

## Umowa powierzenia przetwarzania danych osobowych

obowiązująca od 27 grudnia 2020 roku

Zakładając konto w Programie wyrażasz w formie elektronicznej zgodę na warunki poniższej Umowy Powierzenia Przetwarzania Danych Osobowych, zwanej dalej: „Umową”. Kopia Umowy będzie zawsze dostępna do pobrania na twoim koncie.

Umowa stanowi integralną część umowy między **AceSender**, a **Użytkownikiem** obowiązującej na podstawie Umowy Głównej.

**Użytkownik** i **AceSender** są dalej zwani łącznie „Stronami”.

Zważywszy na to, iż:

1. **AceSender** oraz **Użytkownik** współpracują w przedmiocie prowadzenia działań z zakresu e – mail marketingu, oraz obsługi baz danych przy wykorzystaniu Programu na zasadach przewidzianych w Umowie Głównej;
2. W ramach współpracy dochodzi do przekazywania Danych Osobowych przez **Użytkownika**, działającego jako administrator tych danych osobowych, na rzecz **AceSender**, działającego jako podmiot przetwarzający te dane, a następnie do przetwarzania przez **AceSender** tych danych osobowych na polecenie **Użytkownika**,
3. Strony postanawiają zawrzeć umowę powierzenia przetwarzania w formie elektronicznej, poprzez akceptację Umowy Głównej i niniejszej Umowy,

Strony zgodnie postanawiają co następuje:

### §1. Definicje

1. **Dane Osobowe** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej będące przedmiotem niniejszej umowy, a określone w Zleceniach; możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej. Przy wykonywaniu Umowy Głównej

- dochodzi do przekazywania przez **Użytkownika** zebranych przez niego Danych Osobowych do Programu w celu realizacji kampanii marketingowych;
2. **Program** – oprogramowanie udostępnione online **Użytkownikowi** przez **AceSender**, służące do wykonywania przedmiotu Umowy Głównej;
  3. **Umowa Główna** – umowa zawarta pomiędzy **AceSender** a **Użytkownikiem** dotycząca świadczenia usług e-mail marketingu. Na treść Umowy Głównej składają się: Regulamin Serwisu, Polityki Antyspamowej i polityki prywatności oraz niniejsza Umowa, które **Użytkownik** zaakceptował, podczas rejestracji konta, dostępne na stronie <http://AceSender.com/regulamin-serwisu>;
  4. **Upoważnieni** – oznaczają po stronie **Użytkownika**: osoby upoważnione na podstawie Umowy Głównej do składania Zleceń, jak i do uzyskiwania informacji związanych z przedmiotem Umowy Głównej, a po stronie **AceSender**: osoby upoważnione zgodnie z wewnętrznymi procedurami **AceSender** do przyjęcia Zlecenia oraz przetwarzania Danych Osobowych, jak i do udzielania **Użytkownikowi** wszelkich informacji związanych z przedmiotem Umowy Głównej;
  5. **Zlecenie** – oznacza polecenie przetwarzania Danych Osobowych dokonane przez **Użytkownika** na rzecz **AceSender** poprzez każdorazowe wprowadzenie Danych Osobowych do Programu;
  6. **RODO** – oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku 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).
  7. **Użytkownik** – podmiot korzystający z usług świadczonych przez **AceSender** na podstawie Umowy Głównej oraz określony w niej jako Użytkownik.
  8. **AceSender** - Łukasz Wadas prowadzący działalność gospodarczą pod firmą *CleanScripts.com* Łukasz Wadas, 71-784 Szczecin, ul. Maciejkowa 29/4, NIP: 8522488559, REGON: 321435123.

## §2. Przedmiot Umowy

1. Przedmiotem niniejszej Umowy jest powierzenie przez **Użytkownika** Danych Osobowych do przetwarzania w Programie przez **AceSender** zgodnie ze Zleceniami. Zawierając z **AceSender** Umowę Główną i niniejszą Umowę, **Użytkownik** oświadcza, że wydaje **AceSender** polecenie przetwarzania Danych Osobowych zawartych w każdym Zleceniu w celu i w zakresie niezbędnym do wykonania obowiązków **AceSender** wynikających z Umowy Głównej, tj. wyłącznie w celu realizacji usługi e-mail marketingu oraz czynności towarzyszących tej usłudze. Opis przetwarzania Danych Osobowych, wraz z ich informacjami o tym jakie Dane Osobowe i jakich kategorii osób są przetwarzane zawiera **Załącznik nr 1** do Umowy.

2. **Użytkownik:**

- a) Powierza **AceSender** Dane Osobowe, w tym czynności przetwarzania Danych Osobowych na potrzeby wykonywania usług określonych w Umowie Głównej;
- b) Powierza **AceSender** Dane Osobowe zwykłe, tzn. nie powierza danych szczególnych kategorii (Lista powierzanych danych osobowych znajduje się w **Załączniku 1 do Umowy**).
- c) Wyraża zgodę na podpowierzenie Danych Osobowych przez **AceSender** do podmiotów, które zapewniają obsługę informatyczną dla **AceSender** w czasie trwania Umowy Głównej (lista wszystkich podmiotów znajduje się w **Załączniku nr 3** do Umowy). Podpowierzenie odbywa się również do państw trzecich (poza Europejski Obszar Gospodarczy) zapewniających należyty poziom bezpieczeństwa Danych Osobowych.

3. **AceSender:**

- a) Podejmuje się wykonania czynności przetwarzania Danych Osobowych w celu i w zakresie niezbędnym do wykonywania Umowy Głównej;
- b) Będzie przetwarzał Dane Osobowe wyłącznie w zakresie i celu niezbędnym dla realizacji postanowień Umowy Głównej na podstawie Zleceń;
- c) Będzie przetwarzał Dane Osobowe w sposób ciągły – tak jak tego wymaga specyfika usługi e-mail marketingu;
- d) zabezpiecza przetwarzane Dane Osobowe w sposób opisany w **Załączniku nr 2** do Umowy.

### **§3. Oświadczenia i zobowiązania Stron**

- 1. **Użytkownik** oświadcza, że jest administratorem wszelkich Danych Osobowych wprowadzanych przez niego do Programu
- 2. **AceSender** oświadcza, że jest podmiotem przetwarzającym Dane Osobowe na zlecenie **Użytkownika** zgodnie z niniejszą Umową.
- 3. **AceSender** oświadcza, że posiada środki techniczne i organizacyjne zapewniające ochronę przetwarzania Danych Osobowych w zakresie wymaganym przez obowiązujące przepisy prawa, a w szczególności zabezpiecza Dane Osobowe przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów prawa oraz zmianą, utratą, uszkodzeniem lub zniszczeniem tych danych, a także spełnia inne wymagania określone w przepisach prawa dotyczące ochrony danych osobowych;
- 4. **Użytkownik** oświadcza, że Dane Osobowe wprowadzane przez niego do Programu zostały zgromadzone i są przetwarzane w sposób zgodny z prawem, w szczególności pozyskano

odpowiednie zgody subskrybentów **Użytkownika**, albo istnieje inna legalna podstawa do przetwarzania Danych Osobowych przez **Użytkownika**.

5. Wykonywanie niniejszej Umowy nie wiąże się z żadnymi dodatkowymi świadczeniami pieniężnymi ze strony **Użytkownika**, a wszelkie rozliczenia finansowe dokonane zostaną w ramach Umowy Głównej.
6. **AceSender** zobowiązuje się, że:
  - a) zachowa w tajemnicy Dane Osobowe oraz inne dane, a w szczególności informacje stanowiące tajemnicę przedsiębiorstwa, do których **AceSender** mógł uzyskać dostęp w związku z wykonywaniem postanowień niniejszej umowy lub Umowy Głównej, także po wygaśnięciu lub rozwiązaniu Umowy Głównej;
  - b) przy wykonywaniu postanowień niniejszej umowy dołoży staranności, wynikającej z profesjonalnego charakteru wykonywanej działalności;
  - c) niezwłocznie poinformuje **Użytkownika** o każdym stwierdzonym przypadku naruszenia bezpieczeństwa jakichkolwiek informacji udostępnionych **AceSender** przez **Użytkownika** w związku lub w trakcie wykonywania Umowy Głównej, w tym w szczególności w przypadku naruszenia zasad ochrony Danych Osobowych;
  - d) zobowiąże na piśmie pracowników oraz inne osoby współpracujące na podstawie umów cywilnoprawnych z **AceSender**, posiadające lub mogące posiadać dostęp do danych udostępnionych przez **Użytkownika** w związku z wykonywaniem Umowy Głównej do ich zachowania w tajemnicy również po ustaniu stosunku pracy lub innego stosunku cywilnoprawnego łączącego dany podmiot z **AceSender**;
  - e) poinformuje **Użytkownika** o każdym przypadku naruszenia zobowiązań wynikających z niniejszej umowy niezwłocznie, nie później niż w terminie 2 dni roboczych od chwili stwierdzenia naruszenia;
  - f) podejmuje wszelkie środki wymagane na mocy art. 32 RODO;
  - g) przetwarza dane osobowe wyłącznie na udokumentowane polecenie **Użytkownika** zgodnie z Umową Główną i Zleceniami – co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej – chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega **AceSender**; w takim przypadku przed rozpoczęciem przetwarzania **AceSender** informuje **Użytkownika** o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny;
  - h) w miarę możliwości będzie pomagać **Użytkownikowi** - poprzez odpowiednie środki techniczne i organizacyjne - wywiązać się z obowiązku odpowiadania na żądania osoby, której Dane Osobowe dotyczą, w zakresie wykonywania praw tej osoby określonych w art.

32-36 RODO – realizowane jest to bez dodatkowych opłat na poziomie dostępnych funkcjonalności Programu; w innych przypadkach realizowane jest to na podstawie Regulaminu Serwisu;

- i) uwzględniając charakter przetwarzania Danych Osobowych oraz dostępne informacje **AceSender** - wyłącznie w zakresie związanym z wykonywaniem Umowy Głównej - w miarę możliwości pomaga **Użytkownikowi** poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III - realizowane jest to bez dodatkowych opłat na poziomie dostępnych funkcjonalności Programu; w innych przypadkach realizowane jest to na podstawie Regulaminu Serwisu usuwa dane po zakończeniu trwania Umowy Głównej w terminie wskazanym w ust. 3.7 pkt. a) z możliwością nieusuwania danych jeżeli jest to niezbędne do ustalenia, dochodzenia lub obrony roszczeń prawnych (art. 17 ust. 3 pkt. e RODO);
- j) wyłącznie w zakresie związanym z wykonywaniem Umowy Głównej udostępni **Użytkownikowi** wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 RODO przez **AceSender** oraz umożliwia **Użytkownikowi** lub audytorowi upoważnionemu przez **Użytkownika** przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich na zasadach zgodnych z § 6 ust. 3. niniejszej umowy;
- k) całkowita odpowiedzialność **AceSender**, niezależnie od liczby i podstawy roszczeń **Użytkownika** ograniczona jest do równowartości wynagrodzenia **AceSender** za okres 3 (trzech) miesięcy, zapłaconego przez **Użytkownika** za wykonywanie Umowy Głównej w okresie rozliczeniowym bezpośrednio poprzedzającym datę, w której doszło do zdarzenia wywołującego szkodę. **Użytkownik** zwalnia **AceSender** z wszelkich zobowiązań przekraczających powyższe ograniczenie.

7. **Użytkownik** zobowiązuje się do:

- a) pobrania wszystkich Danych Osobowych wprowadzonych przez siebie do Programu lub polecenia **AceSender** usunięcia z Programu wszystkich powierzonych Danych Osobowych - wraz z rozwiązaniem Umowy Głównej oraz niniejszej Umowy. W przypadku niedokonania tych czynności w ciągu 30 dni, **AceSender** będzie uprawniony usunąć Dane Osobowe bez powiadamiania o tym **Użytkownika**. Jeśli **Użytkownik** zdecyduje się pobrać Dane Osobowe wcześniej powierzone **AceSender**, to **AceSender** również usuwa wszystkie kopie zapasowe Danych Osobowych;
- b) zwolnienia **AceSender** ze wszelkich obowiązków informacyjnych względem osób, których Dane Osobowe są wykorzystywane w ramach Zlecenia oraz do wypełnienia tych obowiązków samodzielnie – pod rygorem wszelkiej odpowiedzialności przewidzianej

odpowiednimi przepisami prawa, a także pod rygorem odpowiedzialności odszkodowawczej wobec **AceSender**;

- c) samodzielnego ustanawiania i odwoływania Osób upoważnionych tak, aby osoby nieuprawnione nie miały dostępu do Danych Osobowych ani możliwości przekazywania Zleceń do **AceSender**;
- d) wykonania żądań osób, których dotyczą Dane Osobowe oraz przygotowania odpowiedzi na te żądania;
- e) zaspokojenia roszczeń osób, których Dane Osobowe są przetwarzane, z tytułu szkód wywołanych na skutek nieprawidłowego przetwarzania Danych Osobowych, chyba że wykaże, że szkoda wynikłą z wyłącznej winy **AceSender** lub jego podwykonawców.

#### **§4. Obowiązki Umowy**

1. Niniejsza Umowa obowiązuje Strony od dnia 25 maja 2018 roku lub jeżeli umowa Główna została zawarta później – od dnia zawarcia Umowy Główniej, przez dalszy czas obowiązywania Umowy Główniej. **AceSender** będzie przetwarzać Dane Osobowe tylko w okresie obowiązywania Umowy Główniej, z zastrzeżeniem okresu karencji wskazanego w § 3 ust. 7 lit. a) powyżej.
2. Niniejsza Umowa może zostać zmieniona w trakcie trwania Umowy Główniej. **Użytkownik** zostanie poinformowany na co najmniej 10-dni przed planowanym wejściem w życie nowej umowy powierzenia. **AceSender** prześle stosowną wiadomość na adres e-mail **Użytkownika** lub wyświetli powiadomienie w Programie. **Użytkownik** ma prawo rozwiązać w takim wypadku niniejszą umowę jednak spowoduje to także obowiązek rozwiązania Umowy Główniej. Niezgłoszenie chęci rozwiązania niniejszej umowy bądź jej nierozwiązanie do tego czasu poczytuje się za zgodę Użytkownika na świadczenie umowy powierzenia, na zasadach zgodnych z nową umową.
3. Wypowiedzenie Umowy Główniej powoduje wygaśnięcie obowiązywania w stosunku do **Użytkownika** niniejszej Umowy.
4. Wypowiedzenie niniejszej Umowy powoduje uniemożliwienie wykonywania Umowy Główniej przez **AceSender**.

#### **§ 5. Podpowierzenie i przekazywanie danych do państw trzecich**

Zgodnie z § 2 ust. 2 lit. c Umowy, **Użytkownik** wyraża zgodę na podpowierzenie Danych Osobowych podmiotom wskazanym w **załączniku nr 3**. **AceSender** oświadcza, że podmioty te zapewniają co najmniej taki sam poziom bezpieczeństwa danych osobowych, jak wymagany od **AceSender** na podstawie niniejszej umowy. W wypadku przekazywania Danych Osobowych poza teren EOG, do

przekazania dojdzie wyłącznie do krajów, do których przekazanie jest dozwolone zgodnie z art. 45 ust 1 RODO, w tym w szczególności na podstawie decyzji, o której stanowi art. 45 ust. 3 RODO. W razie braku takich decyzji, do przekazania dojdzie zgodnie z art. 46 ust. 1 RODO.

## §6. Postanowienia końcowe

1. Wygaśnięcie niniejszej Umowy, niezależnie od przyczyn, skutkować może niemożnością realizacji Umowy Głównej w całości lub części, o czym **Użytkownik** został poinformowany i co akceptuje.
2. W zakresie nieuregulowanym przez niniejszą umowę zastosowanie znajdą odpowiednie przepisy prawa Unii Europejskiej i prawa polskiego. W przypadku rozbieżności treści niniejszej Umowy oraz Umowy Głównej pierwszeństwo mają postanowienia niniejszej umowy za wyjątkiem zapisów Umowy Głównej, Regulaminu czy innych dokumentów wiążących Strony, odnoszących się do generowania Zlecenia oraz obowiązków **Użytkownika** z nim związanych. Sądem właściwym jest sąd powszechny w Szczecinie, Polska.
3. **Użytkownik** ma prawo przeprowadzić audyt lub inspekcję w siedzibie lub innym miejscu gdzie przetwarzane są dane osobowe przez **AceSender** z zachowaniem umówienia terminu i zatwierdzenia czynności objętych audytem przez Strony. Audyt może zostać przeprowadzony każdorazowo gdy **Użytkownik** ma uzasadnienie, że dane osobowe nie są przetwarzane zgodnie z Umową. W przypadku gdy **AceSender** posiada certyfikację lub jest audytowany przez podmiot uznany przez **Użytkownika**, **Użytkownik** ma prawo odstąpić od własnego audytu i posiłkować się raportem poaudytowym uznanej jednostki lub certyfikatem uzyskanym zgodnie z certyfikacją, o której mowa w RODO. W przypadku jednak jeżeli **Użytkownik** ma przeprowadzić audyt z udziałem wybranego przez siebie audytora to przeprowadzany jest na koszt **Użytkownika**. Audyt nie może prowadzić do zakłócenia pracy **AceSender** lub prowadzić do usiłowania lub naruszenia tajemnic, w tym tajemnicy przedsiębiorstwa. Audytor nie będzie powiązany z podmiotami konkurencyjnymi dla **AceSender**.
4. Zmiana Upoważnionych nie stanowi zmiany niniejszej umowy i nie wymaga aneksu.
5. Niniejsza umowa zostaje zawarta drogą elektroniczną lub w innej formie zgodnie z Umową Główną.
6. Strony zobowiązują się dołożyć wszelkich starań przy rozwiązywaniu wszelkich sporów mogących wystąpić w przyszłości w związku z wykonaniem przedmiotu Umowy, w drodze obustronnych uzgodnień i porozumień. W przypadku, gdy powstałego sporu nie da się rozstrzygnąć w sposób określony powyżej, spór będzie rozstrzygany przez sąd właściwy dla siedziby **AceSender**.

7. Jeżeli jakiegokolwiek postanowienia niniejszej Umowy okażą się nieważne nie uchybia to mocy pozostałym, a Strony będą dążyć do zastąpienia nieważnego postanowienia ważnym zapisem odzwierciedlającym pierwotną wolę Stron.

*Umowa została zawarta poprzez akceptację Umowy Głównej w podczas rejestracji Użytkownika w Programie.*

Załączniki:

1. Opis przetwarzania Danych Osobowych;
2. Opis wdrożonych środków organizacyjnych i technicznych służących ochronie danych osobowych;
3. Lista podwykonawców.



# **Załącznik 1 – Opis przetwarzania Danych Osobowych**

## **A. Cel przetwarzania powierzonych Danych**

Dane Osobowe będą przetwarzane przez AceSender w celu korzystania przez Użytkownika z Programu świadczonej przez AceSender.

## **B. Charakter i czynności przetwarzania**

- 1) Przetwarzanie AceSender będzie miało charakter zautomatyzowany oraz niezautomatyzowany. Przetwarzanie Danych Osobowych przez AceSender następować będzie przy wykorzystaniu systemów informatycznych dostarczanych w ramach Programu i obejmować będzie następujące czynności przetwarzania: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, wykonywanie kopii zapasowych Danych Osobowych, a także inne operacje niezbędne do realizacji Programu.
- 2) W ramach przetwarzania Danych Osobowych AceSender nie będzie komunikował się w imieniu Użytkownika bezpośrednio z osobami, których dane dotyczą.
- 3) Rola AceSender ograniczona jest do udostępnienia Użytkownikowi narzędzi Programu do wykorzystania w celu przetwarzania Danych Osobowych. AceSender nie ma wpływu na zakres Danych Osobowych przetwarzanych przez Użytkownika w Usłudze, nie ustala celów i sposobów ich przetwarzania i nie monitoruje zakresu takich Danych.

## **C. Kategorie osób, których dotyczą dane**

Użytkownik powierza AceSenderowi przetwarzanie Danych Osobowych następujących kategorii osób:

- 1) Kontakty – w tym osoby, których Dane Osobowe znajdują się na Liście Kontaktów lub których Dane Osobowe są zbierane i przechowywane przy pomocy Programu, lub do których Użytkownik będzie kierował komunikację za pomocą Programu, w szczególności mogą nimi być kontrahenci, klienci, potencjalni klienci, osoby kontaktowe u partnerów biznesowych Użytkownika, subskrybenci newslettera Użytkownika;
- 2) osoby, których dane gromadzone są poprzez formularze.

Program nie jest przeznaczony do przetwarzania szczególnych kategorii danych osobowych, o których mowa w art. 9 RODO, danych osobowych dotyczących wyroków skazujących i naruszeń prawa o których mowa w art. 10 RODO, ani też danych osobowych dzieci. Decydując się umieścić w usłudze dane, Użytkownik potwierdza, że środki zabezpieczeń wdrożone przez AceSender są w jego ocenie wystarczające do ochrony powierzonych Danych Osobowych.

## **D. Kategorie powierzonych Danych Osobowych**

Użytkownik powierza AceSender do przetwarzania następujące kategorie Danych Osobowych:

- 1) w odniesieniu do Kontaktów:
  - a) adres e-mail.  
- Program daje możliwość przetwarzania również dodatkowych informacji, tj.:
  - b) imię i nazwisko
  - c) nazwę firmy
  - d) numer telefonu
  - e) płeć, data urodzin
  - f) miejsce pracy
  - g) dane adresowe kontaktu (Ulica, Miasto, Kod pocztowy, Województwo)
- 2) Dane Osobowe zawarte w treściach wysyłanych przez Użytkownika przy pomocy Programu
- 3) dodatkowe informacje o Kontakcie wpisane przez Użytkownika (komentarz).
- 4) w odniesieniu do osób, których dane gromadzone są przez formularze: adres email. Program daje możliwość przetwarzania również dodatkowych informacji, takich jak w odniesieniu do Kontaktów - zależnie od wyboru Użytkownika.
- 5) w odniesieniu do wszystkich powyższych kategorii: dane przetwarzane automatycznie w toku korzystania z Programu (dane o korzystaniu z Programu; dane gromadzone przy użyciu plików cookie lub innych technologii służących do śledzenia aktywności użytkowników; dane IP urządzenia, z którego dokonano zapisu do listy Kontaktów Użytkownika lub na którym otworzył maila wysłanego do niego przez Użytkownika w ramach korzystania z Programu; dane o lokalizacji, dane o przeglądarce internetowej).

## **Załącznik nr 2. Opis wdrożonych środków organizacyjnych i technicznych służących ochronie danych osobowych.**

### **A. Organizacyjne środki bezpieczeństwa.**

#### Organizacja bezpieczeństwa danych i zarządzanie dostępem.

- 1) AceSender czuwa nad każdym etapem przetwarzania danych osobowych odbywającym się w infrastrukturze informatycznej AceSender w ramach czynności wykonywanych przez osoby uprawnione.
- 2) AceSender zarządza uprawnieniami i dostępem do czynności wykonywanych przez osoby uprawnione wewnątrz organizacji, zapewniając pełną rozliczalność operacji.
- 3) Zapewniono, iż osobom uprawnionym do przetwarzania danych osobowych przydzielane są minimalne uprawnienia dostępu, uzależnione od realizowanych zadań.
- 4) Zapewniono, iż uprawnienia dostępu do danych osobowych są doraźnie monitorowane i kontrolowane.
- 5) Zapewniono, iż dla każdej osoby uprawnionej do dostępu do systemu informatycznego, elementu infrastruktury informatycznej lub sieci nadawany jest unikalny identyfikator, który nie może zostać przypisany innej osobie.
- 6) Przeprowadzane są przeglądy dostępu wszystkich użytkowników, kont systemowych, kont testowych oraz kont ogólnych.
- 7) Zapewniono, iż dla każdej osoby uprawnionej do dostępu do systemu informatycznego, elementu infrastruktury informatycznej lub sieci autoryzacja realizowana jest przy użyciu bezpiecznych metod transmisji danych służących do uwierzytelnienia.
- 8) Zapewniono, iż ustanowione dla każdej osoby uprawnionej do dostępu do systemu informatycznego, elementu infrastruktury informatycznej lub sieci hasło dostępu podlega zmianie w ustalonym okresie czasu.
- 9) AceSender stosuje standard bezpiecznego przekazywania haseł w przypadku konieczności przekazania użytkownikowi systemu informatycznego hasła tymczasowego.
- 10) AceSender stosuje standard dotyczący tworzenia bezpiecznych haseł użytkowników systemów informatycznych.
- 11) Osoby uprawnione wewnątrz organizacji do przetwarzania danych osobowych posiadają gruntowne przeszkolenie oraz wiedzę teoretyczną i praktyczną z zakresu bezpieczeństwa informatycznego.

#### Bezpieczeństwo Programu

- 1) Elementy infrastruktury sieciowej służącej do przetwarzania danych osobowych zabezpiecza się przed utratą dostępności poprzez zastosowanie i zapewnienie usług serwisowych świadczonych przez producentów i dystrybutorów.

- 2) Przeprowadzane jest okresowe skanowanie luk bezpieczeństwa na platformach i sieciach przetwarzających dane osobowe w celu zapewnienia zgodności z powszechnymi normami bezpieczeństwa związanymi konkretnie z wzmocnieniem systemu.

#### Zarządzanie incydentami

AceSender na bieżąco reaguje na incydenty naruszenia bezpieczeństwa, stosując środki techniczne które umożliwiają wykrywanie, badanie, reagowanie, łagodzenie skutków i powiadamianie o zdarzeniach, które obejmują zagrożenie dla poufności, integralności i/lub dostępności do danych osobowych.

#### Ochrona prywatności

- 1) AceSender uwzględnia cel w postaci ochrony prywatności w fazie projektowania oprogramowania, w tym poprzez stosowanie niezbędnych zabezpieczeń i minimalizację danych by chronić prawa osób, których dane dotyczą.
- 2) AceSender uwzględnia cel w postaci zachowania zasady ochrony prywatności w ustawieniach domyślnych w fazie projektowania oprogramowania.

### **B. Techniczne środki bezpieczeństwa.**

#### Bezpieczeństwo obszaru przetwarzania

- 1) AceSender, korzysta z usług zaufanych podwykonawców, zapewniających bezpieczeństwo serwerów wykorzystywanych przez AceSender, w tym zapewniając że w zakresie serwerów:
  - a) budynki i obszary, w których znajdują się pomieszczenia i ich części służące do przetwarzania danych osobowych zabezpiecza się przed dostępem osób nieuprawnionych poprzez zastosowanie systemów kontroli dostępu, systemu sygnalizacji włamania i napadu, systemu dozoru realizowanego przez pracowników ochrony fizycznej, zamków mechanicznych lub szyfrowych;
  - b) budynki i obszary, w których znajdują się pomieszczenia i ich części służące do przetwarzania danych zabezpiecza się przed pożarem poprzez zastosowanie drzwi o podwyższonej klasie odporności na ogień;
  - c) budynki i obszary, w których znajdują się pomieszczenia i ich części służące do przetwarzania danych zabezpiecza się przed zniszczeniem na skutek pożaru lub zalania poprzez zastosowanie systemu alarmu pożarowego oraz systemu sygnalizacji włamania i napadu;
  - d) budynki i obszary, w których znajdują się pomieszczenia i ich części służące do przetwarzania danych zabezpiecza się w celu monitorowania oraz identyfikowania

zagrożeń i zdarzeń niepożądanych przez zastosowanie systemu telewizji przemysłowej.

- 2) AceSender zapewnia bezpieczeństwo punktów dostępowych wykorzystywanych przez AceSender w celu komunikacji z serwerami, zapewniając m.in. że:
  - a) punkty dostępowe znajdują się w pomieszczeniach chronionych przeciwwłamaniowymi zamkami mechanicznymi i roletami przeciwwłamaniowymi;
  - b) pomieszczenia w których znajdują się punkty dostępowe są objęte stosowaną w budynku, zatwierdzoną przez straż pożarną, instalacją przeciwpożarową.

#### Bezpieczeństwo transmisji danych

- 1) Dane osobowe przekazywane drogą teletransmisji zabezpiecza się przed utratą poufności i integralności przy pomocy kryptograficznych środków ochrony danych osobowych (szyfrowanie danych w tranzycie).
- 2) Dane osobowe przekazywane drogą teletransmisji zabezpiecza się przed utratą poufności poprzez zastosowanie segmentacji sieci teleinformatycznych (segmentacja sieci).
- 3) Klucze szyfrujące służące do zabezpieczenia teletransmisji danych przechowywane są w bezpiecznym miejscu z zarządzaniem dostępem do nich oraz z wykazaną możliwością odtwarzania klucza.

#### Bezpieczeństwo nośników danych

- 1) Dane osobowe przechowywane na nośnikach danych w stanie spoczynku zabezpiecza się przed utratą poufności i integralności przy pomocy kryptograficznych środków ochrony danych osobowych. (szyfrowanie danych w spoczynku)
- 2) Dane osobowe przechowywane na nośnikach danych zabezpiecza się przed utratą poufności poprzez zastosowanie fizycznej lub logicznej separacji danych. (separacja danych)
- 3) Dane osobowe przechowywane na nośnikach danych zabezpiecza się przed utratą dostępności i integralności poprzez zastosowanie mechanizmów tworzących kopie danych w czasie rzeczywistym. (replikacja danych)
- 4) Dane osobowe przechowywane na nośnikach danych zabezpiecza się przed utratą dostępności i integralności poprzez zastosowanie mechanizmów tworzących przyrostowe lub całościowe kopie bezpieczeństwa danych w ustalonym interwale czasowym. (backup danych)
- 5) Dane osobowe przechowywane na nośnikach danych zabezpiecza się przed utratą dostępności poprzez zastosowanie mechanizmów i procedur przywracania danych, przełączania źródeł danych oraz odtwarzania kopii bezpieczeństwa danych.

- 6) Nośniki danych (dyski twarde) służące do przetwarzania danych osobowych, przed zainstalowaniem w urządzeniu, zabezpiecza się przed dostępem osób nieuprawnionych poprzez ograniczenie i kontrolę dostępu realizowaną za pomocą szaf pancernych i sejfów.
- 7) Nośniki danych (dyski twarde) służące do przetwarzania danych osobowych zabezpiecza się przed utratą poufności danych przez zastosowanie wbudowanych procedur kryptograficznej ochrony danych. (kryptograficzna ochrona nośników danych)
- 8) Nośniki danych (dyski twarde) służące do przetwarzania danych osobowych zabezpiecza się przed utratą dostępności poprzez zastosowanie systemów automatycznego monitoringu działania, wykorzystania pojemności i czasu dostępności.
- 9) Nośniki danych służące do przetwarzania danych osobowych zabezpiecza się przed niedozwolonym wykorzystaniem poprzez zastosowanie procedur użycia i konfiguracji elementów infrastruktury informatycznej (zarządzanie konfiguracją).
- 10) Nośniki danych służące do przetwarzania danych osobowych przeznaczone do ponownego wykorzystania zabezpiecza się przed ujawnieniem danych osobie nieuprawnionej lub systemowi informatycznemu poprzez zastosowanie bezpiecznych metod usuwania danych.
- 11) Nośniki danych służące do przetwarzania danych osobowych przeznaczone do likwidacji zabezpiecza się przed ponownym wykorzystaniem poprzez trwałe i celowe mechaniczne uszkodzenie.

#### Bezpieczeństwo baz danych

- 1) Dane osobowe przechowywane w bazach danych zabezpiecza się przed utratą integralności poprzez zastosowanie reguł spójności w zakresie semantycznym (definicja typu danych), zakresie encji (definicja kluczy podstawowych) oraz w zakresie referencyjnym (definicja kluczy obcych).
- 2) Dane osobowe zabezpiecza się przed utratą rozliczalności poprzez zastosowanie rozwiązań pozwalających przypisać określone działania konkretnej osobie lub systemowi informatycznemu.

#### Bezpieczeństwo infrastruktury informatycznej

- 1) Dane osobowe zabezpiecza się przed utratą poufności za pomocą bezpiecznych metod uwierzytelniania dostępu dla osób i systemów informatycznych.
- 2) Dane osobowe zabezpiecza się przed utratą poufności i dostępności za pomocą monitorowania poprawności działania oraz sposobu użycia bezpiecznych metod uwierzytelniania dostępu dla osób i systemów informatycznych.

- 3) Dane osobowe zabezpiecza się przed utratą dostępności poprzez zastosowanie dodatkowych, zapasowych i awaryjnych źródeł zasilania infrastruktury informatycznej służącej do przetwarzania danych osobowych.
- 4) Elementy infrastruktury informatycznej służącej do przetwarzania danych osobowych (komputery, serwery, urządzenia sieciowe) zabezpiecza się przed dostępem osób nieuprawnionych oraz systemów informatycznych przez zastosowanie bezpiecznych metod uwierzytelniania dostępu.
- 5) Elementy infrastruktury informatycznej służącej do przetwarzania danych osobowych zabezpiecza się przed dostępem osób nieuprawnionych, systemów informatycznych oraz utratą dostępności poprzez monitorowanie aktualności systemu operacyjnego i zainstalowanego oprogramowania.
- 6) Elementy infrastruktury informatycznej służącej do przetwarzania danych osobowych zabezpiecza się przed dostępem osób nieuprawnionych, systemów informatycznych oraz utratą dostępności poprzez zastosowanie oprogramowania typu Firewall, Anty DDOS.
- 7) Elementy infrastruktury informatycznej służącej do przetwarzania danych osobowych zabezpiecza się przed utratą dostępności poprzez zastosowanie automatycznych procesów monitorowania dostępności, obciążenia i wydajności.
- 8) Elementy infrastruktury informatycznej służącej do przetwarzania danych osobowych zabezpiecza się przed utratą dostępności poprzez zastosowanie zapasowych źródeł zasilania oraz automatycznych procedur zmiany źródła zasilania.
- 9) Punkty dostępowe AceSender chronione są poprzez silne szyfrowanie dysków.
- 10) punkty dostępowe AceSender wymagają logowania w sposób identyfikujący użytkownika.
- 11) punkty dostępowe AceSender posiadają regularnie aktualizowane oprogramowanie systemowe oraz antywirusowe.

## Załącznik nr 3 – Lista podwykonawców

Podczas świadczenia usług program, korzysta ze wsparcia zewnętrznych podwykonawców, którym przekazuje dane osobowe na zasadzie powierzenia lub udostępnienia. Podwykonawcy wskazani poniżej świadczą usługi obejmujące niektóre funkcjonalności Programu, takie jak wysyłanie email, usługi hostingu, wsparcia w obsłudze Użytkownika, obsługa płatności.

### Lista podwykonawców

Nazwa i dane kontaktowe pod-procesora	Kategorie przetwarzania	Czas trwania przetwarzania	Nazwy państw trzecich lub organizacji międzynarodowych, do których dane są przekazywane
PayU S.A. ul. Grunwaldzka 186, 60-166 Poznań, Polska <a href="https://corporate.payu.com/data-subject-request/">https://corporate.payu.com/data-subject-request/</a>	Dane udostępnianie podwykonawcy działającemu jako niezależny administrator danych w celu przeprowadzenia transakcji płatniczych inicjowanych przez użytkownika w celu opłacenia usług w systemie acesender.	Ustalany przez podwykonawcę jako niezależnego administratora	Nie dotyczy
Elastic Email Inc. Unit 107 1208 Wharf Street Victoria, British Columbia, Canada V8W 3B9 Tax ID: 847034899RC0001 <a href="mailto:privacy@elasticemail.com">privacy@elasticemail.com</a>	Udostępnienie i utrzymywanie zdalnej platformy programistycznej pozwalającej na wysyłanie wiadomości e-mail przez Użytkownika do jego odbiorców i gromadzeniu statystyk na temat skuteczności dostarczania wiadomości w środowisku sprzętowo-programowym wynajętym przez przetwarzającego.	Do czasu gdy umowa główna lub umowa powierzenia przetwarzania danych osobowych nie wygaśnie lub zostanie wypowiedziana przez którąkolwiek z stron.	Kanada zapewniająca ekwiwalentną do RODO ochronę prawną w zakresie ochrony danych osobowych



