Umowa powierzenia przetwarzania danych osobowych

Wykaz stron

Umowa powierzenia pomiędzy

Użytkownikiem zwanym dalej Administratorem Danych Osobowych (ADO)

a

Podmiotami przetwarzającymi (podmioty przetwarzające):

1. Imię i nazwisko lub nazwa: **Stowarzyszenie Mierz Wysoko**

   Reprezentowany przez: Emilia Szenderłata

   Adres: **ul. Wolność 2, 01-018 Warszawa**

   Imię i nazwisko, stanowisko i dane kontaktowe osoby wyznaczonej do kontaktów: Natalia Kata-Gawlik

2. Imię i nazwisko lub nazwa: **Fundacja „2do2”**

   Reprezentowany przez: Magdalena Szeniawska, Natalia Kata- Gawlik

   Adres: **ul. Maszewska 20 lok.7, 01-925 Warszawa**

   Imię i nazwisko, stanowisko i dane kontaktowe osoby wyznaczonej do kontaktów: Magdalena Szeniawska

SEKCJA I

Klauzula 1

Cel i zakres

1. 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).
2. Administrator i podmiot przetwarzający uzgodnili niniejsze klauzule w celu zapewnienia przestrzegania art. 28 ust. 3 i 4 rozporządzenia (UE) 2016/679.
3. Niniejsze klauzule mają zastosowanie do przetwarzania danych osobowych określonego w załączniku I.
4. Załączniki I–III stanowią integralną część klauzul.
5. Niniejsze klauzule pozostają bez uszczerbku dla obowiązków, którym podlega administrator danych na mocy rozporządzenia (UE) 2016/679.
6. 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

1. Strony zobowiązują się nie zmieniać klauzul z wyjątkiem dodawania informacji do załączników lub aktualizowania zawartych w nich informacji.
2. 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

1. Jeżeli w niniejszych klauzulach użyto terminów zdefiniowanych w rozporządzeniu (UE) 2016/679, terminy te mają takie samo znaczenie jak w tych rozporządzeniach.
2. Niniejsze klauzule odczytuje się i interpretuje w świetle przepisów rozporządzenia (UE) 2016/679.
3. 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.

SEKCJA II

OBOWIĄZKI STRON

Klauzula 5

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 I.

Klauzula 6

Obowiązki stron

6.1. Polecenia

1. 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.
2. 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.

6.2. Ograniczenie celu

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

6.3. Czas trwania przetwarzania danych osobowych

Przetwarzanie przez podmiot przetwarzający odbywa się przez okres określony w załączniku I oraz klauzuli 9.

6.4. Bezpieczeństwo przetwarzania

1. W celu zapewnienia bezpieczeństwa danych osobowych podmiot przetwarzający wdraża co najmniej środki techniczne i organizacyjne określone w załączniku II. 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.
2. Podmiot przetwarzający ma obowiązek nie rzadziej niż raz w roku testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych (nadzór i monitorowanie prac rozwojowych nad systemami) mających

zapewnić bezpieczeństwo przetwarzanych danych osobowych w systemach informatycznych oraz przedstawiać nie rzadziej niż raz w roku Administratorowi raporty z prowadzonych testów.

3. 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.

6.5. 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.

6.6. Dokumentacja i zgodność

1. Strony są w stanie wykazać zgodność z niniejszymi klauzulami.
2. Podmiot przetwarzający niezwłocznie i odpowiednio rozpatruje zapytania administratora dotyczące przetwarzania danych zgodnie z niniejszymi klauzulami.
3. 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.
4. 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.
5. Na wniosek właściwego organu nadzorczego strony udostępniają mu informacje, o których mowa w niniejszej klauzuli, w tym wyniki wszelkich audytów.

6.7. Korzystanie z usług podmiotów podprzetwarzających

1. Podmiot przetwarzający ma ogólną zgodę administratora na korzystanie z usług podmiotów podprzetwarzających wpisanych do uzgodnionego wykazu. Podmiot przetwarzający informuje administratora na piśmie o wszelkich zamierzonych zmianach w tym wykazie polegających na dodaniu lub **zastąpieniu podmiotów podprzetwarzających z wyprzedzeniem co najmniej 14 dni, dając tym samym administratorowi wystarczająco dużo czasu na wyrażenie sprzeciwu** wobec takich zmian przed rozpoczęciem korzystania z usług danego podmiotu podprzetwarzającego (podmiotów podprzetwarzających). Podmiot przetwarzający przekazuje administratorowi niezbędne informacje umożliwiające mu skorzystanie z prawa sprzeciwu. Załącznik III zawiera wykaz podmiotów podprzetwarzających upoważnionych przez administratora. Strony są obowiązane do aktualizacji Załącznika III.
2. 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 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.
3. 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.
4. 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.

5. 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.

6.8. Międzynarodowe przekazywanie danych

1. 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.
2. Jeżeli zgodnie z klauzulą 6.7 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 7

Pomoc dla administratora

1. 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.
2. 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 ust. 1 i 2 podmiot przetwarzający stosuje się do poleceń administratora.
3. Oprócz spoczywającego na podmiocie przetwarzającym obowiązku pomagania administratorowi zgodnie z klauzulą 7 ust. 2 podmiot przetwarzający pomaga mu ponadto w zapewnieniu wypełniania następujących obowiązków, z uwzględnieniem charakteru przetwarzania danych oraz informacji, którymi dysponuje podmiot przetwarzający:
   a) 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;
   b) obowiązek skonsultowania się z właściwym organem nadzorczym przed rozpoczęciem przetwarzania, jeżeli ocena skutków dla ochrony danych wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby administrator nie zastosował środków w celu jego ograniczenia;
   c) 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;
   d) obowiązki określone w art. 32 rozporządzenia (UE) 2016/679.
4. Strony określają w załączniku II odpowiednie środki techniczne i organizacyjne, za pomocą których podmiot przetwarzający jest zobowiązany pomagać administratorowi w stosowaniu niniejszej klauzuli, jak również zakres wymaganej pomocy.

Klauzula 8

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.

8.1. Naruszenie ochrony danych dotyczące danych przetwarzanych przez administratora

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

1. przy zgłaszaniu naruszenia ochrony danych osobowych właściwemu organowi nadzorczemu 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);
2. 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:
   a) 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;
   b) możliwe konsekwencje naruszenia ochrony danych osobowych;
   c) 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;

3. 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.

8.2. 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, nie później niż 24h od powzięcia informacji. Jeśli administrator podlega ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa to incydent należy zgłosić administratorowi w ciągu 8h od powzięcia informacji. Zgłoszenie to powinno zawierać co najmniej:

1. opis charakteru naruszenia (w tym, w miarę możliwości, kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz wpisów danych, których dotyczy naruszenie);
2. dane punktu kontaktowego, w którym można uzyskać więcej informacji na temat naruszenia ochrony danych osobowych;
3. 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 II 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 9

Naruszenie klauzul i rozwiązanie umowy

1. 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.
2. Administrator jest uprawniony do rozwiązania umowy w zakresie, w jakim dotyczy ona przetwarzania danych osobowych zgodnie z niniejszymi klauzulami, jeżeli:
   a) administrator zawiesił przetwarzanie danych osobowych przez podmiot przetwarzający zgodnie z ust. 1 i jeżeli zgodność z niniejszymi klauzulami nie zostanie przywrócona w rozsądnym terminie, a w każdym razie w terminie jednego miesiąca od zawieszenia;

b) podmiot przetwarzający poważnie lub stale narusza niniejsze klauzule lub swoje obowiązki wynikające z rozporządzenia (UE) 2016/679;
c) podmiot przetwarzający nie stosuje się do wiążącej decyzji właściwego sądu lub właściwego organu nadzorczego dotyczącej jego obowiązków wynikających z niniejszych klauzul lub z rozporządzenia (UE) 2016/679.

3. 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 6.1 ust. 2, administrator nalega na wypełnienie polecenia.
4. 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.

Administrator	Podmiot przetwarzający

ZAŁĄCZNIK I

Opis przetwarzania

Kategorie osób, których dane osobowe są przetwarzane

Grupa 1: Członkowie organu zarządzającego organizacją
Grupa 2: Pracownicy/ pracowniczki, wolontariusze/ wolontariuszki organizacji
Grupa 3: Dane współpracowników i kontrahentów

Kategorie przetwarzanych danych osobowych

- Imię, Nazwisko, adres e-mail zakres uprawnień (dot. gr 1 i 2)
- Imię i Nazwisko, wysokość wystawionego rachunku/ faktury (dot. gr. 3)

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.

Charakter przetwarzania: cykliczny

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

- Podpisanie umowy na prowadzenie konta (gr. 1)
- Utworzenie konta w Aplikacji 2do2 (dot. gr 1 i 2)
- Gromadzenie danych w Aplikacji 2do2 (gr 3)

Czas trwania przetwarzania:

5 lat od daty wygaśnięcia dostępu, chyba, że Administrator zgłosi pisemny wniosek o wcześniejsze zakończenie przetwarzania.

W przypadku przetwarzania przez podmioty przetwarzające lub podprzetwarzające należy również określić przedmiot, charakter i czas trwania przetwarzania.

ZAŁĄCZNIK II

Środki techniczne i organizacyjne

Środki techniczne i organizacyjne, w tym środki techniczne i organizacyjne w celu zapewnienia bezpieczeństwa danych przez podmiot przetwarzający:

Środki umożliwiające pseudonimizację i szyfrowanie danych osobowych: posiadanie programów umożliwiających szyfrowanie/pseuonimizację, procedury,

Środki zapewniające zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania: szyfrowanie dysków/katalogów/nośników, transmisja danych szyfrowana (np. SSL, TLS, VPN), zaszyfrowane pliki, które są przesyłane, szyfrowanie wiadomości, uwierzytelnianie dwuetapowe, automatyczna procedura wylogowania, zarządzanie uprawnieniami dostępowymi, automatyczne wygaszanie ekranu, wymuszanie zmiany hasła, aktualizacja systemów. Stosowanie UPS, regularne kopie zapasowe, stosowanie podpisów elektronicznych, znakowanie czasem,

Środki zapewniające zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego – kopie zapasowe wykonywane w regularnych odstępach czasu zapisywane na odrębnym serwerze, aktualizacja procedur dotyczących tworzenia kopii zapasowych,

Procesy umożliwiające regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania – sprawdzanie ważności certyfikatów, sprawdzanie ważności aktualizacji, stosowanie norm ISO, sprawdzenie systemu pod kątem uprawnień, automatyczne wylogowanie z systemu, automatyczne wylogowanie przy próbie przekroczenia uprawnień.

Środki umożliwiające identyfikację i autoryzację użytkowników – podwójna weryfikacja, odrębny identyfikator dla każdego użytkownika oraz hasło, potwierdzenia rejestracji przez e-mail lub inny kanał komunikacji.

Środki zapewniające ochronę danych w czasie ich przekazywania – szyfrowanie, anonimizacja, nieklikanie w niebezpieczne hiperłącza, weryfikacja odbiorcy,

Środki zapewniające ochronę danych w czasie ich przechowywania – zabezpieczenie dokumentów podczas opuszczenia stanowiska pracy: zamknięcie dokumentów, wylogowanie się z aplikacji, zasada czystego biurka, właściwe niszczenie dokumentów, zabezpieczenie kopii zapasowej

Środki służące zapewnieniu bezpieczeństwa fizycznego miejsc, w których przetwarzane są dane osobowe – zamykane drzwi i szafy, nadzorowane wejścia, monitoring, alarm, nakładki maskujące, kraty/rolety w oknach, polityka kluczy, nadstawki do biurek, stosowanie zamków na kartę, serwerownia w odrębnym pomieszczeniu z ograniczonym dostępem.

Środki umożliwiające rejestrowanie zdarzeń – zapisywanie w bazie/na serwarach, logi

Środki służące do konfiguracji systemu, w tym konfiguracji domyślnej – upoważnieni pracownicy do wykonywania wskazanych czynności.

Środki dotyczące zarządzania wewnętrznym systemem IT i bezpieczeństwem IT – przyjęta polityka ochrony danych, zarządzanie uprawnieniami

Środki dotyczące certyfikacji / zapewnienia jakości procesów i produktów – jeśli są certyfikaty/normy to tu wpisać

Środki zapewniające minimalizację danych - okresowe przeglądy przydatności, weryfikacja i analiza zakresu zbieranych danych,

Środki zapewniające odpowiednią jakość danych – regularny nadzór nad prawidłową jakością danych, walidacja formularzy

Środki zapewniające ograniczone zatrzymywanie danych – stosowanie JRWA, instrukcji kancelaryjnej, współpraca z archiwistą, usuwanie dokumentów po zakończeniu celu przetwarzania, kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną;

Środki zapewniające rozliczalność – stosowanie załączników do polityki ochrony, stosowanie podpisów pod dokumentami, audyty, przestrzeganie zasady w fazie projektowania, powołanie IOD, szkolenia, odrębne bazy danych, unikali użytkownicy, odrępne uprawnienia, wydzielone miejsca na serwerach, lokalne bazy danych

Środki umożliwiające przenoszenie danych i zapewnienie ich usuwania - Uprawnieni pracownicy usuwają dane osobowe po okresie przetwarzania lub przenoszą we wskazane przez Administratora Danych Osobowych, czasem może to zrobić osoba uprawniona w aplikacji,

---

ZAŁĄCZNIK III

Wykaz podmiotów podprzetwarzających

Administrator zezwolił na korzystanie z usług następujących podmiotów podprzetwarzających:

1. ADMIN.NET.PL Tomasz Rzepka Arkadiusz Nowara S.C.

Adres: ul. Bitwy Pod Monte Cassino 5/198

Opis przetwarzania: prowadzenie serwera

2.Google LLC

Adres: 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA.

Opis przetwarzania: Google Workspace

3.Fundacja Rozwoju Społeczeństwa Obywatelskiego,

z siedzibą: ul. Kłopotowskiego 6 lok. 59/60, 03-717 Warszawa

Opis przetwarzania: prowadzenie księgowości