

## DATA PROCESSING AGREEMENT

This Data Processing Agreement (**Agreement**) forms part of the Tessera Design Terms and Conditions (**Terms**) between Tessera Security Ltd (**Processor**) and the customer identified in that agreement (**Customer**) and takes effect when that agreement takes effect. Where this Agreement is appended to or incorporated by reference in the Terms, it does not require separate execution.

Under this Agreement, the Processor processes Personal Data on the documented instructions of the Customer as Controller. The Customer acts as Controller for the purposes of this Agreement, except where it acts as Processor for another Controller in accordance with clause 2. The Processor does not act as a Joint-Controller or independent Controller in respect of any Protected Data processed under this Agreement.

### DEFINITIONS

For the purposes of this Agreement, the following terms: “**Controller**”, “**Data Subject**”, “**Joint-Controller(s)**”, “**Personal Data**”, “**Personal Data Breach**”, “**processing**”, “**Processor**” and “**Sub-Processor**” shall have the meanings given to them in Article 4 of the UK GDPR. The following terms shall have the meanings:

|                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Applicable Privacy Laws</b> | means all data protection and privacy laws applicable to a party, including the UK GDPR as defined in section 3(10) of the DPA 2018; the Data Protection Act 2018 (DPA 2018) and regulations made under it; the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426), as amended; and the General Data Protection Regulation ((EU) 2016/679) to the extent separately applicable to a party. Each party shall have regard to applicable guidance and codes of practice issued by the Information Commissioner ( <b>ICO</b> ) or another relevant supervisory authority ( <b>Supervisory Authority</b> ), but such guidance shall not of itself constitute Applicable Privacy Laws. |
| <b>Customer</b>                | means the customer identified in the Terms.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Protected Data</b>          | means the Personal Data explicitly set out in Part A of this Agreement, which is received from or on behalf of the Customer and/or otherwise processed by the Processor in its capacity as Processor on behalf of the Customer.                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Services</b>                | means the Solution (as defined in the Terms) and any related services provided under the Terms.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

Any other capitalised terms used in this Agreement have the meanings given to them by Applicable Privacy Laws or, where not defined there, in the Terms unless the context requires otherwise.

### Schedule 1 Data Processing

#### 1 SCOPE OF THIS AGREEMENT

For the purposes of this Agreement, the parties acknowledge and agree that:

- (a) This Agreement does not apply to any data which does not constitute Personal Data under the Applicable Privacy Laws, taking into account all means reasonably likely to be used to identify an individual.
- (b) For the avoidance of doubt, the Processor acts solely as Processor in respect of all Protected Data processed under this Agreement. The Processor does not act, and shall not purport to act, as a Controller or Joint-Controller in respect of any Protected Data processed on behalf of the Customer pursuant to this Agreement. The Processor shall process Protected Data only on the documented instructions of the Customer, in accordance with the UK GDPR and the terms of this Agreement.

#### 2 ROLES OF THE PARTIES

The parties agree that this Agreement shall only apply to processing activities whereby:

- (a) Customer acts as Controller and Processor acts as Processor in respect of Protected Data processed by Processor in providing the Tessera Design platform, which uses AI to

generate security design artefacts (including threat models, security requirements, vulnerability and weakness assessments, risk assessments and security architecture material) from Customer-submitted system descriptions, architecture documents and diagrams.

- (b) Where Customer acts as a Processor on behalf of another Controller, Customer warrants that it has that Controller's authority to appoint Processor as a Sub-Processor, that Customer's instructions to Processor are consistent with that Controller's instructions, and that this Agreement satisfies Customer's obligations to flow down the requirements of the UK GDPR. Customer shall indemnify Processor against losses, liabilities, damages, costs and expenses reasonably incurred as a result of any third-party claim arising from a breach of this warranty, and clause 16(f) applies to the conduct of any such claim.

Nothing in this Agreement relieves either party of any of their respective responsibilities or liabilities under the Applicable Privacy Laws.

### **3 CUSTOMER'S COMPLIANCE WITH APPLICABLE PRIVACY LAWS.**

- (a) When acting as Controller, Customer shall at all times comply with all Applicable Privacy Laws. Customer shall ensure all instructions given by it to Processor in respect of Protected Data (including the terms of this Agreement) shall at all times be in accordance with Applicable Privacy Laws. Customer shall be solely responsible for ensuring that it has established and maintains a valid lawful basis for the processing contemplated hereunder, has obtained all applicable consents where required, and has provided all advance notice and information of the processing to any Data Subjects, as required of it under Applicable Privacy Laws.
- (b) The Services are not intended to process special categories of personal data under Article 9 of the UK GDPR or personal data relating to criminal convictions and offences under Article 10 of the UK GDPR. Customer warrants that it shall not submit any such data to the Services without Processor's prior written consent.

### **4 PROCESSOR'S COMPLIANCE WITH APPLICABLE PRIVACY LAWS.**

Processor shall process Protected Data in compliance with the obligations placed on it under Applicable Privacy Laws and the terms of this Agreement.

### **5 INSTRUCTIONS.**

- (a) Processor shall only process (and shall ensure that its personnel and Sub-Processors only process) the Protected Data in accordance with the Customer's documented instructions set out at Part A of this Agreement and the terms of this Agreement, except to the extent:
  - (i) that alternative processing instructions are agreed between the parties in writing; or
  - (ii) otherwise required by Applicable Privacy Laws (in which case, Processor shall inform Customer of that legal requirement before processing, unless applicable law prevents it doing so on important grounds of public interest).
- (b) Processor shall immediately inform Customer if, in its opinion, an instruction infringes Applicable Privacy Laws, and may suspend the affected processing, without liability, until Customer confirms or amends the instruction in a manner that is not infringing.

### **6 SECURITY**

To protect the Protected Data against accidental, unauthorised or unlawful destruction, loss, alteration, disclosure or access, Processor shall implement and maintain appropriate technical and organisational measures in accordance with the UK GDPR and Processor's security commitment set out in Part B of this Agreement.

**7****SUB-PROCESSING**

- (a) Customer grants Processor general written authorisation to appoint Sub-Processors. Processor shall maintain the Sub-processor List referred to in Part C and give Customer at least 30 days' prior written notice of any intended addition or replacement. Customer may object during that notice period on reasonable data-protection grounds. If Customer does not object during that period, the change is deemed authorised.
- (b) If Customer reasonably objects, the parties shall work in good faith to resolve the objection. If they cannot do so before the proposed change takes effect, Customer may terminate the affected Services by written notice and Processor shall refund any prepaid fees for the terminated Services on a pro-rata basis for the unused period.
- (c) Prior to the relevant Sub-Processor(s) carrying out any processing activities in respect of the Protected Data, Processor shall ensure that each such Sub-Processor(s) is bound by a written contract that imposes data protection obligations satisfying Article 28(4) of the UK GDPR and no less protective of Protected Data than those in this Agreement, and that is enforceable by Processor. Processor shall:
  - (i) remain fully liable to the Customer under this Agreement for all the acts and omissions of each Sub-Processor in respect of the Sub-Processor's data protection obligations under this Agreement, as if they were its own (but not to a greater extent than that); and
  - (ii) ensure that all persons authorised by Processor (including Processor's personnel) or any Sub-Processor to process Protected Data are subject to a binding written contractual obligation to keep the Protected Data confidential.
- (d) Where Customer enables an integration with a third-party service that Customer selects and connects using its own credentials (including Jira, Slack, Microsoft Teams or Miro), Processor transmits the relevant Protected Data to that service on Customer's documented instruction. The provider of that service is engaged by Customer, is not a Sub-Processor of Processor, and Customer is responsible for that provider's processing of Protected Data.

**8****DATA SUBJECTS RIGHTS**

- (a) Processor shall (at the Customer's cost and reasonable charge) assist Customer in ensuring compliance with Customer's obligations pursuant to Articles 32 to 36 of the UK GDPR (and any similar obligations under the Applicable Privacy Laws) taking into account the nature of the processing, the information available to Processor, and the extent to which the relevant assistance is within Processor's reasonable ability. Taking into account the nature of the processing, Processor shall (at the Customer's cost and reasonable charge) assist Customer by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer's obligations to respond to requests for exercising the Data Subjects' rights under Chapter III of the UK GDPR (and any similar obligations under Applicable Privacy Laws) in respect of any Protected Data, as this relates to Protected Data.
- (b) Processor shall notify the Customer within 5 Business Days if it receives a request from a Data Subject under Applicable Privacy Laws in respect of Customer's Personal Data; and ensure that it does not respond to that request except on the documented instructions of the Customer or as required by applicable laws to which Processor is subject, in which case Processor shall to the extent permitted by applicable laws inform Customer of that legal requirement before responding to the request.

**9****INTERNATIONAL TRANSFERS**

Protected Data is hosted at rest in the United Kingdom. Processor shall not transfer Protected Data outside the United Kingdom unless the transfer is made under a valid transfer mechanism under Chapter V of the UK GDPR, including applicable adequacy regulations, the UK International Data Transfer Agreement or the UK Addendum to the EU Standard Contractual Clauses, together with supplementary measures where required (including the minimisation measures in Part B). Processor shall put in place, and maintain for the duration of the relevant processing, the applicable transfer mechanism, and shall provide Customer with a copy of the relevant clauses and a summary of the supplementary measures on reasonable request. Processor shall ensure that

any Sub-Processor processing Protected Data outside the United Kingdom is subject to equivalent transfer obligations. Any transfer of Protected Data outside the United Kingdom shall occur only in accordance with this clause, and where a transfer is required by law, Processor shall inform Customer before the transfer to the extent permitted by law.

## **10 AUDITS AND PROCESSING**

Processor shall make available to Customer all information reasonably necessary to demonstrate compliance with Article 28 of the UK GDPR and this Agreement. Customer shall first review documentation made available by Processor. If that is insufficient, Customer may submit a reasonable written questionnaire no more than once in any twelve-month period. If the information and questionnaire are insufficient and an on-site audit is reasonably necessary, Processor shall allow and contribute to an audit by Customer or an independent auditor mandated by Customer (provided such auditor is not a competitor of Processor and has entered into confidentiality undertakings acceptable to Processor), on at least 30 days' written notice. Audits shall be at Customer's cost, subject to confidentiality obligations, conducted during normal business hours and with reasonable protections for Processor's security, other customers and operations. An on-site audit may occur no more than once in any twelve-month period, except following a Personal Data Breach or where required by a Supervisory Authority.

## **11 PERSONAL DATA BREACH**

Processor shall notify Customer without undue delay and, in any event, within 48 hours after becoming aware of any Personal Data Breach in respect of Protected Data, and shall provide, as it becomes available, information reasonably required by Customer to meet its obligations under Applicable Privacy Laws, including the nature of the breach, the categories and approximate numbers of Data Subjects and records affected, the likely consequences, and the measures taken or proposed. Processor shall (at the Customer's cost) cooperate with Customer and take reasonable commercial steps as directed by Customer to assist in the investigation, mitigation and remediation of the Personal Data Breach. Processor's notification of, or response to, a Personal Data Breach shall not be construed as an acknowledgement by Processor of any fault or liability in respect of the Personal Data Breach.

## **12 DELETION/RETURN**

- (a) Upon expiry or termination of the affected Services, Customer shall have thirty (30) days to export Protected Data. Processor shall then securely delete Protected Data and existing copies within a further 30 days, unless Applicable Privacy Laws require continued storage. At Customer's written instruction during the export period, Processor shall return Protected Data or delete it earlier. Protected Data in backups shall be deleted or rendered inaccessible within 90 days after deletion from live systems, subject to any mandatory legal retention requirement.
- (b) Uploaded source files are deleted once read, when the run that references them reaches a terminal state, including success, failure, cancellation, a refused upload or a sweep after a crash, and each deletion is recorded in the audit log. The extracted model, Customer-entered text and Outputs are retained in accordance with clause 12(a) and, where Customer selects extended retention, clause 13.

## **13 EXTENDED RETENTION (WORM)**

- (a) Where Customer enables extended retention, its selection is optional and its selected retention period and storage mode constitute its documented instruction to Processor. At the end of the standard retention period, the affected Protected Data shall be transferred to write-once-read-many immutable storage using AWS S3 Object Lock. Extended retention, the maintenance of WORM storage and any assistance with the override procedure described below are provided at Customer's cost.
- (b) In Governance mode, the data is immutable in normal operation and may be overridden only on Customer's written instruction and only where Customer, or its Controller where Customer acts as Processor, has determined that erasure is required under Applicable Privacy Laws and that Article 17(3)(b) of the UK GDPR does not permit continued retention. Processor acts solely on that determination and instruction, is not required to

assess the legal merits of the determination, and shall have no liability for acting on, or for declining to act in the absence of, such written instruction. Where instructed, Processor shall effect the override under its documented procedure, with a written record of the legal basis provided by Customer, authorisation by a senior member of Processor's security team in accordance with Processor's documented override procedure, dual control where practicable, a tamper-evident audit record and notice to Customer.

- (c) In Compliance mode, no person, including Processor, can delete the data before the selected retention period expires. Customer acknowledges and accepts that it has selected Compliance mode with knowledge that no erasure (including in response to a Data Subject request under Article 17 of the UK GDPR or a request or order from a Supervisory Authority or court) can be actioned until the selected retention period expires, and Customer, or its Controller where Customer acts as Processor, accepts and bears that risk.
- (d) The standard deletion timelines are suspended during an active extended retention period and the affected data shall be deleted within 30 days after that period expires.
- (e) Customer, or its Controller where Customer acts as Processor, is responsible for determining whether its selected retention period and storage mode are necessary and compliant with Applicable Privacy Laws (including Articles 5(1)(e) and 17 of the UK GDPR), remains responsible for its retention selection, and shall be responsible for any claim or liability arising from that selection. Processor's retention and storage of Protected Data in accordance with Customer's selection shall be deemed processing on Customer's documented instructions.

## **14 AI AND MODEL TRAINING**

- (a) The Processor shall not use Protected Data to train its own models or any Sub-Processor's models, and shall ensure that no-training contractual terms apply to any artificial intelligence, machine learning or large language model processing of Protected Data.
- (b) Customer specifically authorises Processor to use Anthropic as a Sub-Processor under the commercial API terms in force between Processor and Anthropic from time to time, provided that those terms include protections materially equivalent to the no-training and zero-data-retention commitments described in this clause. Processor has contracted for, and shall use reasonable endeavours to maintain, terms under which Protected Data is not used to train models and is not retained after completion of the relevant request (a zero-data-retention arrangement). If Processor becomes aware that such terms are no longer in effect, Processor shall promptly notify Customer under clause 7. Any processing of Protected Data by Anthropic outside the United Kingdom shall be subject to a valid transfer mechanism and the supplementary measures described in this Agreement, and the applicable Sub-Processor details and transfer mechanism shall be recorded on the Sub-processor List.
- (c) Outputs are generated by automated means for Customer's review. Processor does not use Protected Data to take decisions about Data Subjects. Customer is responsible for reviewing, verifying and approving each Output before it relies on or exports it, as set out in the Terms. Nothing in this clause makes Processor a Controller of any Protected Data.

## **15 LIABILITY**

As between the parties, each party shall only be liable for their own breach of the Applicable Privacy Laws or of this Agreement and shall not be jointly and/or severally liable for the other party's breach. Liability under this Agreement is subject to the exclusions and limitations of liability in the Terms. Nothing in this Agreement limits any Data Subject's rights or either party's liability to Data Subjects under Applicable Privacy Laws. To the extent that Processor incurs liability to a Data Subject arising from or in connection with Customer's breach of its obligations as Controller under Applicable Privacy Laws or this Agreement, Customer shall indemnify Processor against such liability, and clause 16(f) applies to the conduct of any related claim.

## 16 GENERAL TERMS.

- (a) Confidentiality. Each party must keep confidential all information and data contemplated under this Agreement and must not disclose that information or data except to the extent required to perform or enforce this Agreement, to comply with Applicable Privacy Laws, or as otherwise required by law. This obligation does not apply to information that is or becomes publicly available other than through a breach of this clause, was already known to the receiving party without restriction, was independently developed by the receiving party, or was lawfully received from a third party without restriction. This clause shall survive the expiry or termination of this Agreement.
- (b) Notices. All notices and communications given under this Agreement must be in writing and will be delivered personally, sent by post or by email to the recipient's registered office, principal place of business, or any other address or email the recipient has notified in writing. A notice is deemed received: if delivered personally, at the time of delivery; if sent by pre-paid first class post, on the second Business Day after posting; and if sent by email, on the next Business Day after sending, provided no bounce-back or delivery failure notification is received.
- (c) Governing Law and Jurisdiction. This Agreement is governed by the laws of England and Wales. Any dispute arising in connection with this Agreement will be submitted to the exclusive jurisdiction of the courts of England and Wales.
- (d) If there is any conflict between this Agreement and the Terms concerning the subject matter of this Agreement, this Agreement prevails to the extent of the conflict.
- (e) Processor confirms that it is, and shall remain throughout the term of this Agreement, registered with, or has paid the required data protection fee to, the ICO, as applicable.
- (f) A party seeking to rely on an indemnity in this Agreement must notify the other party promptly of the claim, allow it reasonable control of the defence and settlement, and provide reasonable assistance at its cost. The indemnifying party must not settle a claim in a way that admits liability on behalf of, or imposes an obligation on, the indemnified party without its prior written consent, not to be unreasonably withheld or delayed.

## EXECUTION

**Signed for and on behalf of Processor by a  
duly Authorised Person:**

\_\_\_\_\_  
Signature of Authorised Person

\_\_\_\_\_  
Full Name of Authorised Person

\_\_\_\_\_  
Date

**Signed for and on behalf of Customer by a duly  
Authorised Person:**

\_\_\_\_\_  
Signature of Authorised Person

\_\_\_\_\_  
Full Name of Authorised Person

\_\_\_\_\_  
Date

## Part A Processing Activities

Processing of the Protected Data by Processor under this Agreement shall be for the subject-matter, duration, nature and purposes and involve the types of Personal Data and categories of Data Subjects set out in this Part A.

### Processing particular | Description

|                                             |                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Subject-matter of processing</b>         | Provision of the Tessera Design service: generation of security design artefacts from Customer-submitted system descriptions, architecture documents and diagrams.                                                                                                                                                                      |
| <b>Duration of the processing</b>           | The term of the Agreement, together with the export, deletion and any extended retention periods set out in this Agreement.                                                                                                                                                                                                             |
| <b>Nature and purpose of the processing</b> | Receipt, extraction, hosting, storage, display and analysis of Customer-submitted materials; AI-assisted generation of security design artefacts; transmission to authorised Sub-Processors for hosting and generation; and export and deletion.                                                                                        |
| <b>Type of Personal Data</b>                | Personal Data embedded in Customer Content: names, roles and contact details in architecture documents and system descriptions; identifiers in diagrams; and, where they constitute Personal Data, component and system names, hostnames and IP addresses. Special category data and criminal offence data are excluded under clause 3. |
| <b>Categories of Data Subjects</b>          | Customer's personnel, its clients' personnel and other individuals referenced in submitted system documentation.                                                                                                                                                                                                                        |

## Part B Technical and organisational security measures

In accordance with Applicable Privacy Laws, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing of the Protected Data to be carried out under or in connection with this Agreement, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons and the risks that are presented by the processing, especially from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the Protected Data transmitted, stored or otherwise processed, Processor shall implement appropriate technical and organisational security measures appropriate to the risk, including, as appropriate, those matters mentioned in Articles 32(1)(a) to 32(1)(d) (inclusive) of the UK GDPR, to Protected Data.

### Encryption and key management

The Processor shall encrypt Protected Data in transit using TLS and encrypt Protected Data at rest using appropriate encryption controls. Protected Data is hosted in the United Kingdom on AWS in the eu-west-2 region.

### Access control and authentication

The Processor shall maintain role-based access controls designed to ensure that only authorised personnel with an operational need can access Protected Data, with authentication through the platform identity provider and multi-factor authentication for administrative access.

### Tenant isolation

The Processor shall maintain tenant-scoped data isolation at the data layer and controls designed to prevent unauthorised cross-customer access to Protected Data.

### Audit logging and accountability

The Processor shall maintain security logging and monitoring appropriate to the Services, including an audit trail of engagement activity attributed to the acting principal.

### Data residency and sub-processor governance

Protected Data at rest shall be hosted in the United Kingdom in AWS eu-west-2. The Processor shall assess each Sub-Processor before Protected Data is made available to that Sub-Processor and maintain governance over Sub-Processor access to Protected Data.

**Resilience, backup and recovery**

The Processor shall maintain backup, restoration and resilience measures appropriate to the Services and the risks associated with the processing of Protected Data, with defined purge cycles and a maximum 90-day retention period for deleted data in backups.

**Vulnerability and patch management**

The Processor shall maintain vulnerability and patch management processes appropriate to the Services and the risks associated with the processing of Protected Data.

**Secure development and change control**

The Processor shall maintain change control processes for production systems used to process Protected Data, including appropriate review and validation before deployment.

**Incident detection and response**

The Processor shall maintain an incident response procedure covering detection, triage, containment, notification, recovery and review.

**Personnel and confidentiality**

The Processor shall bind personnel and Sub-Processors by written confidentiality obligations and shall restrict access to Protected Data to personnel with a specific operational need.

**Human oversight of automated processing**

The Services require a Customer user to review and confirm each Output before it can be exported. Processor's personnel do not review Outputs or take decisions about Data Subjects.

**Data minimisation before AI transmission**

Before transmitting text to an AI Sub-Processor, Processor shall use reasonable-endavours, pattern-based minimisation on text only. This process does not cover text in images, diagrams, screenshots or images embedded in uploaded documents. Structural identifiers, including component and system names, hostnames and IP addresses, are transmitted.

**Part C Processor's appointed Sub-Processors**

| <b>Sub-Processor</b>          | <b>Processing Activity</b>                                                                                                                                                                                                                                                                                                                                                    | <b>Location (inside or outside of the UK or EEA)</b> | <b>Compliance URL</b>                                                                                                           | <b>International Transfer Mechanism</b>                                                                                                                                                                                                                                          |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Amazon Web Services EMEA SARL | Hosting and operation of the Services: compute, managed database (engagement data and Outputs at rest) and object storage (uploaded source files, transiently). Authentication (Amazon Cognito), transactional email (Amazon SES) and optional SMS notifications (Amazon SNS), which carry only account and contact details, the engagement name, headline counts and a link. | United Kingdom (AWS eu-west-2, London)               | <a href="https://aws.amazon.com/service-terms/">https://aws.amazon.com/service-terms/</a> (AWS Data Processing Addendum)        | None: no restricted transfer. Protected Data is hosted and processed in AWS eu-west-2 and encrypted in transit and at rest.                                                                                                                                                      |
| Anthropic Ireland, Limited    | AI generation: after minimisation under Part B, the Customer's system description is sent to the Claude API and generated content is returned. Processing is transient, under zero-data-retention and no-training terms (clause 14). This is the only point at which Customer Content leaves AWS.                                                                             | Outside the UK (principally the United States)       | <a href="https://www.anthropic.com/legal/data-processing-addendum">https://www.anthropic.com/legal/data-processing-addendum</a> | UK Addendum to the EU Standard Contractual Clauses (Module Three), incorporated in Anthropic's Data Processing Addendum. Supplementary measures: zero data retention, no training, minimisation of text (not text in images, diagrams or screenshots) and encryption in transit. |