użyte do tego należy wyczyścić (skasować nieodwracalnie), aby nie zostały na nich dane osobowe.
7. W wypadku niemożliwości skasowania danych z nośnika (płyta CD-ROM) należy taką płytę zniszczyć fizycznie.
8. W przypadku wykorzystania do przenoszenia dysków, dane należy kasować z tych dysków.
9. Niezabezpieczonych danych osobowych nie należy przesyłać drogą elektroniczną.
10. Sieć komputerowa zabezpieczona jest przed dostępem z zewnątrz sieci ruterem brzegowym.
11. Do zabezpieczenia sieci stosuje się:
    a. systemy antywirusowe,
    b. dostęp do poczty elektronicznej tylko na serwerach autoryzowanych przez BGT Sp. z o.o.,
    c. zabezpieczenia stacji roboczych oraz programów poprzez indywidualne loginy i hasła logowania.

Naruszenie bezpieczeństwa danych

Procedura obsługi incydentu opisana jest w Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych stanowiącej Załączniku nr 4 do Polityki Ochrony Danych.

6. Ochrona przed szkodliwym oprogramowaniem

ASI jest odpowiedzialny za prowadzenie działań mających na celu zabezpieczenie systemu informatycznego przetwarzającego dane, w tym dane osobowe, przed zainfekowaniem wirusami lub innymi niebezpiecznymi kodami, a także za działania zmierzające do wykrycia ewentualnej infekcji i usunięcie jej skutków. Z tego względu Administrator Systemu Informatycznego ma prawo ograniczać uprawnienia użytkowników, w szczególności w zakresie wymiany informacji z wykorzystaniem publicznych sieci informatycznych, jeżeli może to wpłynąć na redukcję ryzyka wprowadzenia wirusów lub innych wrogich kodów do systemu informatycznego przetwarzającego dane osobowe i nie będzie miało wpływu na możliwość realizacji przez pracowników BGT Sp. z o.o. ich obowiązków służbowych.

Pracownicy BGT Sp. z o.o. korzystający z systemu informatycznego są zobowiązani do stosowania się do szczegółowych zaleceń w zakresie ochrony antywirusowej, a także do przedmiotowych zaleceń wydawanych przez Administratora Systemu Informatycznego.

7. ***Zapewnienie ciągłości działania***

W przypadku awarii programów wykorzystywanych do przetwarzania danych osobowych informujemy Administratora Systemów Informatycznych, który przywraca program do właściwej funkcjonalności. W zależności od usterki naprawia błąd, przywraca bazę danych z kopii bezpieczeństwa lub reinstaluje program oraz odtwarza bazę z kopii bezpieczeństwa.

8. Kształcenie pracowników

Wszyscy pracownicy BGT Sp. z o.o. mający dostęp do systemu informatycznego przetwarzającego dane osobowe są poddawani przeszkoleniu obejmującemu zapoznanie z obowiązującymi regulacjami prawnymi w zakresie ochrony tych danych, jak również obowiązującymi w BGT Sp. z o.o. zasadami bezpiecznego ich przetwarzania. Za organizację szkolenia odpowiada IOD. Przeszkolenie pracownika jest warunkiem koniecznym do dopuszczenia go do korzystania z systemu informatycznego przetwarzającego dane osobowe.

Zakres rozpowszechniania i stosowania Polityki Ochrony Danych

Zasady określone przez dokumenty Polityki Ochrony Danych mają zastosowanie do całego systemu informacyjnego BGT Sp. z o.o. a w szczególności do:

- wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są lub będą informacje podlegające ochronie,
- informacji będących własnością BGT Sp. z o.o.,
- wszystkich nośników papierowych, magnetycznych lub optycznych, na których są lub będą znajdować się informacje podlegające ochronie,
- wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,
- wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, stażystów i innych osób mających dostęp do informacji podlegających ochronie.

Do stosowania zasad określonych przez dokumenty Polityki Ochrony Danych zobowiązani są wszyscy pracownicy w rozumieniu przepisów Kodeksu Pracy, stażyści i inne osoby mające dostęp do informacji podlegającej ochronie.

Z treścią niniejszego dokumentu powinni zapoznać się wszyscy pracownicy BGT Sp. z o.o. i osoby mające dostęp do informacji przetwarzanych w BGT Sp. z o.o., którzy zobowiązani są do podpisania oświadczenia o zapoznaniu się z dokumentacją.

Spis załączników

Niniejsza Polityka Ochrony Danych zawiera następujące załączniki:

Załącznik nr 1a - Oświadczenie o zapoznaniu się z Polityką Ochrony Danych;
Załącznik nr 1b - Upoważnienie do przetwarzania danych osobowych;
Załącznik nr 2 – Rejestr osób upoważnionych do przetwarzania danych osobowych;
Załącznik nr 3a – Rejestr czynności przetwarzania;
Załącznik nr 3b – Rejestr kategorii czynności;
Załącznik nr 4 - Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych;
Załącznik nr 5 - Rejestr incydentów i naruszeń;
Załącznik nr 6 - Zgłoszenie naruszenia ochrony danych osobowych;

Załącznik nr 7 - Wzór klauzuli informacyjnej;
Załącznik nr 8 – Wzór umowy powierzenia przetwarzania danych;
Załącznik nr 9 - Rejestr umów powierzenia;
Załącznik nr 10 – Analiza ryzyka przy przetwarzaniu danych osobowych.
Załącznik nr 11 – Instrukcja zarządzania systemem informatycznym.