BILDERLINGS PAY

BILDERLINGS PERSONAL DATA PROCESSING POLICY

Contents

1. About this Policy..... 2
2. Definitions 3
4. Data Protection Principles..... 5
5. Fair and Lawful Processing 6
6. Processing for limited purposes..... 6
7. Categories of Data Subjects..... 7
8. Adequate, Relevant and Non- Excessive Processing 7
9. Accurate Data 8
10. Not kept longer than necessary for the purpose 8
11. Data protection impact assessment 9
12. Records of Processing activities 9
13. Processing in Line with Data Subject's Rights..... 9
14. Data Security.....10
15. Transferring Personal Data to a Country Outside the EEA 12
16. Disclosure and Sharing of Personal Information.....12
17. Subject Access Requests 13
18. Reporting Breaches.....14
19. Document Control 14
Appendix A: Data Processor Security Controls.....15

1. About this Policy

1.1 The types of Personal Data that **Bilderlings Group Companies**[1] ("**Bilderlings**", "**we**", "**us**", "**our**") may be required to handle include information about current, past and prospective suppliers, customers, contractors, and any other users of any of our services (such as Website users) and others that we communicate with for the purposes of carrying out our business. The Personal Data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards including those specified in the General Data Protection Regulation, Regulation (EU) 2016/679 (the "GDPR"), Personal Data Protection Law of Republic of Latvia, UK Data Protection Act (2018) and other regulations.

1.2 This policy and any other documents referred to in it sets out the basis on which we will process any Personal Data we collect from Data Subjects, or that is provided to us by Data Subjects or other sources. Data Users are obliged to comply with this policy when Processing Personal Data on our behalf. Any breach of this policy may result in disciplinary action and statutory responsibility. This policy focuses on our obligations as a Data Controller and we may be under different or additional obligations in respect of any Processing which we carry out as a Data Processor.

1.3 This is actual version of Policy and will be reviewed at least once a year and periodically updated by the Data Protection Officer to reflect any changes in legislation or in our methods or practices. The current issue of the Policy will be available from our website at Bilderlingspay.com or from our Data Protection Officer.

[1] Bilderlings Group Companies are the companies: Bilderlings Pay Limited, a company registered in the UK, company number: 09908958, registered office address: 66 Prescot Street, London, United Kingdom, E1 8NN, FCA reference number: 900637 and Bilderlings Pay SIA, company registered in the Republic of Latvia, reg.no.: 40103869042, legal address: Riga, Pils iela 8/10, LV-1050.

2. Definitions

2.1 **Data Subjects** means all living identifiable individuals about whom we hold Personal Data. A Data Subject does not need to be an EU national or resident. All Data Subjects have legal rights in relation to their personal information.

2.2 **Personal Data** means data relating to a living individual who can be identified, directly or indirectly, from that data (or from that data and other information in our possession). Personal Data can be factual (for example, a name, address or date of birth) or it can be an opinion and description about that person, their actions and behavior.

2.3 **Data Controllers** are the people who, or organizations which, determine the purposes for which, and the manner in which, any Personal Data is processed. They are responsible for establishing practices and policies in line with the GDPR. **Data Users** are those of our employees, agents, partners and contractors whose work involves Processing Personal Data. Data Users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

2.4 **Data Processors** include any person or organization that processes Personal Data on our behalf and on our instructions. Employees of Data Controllers are excluded from this definition, but it could include suppliers that handle Personal Data on our behalf.

2.5 **Website** means our website at https://www.bilderlingspay.com/ .

2.6 **Processing** is any activity or set of activities which is performed on Personal Data or sets of Personal Data, whether or not by automated means. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organizing, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring Personal Data to third parties.

2.7 **Profiling** means any form of automated Processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, locations or movements.

2.8 **Personal Data Processing Policy** is the most recent version of our policy, available via the Website, relating to the collection, storage and use of Personal Data (as amended from time-to-time).

2.9 **Pseudonymisation** means the Processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organization measures to ensure that the Personal Data are not attributed to an identified or identifiable natural person. Note, pseudonymised data is still Personal Data.

2.10 **Sensitive Personal Data** includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. The GDPR includes biometric data and genetic data as Sensitive Personal Data. Sensitive Personal Data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned, if applicable laws do not state otherwise.

2.11 **Services** means: (i) access to the relevant Bilderlings solutions provided via Customer's login link at the Bilderlings website or another designated web site or IP address; and/or (ii) ancillary online or offline products and services provided or licensed to Customer by Bilderlings.

2.12 Register – Bilderlings defined personal data processing Register in accordance with GDPR Article 30.

3. Accountability

3.1 The GDPR accountability principle requires organizations to be able to demonstrate compliance with data protection requirements. We need to ensure data protection compliance is integrated into any new technology planning or new Processing activities.

3.2 The Data Protection Officer ("DPO" hereinafter) is responsible for ensuring compliance with the GDPR and with this policy. Bilderlings have a designated DPO, whose email address is: DPO@bilderlings.eu. Any questions about the operation of this policy or any concerns that

the policy has not been followed should be referred in the first instance to the Data Protection Officer.

3.3 The DPO will be an independent officer, appointed to carry out the following tasks on behalf of Bilderlings:

- Inform and advise us or our Data Processors who carry out Processing activities of their obligations under the GDPR or particular jurisdiction data protection provisions.
- Monitor our compliance with the GDPR, or relevant data protection legislation which may apply to us and monitor our compliance with our policies or the policies of the Data Processor's.
- Provide advice where requested with regards to the data protection impact assessment and monitor its performance.
- To cooperate with the supervisory authority and act as a contact point for the supervisory authority on issues relating to Processing.

3.4 Data Subjects may contact the DPO with regards to all issues related to Processing of their Personal Data and in respect of their rights under the GDPR.

3.5 All Bilderlings employees have a responsibility to comply with the GDPR and are required to complete appropriate training to ensure compliance with this policy. To ensure the DPO has the necessary support in carrying out their obligations, this position reports to Bilderlings Executive Management team.

4. Data Protection Principles

Anyone Processing Personal Data must comply with principles of good practice. These provide that Personal Data must be:

- Processed fairly, lawfully and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed.
- Accurate and where necessary, kept up to date. Where Personal Data is inaccurate with regards to the purpose for which it is processed, every reasonable step must be taken to either erase or rectified it without delay.

- Not kept longer than necessary for the purpose for which the Personal Data is processed.
- Processed in line with Data Subjects' rights.
- Processed in a manner that ensures appropriate security of the Data Subject, including protection against unauthorized Processing and accidental loss, destruction or damage.
- Not transferred to people or organizations situated in countries without adequate protection without putting in place appropriate safeguards.

5. Fair and Lawful Processing

5.1 The GDPR is not intended to prevent the Processing of Personal Data, but to ensure that it is done fairly, transparently and without adversely affecting the rights of the Data Subject. The specific purposes for which Personal Data is being processed should be explicitly and legitimately communicated to the Data Subject's and should be determined at the time of the collection of the Personal Data.

5.2 For Personal Data to be processed lawfully, it must be processed on the basis of one of the legal grounds set out in the GDPR. These include, among other things, the Data Subject's consent to the Processing, or that the Processing is necessary for the performance of a contract with the Data Subject, for the compliance with a legal obligation to which the Data Controller is subject, or for the legitimate interest of the data controller or the party to whom the data is disclosed. When Sensitive Personal Data is being processed, additional conditions must be met. When Processing Personal Data as Data Controllers in the course of our business, we will ensure that those requirements are met.

6. Processing for limited purposes

6.1 In the course of our business, we may collect and Process Personal Data. This may include data we receive directly from a Data Subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, business partners, sub- contractors in technical, payment and delivery services, credit reference agencies and others).

We will only Process Personal Data for the specific purposes set out in our Personal Data Processing Policy or for any other purposes specifically permitted by the GDPR. We will notify those purposes to the Data Subject when we first collect the data. We will continually review our notices to ensure that they accurately reflect our Processing activities and where we

Process the data for a new purpose which was not indicated in the initial notification, then we will provide a new notice to cover this.

7. Categories of Data Subjects

7.1 Bilderlings collects and processes a range of information about you. This includes:

- Your name, surname, address, identity number and/or date of birth;
- contact details, including email address and telephone number;
- copy (hard copy or scanned) of identity document, number, date of issue / validity, issuing authority;
- information about your nationality and residence (including facility payments), bank account, job or employment statuss;
- Other information and data about you, depending on our mutual relationship or any other personal data processed by Bilderlings in accordance with the law, other local legislation or international laws/regulations;

7.2 Bilderlings collects this information in a variety of ways. For example, data is collected through application forms, CVs or resumes; obtained from your passport or ID card; from forms completed by you at the start of or during employment (such as benefit nomination forms); from correspondence with you; or through interviews, meetings or other assessments.

7.3 In some cases, Bilderlings may collect personal data about you from third parties, such as references supplied by former employers, information from employment background check providers, information from credit reference agencies and information from criminal records checks permitted by law, and other justified information from other institutions.

8. Adequate, Relevant and Non- Excessive Processing

8.1 If we collect Personal Data directly from Data Subjects, it will only be:

- Used for the purpose or purposes as set out in our Personal Data Processing Policy or as permitted by the GDPR;
- Processed as set out in our Personal Data Processing Policy or as permitted by the GDPR; and

- Disclosed to the third parties set out in our Personal Data Processing Policy or as permitted by the GDPR.

8.2 If we receive Personal Data about a Data Subject from other sources, we will provide the Data Subject with this information as soon as possible thereafter.

8.3 Bilderlings needs to process data to enter into an customer contract with you and to meet its obligations under your customer contract.

8.4 In some cases, Bilderlings needs to process data to ensure that it is complying with its legal obligations. For example, Anti-Money Laundering laws.

8.5 In other cases, Bilderlings has a legitimate interest in processing personal data before, during and after the end of the employment/contractual relationship.

9. Accurate Data

We will ensure that Personal Data we hold is accurate and kept up to date. We will check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

10. Not kept longer than necessary for the purpose

10.1 We will not keep Personal Data longer than is necessary for the use or provision of the Services and/or the purpose or purposes for which they were collected. The DPO will perform periodic reviews of retained data against the collection schedule.

10.2 Personal Data will only be retained for the period reasonably necessary to perform the Services and to fulfil the purposes as set out in our Personal Data Processing Policy. For example, we will retain Personal Data of Data Subjects whilst they continue to use or contribute to providing the Services and for a reasonable period thereafter, as detailed in the Register, unless a longer retention period is required or permitted by law.

10.3 During the contract term, Customers may export a copy of Customer Data processed by the Services. Within 30 days of termination of the applicable Service, Customers may: 1) request return of Customer Data submitted to the Services; or 2) access their account to export or download Customer Data submitted to Services.

10.4 After termination of the Service, following the 30-day period for return of Customer Data, Customer Data submitted to the Services is retained in inactive status for up to 90 days, after which it is securely overwritten or deleted, if applicable laws do not state otherwise.

11. Data protection impact assessment

11.1 In the event new Processing activities are introduced or we develop new technologies into our business, an assessment of the impact of the change in operations on the protection of such Personal Data shall be carried out in order to address any Processing operations that present a high risk to the rights and freedoms of the Data Subjects or risk non-compliance with the GDPR.

11.2 Such assessment will be carried out with the advice of the Data Protection Officer.

12. Records of Processing activities

We shall maintain a record of the Processing activities (in Register) which we carry out. The record will contain the following information:

- the name and contact details of the Data Controller.
- purpose of the Processing.
- description of the categories of Data Subjects and categories of Personal Data.
- the categories of recipients to whom the Personal Data have been or will be disclosed including recipients in third countries or international organizations and the documentation of suitable safeguards concerning this disclosure.
- Time limits of erasure of the different categories of data.

13. Processing in Line with Data Subject's Rights

13.1 We will Process all Personal Data in line with Data Subjects' rights, in particular their right, in certain circumstances, to:

- Request access to any data held about them by a Data Controller in a commonly used and machine-readable format.
- Transmit their data to another Data Controller (free of charge), where such Personal Data is Processed on the basis of consent or contractual performance, unless in doing so, it would

adversely affect the rights or freedoms of other Data Subject's or others e.g. including trade secrets or intellectual property.

- Prevent the Processing of their data or withdraw their consent at any time in certain circumstances.
- Ask to have inaccurate data amended.
- Erasure of their Personal Data where data is no longer required for the original purpose or where the Data Subject has withdrawn their consent and no other lawful Processing grounds apply.
- Object to the Processing of their Personal Data in certain circumstances.
- Be notified where their Personal Data is subject to automated decision making i.e. Profiling, including the logic involved, as well as the significance and the envisaged consequence of such Processing for the Data Subject and object to such Profiling in certain circumstances.

13.2 Where we are required to provide a copy of Personal Data this will be a free charge, however, any further copies requested may be subject to reasonable fee based on administration costs.

13.3 Where we stop Processing Personal Data or delete a Data Subject's Personal Data, it will possibly mean that that particular Data Subject is unable to continue using or contributing to the provision of some of our Services, and they shall be notified accordingly.

13.4 Where a Data Subject requests to rectify or erase (except data required by any legal obligations) their Personal Data or restrict any Processing of such Personal Data, we may be required to notify, certain third parties to whom such Personal Data has been disclosed of such request.

14. Data Security

14.1 following policy describes how Bilderlings handles personal data within its organization and the key data privacy principles which it complies with. This section focuses on Bilderlings role as a data controller and does not form part of Bilderlings data processing addendum.

14.2 Bilderlings has implemented procedures designed to ensure that Customer Data is processed only as instructed by the Customer as described in Appendix A ("Security Controls", throughout the entire chain of processing activities by Bilderlings and its sub-processors.

Additionally, the Services undergo security assessments by internal personnel and third parties, which include infrastructure vulnerability assessments and application security assessments.

14.3 Bilderlings takes the security of your data seriously. Bilderlings has internal policies and controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by its employees in the performance of their duties. But remember that no method of transmission over the Internet, and no method of electronic storage, is 100% secure and reliable, and we cannot guarantee its absolute security.

14.4 Where Bilderlings engages third parties to process personal data on its behalf, they do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and Company measures to ensure the security of data.

14.5 We will maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

- **Confidentiality** means that only people who are authorized to use the data can access it.
- **Integrity** means that Personal Data should be accurate and suitable for the purpose for which it is processed.
- **Availability** means that authorized users should be able to access the data if they need it for authorized purposes. Personal Data should therefore be stored in authoritative data repositories.

14.6 Security procedures include:

- **Physical security controls.** Bilderlings facilities feature controls (e.g., alarms, visitor escort process, and access control badges) to prevent unauthorized access.
- **Secure lockable desks and cupboards.** Desks and cupboards are required to be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
- **Methods of disposal.** Paper documents are shredded, and digital storage media are physically destroyed or securely overwritten when they are no longer required.
- **Equipment.** Data Users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC or lock the session when it is left unattended.
- **Incident Management.** Bilderlings maintains security incident management policies and procedures. Bilderlings notifies impacted Data Subjects without undue delay of any

unauthorized disclosure of their respective Personal Data by Bilderlings or its agents of which Bilderlings becomes aware to the extent required by Data Protection Laws and Regulations.

- **Technical safeguards.** Bilderlings ensures that technical and organizational measures are in place to ensure data security and minimization, this includes anti-virus, intrusion detection, user authentication services, Pseudonymisation and encryption of data where appropriate.

15. Transferring Personal Data to a Country Outside the EEA

15.1 We may transfer any Personal Data we hold to a country outside the European Economic Area ("EEA"), provided that one of the following conditions applies:

- The country (or organization) to which the Personal Data is transferred ensures an adequate level of protection for the Data Subjects' rights and freedoms (e.g. based on adequacy decisions, approved binding corporate rules, standard contractual clauses).
- The Data Subject has given his or her consent.
- The transfer is necessary for one of the reasons set out in the GDPR, including the performance of a contract between us and the Data Subject, or to protect the vital interests of the Data Subject.
- The transfer is legally required on important public interest grounds or for the establishment, exercise or defense of legal claims.
- The transfer is authorized by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the Data Subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

15.2 Subject to the requirements in paragraph 15.1 above, Personal Data we hold may also be processed by staff operating outside the EEA who work for us or for one of our suppliers. That staff may be engaged in, among other things, the fulfilment of contracts with the Data Subject, the Processing of payment details and the provision of support services.

16. Disclosure and Sharing of Personal Information

16.1 Subject to paragraph 15, we may share Personal Data we hold with any member of our Group.

16.2 We may also disclose Personal Data we hold to third parties:

- In the event that we sell or buy any business or assets, in which case we may disclose Personal Data we hold to the prospective seller or buyer of such business or assets on a need to know basis.

- If we or substantially all of our assets are acquired by a third party, in which case Personal Data we hold will be one of the transferred assets.
- If we are under a duty to disclose or share a Data Subject's Personal Data in order to comply with any legal obligation, or in order to enforce or apply any contract with the Data Subject or other agreements; or to protect our rights, property, or safety of our customers or others. This includes exchanging information with other companies and organizations for the purposes of fraud protection and credit risk reduction.

16.3 We may also share Personal Data we hold with selected third parties, including but not limited to our business partners, service providers and sub-contractors for the performance of any contract we enter into with them or a Data Subject when we have notified the Data Subjects accordingly.

16.4 Disclosing/sharing Personal Data outside of our organization carries further risks and we must ensure the right organizational, technical and contractual measures are in place before transferring or allowing access to Personal Data.

17. Subject Access Requests

17.1 Under GDPR, data subjects have a number of rights to access, rectify, erase, and restrict processing of Personal Data. These rights include:

- access and obtain a copy of your data on request;
- require Bilderlings to change incorrect or incomplete data;
- require Bilderlings to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing;
- object to the processing of your data where Bilderlings is relying on its legitimate interests as the legal ground for processing; and
- ask Bilderlings to stop processing data for a period if data is inaccurate or there is a dispute about whether or not your interests override Bilderlings's legitimate grounds for processing

17.2 Data Subjects must make a formal request for information we hold about them. This must be made in writing. Employees who receive a written request should forward it to the Data Protection Officer immediately.

17.3 Our employees will refer a request to the Data Protection Officer for assistance in difficult situations. Employees should not be bullied into disclosing personal information.

17.4 All Data Subject Access requests must be dealt with within a month of receiving them and no Data Subject shall be charged for making such request.

17.5 We will not charge Data Subject Access requests unless any requests which we receive are made excessively, repetitive or are manifestly unfounded requests, we may charge them an administration fee in order to Process such requests or refuse to act on such requests.

18. Reporting Breaches

18.1 Where there has been a Personal Data breach and the breach is likely to result in a high risk to the rights and freedoms of the Data Subject we will report the breach to the Information Commissioners Office without undue delay and, where feasible, not later than 72 hours after having become aware of it.

18.2 Where there has been a Personal Data breach and the breach is likely to result in a high risk to the rights and freedoms of the Data Subject we will report the breach to the Data Subject without undue delay. The communication to the Data Subject will describe the nature of the Personal Data breach as well as recommendations for the Data Subject concerned to mitigate potential adverse effects. Such communications to Data Subjects will be made as soon as reasonably feasible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities.

19. Document Control

APPROVAL AND OWNERSHIP

Created By	Title	Date	Name
Policy Author	DPO	02.05.2018	Sergejs Kravcenko

Approved By	Title	Date	Name
Executive Sponsor	Member of Board	03.05.2018	Andrej Kuzins

REVISION HISTORY

Version	Revision Date	Review Date	Description
Initial			

Appendix A: Data Processor Security Controls

1. Nature and Purpose of Processing

1.1 Bilderlings will Process Personal Data as necessary to perform the Bilderlings services and as further instructed by the Customer in its use of the Services, as a Data Controller. This shall

include automated processing of Personal Data to evaluate and analyze certain personal aspects relating to the Data Subject, in particular to analyze or predict aspects concerning that Data Subject's personal preference, interests, behavior and location.

2. Categories of Data Subjects

2.1 Customer may submit Personal Data to the Bilderlings services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Prospects, customers, business partners and vendors of Customer (who are natural persons);
- Employees or contact persons of Customer's prospects, customers, business partners and vendors;
- Employees, agents, advisors, freelancers of Customer (who are natural persons);
- Customer's users authorized by Customer to use the Services.

3. Type of Personal Data

3.1 Customer may submit, or allow collection of, Personal Data in the use of the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- First and last name;
- Title;
- Position;
- Employer;
- Contact information (company, email, phone, physical business address);
- ID data;
- Behavioral and profile data;
- Personal preferences;
- Connection data;
- Location data;

- Other data and information in accordance with the law, other local legislation or international regulations.

4. Data Segregation

4.1 The Services are operated in a multitenant architecture that is designed to segregate and restrict Customer Data storage and access based on business needs. The architecture provides an effective logical data separation for different Customers via Customer-specific unique IDs and allows the use of customer and user role-based access privileges. Additional data segregation is ensured by providing separate environments for different functions, especially for testing and production.

5. Security Controls

5.1 Bilderlings has implemented procedures designed to ensure that Customer Data is processed only as instructed by the Customer, throughout the entire chain of processing activities by Bilderlings and its sub-processors. Additionally, the Services undergo security assessments by internal personnel and third parties, which include infrastructure vulnerability assessments and application security assessments.

5.2 Bilderlings adopts a number of security controls, which include:

- Unique user identifiers to allow Customers to assign unique credentials for their users and assign and manage associated permissions and entitlements;
- Controls to ensure initial passwords must be reset on first use;
- Controls to limit password re-use;
- Password length and complexity requirements;
- Customers have the option to integrate Single Sign-On technologies to directly control the authentication and credential complexity, expiration, account lockout, IP white/black listing;
- Customers have the option to manage their application users, define roles, and apply permissions and rights within their implementation of the Services;
- User passwords are stored using a one-way salted hash format and are not transmitted unencrypted;
- Password data Vault encrypted using 256-bit AES encryption;
- User access log entries will be maintained, containing date, time, User ID, URL executed or identity ID operated on, operation performed (accessed, created, edited, deleted,);

- If there is suspicion of inappropriate access to the Services, Bilderlings can provide Customer log entry records to assist in forensic analysis. This service will be provided to Customers on a time and materials basis;
- User access logs will be stored in a secure centralized host to prevent tampering;
- User access logs will be kept for a minimum of 90 days;
- Bilderlings personnel will not set a defined password for a user.

6. Intrusion Detection

6.1 **Bilderlings**, or an authorized independent third party, will monitor the Services for unauthorized intrusions using host-based intrusion detection mechanisms.

7. Security Logs

7.1 All Bilderlings systems used in the provision of the Services, including firewalls, routers, network switches and operating systems, log information to their respective system log facility or a centralized syslog server (for network systems) in order to facilitate security reviews and analysis.

8. Incident Management

8.1 Bilderlings maintains security incident management policies and procedures. Bilderlings notifies impacted Customers without undue delay of any unauthorized disclosure of their respective Customer Data by Bilderlings or its agents of which Bilderlings becomes aware to the extent required by Data Protection Laws and Regulations.

9. User Authentication

9.1 Access to the Services requires a valid user ID and password combination (or via integrated Single Sign-On mechanism), which are encrypted via TLS while in transmission, as well as machine specific information for identity validation as described under “Security Controls,” above. Following a successful authentication, a random session ID is generated and stored in the user’s browser to preserve and track session state.

10. Physical Security

10.1 Production data centers used to provide the Services have access control systems. These systems permit only authorized personnel to have access to secure areas. These facilities are designed to withstand adverse weather and other reasonably predictable natural conditions, are secured by around the-clock guards, two-factor access screening, including biometrics, and escort-controlled access, and are also supported by on-site back-up generators in the event of a power failure.

11. Reliability and Backup

11.1 All infrastructure components are configured in a high availability mode or in a redundant fashion. All Customer Data submitted to the Services is stored on infrastructure that supports high availability and is backed up on a regular basis. This backup data is retained for at least 1 month. Backups are transmitted and stored in encrypted form and held in a secondary data center.

12. Disaster Recovery

12.1 The Services' production systems are protected by disaster recovery plans which provide for backup of critical data and services. A comprehensive system of recovery processes exists to bring business-critical systems back online within the briefest possible period of time. Recovery processes for database security, systems administration, and network configuration and data provide a roadmap for personnel to make processes available after an outage.

13. Malware

13.1 The Services have controls in place that are designed to prevent and detect the introduction of malware to the Services' respective platforms.

14. Data Encryption

14.1 The Services use, or enable Customers to use, industry-accepted encryption products to protect Customer Data and communications during transmissions between a Customer's network and the Services, including 128-bit TLS Certificates and 2048-bit RSA public keys at a minimum.

15. Return of Customer Data:

15.1 During the contract term, Customers may export a copy of Customer Data processed by the Services. Within 30 days of termination of the applicable Service, Customers may: 1) request return of Customer Data submitted to the Services; or 2) access their account to export or download Customer Data submitted to Services.

16. Deletion of Customer Data

16.1 After termination of the Service, following the 30-day period for return of Customer Data, Customer Data submitted to the Services is retained in inactive status for up to 90 days, after which it is securely overwritten or deleted, unless laws, regulations or other our commitments do no instruct us otherwise.

17. Usage and Trend Reporting

17.1 Bilderlings may track and analyze the usage of the Services for purposes of security and helping Bilderlings improve both the Services and the user experience in using the Services. For example, we may use this information to understand and analyze trends or track which of our features are used most often to improve product functionality.

17.2 Bilderlings may share anonymous usage data with Bilderlings's service providers for the purpose of helping Bilderlings in such tracking, analysis and improvements. Additionally, Bilderlings may share such anonymous usage data on an aggregate basis in the normal course of operating our business; for example, we may share information publicly to show trends about the general use of our Services.

18. Sub-processors

18.1 Bilderlings and its affiliates have entered into written agreements with their sub-processors containing privacy, data protection, and data security obligations that provide a level of protection appropriate to their processing activities.

18.2 Bilderlings utilizes the services of the following sub-processors to provide part of the Bilderlings infrastructure to host Customer Data and provide the Services:

- **For ensuring card payments** - SIA Worldline Latvia (Reg.Nr. 40003072814, Dzirnavu street 37, LV-1010, Rīga)

- **For ensuring card payments (as acquirer)** – BlueOrangeBank JSC (Reg.Nr. 40003551060, Smilšu street 37, LV-1050, Rīga)
- **For data storage and email services MSO365** – Squalio LLC JSC (Reg.Nr. 40003351675, Krišjāņa Valdemāra 21-19, LV-1010, Rīga)
- **For customer resource management -** SalesForce.com INC. (Reg.Nr. The Landmark @ One Market street, San Francisco, CA 94105, USA)
- **For preparation of insurance proposals** - AAS "ERGO" (Reģ.Nr. 40003131253, Skanstes iela 50, LV-1013, Rīga)
- **For ensuring payment services** - SIA DEAC (Reg.Nr. 40103255973, Maskavas street 459, LV-1063, Rīga)

19. European specific provisions – Overseas Transfers

19.1 The GDPR requires that Personal Data must not be transferred to a country or territory outside the European Economic Area (i.e. the member states of the EU plus Iceland, Liechtenstein and Norway, UK - after 29 March 2019), unless that country or territory or organization ensures an adequate level of protection for the rights and freedoms of Data Subjects in relation to the Processing of Personal Data.

19.2 Subject to paragraph 3.20, where the Customer entity and the Bilderlings entity are based inside the EEA, Bilderlings shall not transfer Personal Data to any country outside of the EEA without prior written consent from the Customer, except for transfers to and from: (i) any country which has a valid adequacy decision from the European Commission; or (ii) any organization which ensures an adequate level of protection in accordance with the applicable Data Protection Laws and Regulations.