Data Processing Agreement (DPA)

Version ID: dpa/2026-11/en

Annex to the Halocline Desktop License Terms and the Halocline Web & XR Terms of Use

This English version is a convenience translation. The German version is legally binding.

Version 2026-11, valid from November 18, 2026

between

the Customer, as identified by the data provided during registration or ordering or by the offer

– hereinafter referred to as the "Controller" –

and

Halocline GmbH & Co. KG, Netter Platz 3, 49090 Osnabrück

– hereinafter referred to as the "Processor" –

and jointly referred to as the "Contracting Parties",

the following is agreed:

Section 1 Subject matter and duration of the processing

The Processor carries out the data processing operations listed in Annex 1. That Annex describes the subject matter, nature, purpose and duration of the processing as well as the categories of data processed and of data subjects. This Agreement applies to all products of the Processor that the Controller uses (Halocline Desktop, Halocline Web & XR), to the extent that processing on behalf of the Controller pursuant to Annex 1 takes place in them.

Section 2 Instructions of the Controller

(1) The Processor shall process personal data only for the purposes listed in Annex 1 or only on documented instructions from the Controller, unless required to do so by Union law or by the law of a Member State to which the Processor is subject. In such a case, the Processor shall inform the Controller of those legal requirements before processing, unless that law prohibits such information on important grounds of public interest.

(2) The Processor shall inform the Controller without undue delay if, in its opinion, an instruction given infringes applicable data protection provisions of the Union or of a Member State.

(3) Processing by the Processor of the personal data provided to it for other purposes, in particular for its own purposes, is not permitted.

(4) The Controller shall ensure that no special categories of personal data (Art. 9 GDPR) and no personal data that are not necessary for handling the respective support case are transmitted via the Processor's support channels.

Section 3 Technical and organizational measures

(1) The Processor shall implement at least the technical and organizational measures listed in Annex 3 to ensure the security of the personal data. The measures shall ensure a level of protection appropriate to the risk. In assessing the appropriate level of protection, the Contracting Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of the processing and of the data categories (in particular pursuant to Art. 9(1) or Art. 10 GDPR) as well as the varying likelihood and severity of the risk for the data subjects.

(2) The technical and organizational measures listed in Annex 3 are subject to technical progress and further development. They shall be adapted by the Processor if the level of security defined at the time of conclusion of the Agreement can no longer be ensured. The adaptation must achieve at least the level of protection of the previous measures. Unless otherwise specified, the Processor shall notify the Controller of material adaptations, without being requested to do so, in text form to the Controller's Admins.

Section 4 Obligations of the Processor

(1) The Processor confirms that it is aware of the relevant data protection provisions. Within its area of responsibility, it shall organize its internal organization in such a way that it meets the specific requirements of data protection.

(2) The Processor shall grant its personnel access to the personal data undergoing processing only to the extent strictly necessary for implementing, managing and monitoring the Agreement. The Processor shall ensure that the persons authorized to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(3) To the extent required by law, the Processor shall designate a data protection officer and communicate that officer's contact details in Annex 2. The Processor shall provide information without undue delay and without being requested to do so about any change of the data protection officer.

(4) The Processor shall perform the processing on behalf of the Controller in the territory of the Federal Republic of Germany, in a Member State of the European Union or within the European Economic Area. The processing of personal data in a third country always requires the prior documented consent of the Controller and may only take place if the specific statutory requirements of the GDPR are met. Consent is deemed given for the third-country references stated in Annex 1.

Section 5 Assistance obligations of the Processor

(1) Taking into account the nature of the processing and the information available to it, the Processor shall assist the Controller in carrying out a data protection impact assessment and any consultation of the supervisory authorities that may be required, and in fulfilling the Controller's obligation to respond to requests from data subjects to exercise their rights. The Processor shall inform the Controller without undue delay of any assertion of rights by the data subjects affected by the data processing operations.

(2) The Processor assures assistance in examining data protection breaches and in implementing any reporting and notification obligations, as well as in complying with the obligation to ensure that the personal data are accurate and up to date.

(3) Furthermore, the Processor shall provide assistance by means of appropriate technical and organizational measures so that the Controller can fulfill its existing obligations towards the data subject.

Section 6 Authorization to establish sub-processing relationships

(1) The Processor has the Controller's general authorization for the engagement of sub-processors. The Processor shall inform the Controller at least three weeks in advance, in text form to the Controller's Admins, of all intended engagements of sub-processors, so that the Controller can raise objections before the engagement. The Processor shall provide the information that the Controller needs in order to decide on the exercise of its right to object together with the information on the planned engagement. The current list of sub-processors is available at https://halocline.io/en/sub-processors. The use of the sub-processors listed in Annex 1 at the time of conclusion of the Agreement is deemed authorized, provided that the requirements set out in Section 6(2) of this Agreement are implemented. If the Controller raises justified objections within two weeks of receipt of the notification and the parties do not find an amicable solution, the Controller may terminate the contract for the affected product without notice as of the time of the intended engagement.

(2) Access to personal data by the sub-processor may only take place once the Processor has ensured, by way of a written contract, which may also be concluded in an electronic format, with the sub-processor that the provisions agreed in this Agreement also apply to the sub-processor. At the Controller's request, the Processor shall provide the Controller with a copy of the contract and of any subsequent amendments. The Processor shall be fully liable to the Controller for the sub-processor's compliance with its contractual obligations. The Processor shall notify the Controller of contractual breaches of duty by the sub-processor.

(3) In the case of sub-processing that involves a transfer of personal data within the meaning of Chapter V of the GDPR, the Processor shall ensure compliance with the provisions of Articles 44 et seq. GDPR by providing, where necessary, appropriate safeguards pursuant to Article 46 GDPR.

(4) In cases in which it uses a sub-processor and in which the processing activities involve a transfer of personal data within the meaning of Chapter V of the GDPR, the Processor undertakes to conclude Standard Contractual Clauses pursuant to Art. 46 GDPR with the sub-processor, provided that the conditions for the use of those Standard Contractual Clauses are met.

(5) In the case of Section 6(4), the Processor shall carry out an assessment pursuant to Clause 14 of the Standard Contractual Clauses (Transfer Impact Assessment) and make it available to the Controller on request; the obligations under Clause 15 of the Standard Contractual Clauses shall be observed. If the Processor or the Controller concludes that further measures must be taken in order to achieve an adequate level of protection, those measures shall be taken by the Processor or by the sub-processor, as the case may be. The sub-processor may only be involved in the data processing once an adequate level of protection has been ensured.

Section 7 Audit rights of the Controller

(1) The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in this Agreement or stemming directly from the GDPR. At the Controller's request, the Processor shall also allow for the audit of the processing activities covered by this Agreement at reasonable intervals or if there are indications of non-compliance, and shall contribute to such an audit. In deciding on a review or an audit, the Controller may take into account relevant certifications within the meaning of Art. 28(5) GDPR held by the Processor. Evidence shall be provided primarily by making available suitable documentation and relevant certifications; on-site audits may be considered to the extent that such evidence is not sufficient in the individual case.

(2) The Controller may carry out the audit itself or mandate an independent auditor. The audits may, where appropriate, also include inspections at the premises or physical facilities of the Processor and shall be carried out with reasonable notice and in compliance with the Processor's trade and business secrets and, where possible, without disrupting business operations. Regular audits shall take place no more than once per calendar year and shall be announced at least four weeks in advance; event-driven audits where there are indications of non-compliance remain unaffected. The costs of an auditor mandated by the Controller shall be borne by the Controller.

(3) The Contracting Parties shall make the information referred to in this Agreement, including the results of audits, available to the competent supervisory authorities on request.

Section 8 Infringements to be notified

(1) The Processor shall inform the Controller without undue delay of disruptions to business operations that entail risks for the Controller's data, as well as when it becomes aware of data protection breaches in connection with the Controller's data. The same applies if the Processor finds that the security measures it has taken do not meet the statutory requirements.

(2) The Processor is aware that the Controller is obliged to comprehensively document all personal data breaches and, where applicable, to report them to the supervisory authorities or to the data subject. It shall report breaches to the Controller without undue delay and, in doing so, communicate at least the following information:

- a description of the nature of the breach, where possible including the categories and approximate number of data subjects and data records concerned,
- name and contact details of contact persons for further information,
- a description of the likely consequences of the breach, and
- a description of the measures taken or proposed to address the breach or to mitigate its resulting adverse effects.

Section 9 Termination of the processing

(1) Upon termination of the processing on behalf of the Controller, personal data shall, at the choice of the Controller, be deleted from the active systems or returned, unless there is a statutory obligation to store them. Return takes place by making the data available for retrieval in accordance with the terms of the respective product. If the Controller does not make a choice by the end of this provision period, the data are deleted. Existing backup copies are overwritten on a rotating basis as part of the regular backup cycle and are no longer available after expiry of the retention period defined in the technical and organizational measures; deleted data are not restored from backups. The deletion shall be notified to the Controller in text form.

(2) The Controller may terminate the processing relationship without notice if the Processor commits a serious breach of the provisions of this Agreement or of data protection provisions and the Controller therefore cannot reasonably be expected to continue the processing on its behalf until the expiry of the notice period or until the agreed termination of the processing.

(3) The Processor may terminate the processing relationship without notice if the Controller insists on compliance with its instructions although those instructions infringe applicable legal requirements or this Agreement and the Processor has informed the Controller thereof.

Section 10 Conclusion, form and final provisions

(1) This Agreement is an annex to the Halocline Desktop License Terms and the Halocline Web & XR Terms of Use. It is concluded when the Controller accepts the respective Terms in the registration or ordering process or accepts an offer of the Processor to which it is attached (Art. 28(9) GDPR, electronic format). The version valid at the time of conclusion is authoritative; the Processor shall make that version available to the Controller in a storable form together with the confirmation of the conclusion of the contract and shall keep it available for retrieval.

(2) The term of this Agreement corresponds to the term of the contract for the use of the respective product. It ends upon termination of that contract, to the extent that the Processor no longer processes any personal data of the Controller.

(3) Should the Controller's property held by the Processor be endangered by measures of third parties (for example by attachment or seizure), by insolvency proceedings or by other events, the Processor shall notify the Controller without undue delay. A right of retention is excluded with regard to data carriers and data stocks of the Controller.

(4) Amendments to the Agreement and ancillary agreements shall be made in writing, which may also be done in an electronic format. Amendments to this Agreement by the Processor are governed by the amendment procedure of the Terms (E.7 there): announcement in text form to the Admins, acceptance by an Admin; without acceptance, the previous version applies. For free contracts and educational licenses, continued use after the amendment takes effect is possible only after acceptance; for paid contracts, the amended version is deemed accepted from the next renewal if the Controller does not terminate by the end of the current term. The engagement of new sub-processors is governed exclusively by Section 6.

(5) In the event of a contradiction between these contractual clauses and the provisions of related agreements that exist between the parties or are entered into or concluded later, these clauses shall prevail in matters of data protection.

(6) Should individual parts of this Agreement be invalid, this shall not affect the validity of the remainder of the Agreement.

Where concluded by way of an offer:

Controller	**Processor**
Place, date:	Place, date:
Signature:	Signature:

Annex 1

List of the commissioned services and the sub-processors, including the processing locations

Halocline processes license, authentication, analytics and support communication data as an independent controller (Art. 4(7) GDPR); the support communication itself (contact details, case description, correspondence) is not subject matter of this Agreement. Details are set out in the public privacy notice for the respective product (Halocline Desktop: https://halocline.io/en/privacy/desktop; Halocline Web & XR: https://halocline.io/en/privacy/web-xr). The entry "Support attachments" below applies to attachments that the Controller or its Users transmit in the context of a support request.

Which of the following processing activities take place in the individual case depends on the product used by the Controller and the features activated.

Processing activity	**Provision and operation of the cloud service Halocline Web & XR**
Purpose	Hosting and processing of the data contributed by the Controller in tenant-specific product databases and file containers
Data categories	Content entered or uploaded by the Controller and its Users, to the extent that it contains personal data (e.g. names in planning states, comments, files); editor and change attributions
Legal basis	Processing on behalf of the Controller (Art. 28 GDPR); the legal basis of the processing is determined by the Controller
Data subjects	Users of the Controller; persons whose data are contained in the contributed content
Recipients / sub-processor	Microsoft Ireland Operations Limited (Azure Frankfurt/DE; SQL databases, Blob Storage); DPA via the Microsoft Products and Services DPA. Hetzner Online GmbH (Nuremberg/DE; databases administered by Halocline); DPA concluded
Retention period	Duration of the processing on behalf of the Controller; upon termination, deletion or return pursuant to Section 9 (deletion of product database and file container as a unit)
Third-country transfer	No third-country transfer

Processing activity	**Data-Sync for Halocline Desktop (optional add-on service, only if commissioned by the Controller)**
Purpose	Synchronization of planning data between devices
Data categories	Synchronized project data of the Controller, to the extent that they contain personal data (e.g. names in planning states, comments, files); synchronization metadata; editor and change attributions
Legal basis	Processing on behalf of the Controller (Art. 28 GDPR); the legal basis of the processing is determined by the Controller
Data subjects	Users of the Controller; persons whose data are contained in the synchronized project data
Recipients / sub-processor	Hetzner Online GmbH (Nuremberg/DE; databases administered by Halocline); DPA concluded. Microsoft Ireland Operations Limited (Azure Frankfurt/DE; synchronization service, Blob Storage); DPA via the Microsoft Products and Services DPA
Retention period	Duration of the processing on behalf of the Controller; upon termination, deletion or return pursuant to Section 9
Third-country transfer	No third-country transfer

Processing activity	**Support attachments (files that the Controller or its Users attach to a support request; all products)**
Purpose	Handling of the respective support case
Data categories	Personal data in attached files (e.g. screenshots, excerpts from planning states, log files), where present; which files are attached is determined by the Controller or its Users

Processing activity	Support attachments (files that the Controller or its Users attach to a support request; all products)
Legal basis	Processing on behalf of the Controller (Art. 28 GDPR); the legal basis of the processing is determined by the Controller
Data subjects	Users of the Controller; persons whose data are contained in the attached files
Recipients / sub-processor	Support ticket system: Zendesk, Inc. (USA); storage in the EU data region (data center in Ireland). For support or other services that Halocline requests from Zendesk, Zendesk and its sub-processors may process data outside the EEA in individual cases; Halocline's support for its customers is not affected by this. The basis is the adequacy decision on the EU-U.S. Data Privacy Framework (Art. 45 GDPR), under which Zendesk, Inc. is certified; in addition, Zendesk's approved Binding Corporate Rules apply (Art. 46(2)(b), Art. 47 GDPR). DPA concluded. Until handover to Zendesk for requests via the website: Hetzner Online GmbH (Nuremberg/DE, website server); attachments deleted immediately after handover, backups of the website server are overwritten after 14 days. If Zendesk is not reachable: Microsoft Ireland Operations Limited (Azure Communication Services, Frankfurt/DE; email dispatch to the support team)
Retention period	Deletion with the respective ticket, at the latest 3 years after closure of the support case. Upon termination, the attached files are removed from the organization's tickets pursuant to Section 9. On documented instruction, individual attached files are removed from the affected ticket; this is also possible for tickets that have already been closed. If removal is not technically provided for the respective inbound channel, removal takes place by deleting the affected ticket.
Third-country transfer	Possible in individual cases (Zendesk, see recipients); safeguarded by the EU-U.S. Data Privacy Framework (Art. 45 GDPR) and Binding Corporate Rules (Art. 46(2)(b), Art. 47 GDPR)

Annex 2

Contact details of the data protection officers

Role	Contact
Data protection officer of the Controller	As communicated by the Controller; where concluded by way of an offer, named in the offer
Data protection officer of the Processor	datenschutz nord GmbH, Konsul-Smidt-Str. 88, 28217 Bremen, Germany, email: office@datenschutz-nord.de

Annex 3

Technical and organizational measures for IT security pursuant to Art. 32 GDPR

Status of the technical and organizational measures at the time of conclusion of the Agreement. Adaptations are governed by Section 3(2) of this Agreement.

0. Scope and updating

These measures apply to the cloud service operated by Halocline, including Data-Sync. The client software operated locally at the Customer's site is within the Customer's operational responsibility; it is subject to the measures of the respective customer organization.

The measures are subject to technical progress and further development; they may be adapted provided that the level of protection of the agreed measures is not undercut. Material adaptations are communicated to the Controller.

1. Technical measures

1.1 Encryption

Transmission (in transit):

- All externally reachable endpoints enforce HTTPS with current transport encryption (TLS 1.2 or higher; modern TLS policy at the gateway, permanent redirection of unencrypted requests).
- No unencrypted transmission of personal data; the connections to the databases administered by Halocline on rented hosting infrastructure also require TLS.

Storage (at rest):

- Microsoft Azure SQL databases: Transparent Data Encryption (TDE).
- Azure Storage: encryption at rest with Microsoft-managed keys.
- Disks of the databases administered by Halocline on rented hosting infrastructure: full-disk encryption (AES-256); the protection is effective against physical access to the storage media.

Key management:

- Cryptographic material is held in managed key vaults, separate from the application and middleware layer; application secrets of the platform-hosted services are resolved at runtime via the managed identity of the respective service.
- TLS certificates are issued and renewed automatically.
- Access secrets outside this pattern are rotated on a fixed schedule.

1.2 Access control for production systems

- Access to production systems takes place via personalized accounts with role-based access control (RBAC) in accordance with the principle of least privilege.
- Administrative privileges reside on dedicated accounts that are separate from the everyday account; administrative sign-ins to the cloud management consoles require phishing-resistant multi-factor authentication via a controlled network path; the console of the hosting provider requires a personal account with a second factor. The only exceptions are sealed, monitored emergency access accounts.
- Sealed emergency access (break-glass) with sign-in alerting is set up.
- Technical identities are inventoried and assigned to a named responsible person.
- Company devices are centrally managed and fully encrypted; remote lock and remote wipe are available.
- Access rights are centrally managed and are revoked upon departure as part of the documented offboarding process.

- The managed Azure databases do not accept public network access; storage accounts for customer data and backups deny public network access by default. Databases that Halocline administers under its own software responsibility on rented infrastructure of a hosting provider are reachable exclusively via controlled network paths; access requires multi-factor authentication.

1.3 End-user authentication

- Customer authentication takes place via Microsoft Entra External ID (B2C) with secure local accounts.
- Integrated password complexity requirements and account lockout mechanisms in accordance with Microsoft Entra Security Standards.
- Token-based session management; passwords are not stored in Halocline's own systems.
- Authentication processes are based on secure OAuth2/token mechanisms.

Note: Password quality on the end-user side is the responsibility of the respective customer organization. Halocline provides the technical security mechanisms (complexity rules, lockout) via Entra External ID, but cannot exercise any control over actual user behavior.

1.4 Network security

- Exclusively encrypted external communication (see 1.1).
- Network segmentation via virtual networks and dedicated subnets; network access rules restrict inbound and outbound traffic to defined rules.
- A web application firewall at the gateway detects and logs attack patterns; the authentication endpoints are subject to rate limiting.
- Baseline protection mechanisms of the cloud platform against volumetric attacks.

1.5 Physical access control and tenant separation

Server infrastructure: Halocline does not operate its own hosting data center for the cloud service; the production infrastructure is provided entirely via Microsoft Azure (Frankfurt) and Hetzner Online GmbH (Nuremberg). The physical protection of the data centers is the responsibility of the respective providers (Microsoft: among others, ISO 27001-certified data centers; Hetzner: its own data centers in Germany with physical access control systems, video surveillance and security personnel). The company's own equipment room serves exclusively internal build and CI infrastructure and lies outside the customer data path.

Office premises: Access to Halocline's office premises is secured by an electronic physical access control system. Only authorized employees are granted access.

Home office: Halocline employees are contractually obliged to adequately secure their work area in the home office against unauthorized physical access. Access to company systems takes place via centrally managed devices; administrative access requires multi-factor authentication (see 1.2).

Tenant separation:

- Customer data are kept separate per tenant: product databases and file containers are dedicated per Customer; a documented separation concept specifies, per service, how the separation is achieved and where it is enforced.

- Cross-tenant access is prevented by role-based and token-based access controls of the authorization layer.

1.6 Availability, data backup and recoverability

- Automated, regular backups of the production databases over defined retention periods: backups of the self-operated data stores are transferred in encrypted form to a separate location of a different provider; the platform-managed data stores are protected by the mechanisms of the platform (point-in-time restore for the managed Azure databases, soft delete for stored files). Details are governed by the backup and recovery concept.
- The databases administered by Halocline on rented hosting infrastructure are designed redundantly with automatic failover.
- Restores are tested regularly; execution and result are documented.
- A documented emergency and restart plan with defined recovery objectives is in place.
- The availability of the monitoring components is itself monitored, supplemented by independent external availability checks outside the primary cloud environment; disruptions are alerted to responsible employees.
- Infrastructure deployments take place via infrastructure as code for consistent and reproducible environments.

1.7 Logging and traceability

- Access to personal data and administrative activities are logged; the operational logging of the cloud service takes place within the cloud platform environment.
- Changes to personal data and to system configurations are traceable (logging of administrative activities, versioning of the infrastructure as code, deployment history).
- Authentication events are recorded via Microsoft Entra Audit Logging.
- Log data are retained for the period defined in the logging policy and then deleted automatically.
- Security-relevant events are monitored automatically; alerts are prioritized by severity.
- Access to log data is governed by role-based access controls.

1.8 Vulnerability and patch management, secure development

- Security updates are applied within defined time windows; the server hosts under Halocline's own operating system responsibility receive scheduled signature-based malware scans and automatic security updates.
- Host configurations are regularly checked against documented hardening baselines.
- The development process comprises code reviews by qualified developers, static analysis of Halocline's own source code and the continuous evaluation of confirmed vulnerability information for third-party libraries in use; findings are classified according to defined severity criteria and remediated within defined time windows.
- Security and data protection requirements are integrated into the development process.

1.9 Separation of test and production environments

- Production environments are logically separated from test and development environments by separate subscriptions and separate deployments; data from the production environment are not used in test or development environments.
- A shared analytics component ingests exclusively telemetry of the client software (from production and internal use together); data from the operation of the cloud service are not processed there. Access and data stocks are strictly separated via indices and access rights, access lies with a few named administrators, Customers have no access.

2. Organizational measures

2.1 Governance, responsibilities and effectiveness review

- Halocline operates a structured information security governance framework; information security responsibilities are assigned to clearly defined roles (CISO, external data protection officer).
- Processing activities are assessed on a risk basis with regard to technical and organizational security measures pursuant to Art. 32 GDPR; the assessments are documented.
- A process for regularly testing, assessing and evaluating the effectiveness of the measures is established: internal audits, annual management review and defined technical checks per area of measures.

2.2 Confidentiality, training and awareness

- Employees with access to personal data are bound to confidentiality under their employment contracts.
- Regular data protection and information security training is carried out; participation is documented.

2.3 Sub-processor management

- Service providers are selected on the basis of defined security and data protection criteria; new service providers undergo an internal review before onboarding.
- Data Processing Agreements pursuant to Art. 28 GDPR are concluded with all relevant service providers.
- Compliance with the requirements is verified on the basis of the contractually provided evidence; the review frequency follows the risk classification of the service provider.

2.4 Privacy by design and by default

- Personal data are limited to the minimum necessary for the purpose of the processing (data minimization).
- Tracking and analytics data are processed without direct identifiers (name, email address).

2.5 Handling of security incidents and data protection breaches

- A documented process for the identification, assessment, classification and escalation of security incidents is established; a designated response function with a deputy arrangement coordinates the handling.
- In the event of personal data breaches, the Controller is informed without undue delay, with the information pursuant to Art. 33(3) GDPR (nature of the breach, categories concerned and approximate number, contact point, likely consequences, measures taken and proposed), so that the Controller can fulfill its reporting and notification obligations (Art. 33, 34 GDPR) in due time.
- Halocline assists the Controller in the investigation, in notifications to supervisory authorities and in the communication to data subjects within the scope of the contractual obligations.
- Security incidents are documented; after closure, the remediation is recorded and affected Customers are informed in accordance with the contractual agreements.

2.6 Deletion and return of personal data

- Upon termination of the processing on behalf of the Controller, personal data are, at the choice of the Controller, deleted or returned, unless there is a statutory retention obligation; the deletion is notified in text form.
- Deletion takes place at tenant level: the Customer's product database and file container are deleted as a unit.
- Existing backup copies are overwritten on a rotating basis as part of the regular backup cycle and are no longer available at the latest 379 days after deletion from the active systems (retention of twelve monthly generations plus 14 days of deletion protection of the backup storage); deleted data are not restored from backups.
- A documented deletion concept governs responsibilities, deadlines and evidence.