

Privacy Policy

Effective date: March 10th, 2026

Version [11]

At Learn2Esport, we take your privacy seriously. We do not use student personal data or de-identified student data for advertising, marketing, product promotion, or commercial profiling. Student data is processed solely to provide and improve the educational service to the institution.

Please read this Privacy Policy to learn how we treat your personal data.

For Consumer Accounts. By accessing or using the Services, you acknowledge that you have read and understood this Privacy Policy and that we may collect, use, and disclose your personal data as described herein.

For Institution Accounts. "Institution Accounts" are accounts created, purchased, or administered by a school, district, university, company, organization, or other entity that makes the Services available to its students, employees, staff, contractors, or other authorized users. For Institution Accounts, Learn2Esport processes personal data on behalf of, and under the instructions of, the applicable institution or organization in accordance with the relevant service agreement, data processing agreement, and applicable law. Access to or use of the Services by a student, educator, staff member, or other authorized user of an Institution Account does not, by itself, constitute separate consent to the collection, use, disclosure, or international transfer of personal data beyond what is authorized by the institution or organization and applicable law.

Remember that your use of Learn2Esport's Services is at all times subject to our Terms of Use (can be found here: <https://app.gameplan.com/tos>), which incorporates this Privacy Policy. Any terms we use in this Policy without defining them have the definitions given to them in the Terms of Use.

As we continually work to improve our Services, we may need to change this Privacy Policy from time to time. When we do, a new version of the Privacy Policy will be posted on our website (can be found here: <https://app.gameplan.com/privacy-policy>). They take effect only if you agree with the changes.

Privacy Policy Table of Contents

What this Privacy Policy Covers

Personal Data

- [– Categories of Personal Data We Collect](#)*
- [– Categories of Sources of Personal Data](#)*
- [– Our Business Purposes for Collecting or Disclosing Personal Data](#)*

How We Disclose Your Personal Data

How We Use Cookies

Data Security

Personal Data of Children

Personal Data of Children (B2C Services)

State Law Privacy Rights

European Union and United Kingdom Data Subject Rights

[Contact Information](#)

What this Privacy Policy Covers

This Privacy Policy covers how we treat Personal Data that we gather when you access or use our Services. “Personal Data” means any information that identifies or relates to a particular individual and also includes information referred to as “personally identifiable information” or “personal information” under applicable data privacy laws, rules or regulations. This Privacy Policy does not cover the practices of companies we don’t own or control or people we don’t manage.

Personal Data

Categories of Personal Data We Collect

This chart details the categories of Personal Data that we collect:

<u>Category of Personal Data</u>	<u>Examples of Personal Data We Collect</u>	<u>Categories of Third Parties With Whom We Share this Personal Data:</u>
Profile or Contact Data	• First and last name • Email • Unique identifiers such as passwords • Student, Educator or Other (text input)	• Service Providers • Parties You Authorize, Access or Authenticate
Payment Data	• Financial account information • Payment card type • Last 4 digits of payment card • Billing address, phone number, and email	• Service Providers (specifically our payment processing partner, currently Stripe, Inc. and Chargebee Inc.)
Device/IP Data	• IP address • Type of device/operating system/browser used to access the Services • Cookies used to store authentication data • Data on who is logged in • Voucher authentication data	• Service Providers
Geographic Data	• Country • State • District (if applicable) • School (if applicable)	• Service Providers • Parties You Authorize, Access or Authenticate
Social Network Data	• Email • User name or other identifiers	• Service Providers • Parties You Authorize, Access or Authenticate
Consumer Demographic Data	• Age / date of birth • Gender & Ethnicity (optional)	• Service Providers • Parties You Authorize, Access or Authenticate
Professional or Employment-Related Data	• Job title	• Service Providers • Parties You Authorize, Access or Authenticate
Non-Public Education Data	• Grades, transcripts, or other feedback • Classes enrolled in • Identifying information in student assignments or discussions	• Service Providers • Parties You Authorize, Access or Authenticate

Photos, Videos and Recording	• Photos, videos or recordings of you • Photos, videos or recordings of your environment	• Service Providers • Parties You Authorize, Access or Authenticate
Other Identifying Information that You Voluntarily Choose to Provide	• Identifying information in any Content, emails, letters, texts, or other communication you send us or disclose through the Services	• Service Providers • Parties You Authorize, Access or Authenticate

Categories of Sources of Personal Data

We collect Personal Data about you from the following categories of sources:

- **You**
 - When you provide such information directly to us.
 - When you create an account or use our interactive tools and Services.
 - When you voluntarily provide information in free-form text boxes through the Services or through responses to surveys or questionnaires.
 - When you send us an email or otherwise contact us.
 - When you use the Services and such information is collected automatically.
 - Through Cookies (defined in the “How We Use Cookies” section below).
 - If you use a location-enabled browser, we may receive information about your location.
- **Third Parties**
 - Sub-processors
 - These providers process anonymized data only on our behalf and under our instructions to operate, secure, and improve the educational service for the Institution. They are contractually prohibited from using the data for advertising, marketing, profiling, or any independent commercial purpose, and may not sell or share the data with other parties.

Our Business Purposes for Collecting or Disclosing Personal Data

- **Providing, Customizing and Improving the Services**
 - Creating and managing your account or other user profiles.
 - Processing orders or other transactions; billing.
 - Providing you with the products, services or information you request.
 - Meeting or fulfilling the reason you provided the information to us.
 - Providing support and assistance for the Services.
 - Personalizing the Services, website content and communications based on your preferences.
 - Doing fraud protection, security and debugging.

- Carrying out other business purposes stated when collecting your Personal Data or as otherwise set forth in applicable data privacy laws.

With respect to education records and other institution-provided student data, Learn2Esport acts as a school official or service provider performing an institutional service for the Institution, is under the Institution's direct control regarding the use and maintenance of such data, and will use such data only for the purposes set forth in the Agreement and the Institution's written instructions. Learn2Esport shall not disclose such data except as permitted by law and this Agreement.

- **Educational Content Integrations**

- YouTube API: Our Product integration with the YouTube API Service allows our customers to utilize certain YouTube services directly in our Services. For example, educators can embed videos into course materials. For more information about the YouTube API Service, please refer to YouTube's [Terms of Service](#). You can learn more about how YouTube uses your personal information in the [Google Privacy Policy](#).

- **Corresponding with You**

- Responding to correspondence that we receive from you, contacting you when necessary or requested, and sending you information about Learn2Esport or the Services.

- **Meeting Legal Requirements and Enforcing Legal Terms**

- Fulfilling our legal obligations under applicable law, regulation, court order or other legal process, such as preventing, detecting and investigating security incidents and potentially illegal or prohibited activities.
- Protecting the rights, property or safety of you, Learn2Esport or another party.
- Enforcing any agreements with you.
- Responding to claims that any posting or other content violates third-party rights.
- Resolving disputes.

We will not collect additional categories of Personal Data or use the Personal Data we collected for materially different, unrelated or incompatible purposes without providing you notice.

How We Disclose Your Personal Data

We disclose your Personal Data to the categories of service providers and other parties listed in this section. For more information, please refer to the state-specific sections below.

- **Service Providers.** These parties help us provide the Services or perform business functions on our behalf. They include:
 - Hosting, technology and communication providers.
 - Security and fraud prevention consultants.
 - Support and customer service providers.
 - Content and certification providers.
 - Payment processors.
 - Our payment processing partners Stripe, Inc. ("Stripe") and Chargebee Inc. ("Chargebee") collect your voluntarily-provided payment card information necessary to process your payment.

- Please see Stripe’s and/or Chargebee’s terms of service and privacy policy for information on its use and storage of your Personal Data.
- **Parties You Authorize, Access or Authenticate**
 - Your Institution (as defined below).
 - Third parties you access through the services.
 - Social media services.
 - Other users.

Legal Obligations

We may share any Personal Data that we collect with third parties in conjunction with any of the activities set forth under “Meeting Legal Requirements and Enforcing Legal Terms” in the “Our Business Purposes for Collecting Personal Data” section above.

Business Transfers

All of your Personal Data that we collect may be transferred to a third party if we undergo a merger, acquisition, bankruptcy or other transaction in which that third party assumes control of our business (in whole or in part). Should one of these events occur, we will make reasonable efforts to notify you before your information becomes subject to different privacy and security policies and practices.

How We Use Cookies

Session and Authentication Cookies

When you sign in, we place a small number of cookies on your device to keep you logged in and manage your session. These cookies contain a random session identifier and are transmitted securely over HTTPS. One additional cookie allows the application to warn you before your session expires.

We do not use cookies for advertising, and we do not use cookies for cross-site tracking.

Security and Operational Logging

When you sign in, we record your IP address, browser type, and the page you came from (referrer). Your IP address is stored in encrypted form and is used to determine your approximate location (city and country level only). This information helps us monitor for unauthorized access and maintain the security of our platform.

During normal use of the Services, we may log basic request information, including your IP address and browser type, for operational, security, and troubleshooting purposes. These logs are retained for one week and then deleted or anonymized, unless a longer retention period is required to investigate or prevent security incidents, comply with legal obligations, or resolve disputes.

Data Security

We seek to protect your Personal Data from unauthorized access, use and disclosure using appropriate physical, technical, organizational and administrative security measures based on the type of Personal Data and how we are processing that data. You should also help protect your data by appropriately selecting and protecting your password and/or other sign-on mechanism; limiting access to your computer or device and browser; and signing off after you have finished accessing your account. Although we work to protect the security of your account and other data that we hold in our records, please be aware that no method of transmitting data over the internet or storing data is completely secure.

Data Retention

We retain Personal Data about you for as long as necessary to provide you with our Services or to perform our business purposes for collecting your Personal Data. When establishing a retention period for specific categories of data, we consider who we collected the data from, our need for the Personal Data, why we collected the Personal Data, and the sensitivity of the Personal Data. In some cases we retain Personal Data for longer, if doing so is necessary to comply with our legal obligations, resolve disputes or collect fees owed, or is otherwise permitted or required by applicable law, rule or regulation.

For example:

- We retain your profile information and credentials for as long as you have an account with us.
- We retain your payment data for as long as we need to process your purchase or subscription.
- We retain your device/IP data for as long as we need it to ensure that our systems are working appropriately, effectively and efficiently.

Family Educational Rights and Privacy Act

In the event the Services are provided to you by your Institution (as defined below), certain Personal Data may be subject to the Family Educational Rights and Privacy Act, 34 C.F.R. §99 et seq. ("FERPA"). We remain under the "direct control" of the institution, such as your school or school district (the "Institution"), that we provide the Services to with respect to the use and handling of any FERPA-protected "education records."

Personal Data of Children

We use the Personal Data of children under the age of 13 only to support the legitimate educational interests of the Institution as governed by the agreement with the Institution, and we require Institutions to obtain any necessary consents to use and deploy the Services, including those under the Children's Online Privacy Protection Act ("COPPA").

If you believe that a participant under 13 years of age has provided us with Personal Information (beyond the Required Information) without our obtaining Parental Consent, please contact us at info@gameplan.com. We do not condition use of the Services on disclosure of more Personal Data from any person under 13 years of age than is reasonably necessary for that participation, and we do not

retain Personal Data from children under 13 years of age longer than is reasonably necessary in order to fulfill the purpose for which it was disclosed.

If you are a parent or guardian of a user of the Services who is under 13 years of age, please contact the Institution to address your rights with respect to such data in the first instance.

Personal Data of Children (B2C Services)

When we provide our Services directly to individual consumers (B2C)—such as when students register independently to access our Services—we take special precautions regarding the collection and use of Personal Data from minors.

Age Requirements and Parental Consent:

- Minimum age for use:
 - Users in the United States, United Kingdom, and other non-EU jurisdictions must be 13 years or older to use our Services independently.
 - Users under 13 must provide a parental email address to obtain verifiable parental consent before accessing age-restricted parts of the Services, including exams.
 - Users in the European Union must be 16 years or older to access our Services independently, unless specific member state laws provide for a lower age (not less than 13).
 - Where required, we may request confirmation of the user’s age and seek parental consent as necessary.
- We ask all users to confirm their country of residence and age before taking part in exams or other key activities to ensure compliance with applicable child privacy laws (e.g., COPPA, GDPR).
- Where parental consent is required and not obtained, we will not permit access to key features of the Services and will delete the child’s information as required by law.

State Law Privacy Rights

California Resident Rights

Under California Civil Code Sections 1798.83-1798.84, California residents are entitled to contact us to prevent disclosure of Personal Data to third parties; in order to submit such a request, please contact us at info@gameplan.com.

Nevada Resident Rights

If you are a resident of Nevada, you have the right to opt-out of the sale of certain Personal Data to third parties. You can exercise this right by contacting us at info@gameplan.com with the subject line “Nevada Do Not Sell Request” and providing us with your name and the email address associated with your

account. Please note that we do not currently sell your Personal Data as sales are defined in Nevada Revised Statutes Chapter 603A.

European Union and United Kingdom Data Subject Rights

EU and UK Residents

If you are a resident of the European Union (“EU”), United Kingdom (“UK”), Lichtenstein, Norway or Iceland, you may have additional rights under the EU or UK General Data Protection Regulation (the “GDPR”) with respect to your Personal Data, as outlined below.

For this section, we use the terms “Personal Data” and “processing” as they are defined in the GDPR, but “Personal Data” generally means information that can be used to individually identify a person, and “processing” generally covers actions that can be performed in connection with data such as collection, use, storage and disclosure. Learn2Esport will be the controller of your Personal Data processed in connection with the Services.

If there are any conflicts between this section and any other provision of this Privacy Policy, the policy or portion that is more protective of Personal Data shall control to the extent of such conflict. If you have any questions about this section or whether any of the following applies to you, please contact us at info@gameplan.com. Note that we may also process Personal Data of our customers’ end users or employees in connection with our provision of certain services to customers, in which case we are the processor of Personal Data. If we are the processor of your Personal Data (i.e., not the controller), please contact the controller party in the first instance to address your rights with respect to such data.

Personal Data We Collect

The “Categories of Personal Data We Collect” section above details the Personal Data that we collect from you.

Personal Data Use and Processing Grounds

The “Our Business Purposes for Collecting Personal Data” section above explains how we use your Personal Data.

We will only process your Personal Data if we have a lawful basis for doing so. Lawful bases for processing include consent, contractual necessity and our “legitimate interests” or the legitimate interest of others, as further described below.

- **Contractual Necessity**: We process the following categories of Personal Data as a matter of “contractual necessity”, meaning that we need to process the data to perform under our Terms of Use with you, which enables us to provide you with the Services. When we process data due to contractual necessity, failure to provide such Personal Data will result in your inability to use some or all portions of the Services that require such data. For Institution Accounts, where Learn2Esport processes Institution Data, the legal basis and authority for such processing arise from Learn2Esport’s contract with the Institution, Learn2Esport’s role as processor or school service provider acting on the Institution’s instructions, and other

lawful bases available under applicable law. References in this Privacy Policy to individual consent or direct contractual necessity between Learn2Esport and an individual user do not apply to Institution Data except where applicable law expressly requires individual consent.

- o Profile or Contact Data
 - o Payment Data
 - o Professional or Employment-Related Data
 - o Non-Public Education Data
 - o Photos, Videos and Recording
 - o Other Identifying Information that You Voluntarily Choose to Provide
- **Legitimate Interest:** We process the following categories of Personal Data when we believe it furthers the legitimate interest of us or third parties:
 - o Profile or Contact Data
 - o Payment Data
 - o Device/IP Data
 - o Social Network Data
 - o Consumer Demographic Data
 - o Professional or Employment-Related Data
 - o Non-Public Education Data
 - o Geolocation Data
 - o Photos, Videos and Recording
 - o Other Identifying Information that You Voluntarily Choose to Provide
 - o We may also de-identify or anonymize Personal Data to further our legitimate interests.

Examples of these legitimate interests include (as described in more detail above):

- o Providing, customizing and improving the Services.
 - o Corresponding with you.
 - o Meeting legal requirements and enforcing legal terms.
 - o Completing corporate transactions.
- **Consent:** In some cases, we process Personal Data based on the consent you expressly grant to us at the time we collect such data. When we process Personal Data based on your consent, it will be expressly indicated to you at the point and time of collection.
- **Other Processing Grounds:** From time to time we may also need to process Personal Data to comply with a legal obligation, if it is necessary to protect the vital interests of you or other data subjects, or if it is necessary for a task carried out in the public interest.

Sharing Personal Data

The “How We Share Your Personal Data” section above details how we share your Personal Data with third parties.

EU and UK Data Subject Rights

You have certain rights with respect to your Personal Data, including those set forth below. For more information about these rights, or to submit a request, please email us at info@gameplan.com. Please note that in some circumstances, we may not be able to fully comply with your request, such as if it is frivolous or extremely impractical, if it jeopardizes the rights of others, or if it is not required by law, but

in those circumstances, we will still respond to notify you of such a decision. In some cases, we may also need you to provide us with additional information, which may include Personal Data, if necessary to verify your identity and the nature of your request.

- **Access:** You can request more information about the Personal Data we hold about you and request a copy of such Personal Data. You can also access certain of your Personal Data by logging on to your account.
- **Rectification:** If you believe that any Personal Data we are holding about you is incorrect or incomplete, you can request that we correct or supplement such data. You can also correct some of this information directly by logging on to your account.
- **Erase:** You can request that we erase some or all of your Personal Data from our systems.
- **Withdrawal of Consent:** If we are processing your Personal Data based on your consent (as indicated at the time of collection of such data), you have the right to withdraw your consent at any time. Please note, however, that if you exercise this right, you may have to then provide express consent on a case-by-case basis for the use or disclosure of certain of your Personal Data, if such use or disclosure is necessary to enable you to utilize some or all of our Services.
- **Portability:** You can ask for a copy of your Personal Data in a machine-readable format. You can also request that we transmit the data to another controller where technically feasible.
- **Objection:** You can contact us to let us know that you object to the further use or disclosure of your Personal Data for certain purposes.
- **Restriction of Processing:** You can ask us to restrict further processing of your Personal Data.
- **Right to File Complaint:** You have the right to lodge a complaint about Learn2Esport's practices with respect to your Personal Data with the supervisory authority of your country or EU Member State. A list of Supervisory Authorities is available here: https://edpb.europa.eu/about-edpb/board/members_en.

Transfers of Personal Data

The Services are hosted and operated in the United States ("U.S.") through Learn2Esport and its service providers, and if you do not reside in the U.S., laws in the U.S. may differ from the laws where you reside. By using the Services, you acknowledge that any Personal Data about you, regardless of whether provided by you or obtained from a third party, is being provided to Learn2Esport in the U.S. and will be hosted on U.S. servers.

Contact Information:

If you have any questions or comments about this Privacy Policy, the ways in which we collect and use your Personal Data or your choices and rights regarding such collection and use, please do not hesitate to contact us at:

- <https://gameplan.com>
- info@gameplan.com
- Smedsgränd 3, 753 20 Uppsala, Uppsala, Sweden

Data Processing Agreement for EU customers

This agreement is drafted for the purposes of Article 28(3) of Regulation 2016/679 (the GDPR).

The parties have agreed on the following contractual clauses (the “DPA”) in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subjects.

The following clauses are applicable even if the Data Controller in its processing of personal data is not bound by Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (“General Data Protection Regulation” or “GDPR”), if otherwise is not stated in the specific clause.

1. BACKGROUND

1. This DPA establishes the rights and obligations of the Data Controller and the Data Processor, when processing personal data on behalf of the Data Controller.
2. The DPA has been drafted to ensure the parties’ compliance with Article 28(3) of the General Data Protection Regulation.
3. In the context of the Service provided the Data Controller (as described in the Service Agreement entered into by the Parties), the Data Processor will process personal data on behalf of the Data Controller in accordance with this DPA.

2. RIGHTS AND OBLIGATIONS OF THE DATA CONTROLLER

1. The Data Controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR) and the applicable EU or Member State¹ data protection provisions. This clause is not applicable if the Data Controller is not bound by the GDPR.
2. The Data Controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.
3. The Data Controller shall be responsible, inter alia, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

3. SCOPE OF PROCESSING

1. The Data Processor shall under the Agreement process personal data within the following framework:
 - The purpose of the Data Processor’s processing of personal data on behalf of the Data Controller is to provide the Service as described in the agreement between the Customer and the Data Processor. The Data Processor’s processing of personal data on behalf of the Data Controller shall mainly pertain to personal data obtained and stored on the platform provided as a service. At the platform, data subjects register and submit their data in the context of esports training and tournaments. The service is hosted and maintained by the Data Processor.

¹ References to “Member States” made throughout the Agreement shall be understood as references to “EEA Member States” including the United Kingdom regardless of the outcome of “Brexit”.

- Personal data concerning data subjects using the platform will be processed. Such data will include the following: First and family name, email address, password, IP address, profile picture(s), biography, game account, game journal, results and feedback. Data Processor will furthermore process any additional data that any data subject chooses to submit when using the platform.
- 2. The Data Processor shall process personal data only in accordance with documented instructions from the Data Controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject. Subsequent instructions can be given by the Data Controller throughout the duration of the processing of personal data, but such instructions shall always be provided and kept in writing.
- 3. The Data Processor shall immediately inform the Data Controller if instructions given by the Data Controller, in the opinion of the Data Processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

4. CONFIDENTIALITY

The Data Processor shall only grant access to the personal data being processed on behalf of the Data Controller to persons under the Data Processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

5. SECURITY

1. Pursuant to Article 32 GDPR, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Data Controller and Data Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.
2. Pursuant to Article 32 GDPR, the Data Processor shall also, independently from the Data Controller, evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the Data Controller shall provide the Data Processor with information necessary to identify and evaluate such risks.
3. The Data Processor shall assist the Data Controller in ensuring compliance with the Data Controller's obligations pursuant to Articles 32 GDPR, by *inter alia* providing the Data Controller with information concerning the technical and organisational measures already implemented by the Data Processor pursuant to Article 32 GDPR along with other information necessary for the Data Controller to comply with the Data Controller's obligation under Article 32 GDPR. If subsequently, in the assessment of the Data Controller, mitigation of the identified risks require further measures to be implemented by the Data Processor, than those already implemented by the Data Processor pursuant to Article 32 GDPR, the Data Controller shall in writing specify these additional measures to be implemented. This clause is not applicable if the Data Controller is not bound by the GDPR, insofar it relates to the Data Controllers compliance with the GDPR.
4. The Data Processor may be remunerated for the implementation of additional security measures hereto in accordance with the Service Agreement, subject to any such costs being approved in writing by the Data Controller in advance.

6. SUB-PROCESSORS

1. The Data Processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).

2. The Data Processor shall therefore not engage another processor (sub-processor) for the fulfilment of the DPA without the written authorisation of the Data Controller. The Data Processor shall inform in writing the Data Controller of any intended changes concerning the addition or replacement of sub-processors at least a week in advance, thereby giving the Data Controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). The list of sub-processors already authorised by the Data Controller are the following:

Organization Name	Role	Entity Country
Amazon Web Services, Inc.	Cloud hosting provider	United States
Edlink	Integrations provider	United States
Klaviyo, Inc.	Email delivery	United States
Sendgrid, Inc.	Email delivery	United States
Posthog Product	In-platform survey aggregator	United States
Functional Software, Inc. (Sentry.io)	Error logging	United States
Segment.io, Inc.	Communications services	United States
Crisp IM SAS	Customer support	France
Mixpanel	In-platform insights provider	United States
Clever	Integration provider	United States

3. Where the Data Processor engages a sub-processor for carrying out specific processing activities on behalf of the Data Controller, the same data protection obligations as set out in the DPA shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the DPA and the GDPR. The Data Processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the Data Processor is subject pursuant to the DPA and the GDPR.
4. A copy of such a sub-processor agreement and subsequent amendments shall – at the Data Controller’s request – be submitted to the Data Controller, thereby giving the Data Controller the opportunity to ensure that the same data protection obligations as set out in the DPA are imposed on the sub-processor. Clauses on business-related issues that do not affect the legal data protection content of the sub-processor agreement, shall be excluded from submission to the Data Controller.
5. If the sub-processor does not fulfil its data protection obligations, the Data Processor shall remain fully liable to the Data Controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR, in particular those foreseen in Articles 79 and 82 GDPR, against the Data Controller and the Data Processor, including the sub-processor.

7. ASSISTANCE TO THE DATA CONTROLLER

1. Taking into account the nature of the processing, the Data Processor shall assist the Data Controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the Data Controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR. This entails that the Data Processor shall, insofar as this is possible, assist the Data Controller in the Data Controller's compliance with:
 - a. the right to be informed when collecting personal data from the data subject
 - b. the right to be informed when personal data have not been obtained from the data subject
 - c. the right of access by the data subject
 - d. the right to rectification
 - e. the right to erasure ('the right to be forgotten')
 - f. the right to restriction of processing
 - g. notification obligation regarding rectification or erasure of personal data or restriction of processing
 - h. the right to data portability
 - i. the right to object
 - j. the right not to be subject to a decision based solely on automated processing, including profiling
2. In addition to the Data Processor's obligation to assist the Data Controller, the Data Processor shall, taking into account the nature of the processing and the information available to the Data Processor, notify the Data Controller without undue delay, and in any event no later than 48 hours after becoming aware, of a personal data breach, in order to assist the Data Controller in ensuring compliance with:
 - a. The Data Controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;
 - b. the Data Controller's obligation to without undue delay communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;
 - c. the Data Controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);
 - d. the Data Controller's obligation to consult the competent supervisory authority, prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the Data Controller to mitigate the risk.
3. The Data Processor has right to remuneration for any assistance provided to the Data Controller in accordance with this clause 7, subject to any such costs being approved in writing by the Data Controller in advance.

8. ERASURE AND RETURN OF DATA

Upon termination of the provision of personal data processing services, the Data Processor shall be under obligation to return all the personal data to the Data Controller and delete existing copies unless Union or Member State law requires further storage of the personal data.

9. AUDIT AND INSPECTION

1. The Data Processor shall make available to the Data Controller information necessary to demonstrate compliance with the obligations laid down in Article 28 and the DPA and allow for and contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller.
2. The Data Processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the Data Controller's and Data Processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the Data Processor's physical facilities on presentation of appropriate identification.

10. INDEMNITY

1. The Data Processor agrees to indemnify, keep indemnified and defend at its own expense, the Data Controller against all costs, claims, damages or expenses incurred by the Data Controller or for which the Data Controller becomes liable due to any failure by the Data Processor or its employees, subcontractors or agents to comply with any of its obligations under this DPA or the GDPR or any other applicable data processing legislation.
2. Data Processor is not liable for any indirect or consequential damages under this clause.

11. MISCELLANEOUS

1. The Customer shall ensure that the Data Subjects are provided the Privacy Policy as set out in Exhibit 2 b.
2. The DPA shall be interpreted in accordance with Swedish law without regard to its provisions covering conflict of laws. This shall not hinder a party or a third-party acting on behalf of the party from claiming compensation due to an arbitration award in the jurisdiction that governs the other party's assets and in accordance with the laws of that jurisdiction.
3. Any dispute, controversy, or claim that has not been amicably settled by the parties arising out of or in connection with the DPA or the breach, termination, or invalidity thereof, shall be finally settled by arbitration administered by the Arbitration Institute of the Stockholm Chamber of Commerce (the "SCC"). The Rules for Expedited Arbitrations shall apply, unless the SCC in its discretion determines, taking into account the complexity of the case, the amount in dispute, and other circumstances, that the Arbitration Rules shall apply. In the latter case, the SCC shall also decide whether the Arbitral Tribunal shall be composed of one or three arbitrators.
4. The seat of arbitration shall be Stockholm, Sweden and the language of the arbitral proceedings shall be English.
5. All information disclosed during or otherwise in connection with the arbitral procedure including details of the arbitration proceeding, the arbitration award, settlement, or settlement awards shall be considered confidential information. This shall not prevent a party from seeking compensation due to an arbitration award in the jurisdiction that governs the other party's assets.

12. TERM

The Clauses shall become effective upon acceptance by the Data Controller, be it oral, written, or otherwise. The DPA shall be effective for the duration of the provision of personal data processing services.

*