

UNISENDER

DATA PROCESSING AGREEMENT

This Data Processing Agreement (“**DPA**” or “**Agreement**”) forms part of the agreement between Customer and ECOMZ HOLDING LIMITED and its affiliates (collectively “**UniSender**”) to reflect the parties’ agreement for the provision of the Services (as amended from time to time) and processing of Customer’s Personal Data in accordance with the requirements of the Data Protection Laws.

This Data Processing Agreement will be effective from the Effective Date.

If you are accepting this Data Processing Agreement on behalf of Customer, you warrant that: (a) you have full legal authority to bind Customer to this Data Processing Agreement; (b) you have read and understand this Data Processing Agreement; and (c) you agree, on behalf of Customer, to this Data Processing Agreement. If you do not have the legal authority to bind Customer, please do not accept this Data Processing Agreement.

SCOPE OF DPA

This DPA will only apply to the extent that the Data Protection Laws apply to the processing of Customer Personal Data, including if:

- (a) the processing is in the context of the activities related to Customers registered through the domain names unisender.com, cp.unisender.com or unione.io. Please contact our support for more information for data processing location changes.
- (b) the processing is in the context of the activities of an establishment of Customer in the EEA; and/or
- (c) Customer is offering services to data subjects who are in the EEA.

If the Customer entity signing this DPA is a party to the UniSender Terms of Service, this DPA is an addendum to and forms part of the Terms of Service.

This DPA shall not replace any previously applicable agreements relating to their subject matter (including any data processing amendment or data processing addendum relating to the Services.)

If there is any conflict or inconsistency between the terms of this DPA and the Terms of Service (<https://www.unisender.com/en/terms/>) the terms and conditions set forth in this DPA shall prevail. Subject to the amendments in this DPA, the Terms of Service remain in full force and effect.

HOW TO EXECUTE THIS DPA:

1. This DPA has been pre-signed on behalf of UniSender.
2. To complete this DPA, Customer must:
 - (a) Complete the information in the signature box and sign on Page 8, and
 - (b) Send the signed DPA to UniSender by email to privacy@unisender.com indicating, if applicable, the Customer’s ID (as set out on the applicable Order Form or invoice).

Upon receipt of the validly completed DPA by UniSender at this email address, this DPA will become legally binding.



THE PARTIES HEREBY MUTUALLY AGREE AS FOLLOWS:

1. INTRODUCTION

This DPA reflect the parties' agreement on the terms governing the processing and security of Customer Personal Data in connection with the Data Protection Laws.

1.1 DEFINITIONS AND INTERPRETATION

"Affiliates" means any entity which is controlled by, controls or is in common control with UniSender.

"UniSender" means ECOMZ HOLDING LIMITED and its Affiliates engaged in the Processing of Personal Data.

"Customer Personal Data" means personal data that is processed by UniSender on behalf of Customer as part of UniSender provision of the Services.

"Data Incident" means a breach of UniSender security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data on systems managed by or otherwise controlled by UniSender. "Data Incidents" will not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

"Data Protection Laws" mean, as applicable: (a) the GDPR; and/or (b) the Federal Data Protection Act of 19 June 1992 (Switzerland).

"Effective Date" means, as applicable:

The date on which Customer provided UniSender with duly signed DPA, as indicated in "HOW TO EXECUTE THIS DPA" section above.

"GDPR" means Regulation (EU) 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.

"Notification Email Address" means the email address (if any) designated by Customer, via the user interface of the Services or such other means provided by UniSender, to receive certain notifications from UniSender relating to this DPA.

"Personal Data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic cultural or social identity;

"Processing of personal data" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction ("Process", "Processes" and "Processed" shall have the same meaning).

"Security measures" means measures to protect personal data against accidental or unlawful destruction or accidental loss, alternation, unauthorised disclosure or access and against all other unlawful forms of processing as described in the document (or the

applicable part dependent on what Services Customer purchases from UniSender), as updated from time to time, and described in Appendix 2 to this DPA.

“Services” means the provision of license to use the UniSender or UniOne software, as well as maintenance and support services, consultancy or professional services and the provision of software as a service or any other services provided under the Agreement where UniSender Processes Personal Data of Customer.

“Sub-processors” means third parties authorized by UniSender to have logical access to and process Customer Personal Data in order to provide parts of the Services and any related technical support.

“Term” means the period from the Effective Date until the end of UniSender provision of the Services to Customer under the Agreement.

The terms **“Data controller”**, **“Data subject”**, **“Personal data”**, **“Processing”**, **“Data processor”** and **“Supervisory authority”** as used in this DPA have the meanings given in the GDPR.

2. PROCESSING OF PERSONAL DATA

2.1 Roles and Regulatory Compliance; Authorization.

2.1.1 Processor and Controller Responsibilities. The parties acknowledge and agree that: (a) Appendix 1 to the Standard Contractual Clauses describes the subject matter and details of the processing of Customer Personal Data;

(a) UniSender is a processor of Customer Personal Data under the Data Protection Laws;

(b) Customer is a controller or processor, as applicable, of Customer Personal Data under the Data Protection Laws; and

(c) each party will comply with the obligations applicable to it under the Data Protection Laws with respect to the processing of Customer Personal Data;

(d) Customer shall, in its use or receipt of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Customer will ensure that its instructions for the Processing of Personal Data shall comply with Data Protection Laws. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.

2.2 Authorization by Third Party Controller. If Customer is a processor, Customer warrants to UniSender that Customer's instructions and actions with respect to Customer Personal Data, including its appointment of UniSender as another processor, have been authorized by the relevant controller.

2.3 The parties agree that with regard to the Processing of Personal Data, UniSender or its Affiliates will engage Sub-processors pursuant to the requirements set forth in Section 7 “Sub-processors” below.

2.4 By entering into this Data Processing Agreement, Customer instructs UniSender to process Customer Personal Data only in accordance with applicable law: (a) to provide the Services and any related technical support; (b) as further specified via Customer's use of the Services (including in the settings and other functionality of the Services) and any related technical support; (c) as documented in this Data Processing Agreement; and (d) as further documented in any other written instructions given by Customer and acknowledged by UniSender as constituting instructions for purposes of this Data Processing Agreement.

2.5 Deletion on Term Expiry. On expiry of the Term, Customer instructs UniSender to delete all Customer Personal Data (including existing copies) from UniSender systems in accordance with applicable law. UniSender will comply with this instruction as soon as reasonably practicable and within a maximum period of 30 days, unless United States, EU or EU Member State law requires storage.

2.6 Account deletion and archiving. General Personal Data retention period is 30 days, except for the general delivery and open stats data, which are stored for at least 180 days as of the mailing date. UniSender reserves the right to delete or archive any non-active account (and associated Customer Personal Data), i.e. an account that has not sent any emails for a period exceeding 12 months.

3. RIGHTS OF DATA SUBJECTS

3.1 If the Customer, in its use or receipt of the Services, does not have the ability to correct, amend, block or delete Personal Data, as required by Data Protection Laws, UniSender will (taking into account the nature of the processing of Customer Personal Data and, if applicable, Article 11 of the GDPR) assist Customer in fulfilling any obligation of Customer to respond to requests by data subjects, including (if applicable) Customer's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR, by providing the functionality of the Services;

3.2 UniSender shall, to the extent legally permitted, promptly notify Customer if it receives a request from a Data Subject for access to, correction, amendment, restriction, deletion or exercising any other rights under the GDPR of that person's Personal Data. UniSender shall not respond to any such Data Subject request without Customer's prior written consent except to confirm that the request relates to Customer. UniSender shall provide Customer with cooperation and assistance in relation to handling of a Data Subject's request for access to that person's Personal Data or exercising any other rights under the GDPR, to the extent legally permitted and to the extent Customer does not have access to such Personal Data through its use or receipt of the Services.

4. PERSONNEL

4.1 UniSender shall ensure that its personnel and contractors engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and are subject to obligations of confidentiality as described in Appendix 2 to this DPA and such obligations survive the termination of that persons' engagement with UniSender.

5. DATA SECURITY

5.1 UniSender shall maintain administrative, physical and technical safeguards for protection of the security, confidentiality and integrity of Personal Data, such measures are described in the Appendix 2 to this DPA.

5.2 UniSender Security Measures. UniSender will implement and maintain technical, physical and organisational measures to protect confidentiality and integrity of Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access as described in the Appendix 2 to this DPA (the "**Security Measures**"). As described in the Appendix 2 to this DPA, the Security Measures include measures: (a) to ensure ongoing confidentiality, integrity, availability and resilience of UniSender systems and services; (b) to restore timely access to personal data following an incident; and (c) for regular testing of effectiveness. UniSender may update or modify the



Security Measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Services.

5.3 Security Compliance by UniSender Staff. UniSender will take appropriate steps to ensure compliance with the Security Measures by its employees, contractors and Sub-processors to the extent applicable to their scope of performance, including ensuring that all persons authorised to process Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality as described in the Appendix 2 to this DPA.

5.4 UniSender Security Assistance. Customer agrees that UniSender will assist Customer in ensuring compliance with any obligations of Customer in respect of security of personal data and personal data breaches, including (if applicable) Customer's obligations pursuant to Articles 32 to 34 (inclusive) of the GDPR, by:

- (a) implementing and maintaining the Security Measures in accordance with the Appendix 2 to this DPA; and
- (b) complying with the terms of Section 7 (Data Incidents).

6. SUB-PROCESSORS

6.1 Consent to Sub-processor Engagement. Customer specifically authorizes that UniSender is engaging a number of third-party Sub-processors in connection with the provision of the Service (also accessible at [UniSender Privacy Policy](#)).

UniSender have entered into an agreement with each Sub-processor containing data protection obligations not less protective than those in this DPA with respect to the protection of Customer Data to the extent applicable to the nature of the Services provided by such Sub-processor.

6.2 List of Current Sub-processors and Notification of New Sub-processors. UniSender makes available to Customer the current list of Sub-processors. Such Sub-processor list includes the identities of those Sub-processors, available for Customer on UniSender Website (also accessible at [UniSender Privacy Policy](#)). UniSender has no obligation to notify the Customer of engagement of new Sub-processors and relies on Customer's ability to check the updates to the UniSender Privacy Policy

6.3 Requirements for Sub-processor Engagement. When engaging any Sub-processor, UniSender will ensure via a contract that:

- (i) the Sub-processor only accesses and uses Customer Personal Data to the extent required to perform the obligations subcontracted to it, and does so in accordance with the Agreement (including this DPA); and
- (ii) if the GDPR applies to the processing of Customer Personal Data, the data protection obligations set out in Article 28(3) of the GDPR are imposed on the Sub-processor.

6.4 Objection Right for New Sub-processors.

Customer may object to any new Sub-processor by notifying UniSender in writing. In the event Customer objects to a new Sub-processor, UniSender will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening the Customer. If UniSender is unable to make available such change within a reasonable

period of time, which shall not exceed thirty (30) days, Customer may terminate the applicable Order with respect only to those Services which cannot be provided by UniSender without the use of the objected-to new Sub-processor by providing written notice to UniSender.

7. DATA INCIDENTS

7.1 Incident Notification. If UniSender becomes aware of a Data Incident, UniSender will: (a) notify Customer of the Data Incident promptly and without undue delay (Within 72 hours of being aware of the incident); and (b) promptly take reasonable steps to minimise harm and secure Customer Personal Data.

7.2 Details of Data Incident. Notifications will describe, to the extent possible, details of the Data Breach, including steps taken to mitigate the potential risks and steps UniSender recommends Customer take to address the Data Incident.

7.3 Delivery of Notification. UniSender will deliver its notification of any Data Incident to the Notification Email Address or, at UniSender discretion (including if Customer has not provided a Notification Email Address), by other direct communication (for example, by phone call or an in-person meeting). Customer is solely responsible for providing the Notification Email Address and ensuring that the Notification Email Address is current and valid.

7.4 Third Party Notifications. Customer is solely responsible for complying with breach notification laws applicable to Customer and fulfilling any third-party notification obligations related to any Data Incident.

8. INSPECTIONS OF COMPLIANCE

8.1 To demonstrate compliance by UniSender with its obligations under this DPA, and upon Customer's request, UniSender will provide more detailed information on the security measures described in the Appendix 2 to this DPA.

8.2 Upon Customer's request, and subject to the confidentiality obligations set forth in this DPA, UniSender shall make available to Customer that is not a competitor of UniSender (or Customer's independent, third-party auditor that is not a competitor of UniSender) information regarding UniSender compliance with the obligations set forth in this DPA and the security measures as described in the Appendix 2 to this DPA.

9. DATA PROTECTION IMPACT ASSESSMENT

Upon Customer's request, UniSender will assist Customer in ensuring compliance with any obligations of Customer in respect of data protection impact assessments and prior consultation, including (if applicable) Customer's obligations pursuant to Articles 35 and 36 of the GDPR, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to UniSender. UniSender shall provide reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks.

10. DATA TRANSFERS

10.1 In most of the cases the Customer Data is processed by ECOMZ HOLDING LIMITED registered on Republic of Cyprus inside the European Union Economic Area and hosted inside the European Union in Germany or Latvia by Amazon Web Services or TET (Lattelecom) data centers, which are fully GDPR compliant.



10.2 International transfers. UniSender may process Customer Personal Data in the United States of America or the Russian Federation subject to appropriate safeguards under article 46 GDPR (see clause 10.3).

10.3 Where the Customer is located in the United States of America, the Customer Personal Data may be hosted by UniSender in the United States of America by Amazon Web Services at data centers, which are fully GDPR compliant. Where the Customer is located in the Russian Federation, the Customer Personal Data may be transferred for processing by UniSender to the secured data center in the Russian Federation. The data processing activities in the Russian Federation are protected by appropriate safeguards under article 46 GDPR, specifically by the standard data protection clauses adopted by the European Commission in accordance with the examination procedure. For data transfers from controllers in the EU to processors established outside the EU the security measures are described in the Appendix 2 to this DPA. European Commission decided that standard contractual clauses offer sufficient safeguards on data protection for the data to be transferred internationally. You have a right to request information on those contractual safeguards (Please contact our Data Protection Officer).

11. DURATION OF THIS DPA

11.1 This DPA will take effect on the Effective Date and, notwithstanding expiry of the Term, remain in effect until, and automatically expire upon, deletion of all Customer Personal Data by UniSender as described in this DPA.

12. GOVERNING LAW

12.1 This DPA (including any non-contractual matters and obligations arising therefrom or associated therewith) shall be governed by, and construed in accordance with, the laws of Republic of Cyprus.

12.2 Any dispute, controversy, proceedings or claim between the Parties relating to this Agreement (including any non-contractual matters and obligations arising therefrom or associated therewith) shall fall within the jurisdiction of the courts of Republic of Cyprus.

12.3 For data transfers outside the EEA listed in clause 10.3 protected by appropriate safeguards under article 46 GDPR, specifically by the standard data protection clauses adopted by the Commission in accordance with the examination procedure from controllers in the EU to processors established outside the EU and Customers when the processing is in the context of the activities of an establishment of EEA countries other than Republic of Cyprus and/or Customers offering services to data subjects who are in the EEA countries other than Republic of Cyprus the lead supervisory authority is Republic of Cyprus under article 56 GDPR.

The supervisory authority of the Republic of Cyprus within the EEA is competent to act as lead supervisory authority for the cross-border processing carried out by that processor in accordance with the procedure provided in Article 60 of GDPR under this DPA.

13. CHANGES TO THIS DPA


13.1 UniSender may change this DPA if the change:

- (a) is expressly permitted by this DPA;
- (b) reflects a change in the name or form of a legal entity;
- (c) is required to comply with applicable law, applicable regulation, a court order or guidance issued by a governmental regulator or agency; or



(d) does not: (i) result in a degradation of the overall security of the Services; (ii) expand the scope of, or remove any restrictions on, UniSender processing of Customer Personal Data; and (iii) otherwise have a material adverse impact on Customer's rights under this DPA, as reasonably determined by UniSender.

13.2 Notification of Changes. If UniSender intends to change this DPA, UniSender will inform Customer at least 30 days (or such shorter period as may be required to comply with applicable law, applicable regulation, a court order or guidance issued by a governmental regulator or agency) before the change will take effect by either: (a) sending an email to the Notification Email Address; or (b) alerting Customer via the user interface for the Services. If Customer objects to any such change, Customer may terminate the Agreement by giving written notice to UniSender within 30 days of being informed by UniSender of the change.

CUSTOMER	UNISENDER
Signature: _____	Signature:  _____
Legal Name: _____	Legal Name: <u>ECOMZ HOLDING LIMITED</u>
Reg. number/Country: _____	Reg. number/Country: <u>309897/CYPRUS</u>
Print Name: _____	Print Name: <u>Paraskevi Maltezou</u>
Title: _____	Title: <u>Director</u>
Date: _____	<u>11/05/2020</u>



Appendix 1

SUBJECT MATTER AND DETAILS OF THE DATA PROCESSING

1. Nature and Purpose of Processing

UniSender will Process Customer Personal Data as necessary to provide the Services pursuant to the Agreement, as further instructed by Customer in its use of the Services.

2. Duration of Processing

Subject to Section 11 of the DPA, UniSender will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.


3. Categories of Data Subjects

Customer may submit Personal Data to 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 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

4. Types of Personal Data

Customer may submit Personal Data to 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
 - Country
 - E-mail
 - Phone number
 - Postal address
 - Position
 - Employer
 - Contact information (company, email, phone, physical business address)
 - ID data
 - IP address(es) and domain name
 - Localisation data
- 

5. Special categories of data (if appropriate):

N/A

6. Processing operations

The personal data will be subject to the following basic processing activities (please specify):

- IT, digital, technology or telecom services, including provision of technology products or services, telecoms and network services, digital services, hosting, cloud and support services or software licensing. Including, but not limited to:
 - Collecting, recording, organizing, structuring, storing, retrieving, using, disclosing, erasing and destroying) Customer Personal Data for the purpose of providing the Services and any related technical support to Customer in accordance with this Data Processing Agreement. The services include the following: E-mail/SMS/Viber Marketing SaaS Service, Transactional Emails Service, Email Marketing Services, etc.



Appendix 2

SECURITY MEASURES

UniSender will implement and maintain the Security Measures set out in this Appendix 2. UniSender may update or modify such Security Measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Services.

1. KEY PRINCIPLES OF THE DATA PROTECTION BY UNISENDER

1.1 All UniSender IT Systems are protected against unauthorised access.

1.2 All UniSender IT Systems are used only in compliance with relevant Company Policies.

1.3 All UniSender employees and any third parties authorised to use the IT Systems including, but not limited to sub-processors, must ensure that they are familiar with this Policies and must adhere to and comply with it at all times.

1.4 All line managers ensure that all employees and sub-processors under their control and direction adhere to and comply with this Policies at all times as required under paragraph 2.3.

1.5 All data stored on IT Systems are managed securely in compliance with all relevant parts of EU Regulation 2016/679 General Data Protection Regulation ("GDPR") and all other laws governing data protection whether now or in the future in force.

1.6 All data stored on IT Systems is classified appropriately. All data so classified is handled appropriately in accordance with its classification.

1.7 All data stored on IT Systems is available only to those Users with a legitimate need for access.

1.8 All data stored on IT Systems is protected against unauthorised access and processing.

1.9 All data stored on IT Systems is protected against loss and corruption.

1.10 All breaches of security pertaining to the IT Systems or any data stored thereon are reported and subsequently investigated by the IT Department.

2. SOFTWARE SECURITY MEASURES

2.1 All software in use on the IT Systems (including, but not limited to, operating systems, individual software applications, and firmware) are kept up-to-date and any and all relevant software updates, patches, fixes, and other intermediate releases are applied.

2.2 Where any security flaw is identified in any software that flaw is fixed immediately or the software may be withdrawn from the IT Systems until such time as the security flaw can be effectively remedied.

2.3 No UniSender employees may install any software of their own, whether that software is supplied on physical media or whether it is downloaded, without the approval of the IT Manager. Any software must be approved by the IT Manager and may only be

installed where that installation poses no security risk to the IT Systems and where the installation would not breach any licence agreements to which that software may be subject.

3. ANTI-VIRUS SECURITY MEASURES

3.1 UniSender IT Systems (including all computers and servers) are protected with suitable anti-virus, firewall, and other suitable internet security software. All such software is kept up-to-date with the latest software updates and definitions.

3.2 All UniSender IT Systems protected by anti-virus software are subject to a full system scan at least once a week.

3.3 All physical media (e.g. USB memory sticks or disks of any kind) used by employees for transferring files must be virus-scanned before any files may be transferred. Such virus scans are performed by the IT Staff Manager.

3.4 UniSender employees are permitted to transfer files using cloud storage systems only with the approval of the IT Manager. All files downloaded from any cloud storage system are scanned for viruses during the download process.

3.5 Any files being sent to third parties outside the Company, whether by email, on physical media, or by other means (e.g. shared cloud storage) are scanned for viruses before being sent or as part of the sending process.

4. HARDWARE SECURITY MEASURES

4.1 UniSender on-premises IT Systems are located in rooms which are securely locked (with authorised Users being granted access by means of a smart card).

4.2 All on-premises IT Systems not intended for normal use by Users (including, but not limited to, servers, networking equipment, and network infrastructure) are located in secured, climate-controlled rooms in locked cabinets which may be accessed only by designated members of the IT Department.

4.3 All mobile devices (including, but not limited to, laptops, tablets, and smartphones) provided by the Company are always transported securely and handled with care.

5. ACCESS SECURITY

5.1 Access privileges for all IT Systems is determined on the basis of employee levels of authority within UniSender Company organization structure and the requirements of their job roles. Employees are not granted access to any IT Systems or electronic data which are not reasonably required for the fulfilment of their job roles.

5.2 All IT Systems (and in particular mobile devices including, but not limited to, laptops, tablets, and smartphones) are protected with a secure password or passcode, or such other form of secure log-in system as the IT Department may deem appropriate and approve.

5.3 All passwords are covered with the following security measures:

- a) Are at least 8 characters long;
- b) Contain a combination of upper and lower case letters, numbers, symbols;
- c) Changed at least every 90 days;
- d) Different from the previous password;



- e) Not obvious or easily guessed (e.g. birthdays or other memorable dates, memorable names, events, or places etc.); and
- f) Created by individual Users.

5.4 All IT Systems with displays and user input devices (e.g. mouse, keyboard, touchscreen etc.) are protected with a password protected screensaver that will activate after 5 minutes of inactivity.

6. DATA STORAGE SECURITY

6.1 All data, and in particular personal data is stored securely using passwords.

6.2 No personal data is stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to UniSender or otherwise.

6.3 No data, and in particular personal data, is transferred to any computer or device personally belonging to an employee unless the employee in question is a sub-processor working on behalf of UniSender and that employee has agreed to comply fully with the Company's Data Protection Policy and the GDPR.

7. DATA PROTECTION

7.1 All personal data (as defined in the GDPR) collected, held, and processed by UniSender is collected, held, and processed strictly in accordance with the principles of the GDPR, the provisions of the GDPR and the Company's Data Protection Policy.

7.2 All Users handling data for and on behalf of UniSender are subject to, and must comply with, the provisions of the Company's Data Protection Policy at all times. In particular, the following shall apply:

- a) All emails containing confidential or sensitive personal data are encrypted using TLS SSL protocol;
- b) All emails containing confidential or sensitive personal data are marked "confidential";
- c) Confidential and sensitive personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted under any circumstances;
- d) All confidential and sensitive personal data to be transferred physically, including that on removable electronic media, is transferred in a suitable container marked "confidential".
- e) Where any confidential or sensitive personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the employee must lock the computer and screen before leaving it.

7.3 Any questions relating to data protection should be referred to our Data Protection Officer (privacy@unisender.com).

8. DATA CENTERS & NETWORK SECURITY OF THE HOSTING PROVIDER

UniSender uses Amazon Web Services to store and analyze data, including AWS Cloud infrastructure in Europe (Germany) Region and Europe (Latvia) Region.

9. AVAILABILITY



AWS has identified critical system components required to maintain the availability of our system and recover service in the event of outage. Critical system components are backed up across multiple, isolated locations known as Availability Zones. Each Availability Zone is engineered to operate independently with high reliability. Availability Zones are connected to enable you to easily architect applications that automatically fail-over between Availability Zones without interruption. Highly resilient systems, and therefore service availability, is a function of the system design. Through the use of Availability Zones and data replication, AWS customers can achieve extremely short recovery time and recovery point objectives, as well as the highest levels of service availability.

10. INFRASTRUCTURE MAINTENANCE

Equipment maintenance. AWS monitors and performs preventative maintenance of electrical and mechanical equipment to maintain the continued operability of systems within AWS data centers. Equipment maintenance procedures are carried out by qualified persons and completed according to a documented maintenance schedule.

Environment management. AWS monitors electrical and mechanical systems and equipment to enable immediate identification of issues. This is carried out by utilizing continuous audit tools and information provided through our Building Management and Electrical Monitoring Systems. Preventative maintenance is performed to maintain the continued operability of equipment.

11. GOVERNANCE & RISK

Data Center risk management. The AWS Security Operations Center performs regular threat and vulnerability reviews of data centers. Ongoing assessment and mitigation of potential vulnerabilities is performed through data center risk assessment activities. This assessment is performed in addition to the enterprise-level risk assessment process used to identify and manage risks presented to the business as a whole. This process also takes regional regulatory and environmental risks into consideration.

Third-party security attestation. Third-party testing of AWS data centers, as documented in our third-party reports, ensures AWS has appropriately implemented security measures aligned to established rules needed to obtain security certifications. Depending on the compliance program and its requirements, external auditors may perform testing of media disposal, review security camera footage, observe entrances and hallways throughout a data center, test electronic access control devices, and examine data center equipment.

Networks & Transmission.

Data Transmission. UniSender Datacenters are connected via private links protected by AWS Network firewalls to provide secure data transfer. This is designed to protect the confidentiality, integrity and availability of the network and prevent data from being read, copied, altered or removed without authorization during electronic transfer.

Data Breach Response. UniSender monitors a variety of communication channels for security breaches, and UniSender security personnel will react promptly to known incidents.

External Attack Surface. UniSender considers potential attack vectors and incorporates appropriate purpose built proprietary technologies into external facing systems.



Encryption Technologies. UniSender uses HTTPS encryption (also referred to as SSL or TLS connection).

12. SUBPROCESSOR SECURITY

Before onboarding Sub-processors, UniSender conducts an audit of the security and privacy practices of Sub-processors to ensure Sub-processors provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once UniSender has assessed the risks presented by the Sub-processor then, subject always to the requirements set out in Section 6 of the DPA, the Sub-processor is required to enter into appropriate security, confidentiality and privacy contract terms.

