TrustLayer™

Data Processing Agreement

Version: 1.0

Issued: May 2025

Data Processing Agreement

This Data Processing Agreement ("DPA") forms part of TrustLayer's Master Services Agreement (which can be found at https://trustlayer.co.uk/legal-policy/) and is applicable to the Customer's use of the Service(s) and reflects the Parties agreement with respect to the processing of Personal Data. Capitilised terms not otherwise defined in this DPA will have the respective meanings assigned to them in the Master Services Agreement.

1. Definitions:

1.1 In this Agreement, unless the context otherwise requires, the following words and expressions have the following meanings:

"TrustLayer Personnel"	means all directors, officers, employees, agents, consultants and contractors of TrustLayer and/or any sub-contractor engaged in the performance of its obligations under this Contract.
"Controller"	has the meaning given in the GDPR.
"Data Loss Event"	a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.
"Data Processing Agreement" or "DPA"	means this Agreement, as amended from time to time, made available to Customers by TrustLayer online via its website: https://trustlayer.co.uk/legal-policy/
"Data Subject"	has the meaning given in the GDPR.
"EU Personal Data"	means the processing of Personal Data to which data protection legislation of the European Union, or of a Member State of the European Union or European Economic Area, was applicable prior to its processing by TrustLayer;

"Personal Data"	has the meaning set out in the GDPR and relates only to personal data, or any part of such personal data, of which the Customer is the Controller and in relation to which TrustLayer is providing Service(s) under the Contract.
"Processor" and "processing"	have the meaning set out in the GDPR
"Protected Area"	means, in the case of EU Personal Data, the member states of the European Union and the European Economic Area and any country, territory, sector or international organisation in respect of which an adequacy decision under Art.45 EU GDPR is in force and, in the case of UK Personal Data, the United Kingdom and any country, territory, sector or international organisation in respect of which an adequacy decision under UK adequacy regulations is in force.
"Sub-Processor"	any third party appointed to process Personal Data on behalf of TrustLayer related to this Contract.
"SCCs"	means: (i) in the case of the processing of UK Personal Data, the UK International Data Transfer Agreement issued by the Information Commissioner in accordance with s.119A and in force from 21 March 2022 or the standard contractual clauses for the transfer of personal data to third countries pursuant to the GDPR adopted by the European Commission under Commission Implementing Decision (EU) 2021/914, together with the UK International Data Transfer Addendum issued by the Information Commissioner in accordance with s.119A of the Data Protection Act 2018 and in force from 21 March 2022 as appended to those clauses, populated as appropriate and with any format changes as permitted by clause 17 of such addendum; and (ii) in the case of the processing of EU Personal Data, the standard contractual clauses for the transfer of personal data to third countries pursuant to the GDPR adopted by the European

	Commission under Commission Implementing Decision (EU) 2021/914.
"UK Personal Data"	means the processing of Personal Data to which data protection laws of the United Kingdom were applicable prior to its processing by TrustLayer.

2. Basis for Processing or Sharing:

2.1 Each party shall comply with all applicable requirements of the Data Protection Legislation. This DPA is in addition to, and does not relieve, remove or replace, the Parties obligations under the Data Protection Legislation.

2.2 The Parties acknowledge that for the purposes of the Contract, the Customer is the Controller and TrustLayer is the Processor of any Personal Data.

2.3 The basis for processing and sharing Personal Data under this Contract is in accordance with a lawful basis for processing Personal Data provided for by the Data Protection Legislation. The subject matter of the processing is the performance of the Services (more details of which are set out in Annex A). The obligations and rights of the Customer are as set out in this Contract. Annex C sets out the nature, duration and purpose of the processing, the types of Personal Data we process and the categories of Data Subjects whose Personal Data is processed.

3. Obligations of TrustLayer:

3.1 We shall only process any Personal Data on behalf of you in accordance with the written instructions provided by you and to the extent, and in such a manner, as set out in Annex A and Annex C. If we are required to do otherwise by EU law or EU Member State law (in the case of the processing of EU Personal Data) or by UK law (in the case of the processing of UK Personal Data) then we will promptly notify you of that legal requirement, where possible, before processing the Personal Data unless the law prohibits such information on important grounds of public interest.

3.2 We shall provide all reasonable assistance to you to help you meet your obligations under Articles 32-36 GDPR, taking into account the information available to us and subject to us charging a reasonable fee for such assistance.

3.3 If we receive any complaint, notice or communication which relates directly or indirectly to the processing or sharing of the Personal Data or to either party's compliance with the Data Protection Legislation, we shall promptly notify you and provide reasonable co-operation and assistance (subject to us charging a reasonable fee for such assistance) in relation to any such complaint, notice or communication.

3.4 We shall ensure that we have in place appropriate technical and organisational measures to protect against unauthorised or unlawful processing of Personal Data and to protect against a Data Loss Event. The protective measures take account of:

3.4.1 the nature of the data to be protected;

3.4.2 the harm that might result from a Data Loss Event;

3.4.3 the state of technological development; and

3.4.3 the cost of implementing any measures.

3.5 We shall notify you without undue delay if we become aware of any Data Loss Event or if any Personal Data becomes damaged, corrupted, or unusable. To the extent that we are responsible, we will restore such Personal Data at our own expense.

3.6 At your request, we shall provide you with a copy of all Personal Data held by us in the format and in the media reasonably specified by you.

3.7 Upon termination of the Contract for any reason, we shall cease processing any Personal Data and shall destroy or otherwise dispose of all Personal Data in our possession unless we receive no later than ten (10) days after the effective date of the termination of the Service(s) a request to return that Personal Data to you, unless prevented from doing so by law. You shall pay all reasonable expenses incurred by TrustLayer in disposing of Personal Data.

4. Transfers outside the Protected Area:

4.1 Subject to clause 4.2, we shall not transfer any Personal Data outside of the Protected Area unless your prior written consent has been obtained.

4.2 You acknowledge and consent to the transfer of Personal Data outside of the Protected Area to the Sub-Processors listed in Annex B, as applicable.

4.3 In relation to any transfer of Personal Data to the Sub-Processors outside of the Protected Area (see list in Annex B), we will make such transfer by (i) relying on such Sub-Processor's BCR-

processor instrument (if any); (ii) entering into the appropriate set of SCCs on a processor to processor basis with any such Sub-Processors in relation to such transfer; or (iii) in the case of transfers to the United States, relying on such Sub-Processor's participation in the EU-US Data Privacy Framework and/or the UK Extension to this Framework (together, the "DPF") (if applicable).

4.4 If the SCCs and/or the DPF are subsequently held to be invalid or if any supervisory authority requires transfers made pursuant to such SCCs and/or the DPF to be suspended, we shall discuss in good faith with you ways of providing alternative safeguards or altering the Services so as to meet the requirement.

5. TrustLayer's Personnel:

5.1 We shall ensure that access to the Personal Data is limited to those TrustLayer Personnel who need access to the Personal Data to meet our obligations under the Contract.

5.2 We shall ensure that all TrustLayer Personnel:

5.2.1 are aware both of our duties and their personal duties and obligations under the Data Protection Legislation and this Contract;

5.2.2 are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by you or as otherwise permitted by this Contract;

5.2.3 are subject to appropriate confidentiality undertakings with us (or, if applicable, any Sub-Processor); and

5.2.4 have undertaken adequate training on the Data Protection Legislation relating to the use, care, protection and handling of Personal Data.

6. Rights of the Data Subject:

6.1 We shall notify you promptly if we:

6.1.1 receive a request from a Data Subject for access to that person's Personal Data;

6.1.2 receive a request to rectify, block or erase any Personal Data; or

6.1.3 receive a request from any third party for disclosure of Personal Data where compliance with such a request is required or purported to be required by Law.

6.2 We shall provide you with reasonable co-operation and assistance in relation to any request or event referred to in clause 6.1 (subject to us charging a reasonable fee for such assistance).

6.3 We shall promptly comply with any request from you requiring us to amend, transfer or delete the Personal Data.

6.4 We shall not disclose the Personal Data to any Data Subject or to a third party other than at your request or as provided for in this DPA.

6.5 We will notify you immediately if in our opinion, an instruction to process Personal Data infringes applicable Data Protection Legislation.

7. Rights of the Customer:

You are entitled, on giving us reasonable notice, to audit, inspect or appoint representatives to audit and inspect all facilities, equipment, documents and electronic data relating to the processing of Personal Data by us. We will make available all information to you to demonstrate compliance with our obligations under applicable Data Protection Legislation.

8. Appointment of Sub-Processors:

8.1 Subject to Clause 4, you agree that we can engage the Sub-Processors set out in Annex B to process Personal Data on your behalf. We can at any time appoint a new Sub-Processor provided that we give you 15 days prior notice. If you object to the appointment of a new Sub-Processor within such period you may, by providing written notice to us, terminate the Service which cannot be provided by us without the use of the objected-to Sub-Processor.

8.2 We shall ensure that we enter into written contracts with Sub-Processors which contain provisions which are substantially similar to those set out in this DPA and as are required by applicable Data Protection Legislation.

8.3 We shall remain fully liable to you for all acts or omissions of any Sub-Processor.

9. Review:

We may, at any time, revise this DPA to ensure that it complies with any amendments to the Data Protection Legislation or any guidance issued by the Information Commissioner's Office. Any amendments to this DPA will become effective upon you accepting the terms of any updated Master Services Agreement online.

Annex A – Processing, Personal Data and Data Subjects

1. Introduction:

1.1 The TrustLayer Unified Security Service (USS) platform incorporates multiple security services that may be purchased separately or in any combination, at any time. Not all of the following information may therefore be applicable depending on the specific Service(s) purchased.

Service(s) include:

- Email Security (EMS)
- Compliant Email Archive (CEA)
- Web Security (WS)
- Cloud Access Security Broker (CASB)
- Security Posture Management (SPM)
- Multi-Factor Authentication powered by Entrust (MFA)
- Security Awareness Training (SAT)
- Autonomous Security Engine (ASE) – an integral part of the USS platform

2. Unified Security Service (USS) Platform Security Measures:

2.1 We use world-class, highly accredited providers to deliver USS and associated services that include Amazon and Microsoft. Under GDPR these organisations would be considered Sub-processors.

2.2 In Europe specific data centre locations include London, Frankfurt, Dublin and Amsterdam.

2.3 USS log data is stored in a log database comprised of regional clusters. The region/location is specified at the time of account provisioning.

2.4 We offer a true multi-tenant environment with unique IDs for each tenant/customer and indexes for each service, within a cloud-based data lake. Log data is encrypted at rest.

2.5 A log retention period of thirty (30) days applies to WS, EMS, MFA powered by Entrust, and CASB. These logs can be accessed via the USS user interface for scheduled or on-demand export.

2.6 Log data is archived to Amazon S3 storage in the same 'home' region where it resides for ninety (90) days and is then deleted. This is for backup & recovery purposes only, and not accessible via the USS interface. Log data in S3 is encrypted.

2.7 The only other service-related data is policy/rule/configuration data that is held in a different database called CoreDB. The CoreDB master database is located in Frankfurt. Customers within Europe will be restricted by default to only using EU data centre locations.

2.8 All service-related data is handled in strict accordance with Data Protection Legislation.

3. Service Specific Security Measures:

3.1 Web Security (WS)

The WS service uses the USS infrastructure, notably two databases – one for log data and CoreDB for policy/rule/configuration data described in clause 2 of this DPA.

3.1.1 WS Risks:

- Although the use of https has increased dramatically a significant number of websites still use the unencrypted http protocol. Information sent in requests to and from those sites is therefore unencrypted in clear text and may be intercepted.
- WS is focused on protecting users from harmful, unlawful, offensive or inappropriate content. Harmful content includes web-borne malware as well as phishing sites designed to capture credentials or other confidential information.
- Viewing all an individual user's web activity over time may enable the viewer to make assumptions or gain insight into the particular interests of that user, or draw conclusions in respect of the user's political or religious beliefs.

3.1.2 Scope of Risk:

- TrustLayer Technical Support and Senior Engineering/Development staff could access log information that contains details of user's web browsing activity.
- Only a small number of our staff are involved in the administration of WS systems, or in supporting customers using the service, or those that have access for operational or engineering (software development) reasons have any access to the infrastructure that stores web activity log data.
- An immutable audit trail tracks logins and actions executed within the USS tenant, this data is available in the "Audit Log" report.
- The USS portal supports redaction of report data and this is enabled by default for newly provisioned accounts. Our staff (other than privileged users) cannot see personal information unless you specifically disable the redact data option.

3.1.3 Input data that contains personal data – WS:

- Input data for the WS service is comprised of all http and https web requests and associated metadata. Metadata includes Active Directory (AD) usernames, IP addresses and MAC addresses. Request information is sent securely using ICAP to the TrustLayer cloud and compared against customer configured policy to determine whether the URL is allowed or blocked. A final action is returned to the agent and/or gateway that results in the request being released to the target website, or blocked.
- Each ICAP server stores requests temporarily on an encrypted disk in a transaction log. The servers maintain a transaction log for every log cluster that they are actively handling requests for. A new transaction log is written periodically and shipped to the appropriate log cluster. The temporary log file is then deleted from the ICAP server.

3.1.4 Output data that contains personal data – WS:

- Output data from the WS service is comprised of log data relating to http and https web requests. Log information includes AD usernames, IP addresses and MAC addresses.
- Log data is held online in the regional log cluster specified at the point of account provisioning (the 'home' region) for a period of thirty (30) days. Log data is deleted after that period (but may be downloaded on demand by customers at any time prior to deletion). Archived data is stored on Amazon S3 storage in the same home region and encrypted at rest.

3.2 Cloud Access Security Broker (CASB):

The CASB service uses the USS infrastructure, notably two databases – one for log data and CoreDB for policy/rule/configuration data described in clause 2 of this DPA.

3.2.1 CASB Risks:

- Although the use of https has increased dramatically a number of cloud applications still use the unencrypted http protocol. Information sent in requests to and from those applications is therefore unencrypted in clear text and may be intercepted.
- The TrustLayer CASB service in Inline Mode analyses all http and https requests made to the specific cloud applications included in the Cloud Application Catalogue. The catalogue comprises thousands of business applications and individual user actions that can be performed within those applications.

- The CASB service also includes an Application Programming Interface (API) Mode that uses an API Gateway and API Connectors to major cloud applications.

3.2.2 Scope of Risk:

- Our staff could access log information that contains details of user's cloud application activity.
- Only a small number of our staff are involved in the administration of CASB systems, or in supporting customers using the service, or those that have access for operational or engineering (software development) reasons have any access to the infrastructure that stores cloud application activity log data.
- An immutable audit trail tracks logins and actions executed within the USS tenant, this data is available in the "Audit Log" report.
- The USS portal supports redaction of report data and this is enabled by default for newly provisioned accounts. Our staff (other than privileged users) cannot see personal information unless you specifically disable the redact data option.

3.2.3 Input data that contains personal data – CASB:

- Input data for the CASB service is comprised of all http and https cloud application requests and associated metadata. Metadata includes AD usernames, IP addresses, Real Names, MAC addresses, Email addresses and any captured application data. Request information is sent securely using ICAP to the TrustLayer cloud and compared against customer configured policy to determine whether the user action is allowed, blocked or logged. A final action is returned to the agent and/or gateway that results in the request being released to the target application or blocked (in Inline Mode).
- In Inline Mode each ICAP server stores requests temporarily on an encrypted disk in a transaction log. The servers maintain a transaction log for every log cluster that they are actively handling requests for. A new transaction log is written periodically and shipped to the appropriate log cluster. The temporary log file is then deleted from the ICAP server.
- In API Mode events are written to a transaction file on the API Gateway and shipped periodically to the appropriate log cluster. The temporary log file is then deleted from the API Gateway.

3.2.4 Output data that contains personal data – CASB:

- Output data from the CASB service is comprised of log data relating to http and https cloud application requests. Log information includes AD usernames, IP addresses Real Names, MAC addresses, Email addresses and any captured application data.
- Log data is held online in the regional log cluster specified at the point of account provisioning (the 'home' region) for a period of thirty (30) days. Log data is deleted after that period (but may be downloaded on demand by customers at any time prior to deletion). Archived data is stored on Amazon S3 storage in the same home region and encrypted at rest.

3.3 MFA powered by Entrust (MFA):

The MFA service uses the USS infrastructure, notably two databases – one for log data and CoreDB for policy/rule/configuration data described in clause 2 of this DPA. In addition, an Entrust database stores information to enable authentication requests to be processed that resides on Amazon Web Services (AWS) with locations in Frankfurt, Dublin and the US. The location of AuthDB is selected at the time of service provisioning.

With the exception of CoreDB, the majority of components within the MFA service only store data transiently whilst the user authenticates. Once authentication is complete (successful or failed) the data is deleted.

Lastly the service also includes the actual OTPs that are sent to users by SMS text message, email, using the Entrust mobile app, or a combination of these dispatch methods. For sensitive environments the mobile app for iOS and Android provides full end-to-end encryption of Push Notifications. OTPs are generated in real-time and are only valid for a short period of time. Push Notifications are session specific to prevent phishing or man-in-the-middle attacks.

3.3.1 MFA powered by Entrust Security Risks:

- MFA presents the user with an additional challenge when authenticating to supported applications, services or systems to provide an additional level of identity assurance – and protection – beyond that offered by passwords alone.
- Push Notifications are highly secure and both generated in real-time and session specific.

- If organisations are concerned about the security of the OTP in transit, via SMS or email for example, then use of Push Notifications within the mobile app is recommended as it offers true end-to-end encryption.

3.3.2 Scope of Risk:

- Our staff could access log information that contains details of user's authentication (MFA) activity.
- Only a small number of our staff are involved in the administration of MFA systems, or in supporting customers using the service, or those that have access for operational or engineering (software development) reasons have any access to the infrastructure that stores MFA activity log data.
- An immutable audit trail tracks logins and actions executed within the USS tenant, this data is available in the "Audit Log" report.
- The USS portal supports redaction of report data and this is enabled by default for newly provisioned accounts. Our staff (other than privileged users) cannot see personal information unless you specifically disable the redact data option.

3.3.3 Input data that contains personal data –MFA powered by Entrust:

- Input data for the MFA service is comprised of user authentication requests and associated metadata. Metadata includes Usernames, UPNs, Common Names (Real Names) and IP addresses.
- Requests are transiently held until authentication is complete (successful or failed) at which point all data is deleted.

3.3.4 Output data that contains personal data –MFA powered by Entrust:

- Output data from the MFA service is comprised of authentication log data. Log information includes Usernames, UPNs, Common Names (Real Names), IP addresses and geo location.
- Log data is held online in the regional log cluster specified at the point of account provisioning (the 'home' region) for a period of thirty (30) days. Log data is deleted after that period (but may be downloaded on demand by customers at any time prior to deletion). Archived data is stored on Amazon S3 storage in the same home region and encrypted at rest.
- The Entrust database stores log data online for 6 months in the specified data center (selected at provisioning time). Log data is then archived and deleted after thirty six

(36) months. Archived data is stored on Amazon S3 storage in the same data center as online log data.

- Internal system operation logs are only accessible to a small number of staff and used for troubleshooting only.

3.4 Email Security (EMS):

EMS from TrustLayer is a 100% cloud-based service that analyses email traffic and removes unwanted or malicious messages. The service scans all inbound (and outbound) messages for threats including malware and phishing attacks, and examines URLs embedded in messages protecting users from inappropriate or malicious web pages.

Organisations route email through TrustLayer's Cloud by (a) changing their DNS MX record or (b) using the 'Connector Mode' for Microsoft 365 via Transport Rules.
Certain EMS features use API integration with Microsoft Exchange Online via the MS Graph API and appropriate access must be granted explicitly to use these features (e.g. Post Deliver Deletion of previously delivered messages). Using Microsoft Transport Rules and Connectors requires registration of the TrustLayer Email Security application within Microsoft Entra ID and assigned the Exchange Administrator role.

We use world-class, highly accredited providers to deliver EMS that include Amazon and Microsoft. In Europe specific data centre locations include Frankfurt, Dublin and Amsterdam. Organizations choose which data centre or centres process their mail. In the UK data centre locations include London. In the US data centre locations include Wyoming, Texas and Virginia. Email messages flow through the infrastructure within the selected data centre(s) above and are checked for spam and viruses and other content. If the message is 'clean' it is logged and delivered to the customer's email server. The conversation with the customer's email server is also logged.

Log information includes IP addresses, To, From and Subject fields, server responses, and other metadata, but does not include the message body or any file attachments. Log data is stored in the 'home' region selected at the time of account provisioning. Some log data may be replicated for optimisation, reporting and visualization purposes in the same data centre that processes email traffic. During processing the message is written to disk. Once successfully delivered to the customer's email server it is immediately deleted. This typically takes no more than a few seconds except in the event that processing queues are created through a transient spike in

SMTP traffic. If a message is determined to be spam then the message may optionally be written to a quarantine where it is stored for thirty (30) days. Organization's may choose to delete spam rather than quarantine it. The quarantine is located specifically in the selected regional EMS data centre location used to process messages.

3.4.1 Email Risks:

- It should be noted that email via SMTP is generally sent unencrypted in clear text and routes through numerous network providers, systems and servers between sender(s) and recipient(s). Each of these providers, systems and servers may have a copy of the complete email message.
- The use of Transport Layer Security (TLS) to encrypt server to server transmission of email is becoming increasingly used. There is the option within EMS to use TLS for outbound email with specific domains that support it.
- For sensitive messages, including messages containing personal data, the use of a separate email encryption solution is recommended such as TrustLayer SecureMail.
- It should be further noted that TrustLayer EMS only covers email sent or received externally. Internal messages sent between users is not processed by TrustLayer.

3.4.2 Scope of Risk:

- Our staff could access the message body (including file attachments) of email messages sent or received externally - if they are not encrypted - for the short time that they are written to disk and processed in the TrustLayer Cloud.
- Only a small number of our staff are involved in administration of EMS systems, or in supporting customers using the service, or those that have access for operational or engineering (software development) reasons have any access to the infrastructure that processes and temporarily stores email messages.
- The same small number of our staff could access spam messages that are stored in a quarantine if the service is configured to quarantine messages determined to be spam.
- All service-related data is handled in strict accordance with Data Protection Legislation.

3.4.3 Input data that contains personal data – EMS:

- Input data for the EMS service is comprised of inbound and outbound email messages sent or received externally to or from the organization. Email messages are sent

unencrypted in clear text unless a separate email encryption solution is used or TLS is enforced for outbound email sent to a specified domain.

- Email messages are stored, typically for a few seconds, during analysis and deleted immediately once successfully delivered to your email server.

3.4.4 Output data that contains personal data – EMS:

- Output data from the EMS service is comprised of log data relating to inbound and outbound email messages sent or received externally. Log information includes IP addresses, To, From and Subject fields, URL's, server responses, and other metadata, but does not include the message body or any file attachments unless the message is quarantined.
- Depending on the configuration of the service output data may also include complete email messages that are determined during analysis to be spam messages, if the service is configured to quarantine spam emails rather than delete them. Quarantined messages are stored for thirty (30) days and then deleted.
- Log data is held online for thirty (30) days. Log data is deleted after that period (but may be downloaded on demand by customers at any time prior to deletion).

3.5 Mail Reprocessing and Backup:

3.5.1 In order to maintain a level of service resilience a duplicate copy of any email that enters the 'EventSink' queue for deliver processing will be stored for seven (7) days such that in the unlikely event of a service outage Email messages can be "replayed" for processing and delivery upon service restoration – this mitigates the potential risk of message loss.

3.5.2 Clients are opted-in to this service whereby a TrustLayer Customer ID can be attributed and linked to a message GUID. For messages where the Customer ID is unable to be detected, Email messages will not be saved.

3.5.3 Email messages are kept within a robust cloud-based object storage system (Blob) with service-level encryption. An additional protection layer is present with encryption on the application layer (a unique encryption key per customer is created, and keys stored in a separate secure database from the Blob storage), passwords for this database will follow a regular rotation cadence.

3.6 Compliant Email Archive (CEA):

Compliant Email Archiving is an optional additional service that can be purchased separately or combined with the Email Security (EMS) service.

The Compliant Email Archiving service stores copies of journaled email messages securely. Emails are transferred into the archive either via SMTP from the customer's mail server, or collected via a polling process from a dedicated journal mailbox on the on premise mail server via Exchange Web Services (EWS), or via IMAP connections. Mail servers supported include Office 365 Exchange Online, Exchange 2007/10/13/16/19, and Lotus Domino.

Every archived message is given a unique ID, digitally fingerprinted, encrypted, compressed, timestamped, fully indexed and written to the storage system. All messages at rest are encrypted using 256-bit Advanced Encryption Standard (AES-256)

Data is stored in separate storage repository buckets per tenant / customer. Storage used is Amazon S3 storage buckets within the London or Frankfurt data centres, depending on the location chosen during license provisioning.

Each tenant repository can have its own unique encryption key for the archived data. By default each tenant will use the Global Encryption key which is set up during account creation.

By default, the solution keeps the emails indefinitely. Specific retention periods are available on request.

A secure https portal provides the ability to search the archived messages by date, sender, recipient, keywords in the body and/or attachments. Access to the portal can be within Outlook via a web enabled folder or through any mainstream web browser.

The following pre-defined user roles are available:

- Standard / Basic (LDAP) Users – access to their own nominated email addresses
- Privileged Users – eDiscovery users who can access all/subset of the archived emails, with comprehensive audit trails showing which emails have been searched for and opened

- Data Guardian Users – Date Guardian users have access to audit trails and are able to review Privileged User searches
- Privileged & Delete Users – similar to Privileged Users, with the extended functionality to be able to delete emails from the archive in an audited manner (for example within a 'Right To Be Forgotten' process)
- Administrators – no access to search the archive but can administer accounts and basic settings.

The archiving platform is delivered as a high availability clustered environment layered with Kubernetes and Zookeeper to seamlessly orchestrate archiving activity at very high scale.
The environment is load balanced enabling for load to be shared across the environment.

3.6.1 Scope of Risk

- Only a small number of our staff are involved in administration of CEMA systems, or in supporting customers using the service, or those that have access for operational or engineering (software development) reasons have any access to the infrastructure that processes and stores email messages.
- Our staff could access the message body (including file attachments) of email messages received - if they are errored and not encrypted - for the short time they reside in the error queue prior to being processed into the TrustLayer Archive Cloud.
- All service-related data is handled in strict accordance with Data Protection Legislation.

3.7 Security Awareness Training (SAT):

Security Awareness Training (SAT) is an optional additional service that can be purchased separately or combined with the Email Security (EMS) service. The SAT service provides end users with ongoing, bitesize training and regular phishing simulations delivered directly to their mailbox.

Data is stored in separate storage repository buckets per tenant / customer. Storage used is Amazon S3 storage buckets within the London or Frankfurt data centres, depending on the location chosen during license provisioning. SAT is delivered as a highly resilient, serverless environment not tied to a single geographic location.

The service is administered through a web-based application with all major browsers supported.

By default, the solution stores all reporting and other log data indefinitely. Data can be removed upon request and will be automatically deleted following termination of the service.

The following pre-defined user roles are available:

- Standard – provides standard access for users to their own personalised portal only
- Tenancy Administrators – provides privileged/admin user access for user management, journey management and reporting

3.7.1 Scope of Risk

- Only a small number of staff involved in the administration of SAT systems, or in supporting customers using the service, or those that have access for operational or engineering (software development) reasons, have any accessto the infrastructure that processes and stores course content and other data.
- Our staff could access the email address, first name and last name of users (location and department may also optionally be stored but are not required), along with phishing simulation engagement data (date sent, date passed/failed) and course completion data (status and quiz scores).
- All service-related data is handled in strict accordance with Data Protection legislation – including EU GDPR.

3.8 Security Posture Management (SPM):

The Posture Management module provides a high-level overview of your security risk profile across Infrastructure-as-a-Service (IaaS) and SaaS cloud services. Posture Management scans your connected services for potential misconfigurations and makes recommendations for security and compliance against common regulatory frameworks and standards.

A control is an entity that represents industry best practice, standards, rules and policies. Based on the risk impact and risk likelihood, each control is given a Risk Level (Low, Medium, High, Critical). Scans can be configured to run on a regular cadence, and alerts delivered to email inbox or Microsoft Teams chat channel.

A remediation assistant is available to provide guidance to make the requisite changes for any non-compliant control, either via links to vendor knowledgebase articles, command-line

instructions, or PowerShell scripts. SPM is a tool to help you adhere to best practice, it is not intended as a replacement for a formal audit.

Onboarding of connected applications and services requires configuration within the 3rd party application – depending on the connector this may require creating read-only IAM roles and relevant permissions to access SaaS and IaaS settings to monitor, and/or creating a shared API access key and secret which is input into USS. This is documented for each supported service at: https://help.clouduss.com/posture-management-cspm-sspm/connectors

The Posture Management product uses "connectors" to onboard cloud services for configuration scanning. A license is required per-connector.

3.8.1 Scope of Risk

- The Posture Management module requires read-only access to the connected IaaS or SaaS service. It is the responsibility of the customer to follow the documentation to create the correct permission sets and/or IAM access to the 3rd party service.
- The remediation assistant uses an Open-AI based LLM and custom ChatGPT interface. It is trained based on the 3rd party service provider documentation and answers based on available data and assumes accuracy of said documentation. The assistant is programmed with specific instructions such that it will only provide answers for the specific control within the session and must ignore questions not connected with the control.
- An option exists to mitigate a control that has been marked as non-compliant, for example if a non-connected 3rd party solution is in place (e.g. MFA) or the customer has accepted the risk. When the SPM user marks a control with a "Mitigated" state it is possible to activate a toggle that disables the control from future scans. If this is selected it is the responsibility of the user to ensure the mitigation solution is operational and this setting reversed should the mitigation be removed.

4. Common security considerations across all Services:

4.1 External communication connections:

4.1.1 Infrastructure elements associated with delivery of USS and individual services resides within the data centres described above. Our staff have remote access to these

environments but all connections are protected using Transport Level Security (TLS) encryption (Remote Desktop Protocol and PowerShell), or over Secure Sockets Shell.

4.1.2 Connections to the environments are tightly restricted and only allowed from a list of static IP addresses.

4.2 Authorization and access control:

4.2.1 Access to production systems and associated data is strictly limited to our staff that require that access to perform their role. This includes a small number of staff involved in administration of systems, or in supporting customers using the service, or those that have access for operational or engineering (software development) reasons. No other TrustLayer staff have any access to the infrastructure.

4.2.2 The TrustLayer Joiners Movers Leavers process ensures that authorizations are reviewed whenever an employee joins, changes role, or leaves employment.

4.2.3 In addition to passwords other forms of access control are used extensively throughout the environment – including multi-factor authentication, wherever it is available, to protect user accounts.

4.3 Control of rejected access attempts:

4.3.1 All login attempts – both successful and unsuccessful – are logged. All two-factor authentication events – both successful and unsuccessful – are logged.

4.3.2 Wherever possible user accounts are locked out for thirty (30) minutes if more than 3 unsuccessful login attempts are identified.

4.4 Logging:

4.4.1 All User – and particularly privileged (admin) user activity – carried out by our staff on systems and servers is logged.

4.4.2 All User activity within the admin interface and TrustLayer Unified Security Service portal is also logged. Log data is held for thirty (30) days and then deleted.

4.5 Home offices:

4.5.1 A small number of our staff have company provided PCs that are configured to use VPNs for remote access to infrastructure to enable them to troubleshoot and resolve service issues or to assist customers out of hours. The use of home or private PCs is strictly prohibited.

4.5.2 All connections are protected using TLS encryption.

4.6 Locations for processing:

4.6.1 TrustLayer has the following office locations within the UK:

- Basingstoke
- Bristol

ANNEX B - Sub-processors

As at the date of this Contract, we use the following Sub-processors:

Amazon EC2: Amazon Web Services Inc, 410 Terry Ave North, Seattle, WA, 98109-5210, USA. The Supplier has selected either a specific EU/ESS Datacenter location, or a EU/ESS region (e.g. Western Europe, Northern Europe) depending on the Sub-Processor options provided at the time of provisioning the systems.

AprioriIT: (VRSoft LTD) Headquarters - 34B Kniazia Volodymyra Velykoho St., Dnipro, 49000, Ukraine.

Bitdefender: 15A Orhideelor Road, Orhideea Towers, Bucharest, 6th District, 060071

Boxphish Ltd: 8 Park Row, Leeds, LS1 5HD, UK. *Please note this Sub-processor is only used if Security Awareness Training (SAT) is purchased/used.*

Datadog, Inc.: Headquarters - 620 8th Avenue, 45th Floor, New York, NY 10018, USA.

Entrust Corp: 1187 Park Place, Minneapolis, MN 55379, USA.

Microsoft Azure: Microsoft Ireland Operations Ltd, Atrium Building Block B, Carmenhall Road, Sandyford Industrial Estate, Dublin 18, Ireland. The Supplier has selected either a specific EU/ESS Datacenter location, or a EU/ESS region (eg Western Europe, Northern Europe) depending on the Sub-Processor options provided at the time of provisioning the systems.

Phoenix47 Ltd: 37 Commercial Road, Poole, BH14 0HU.

SendGrid, Inc. (part of Twilio): 1801 California Street, Suite 500, Denver, Colorado 80202, USA. *Please note this Sub-processor is only used if MFA is enabled on portal (USS) logins.*

Sorry App Limited: Building 1, Old Station Business Park, Petworth, West Sussex, UK, GU28 0JF. Please *note this Sub-processor is only used if Customers subscribe to system status updates/notifications.*

Twilio Inc.: 375 Beale Street, Suite 300, San Francisco, CA 94105, USA. *Please note this Sub-processor is only used if MFA is enabled on portal (USS) logins.*

Vade Secure Inc.: 180 Sansome Street, Floor 2 – San Francisco, CA 94104, USA. *Please note this Sub-processor is only used if Email Security is purchased/used.*

zvelo Inc.: 5445 DTC Pkwy #500, Greenwood Village, CO 80111, United States

ANNEX C – Processing Details

1. Data subjects

The personal data processed concern the following categories of data subjects (please specify):

- Customers, Clients and Prospects (including their staff)

2. Categories of Personal Data

The Personal Data processed concern the following categories of data (please specify):

- Basic personal data (for example street name and building number or name (address), postal code, city, country, mobile phone number, first name, last name, initials, email address, domain and related data);
- Authentication data (for example user name, password, audit trail);
- Contact information (for example addresses, email, phone numbers, website address);
- Device identification / Unique identification numbers (for example IP addresses, MAC addresses, logical tag);
- Commercial Information (subscription (license) information, purchase history, payment history);
- Location data (for example, geo-location network data);
- Email activity (inbound and outbound email messages, including attachments);
- Internet activity (for example browsing activity, cloud application activity);
- Any other personal data identified in Article 4 of the GDPR.

Summary of Data Processed (input / output data) by Service:

Service	Input Data	Output Data
Web Security (WS)	• All http and https web requests and associated metadata • Metadata includes Active Directory (AD) usernames, IP addresses and MAC addresses	• Log data relating to http and https web requests. Log information includes AD usernames, IP addresses and MAC addresses
Cloud Application Security (CASB)	• All http and https cloud application requests and associated metadata • Metadata includes AD usernames, IP addresses, Real Names, MAC addresses, Email addresses and any captured application data	• Log data relating to http and https cloud application requests. Log information includes AD usernames, IP addresses Real Names, MAC addresses, Email addresses and any captured application data.

MFA Powered by Entrust (MFA)	• User authentication requests and associated metadata. Metadata includes Usernames, UPNs, Common Names (Real Names) and IP addresses • Mobile phone numbers	• Authentication log data. Log information includes Usernames, UPNs, Common Names (Real Names) and IP addresses
Email Security (EMS)	• Inbound and outbound email messages (including attachments) sent or received externally to or from the organization	• Log data relating to inbound and outbound email messages sent or received externally. Log information includes IP addresses, To, From and Subject fields, server responses, and other metadata, but does not include the message body or any file attachments
Compliant Email Archive (CEA)	• Inbound and outbound email messages (including attachments) sent or received externally to or from the organization	• Inbound and outbound email messages (including attachments) sent or received externally to or from the organization
Security Awareness Training (SAT)	• Email address, first name and last name of user • Location and department (optional)	• Phishing simulation engagement data (date sent, date passed / failed) • Course completion data (status and quiz scores)

3. Special categories of Personal Data (if appropriate)

The Personal Data transferred concern the following special categories of Personal Data:

- None

4. Subject-matter, nature and purposes of processing

The personal data processed will be subject to the following basic processing activities:

Data processing operations are summarised as:

- Receiving data, including collection and recording
- Holding data, including storage, organisation and structuring
- Updating data, including adaptation, alignment and combination
- Computer processing of Personal Data, including data transmission, data retrieval, data access, and network access to allow data transfer if required
- Protecting data, including restricting, encrypting, and security testing.

TrustLayer and TrustLayer's Sub-processors will use and otherwise process Personal Data only in accordance with and as described in the Contract.

Processing to Provide Services

A Service consists of:

- Delivering functional capabilities as licensed, configured, and used by Customer and its users;
- Troubleshooting (preventing, detecting, and repairing problems); and
- Ongoing improvement (making improvements to performance, productivity, reliability, protection offered, and security).

5. Duration of Processing

The Personal Data shall be processed for the term of the Contract or for such longer or shorter period as we provide data processing services under the Contract.

ANNEX D – Security Measures

Description of the technical and organisational security measures implemented by the data importer:

TrustLayer:

The data importer has implemented and will maintain appropriate technical and organisational measures, internal controls, and information security measures intended to protect Customer Data and Personal Data, as defined in TrustLayer's Master Services Agreement, against accidental loss, destruction, or alteration; unauthorised disclosure or access; or unlawful destruction. The technical and organisational measures set forth in Annex A of this DPA are hereby incorporated into this Annex D.

TrustLayer's Sub-processors:

The Sub-processors detailed in Annex B of this DPA all implement and maintain appropriate technical and organisational measures. Details of each Sub-processors' security measures can be found at: https://help.clouduss.com/platform-legal/sccs.