

Powierzenie przetwarzania danych osobowych - standardowe klauzule umowne

SEKCJA I

Klauzula 1

Cel i zakres

- a) Celem niniejszych standardowych klauzul umownych („klauzule”) jest zapewnienie przestrzegania art. 28 ust. 3 i 4 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
- b) Administratorzy i podmioty przetwarzające wymienieni w załączniku I uzgodnili niniejsze klauzule w celu zapewnienia przestrzegania art. 28 ust. 3 i 4 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
- c) Niniejsze klauzule mają zastosowanie do przetwarzania danych osobowych określonego w załączniku II.
- d) Załączniki I–IV stanowią integralną część klauzul.
- e) Niniejsze klauzule pozostają bez uszczerbku dla obowiązków, którym podlega administrator danych na mocy rozporządzenia (UE) 2016/679.
- f) Niniejsze klauzule same w sobie nie zapewniają wypełnienia obowiązków związanych z międzynarodowym przekazywaniem danych zgodnie z rozdziałem V rozporządzenia (UE) 2016/679.

Klauzula 2

Niezmienność klauzul

- a) Strony zobowiązują się nie zmieniać klauzul z wyjątkiem dodawania informacji do załączników lub aktualizowania zawartych w nich informacji.
- b) Postanowienie to nie uniemożliwia stronom umieszczania standardowych klauzul umownych określonych w niniejszych klauzulach w treści umowy o szerszym zakresie ani dodawania innych klauzul lub dodatkowych zabezpieczeń, pod warunkiem że nie będą one bezpośrednio lub pośrednio sprzeczne z klauzulami umownymi ani nie będą naruszały podstawowych praw lub wolności osób, których dane dotyczą.

Klauzula 3

Wykładnia

- a) Jeżeli w niniejszych klauzulach użyto terminów zdefiniowanych odpowiednio w rozporządzeniu (UE) 2016/679, terminy te mają takie samo znaczenie jak w tych rozporządzeniach.
- b) Niniejsze klauzule odczytuje się i interpretuje w świetle odpowiednio przepisów rozporządzenia (UE) 2016/679.
- c) Niniejszych klauzul nie interpretuje się w sposób sprzeczny z prawami i obowiązkami przewidzianymi w rozporządzeniu (UE) 2016/679 ani w sposób naruszający podstawowe prawa lub wolności osób, których dane dotyczą.

Klauzula 4

Hierarchia

W razie sprzeczności między niniejszymi klauzulami a postanowieniami powiązanych umów między stronami istniejących w chwili uzgadniania niniejszych klauzul lub zawartych po ich uzgodnieniu, pierwszeństwo mają niniejsze klauzule.

Klauzula 5 – fakultatywna

Klauzula przystąpienia

Nie dotyczy

SEKCJA II

OBOWIĄZKI STRON

Klauzula 6

Opis przetwarzania

Szczegóły dotyczące operacji przetwarzania, w szczególności kategorie danych osobowych i cele, dla których dane osobowe są przetwarzane w imieniu administratora, określono w załączniku II.

Klauzula 7

Obowiązki stron

7.1. Polecenia

- a) Podmiot przetwarzający przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora, chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający. W takim przypadku przed

rozpoczęciem przetwarzania podmiot przetwarzający informuje administratora o tym obowiązku prawnym, o ile prawo nie zabrania udzielenia takiej informacji z uwagi na ważny interes publiczny. Administrator może wydawać kolejne polecenia przez cały okres przetwarzania danych osobowych. Polecenia te są zawsze dokumentowane.

- b) Podmiot przetwarzający bezzwłocznie powiadamia administratora, jeżeli w opinii podmiotu przetwarzającego polecenie wydane przez administratora narusza rozporządzenie (UE) 2016/679 lub obowiązujące przepisy Unii lub państwa członkowskiego o ochronie danych.

7.2. Ograniczenie celu

Podmiot przetwarzający przetwarza dane osobowe wyłącznie w konkretnym celu lub celach przetwarzania, określonych w załączniku II, chyba że otrzyma dalsze polecenia od administratora.

7.3. Czas trwania przetwarzania danych osobowych

Przetwarzanie przez podmiot przetwarzający odbywa się wyłącznie przez okres określony w załączniku II.

7.4. Bezpieczeństwo przetwarzania

- a) W celu zapewnienia bezpieczeństwa danych osobowych podmiot przetwarzający wdraża co najmniej środki techniczne i organizacyjne określone w załączniku III. Zapewnienie bezpieczeństwa danych obejmuje ochronę danych przed naruszeniem bezpieczeństwa prowadzącym do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych (naruszenie ochrony danych osobowych). Oceniając odpowiedni poziom bezpieczeństwa, strony należycie uwzględniają stan wiedzy technicznej, koszty wdrażania, charakter, zakres, kontekst i cele przetwarzania oraz związane z tym ryzyko dla osób, których dane dotyczą.
- b) Podmiot przetwarzający udziela członkom swojego personelu dostępu do danych osobowych podlegających przetwarzaniu jedynie w zakresie bezwzględnie niezbędnym do wykonania umowy, zarządzania nią i jej monitorowania. Podmiot przetwarzający zapewnia, by osoby upoważnione do przetwarzania otrzymanych danych osobowych zobowiązały się do zachowania poufności lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania poufności.

7.5. Dane wrażliwe

Jeżeli przetwarzanie obejmuje dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne lub dane biometryczne do celów jednoznacznego zidentyfikowania osoby fizycznej, dane dotyczące zdrowia, seksualności lub orientacji seksualnej danej osoby, bądź dane dotyczące wyroków skazujących i czynów zabronionych („dane wrażliwe”), podmiot przetwarzający stosuje szczególne ograniczenia lub dodatkowe zabezpieczenia.

7.6. Dokumentacja i zgodność

- a) Strony są w stanie wykazać zgodność z niniejszymi klauzulami.
- b) Podmiot przetwarzający niezwłocznie i odpowiednio rozpatruje zapytania administratora dotyczące przetwarzania danych zgodnie z niniejszymi klauzulami.
- c) Podmiot przetwarzający udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków, które są określone w niniejszych klauzulach i wynikają bezpośrednio z rozporządzenia (UE) 2016/679. Na wniosek administratora podmiot przetwarzający zezwala również na audyty czynności przetwarzania objętych niniejszymi klauzulami i uczestniczy w tych audytach. Audyty te przeprowadza się w rozsądnych odstępach czasu lub jeżeli istnieją przesłanki wskazujące na niezgodność. Podejmując decyzję w sprawie przeglądu lub audytu, administrator może wziąć pod uwagę odpowiednie certyfikaty, jakie ma podmiot przetwarzający.
- d) Administrator może przeprowadzić audyt samodzielnie lub upoważnić do jego przeprowadzenia niezależnego audytora. Audyty mogą również obejmować inspekcje w pomieszczeniach lub obiektach fizycznych podmiotu przetwarzającego. Audyty te przeprowadza się, informując o nich, w stosownych przypadkach, z odpowiednim wyprzedzeniem.
- e) Na wniosek właściwego(-ych) organu(-ów) nadzorczego(-ych) strony udostępniają mu (im) informacje, o których mowa w niniejszej klauzuli, w tym wyniki wszelkich audytów.

7.7. Korzystanie z usług podmiotów podprzetwarzających

- a) Podmiot przetwarzający nie może podzlecać żadnych operacji przetwarzania dokonywanych w imieniu administratora zgodnie z niniejszymi klauzulami podmiotowi podprzetwarzającemu bez uprzedniej szczegółowej pisemnej zgody administratora. Podmiot przetwarzający składa wniosek o udzielenie szczegółowej zgody **co najmniej 30 dni** przed rozpoczęciem korzystania z usług danego podmiotu podprzetwarzającego wraz z informacjami niezbędnymi do tego, by administrator mógł podjąć decyzję w sprawie zgody. Załącznik IV zawiera wykaz podmiotów podprzetwarzających upoważnionych przez administratora. Strony są obowiązane do aktualizacji załącznika IV.
- b) Jeżeli podmiot przetwarzający korzysta z usług podmiotu podprzetwarzającego w celu przeprowadzenia określonych czynności przetwarzania (w imieniu administratora), dokonuje tego w drodze umowy, która nakłada na podmiot podprzetwarzający zasadniczo takie same obowiązki w zakresie ochrony danych jak obowiązki nałożone na podmiot przetwarzający dane zgodnie z niniejszymi klauzulami. Podmiot przetwarzający zapewnia, aby podmiot podprzetwarzający wypełniał obowiązki, którym podlega podmiot przetwarzający na mocy niniejszych klauzul oraz rozporządzenia (UE) 2016/679.
- c) Na wniosek administratora podmiot przetwarzający przekazuje administratorowi kopię umowy, jaką zawarł z podmiotem podprzetwarzającym, a w razie wprowadzenia zmian przekazuje administratorowi jej zaktualizowaną wersję. W zakresie niezbędnym do ochrony tajemnicy handlowej lub innych informacji poufnych, w tym danych osobowych, podmiot przetwarzający może utajnić tekst umowy przed jej udostępnieniem.
- d) Podmiot przetwarzający pozostaje w pełni odpowiedzialny przed administratorem za wykonanie obowiązków podmiotu podprzetwarzającego zgodnie z jego umową z podmiotem przetwarzającym. Podmiot przetwarzający powiadamia administratora o każdym przypadku niewywiązania się przez podmiot podprzetwarzający z jego zobowiązań umownych.

- e) Podmiot przetwarzający uzgadnia z podmiotem podprzetwarzającym klauzulę dotyczącą beneficjenta będącego osobą trzecią, zgodnie z którą to klauzulą – jeżeli podmiot przetwarzający przestanie istnieć faktycznie lub formalnie lub stanie się niewypłacalny – administrator ma prawo rozwiązać umowę z podmiotem podprzetwarzającym i nakazać mu usunięcie lub zwrot danych osobowych.

7.8. Międzynarodowe przekazywanie danych

- a) Wszelkie przekazywanie danych do państwa trzeciego lub organizacji międzynarodowej przez podmiot przetwarzający odbywa się wyłącznie na udokumentowane polecenie administratora lub w celu spełnienia szczególnego wymogu na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega podmiot przetwarzający, i odbywa się zgodnie z rozdziałem V rozporządzenia (UE) 2016/679.
- b) Jeżeli zgodnie z klauzulą 7.7 podmiot przetwarzający korzysta z usług podmiotu podprzetwarzającego w celu przeprowadzenia określonych czynności przetwarzania (w imieniu administratora), które wiążą się z przekazywaniem danych osobowych w rozumieniu rozdziału V rozporządzenia (UE) 2016/679, administrator wyraża zgodę na to, by podmioty te mogły zapewnić zgodność z rozdziałem V rozporządzenia (UE) 2016/679 za pomocą standardowych klauzul umownych przyjętych przez Komisję zgodnie z art. 46 ust. 2 rozporządzenia (UE) 2016/679, pod warunkiem że spełnione są warunki stosowania tych standardowych klauzul umownych.

Klauzula 8

Pomoc dla administratora

- a) Podmiot przetwarzający niezwłocznie zawiadamia administratora o każdym wniosku otrzymanym od osoby, której dane dotyczą. Podmiot przetwarzający nie odpowiada na taki wniosek samodzielnie, chyba że administrator wyraził na to zgodę.
- b) Podmiot przetwarzający pomaga administratorowi w wypełnianiu jego obowiązków dotyczących udzielania odpowiedzi na wnioski osób, których dane dotyczą, o skorzystanie z przysługujących im praw, z uwzględnieniem charakteru przetwarzania. Wypełniając swoje obowiązki zgodnie z lit. a) i b), podmiot przetwarzający stosuje się do poleceń administratora.
- c) Oprócz spoczywającego na podmiocie przetwarzającym obowiązku pomagania administratorowi zgodnie z klauzulą 8 lit. b) podmiot przetwarzający pomaga mu ponadto w zapewnieniu wypełniania następujących obowiązków, z uwzględnieniem charakteru przetwarzania danych oraz informacji, którymi dysponuje podmiot przetwarzający:
- 1) obowiązek przeprowadzenia oceny wpływu planowanych operacji przetwarzania na ochronę danych osobowych („ocena skutków dla ochrony danych”), jeżeli dany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych;
 - 2) obowiązek skonsultowania się z właściwym(-i) organem(-ami) nadzorczym(-i) przed rozpoczęciem przetwarzania, jeżeli ocena skutków dla ochrony danych wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby administrator nie zastosował środków w celu jego ograniczenia;

- 3) obowiązek zapewnienia prawidłowości i aktualności danych osobowych poprzez niezwłoczne poinformowanie administratora, jeżeli podmiot przetwarzający stwierdzi, że przetwarzane przez niego dane osobowe są nieprawidłowe lub nieaktualne;
 - 4) obowiązki określone w art. 32 rozporządzenia (UE) 2016/679.
- d) Strony określają w załączniku III odpowiednie środki techniczne i organizacyjne, za pomocą których podmiot przetwarzający jest zobowiązany pomagać administratorowi w stosowaniu niniejszej klauzuli, jak również zakres wymaganej pomocy.

Klauzula 9

Zgłaszanie naruszenia ochrony danych osobowych

W przypadku naruszenia ochrony danych osobowych podmiot przetwarzający współpracuje z administratorem i pomaga mu w wypełnianiu jego obowiązków wynikających z art. 33 i 34 rozporządzenia (UE) 2016/679, z uwzględnieniem charakteru przetwarzania i informacji, którymi dysponuje podmiot przetwarzający.

9.1. Naruszenie ochrony danych dotyczące danych przetwarzanych przez administratora

W przypadku naruszenia ochrony danych osobowych dotyczącego danych przetwarzanych przez administratora podmiot przetwarzający wspomaga administratora:

- a) przy zgłaszaniu naruszenia ochrony danych osobowych właściwemu(-ym) organowi(-om) nadzorcemu(-ym) niezwłocznie po tym, jak administrator dowiedział się o naruszeniu, w stosownych przypadkach/(chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych);
- b) przy uzyskiwaniu następujących informacji, które zgodnie z art. 33 ust. 3 rozporządzenia (UE) 2016/679 powinny być zawarte w zgłoszeniu administratora i obejmować co najmniej:
 - 1) charakter danych osobowych, w tym w miarę możliwości kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
 - 2) możliwe konsekwencje naruszenia ochrony danych osobowych;
 - 3) środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Jeżeli przekazanie wszystkich tych informacji równocześnie nie jest możliwe, pierwotne zgłoszenie zawiera informacje dostępne w danej chwili, a po uzyskaniu dostępu do dalszych informacji przekazuje się je bez zbędnej zwłoki;

- c) przy wypełnianiu – zgodnie z art. 34 rozporządzenia (UE) 2016/679 – obowiązku zawiadomienia bez zbędnej zwłoki osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, jeżeli naruszenie to może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych.

9.2. Naruszenie ochrony danych dotyczące danych przetwarzanych przez podmiot przetwarzający

W przypadku naruszenia ochrony danych osobowych dotyczącego danych przetwarzanych przez podmiot przetwarzający podmiot przetwarzający zgłasza naruszenie administratorowi niezwłocznie po tym, jak dowiedział się o naruszeniu. Zgłoszenie to powinno zawierać co najmniej:

- a) opis charakteru naruszenia (w tym, w miarę możliwości, kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz wpisów danych, których dotyczy naruszenie);
- b) dane punktu kontaktowego, w którym można uzyskać więcej informacji na temat naruszenia ochrony danych osobowych;
- c) wskazanie prawdopodobnych konsekwencji naruszenia oraz środków, które zostały lub mają zostać wprowadzone w celu zaradzenia naruszeniu, w tym w celu zminimalizowania jego ewentualnych negatywnych skutków.

Jeżeli przekazanie wszystkich tych informacji równocześnie nie jest możliwe, pierwotne zgłoszenie zawiera informacje dostępne w danej chwili, a po uzyskaniu dostępu do dalszych informacji przekazuje się je bez zbędnej zwłoki.

Strony określają w załączniku III wszystkie inne elementy, które ma przedstawić podmiot przetwarzający, wspomagając administratora w wypełnianiu jego obowiązków określonych w art. 33 i 34 rozporządzenia (UE) 2016/679.

SEKCJA III

POSTANOWIENIA KOŃCOWE

Klauzula 10

Naruszenie klauzul i rozwiązanie umowy

- a) Bez uszczerbku dla przepisów rozporządzenia (UE) 2016/679, w przypadku gdy podmiot przetwarzający narusza swoje obowiązki wynikające z niniejszych klauzul, administrator może polecić mu, by zawiesił przetwarzanie danych osobowych do czasu, gdy podmiot przetwarzający zapewni zgodność z niniejszymi klauzulami, lub umowa ulega rozwiązaniu. Podmiot przetwarzający niezwłocznie zawiadamia administratora, jeżeli z jakiegokolwiek powodu nie jest w stanie zastosować się do niniejszych klauzul.
- b) Administrator jest uprawniony do rozwiązania umowy w zakresie, w jakim dotyczy ona przetwarzania danych osobowych zgodnie z niniejszymi klauzulami, jeżeli:
 - 1) administrator zawiesił przetwarzanie danych osobowych przez podmiot przetwarzający zgodnie z lit. a) i jeżeli zgodność z niniejszymi klauzulami nie zostanie przywrócona w rozsądnym terminie, a w każdym razie w terminie jednego miesiąca od zawieszenia;
 - 2) podmiot przetwarzający poważnie lub stale narusza niniejsze klauzule lub swoje obowiązki wynikające z rozporządzenia (UE) 2016/679;
 - 3) podmiot przetwarzający nie stosuje się do wiążącej decyzji właściwego sądu lub właściwego(-ych) organu(-ów) nadzorczego(-ych) dotyczącej jego obowiązków wynikających z niniejszych klauzul lub z rozporządzenia (UE) 2016/679.
- c) Podmiot przetwarzający ma prawo rozwiązać umowę w zakresie, w jakim dotyczy ona przetwarzania danych osobowych zgodnie z niniejszymi klauzulami, jeżeli po zawiadomieniu administratora o tym, że jego polecenie narusza obowiązujące wymogi prawne zgodnie z klauzulą 7.1 lit. b), administrator nalega na wypełnienie polecenia.

- d) Po rozwiązaniu umowy podmiot przetwarzający, zależnie od decyzji administratora, usuwa wszystkie dane osobowe przetwarzane w imieniu administratora i poświadcza administratorowi, że tego dokonał, lub zwraca administratorowi wszystkie dane osobowe i usuwa istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych. Podmiot przetwarzający zapewnia przestrzeganie niniejszych klauzul do czasu usunięcia lub zwrotu danych.

ZAŁĄCZNIK I

Wykaz stron

Administrator (administratorzy):

Administratorem danych osobowych jest Województwo Śląskie a także jego organy i przedstawiciele: Zarząd Województwa Śląskiego, Sejmik Województwa Śląskiego, Marszałek Województwa jako kierownik Urzędu Marszałkowskiego.

Dane osobowe przetwarzane są w Urzędzie Marszałkowskim Województwa Śląskiego.

Siedziba administratora znajduje się w Katowicach przy ul. Ligonia 46, tel. +48 (32) 20 78 888 (centrala), e-mail: kancelaria@slaskie.pl

Informacje dotyczące kontaktu w formie elektronicznej znajdują się na stronie głównej <https://bip.slaskie.pl/>

Dane identyfikacyjne i kontaktowe administratora: zgodnie z komparcją umowy, do której niniejsze klauzule są załącznikiem.

Osoba do kontaktu w sprawie przetwarzania danych osobowych (inspektor ochrony danych), adres email: daneosobowe@slaskie.pl

Podpis i data przystąpienia: z datą zawarcia umowy, do której niniejsze klauzule są załącznikiem.

Podmiot przetwarzający (podmioty przetwarzające):

EIB Spółka Akcyjna (EIB S.A.) z siedzibą w Toruniu przy ul. Jęczmiennej 21, wpisana do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy w Toruniu VII Wydział Gospodarczy Krajowego Rejestru Sądowego Nr KRS 0000050455; adres e-mail: odo@eib.com.pl

Dane identyfikacyjne i kontaktowe podmiotu przetwarzającego: zgodnie z komparcją umowy, do której niniejsze klauzule są załącznikiem.

Podpis i data przystąpienia: z datą zawarcia umowy, do której niniejsze klauzule są załącznikiem.

Osoba do kontaktu w sprawie przetwarzania danych osobowych (inspektor ochrony danych), adres email Romuald Rojek, odo@eib.com.pl.

ZAŁĄCZNIK II

Opis przetwarzania

Kategorie osób, których dane osobowe są przetwarzane:

ubezpieczeni, uprawnieni z umów ubezpieczenia, uposażeni, sprawcy szkód, poszkodowani, świadkowie zdarzeń i inne osoby zaangażowane w wykonywanie umowy ubezpieczenia.

Kategorie przetwarzanych danych osobowych:

- a) imię (imiona) i nazwisko, imiona rodziców,
- b) adres zameldowania, zamieszkania bądź adres do korespondencji,
- c) data, miejsce urodzenia,
- d) nr ewidencyjny PESEL, nr NIP,
- e) miejsce pracy, zawód, wykształcenie,
- f) seria i numer dokumentu tożsamości,
- g) nr telefonu, adres e-mail,
- h) nr rachunku bankowego,
- i) informacje o stanie zdrowia, o ile ich przetwarzanie jest niezbędne dla wykonania umowy ubezpieczenia, w szczególności dla celów ustalenia zasadności roszczeń i wysokości odszkodowania.

Przetwarzane dane wrażliwe (w stosownych przypadkach) oraz stosowane ograniczenia lub zabezpieczenia, które w pełni uwzględniają charakter danych i związane z nimi zagrożenia, takie jak na przykład ścisłe ograniczenie celu, ograniczenia dostępu (w tym dostęp wyłącznie dla personelu, który odbył specjalistyczne szkolenie), prowadzenie rejestru dostępu do danych, ograniczenia dotyczące dalszego przekazywania danych lub dodatkowe środki bezpieczeństwa.

Strony przewidują ewentualne wystąpienie okoliczności przetwarzania danych szczególnych kategorii (wrażliwych) w celu realizacji procesu likwidacji szkód bądź ubezpieczenia od NNW i kosztów leczenia. Dostęp do danych dotyczących stanu zdrowia będą miały wyłącznie upoważnione osoby. Zbieranie tych danych ograniczone będzie do niezbędnego minimum. Wdrożone zostaną zabezpieczenia i dodatkowo ograniczony zostanie dostęp do tych danych do niezbędnego minimum w celu realizacji celu.

Charakter przetwarzania

wszelkie niezbędne operacje na danych osobowych lub zestawach danych, w sposób zautomatyzowany lub niezautomatyzowany, w szczególności zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

Cel(e), w którym(-ych) dane osobowe są przetwarzane w imieniu administratora:

zawieranie i wykonywanie umów ubezpieczenia, w szczególności likwidacja szkód

Czas trwania przetwarzania:

czas niezbędny do wykonania obowiązków wynikających z umowy brokerskiej

Na etapie zawierania umowy nie zidentyfikowano podmiotów podprzetwarzających.

ZAŁĄCZNIK III

Środki techniczne i organizacyjne, w tym środki techniczne i organizacyjne w celu zapewnienia bezpieczeństwa danych

Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa

Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, Podmiot przetwarzający (EIB S.A.) wdrożył odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, zapewniając:

- a) pseudonimizację i szyfrowanie danych osobowych,
- b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
- c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,
- d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Administrator opracował i wdrożył:

- 1) Politykę Zintegrowanego Systemu Zarządzania obejmującą między innymi zasady zabezpieczenia systemów informatycznych;
- 2) Regulamin zasad bezpieczeństwa R/EIB/10 wraz z dodatkowymi instrukcjami, obejmujący całość zasad związanych z postępowaniem z informacjami, dostosowany do wymagań normy ISO 27001:2013 i przepisów o ochronie danych osobowych.

W celu zabezpieczenia danych zastosowano również następujące środki:

1) ochrona fizyczna danych:

- całodobowa ochrona budynków z centrami przetwarzania danych,
- dostęp do pomieszczeń ze stacjami roboczymi zabezpieczony przed niepowołanym dostępem dzięki systemowi kart hybrydowych lub weryfikacji danych biometrycznych (daktyloskopijnych),
- nośniki z kopiami zapasowymi systemu są przechowywane w pomieszczeniach Spółki w metalowej szafie, do której dostęp mają tylko upoważnione osoby; dodatkowo kopie są przechowywane w specjalnie do tego celu wynajętej skrytce bankowej,
- pomieszczenia zabezpieczone systemem antywłamaniowym z czujnikami ruchu;
- wszystkie budynki posiadają monitoring CCTV co najmniej wejść do budynków;

2) środki sprzętowe, informatyczne i telekomunikacyjne:

- bazy umieszczone na niezawodnych dyskach (macierzach dyskowych),

- serwery zasilane z zasilaczy bezprzerwowych znajdujące się w strefie bezpiecznej,
- organizacja posiada zapasowe centrum przetwarzania danych zlokalizowane w innej miejscowości,
- dostęp do sieci zabezpieczany i monitorowany routerami z funkcjami: firewall, IDS, IPS, spam filtering, web filtering, antyvirus;

3) Środki ochrony w ramach oprogramowania urządzeń teletransmisji:

- dostęp do stacji roboczych autoryzowany certyfikatem przechowywanym na karcie hybrydowej,
- dostęp do systemu możliwy tylko po użyciu karty hybrydowej i prawidłowego kodu PIN (8 cyfrowego) lub użyciu danych daktyloskopijnych,
- przesyłane dane są szyfrowane,
- szyfrowanie i deszyfrowanie odbywa się poza systemem przetwarzającym dane osobowe;
- dane na nośnikach środków przetwarzania informacji poza strefami bezpiecznymi są zawsze szyfrowane; przez środki przetwarzania rozumie się: laptopy, komputery, telefony, tablety, nośniki pamięci itp., na których potencjalnie mogą być przetwarzane dane osobowe;

4) Środki ochrony w ramach oprogramowania systemów:

- unikalne identyfikatory użytkowników,
- tajne hasła i PIN-y dostępu,
- pełne logowanie aktywności użytkownika w systemie,
- wygaszacze monitorów,
- automatyczne blokowanie stacji roboczej po odejściu od niej z kartą hybrydową niezbędną do poruszania się po obiekcie i odbierania wydruków z drukarek;

5) Środki ochrony w ramach narzędzi baz danych i innych narzędzi programowych:

- codzienne kopie baz danych, które podlegają cyklicznym testom odtworzenia,
- okresowe sprawdzanie spójności baz danych (narzędzie wbudowane bazy danych),
- testowane procedury odtwarzania danych i uruchamiania centrum zapasowego,
- plan ciągłości działania jest dorocznie aktualizowany i weryfikowany w czasie testów uruchomienia centrum zapasowego;

6) Środki ochrony w ramach systemu użytkowego:

- dostęp do systemu na podstawie posiadanej karty hybrydowej i unikatowego kodu PIN lub danych biometrycznych,
- dostęp tylko z autoryzowanych stacji roboczych,
- pełne logowanie aktywności użytkowników na poziomie bazy danych i systemu operacyjnego,
- przydział uprawnień dla każdego użytkownika (grupy i poziomy w obrębie grupy);

7) Środki organizacyjne:

- każdy pracownik otrzymał upoważnienie do przetwarzania danych osobowych

- każdy pracownik posiada osobistą kartę hybrydową z przypisanym poziomem uprawnień i hasłem dostępu uniemożliwiającą pozostawienie odblokowanej stacji roboczej,
- dostęp do pomieszczeń z serwerami posiada tylko określona grupa upoważnionych pracowników,
- przeprowadza się szkolenia pracowników w zakresie bezpieczeństwa i ochrony informacji.

W organizacji stosuje się dodatkowo szereg innych zabezpieczeń dla: pracy zdalnej, dostępu klientów itp., których szczegółowy opis znajduje się w dokumentacji ZSZ.

Wymienione środki bezpieczeństwa podlegają cyklicznym przeglądom i uaktualnianiu.

ZAŁĄCZNIK IV

Wykaz podmiotów podprzetwarzających

Na etapie zawierania umowy nie zidentyfikowano podmiotów podprzetwarzających.