Klar Insights GmbH
Clemensstr. 2
80803 München
Deutschland

dpa

Stand: 07.07.2026

Agreement on the Processing of Personal Data

within the Meaning of Art. 28 Para. 3 of Regulation (EU) 2016/679 (GDPR)

> For legal interpretation, the German version of this Document is legally binding. This English translation is provided for convenience only and is a result of automated processing.

– Data Processing Agreement –

on behalf of

Name/Company _____

Street, House Number _____

Postcode, City _____

– Controller within the meaning of Art. 4 No. 7 GDPR –

– hereinafter referred to as "Client" –

by

Klar Insights GmbH

Clemensstr. 2

80803 Munich

– Processor within the meaning of Art. 4 No. 8 GDPR –

– hereinafter referred to as "Processor" –

– hereinafter also individually referred to as "Party" or jointly "Parties" –

§1 Subject Matter and Duration of Data Processing

1. Details regarding the subject matter and duration of processing are set out in the General Terms and Conditions (Terms of Use) concluded between the parties and underlying this Agreement, in their current version published on the website (hereinafter referred to as the Main Agreement). This Agreement is legally independent and shares the legal fate of the Main Agreement; a termination of the Main Agreement automatically also causes a termination of this Agreement. The parties are aware that no (further) data processing may be carried out without a valid data processing agreement.
2. An isolated ordinary termination of this Agreement is excluded.

§2 Specification of the Order Content

1. Within the scope of the order, personal data will be processed by the Processor within the meaning of Art. 4 No. 2 GDPR. The subject matter of the order results from the General Terms and Conditions (Terms of Use) and the description in **Annex 1**.

2. The contractually agreed data processing shall generally take place in a Member State of the European Union (EU) or in another contracting state of the Agreement on the European Economic Area (EEA). Relocations or data processing in a third country may only take place if the special requirements of Art. 44 et seq. GDPR are met. The adequate level of protection is hereby determined by an adequacy decision of the Commission (Art. 45 Para. 3 GDPR) or by the establishment of standard contractual clauses (Art. 46 Para. 2 lit. c and d GDPR). For the sub-processors listed in **Annex 2**, consent is deemed to have been granted.

3. The type of personal data used (data categories) and the categories of data subjects are specifically described in **Annex 1**.

§3 Quality Assurance and Other Obligations of the Processor pursuant to Art. 28 Para. 3 S. 1 GDPR

In addition to complying with the provisions of this order, the Processor has its own statutory obligations as a Processor; in this respect, it particularly guarantees compliance with the following requirements:

1. Where legally obliged, the Processor shall appoint a qualified and reliable person as Data Protection Officer, who shall carry out their activities in accordance with Art. 37 et seq. GDPR. The data protection officer appointed at the BayLDA is: Anne Schweizer dataprotection@getklar.com. All changes concerning the person of the Data Protection Officer must be immediately notified to the Client.

2. The Processor shall ensure, in accordance with Art. 28 Para. 3 S. 2 lit. b GDPR, that persons authorised to process the personal data have committed themselves to confidentiality or are subject to an appropriate statutory obligation of secrecy and have been previously familiarised with the data protection provisions relevant to them.

3. The Processor and any person acting under the authority of the Processor who has access to personal data shall not process those data except on instructions from the Client (Art. 29, 32 Para. 4 GDPR), including the powers granted in this Agreement, unless required to do so by Union or Member State law.

4. The Processor guarantees the implementation and compliance with all technical and organisational measures required for this order in accordance with Art. 28 Para. 3 S. 2 lit. c, Art. 32 GDPR [**Annex 4**].

5. The Client and the Processor (and their representatives, if applicable) shall cooperate with the supervisory authority on request in the performance of its tasks (Art. 31 GDPR).

6. The Processor undertakes to immediately inform the Client about supervisory authority control actions and measures, insofar as they relate to this order. This also applies if a competent authority investigates the Processor in the context of an administrative offense or criminal procedure regarding the processing of personal data during contract processing.

7. Insofar as the Client is subject to a control by the supervisory authority, an administrative offense or criminal procedure, a liability claim by a data subject or a third party, or another claim in connection with

the contract processing at the Processor, the Processor shall provide the Client with the best possible support.

8. The Processor regularly monitors internal processes as well as technical and organisational measures to ensure that processing within its area of responsibility complies with the requirements of applicable data protection law and that the protection of data subjects' rights is guaranteed.

9. The Processor guarantees the verifiability of the technical and organisational measures taken to the Client within the scope of its control powers under § 5 of this Agreement.

§4 Subcontracting Relationships pursuant to Art. 28 Para. 3 S. 2 lit. d GDPR in conjunction with Art. 28 Para. 2 and 4 GDPR

1. Subcontracting relationships are understood to be services that directly relate to the provision of the main service. However, the Processor is obliged to take appropriate and legally compliant contractual agreements and control measures to ensure data protection and data security of the Client's data even for outsourced ancillary services.

2. The Processor uses the sub-processors named in **Annex 2** for the execution of individual processing activities. The change of existing sub-processors or the involvement of new sub-processors is permissible if the Processor notifies the Client of such a change a reasonable time in advance, at least 14 days, and the Client does not object to the planned change in writing or text form to the Processor until the data transfer date. An objection may only be raised by the Client for an important reason to be proven to the Processor. If the Client does not raise an objection within 10 days of receipt of the notification, its right to object to the respective commissioning expires. If the Client refuses consent by objecting for reasons other than important ones, the Processor may terminate this Agreement as well as, if applicable, the Main Agreement at the time of the planned use of the sub-processor. In the event of technical problems or data protection incidents with the sub-processor, the Processor is entitled to immediately change the sub-processor without prior notice to ensure the continued provision of the offered service. A contractual agreement pursuant to Art. 28 Para. 2-4 GDPR is obligatory.

3. To ensure an appropriate level of protection for subcontractors and other suppliers of the Processor, a supplier audit based on ISO/IEC 27001:2022 best practices is conducted for each supplier and business partner to exclude unacceptable risks to integrity, confidentiality, and availability.

§5 Client's Audit Rights pursuant to Art. 28 Para. 3 S. 2 lit. h GDPR

1. The Client has the right to conduct audits, in agreement with the Processor, or to have them carried out by auditors to be designated in individual cases, who must not be in a competitive relationship with the Processor. The Client has the right to satisfy itself of the Processor's compliance with this agreement in its business operations through sample checks, which must be announced at least 14 Days in advance.

2. The Processor shall ensure that the Client can satisfy itself of the Processor's compliance with its obligations under Art. 28 GDPR. The Processor undertakes to provide the Client with the necessary information upon request and, in particular, to demonstrate the implementation of technical and organisational measures.

3. Proof of such measures can be provided by adherence to approved codes of conduct in accordance with Art. 40 GDPR, certification under an approved certification mechanism in accordance with Art. 42 GDPR, or current attestations, reports or excerpts from reports of independent bodies (e.g. auditors, internal audit, data protection officer, IT security department, data protection auditors, quality auditors) or an appropriate certification by an IT security or data protection audit.

4. If an audit reveals that the Processor does not comply with the provisions of this Agreement, it shall take all necessary measures to ensure compliance with the provisions again.

§6 Processor's Notification Obligations pursuant to Art. 28 Para. 3 S. 2 lit. e and f GDPR

1. The Processor shall adequately support the Client, where possible, with suitable technical and organisational measures in fulfilling its obligations pursuant to Chapter 3 of the GDPR. If a data subject asserts rights regarding their data directly against the Processor, the Processor shall immediately refer the data subject to the Client.

2. The Processor shall assist the Client in ensuring compliance with the obligations laid down in Articles 32 to 36 GDPR concerning the security of personal data, notification obligations in the event of data breaches, data protection impact assessments, and prior consultations. This includes ensuring an appropriate level of protection through technical and organisational measures that take into account the circumstances and purposes of the processing as well as the projected probability and severity of a possible legal infringement due to security vulnerabilities and enable immediate identification of relevant infringement events.

3. The Processor is obliged to immediately report personal data breaches to the Client. Likewise, the Processor must support the Client within the framework of its information obligations towards the data subject and immediately provide the Client with all relevant information in this context. The Processor and the Client shall cooperate with requests from the competent supervisory authorities in the performance of their tasks.

4. For support services not included in the service description and not attributable to misconduct by the Processor or a sub-processor, the Processor may claim remuneration of €120/hour.

§7 Client's Right of Instruction

1. The Processor shall process personal data exclusively within the framework of the agreements made and on documented instructions from the Client, unless required to do so by Union or Member State law to which the Processor is subject (Art. 28 Para. 3 S. 3 lit. a, Art. 29 GDPR). In such a case, the Processor shall inform the Client of those legal requirements before processing, unless that law prohibits such information on important grounds of public interest.

2. The Processor shall ensure that the data processing is carried out in accordance with the Client's instructions. If the Processor is of the opinion that an instruction from the Client violates this Agreement or applicable data protection law, it shall immediately inform the Client thereof; after such notification to the Client, the Processor is entitled to suspend the execution of the instruction until the instruction is confirmed or amended by the Client. The Parties agree that the sole responsibility for processing in accordance with instructions lies with the Client.

3. The Client's instructions shall generally be in written or text form. If necessary, the Client may also give instructions verbally (remotely). Instructions given verbally (remotely) shall be confirmed by the Client immediately in written or text form.

§8 Deletion and Return of Personal Data pursuant to Art. 28 Para. 3 S. 2 lit. g GDPR

1. Copies or duplicates of the data shall not be created without the Client's knowledge. Exceptions to this are backup copies, insofar as they are necessary to ensure proper data processing, as well as data that are necessary with regard to compliance with statutory retention obligations.

2. Upon termination of the service agreement, the Processor shall hand over all data records related to the contractual relationship to the Client or destroy them in a data protection compliant manner after prior consent.

3. Documentation serving as proof of data processing in accordance with the order and proper handling must be stored by the Processor beyond the end of the contract in accordance with the respective retention periods.

§9 Technical and Organisational Measures

1. The Processor must document the implementation of the necessary technical and organisational measures before the start of processing, in particular with regard to the specific order execution, and make them available to the Client.

2. The Processor shall ensure security in accordance with Art. 28 Para. 3 lit. c, 32 GDPR, in particular in conjunction with Art. 5 Para. 1, 2 GDPR. Overall, the measures to be taken are data security measures and measures to ensure a level of protection appropriate to the risk with regard to the confidentiality, integrity, availability, and resilience of the systems and services. The state of the art, the costs of implementation, and the nature, scope, context, and purposes of processing as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons pursuant to Art. 32 Para. 1 GDPR shall be taken into account [details in **Annex 1**].

3. The technical and organisational measures are subject to technical progress and further development. In this respect, the Processor is permitted to implement alternative adequate measures. The security level of the defined measures may not be undercut. Significant changes must be documented.

§10 Client's Obligations

1. The Client is obliged to include a reference to the use of Klar! Insights GmbH services in its privacy policy. An exemplary notice is listed in **Annex 3** of this Agreement. The Client ensures that the notice used in its privacy policy is current and correct and complies with the applicable data protection regulations. The current templates can always be found in the data sources settings on the Klar! platform.

§11 Other Provisions

1. Both parties undertake to treat confidentially all knowledge of business secrets and data security measures of the other party obtained within the scope of the contractual relationship, even after the termination of the contract. Should there be doubts as to whether information is subject to the duty of confidentiality, it shall be treated as confidential until written release by the other party.
2. Should the Client's property at the Processor be endangered by third-party measures (e.g. by seizure or confiscation), by insolvency or composition proceedings, or by other events, the Processor shall notify the Client without delay.
3. Ancillary agreements require written form. This applies equally to the waiver of this formal requirement.
4. The right of retention, irrespective of the legal basis, is excluded with regard to the data processed in the order and the associated data carriers.
5. Should individual provisions of the contract prove to be wholly or partially ineffective or unenforceable, or become ineffective or unenforceable as a result of changes in legislation after the conclusion of the contract, the remaining contractual provisions and the validity of the contract as a whole shall remain unaffected. The ineffective or unenforceable provision shall be replaced by the effective and enforceable provision that comes closest to the meaning and purpose of the void provision. Should the contract prove to be incomplete, the provisions shall be deemed agreed upon that correspond to the meaning and purpose of the contract and would have been agreed upon if thought had been given to the matter.
6. The contract is exclusively subject to the law of the Federal Republic of Germany, excluding its international private law rules.

Annex 1 – Specification of the Order Content (incl. Categories of Personal Data, Categories of Data Subjects)

Annex 2 – List of Approved Sub-processors

Annex 3 - Templates for Client's Privacy Notices (Examples)

Annex 4 - TOM

Annex 1

Specification of the Order Content

Type and Purpose of Personal Data Processing:

The processing of the personal data listed below is for the purpose of systematising, tabular and/or graphical evaluation of data for creating forecasts and reach measurements for marketing purposes, as well as anonymisation of data at the Client's request or rendering it unidentifiable for statistical evaluation, maintenance and hosting of the IT systems, software and databases underlying the service, and handling of backups.

In particular, the following activities are part of the data processing:

- Processing of personal data provided by the Client via technical interfaces (APIs), originating from the connected data sources (advertising platforms, social networks or shop systems).

- Processing of personal data generated by the integrated "Klar Pixel" (Klar Attribution) and the associated tracking script. Collection and transmission of personal data about current web sessions for the purpose of efficiency measurement.
- Processing of IP addresses of the Controller's customers for the purpose of analysing and attributing marketing measures and optimising these measures.
- Anonymisation of IP addresses after the storage period of 90 days for further statistical evaluations and long-term success monitoring of marketing strategies without personal reference.

Categories of Personal Data:

Klar Core: Customer number, order number and order ID (according to the Controller's system)

Klar API: Email address (optional), **Order number and order ID (according to the Controller's system)

Klar Attribution / Klar Pixel: User and session IDs, Email address, IP address, Online identifiers (Cookie ID, Device ID)

Amazon Selling Partner API: User ID

Categories of Data Subjects:

To fulfill the Main Agreement, the following categories of data subjects are processed on behalf of the Controller:

- **Employees**
- **Customers**
- **Suppliers**
- **Business Partners**

Annex 2

Sub-processors

Sub-processor	Address/Country	Service
Hetzner Online GmbH	Industriestr. 25 91710 Gunzenhausen Germany	Data Centre, Hosting
Google LLC	Gordon House Barrow Street Dublin 4 Ireland	Authentication
OpenBridge Inc.	119 Braintree St Ste 413 Boston MA, 02134-1697 USA	Data Synchronization Amazon Seller
Cloudflare Germany GmbH	Rosental 7 80331 Munich	Domain Management, DNS Service, ZeroTrust, Cloud Storage, CDN

Sub-processor	Address/Country	Service
Microsoft GmbH	Walter-Gropius-Str. 5 80807 Munich Germany	Authentication, Microsoft Clarity
Shopify International Ltd.	Intertrust Ireland 2nd Floor 1-2 Victoria Buildings Haddington Road Dublin 4 Ireland	Authentication
Intercom R&D Unlimited Company	124 St Stephen's Green Dublin 2 Ireland	Support Chat, Knowledge Base
Twilio	Twilio Ireland Limited 70 Sir John Rogerson's Quay Dublin 2 Ireland	Transactional Mail
Amazon Web Services, Inc.	410 Terry Avenue North Seattle WA 98109 USA	Data Storage Amazon Seller

Annex 3

Templates for Client's Privacy Notices (Examples)

The following text modules serve only as exemplary templates. It is imperative that these examples are adapted according to the specific functions used and, in particular, the URLs for cookie objection are supplemented with your own domain to ensure they function correctly.

For the use of Klar! Insights - Core

Use of Klar! Insights

Klar! Insights - Core

We use the services of **Klar Insights GmbH**, Clemensstr. 2, 80803 Munich, Germany, a SaaS provider for business intelligence solutions for eCommerce companies, to support our business accounting and to analyze the profitability of our marketing measures.

In this context and based on our legitimate interest according to Art. 6 Para. 1 S. 1 lit. f GDPR, we transmit the following personal data, according to our internal structure, to Klar Insights GmbH:

- Customer number
- Order number, Order ID

The processing of this data allows us to evaluate the effectiveness of our marketing activities and to optimize our business processes accordingly. The data is used exclusively for internal analysis purposes and is neither used for advertising purposes nor passed on to third parties without authorization.

Information on data protection and data use by Klar can be found on the following website: https://app.getklar.com/legal/data-protection

You have the right to object to this processing at any time for reasons arising from your particular situation. Further information on your rights as a data subject can be found in this privacy policy.

For the use of Klar! Insights - Attribution

Use of Klar! Insights

Klar! Insights - Attribution

We use the services of Klar Insights GmbH, Clemensstr. 2, 80803 Munich, Germany, a SaaS provider for business intelligence solutions for eCommerce companies. Klar Insights GmbH collects, processes, and stores data (user and session IDs, IP address, online identifiers (cookie ID, device ID)) on this website and its subpages for reach measurement and statistical analysis on our behalf. For this purpose, we have concluded a data processing agreement with Klar Insights GmbH.

The collection of personal data is based on the legal basis of consent pursuant to Art. 6 para. 1 sentence 1 lit. a) GDPR.

If consent is given by the user, the data to be processed is collected in a user-related manner, taking into account § 25 para. 1 sentence 1 TDDDG.

For the aforementioned different types of collection, the following cookies are used to ensure the respective type of collection:

- september_id
- september_has_consent
- september_do_not_track (in case of objection)

Cookie - Objection

To generally object to the use of Klar! Insights, please use this Link. This will set a cookie with the name "september_do_not_track" from the domain "Your-Domain.de". Please do not delete this, otherwise it cannot be guaranteed that you will not be tracked by Klar.

Information on data protection and data use by Klar can be found on the following website: https://app.getklar.com/legal/data-protection

Annex 4

Technical and Organisational Measures according to Art. 32 GDPR

Introduction

This document describes the technical and organisational measures established and implemented by Klar Insights GmbH for the protection of information, particularly personal data, taking into account Art. 32 GDPR. All measures taken consider the risk associated with the respective data processing.

Data Centre Location: **Germany**

1. Confidentiality

Access, System Access, and Data Access Control

Measures suitable to prevent unauthorized persons from gaining access to data processing facilities where personal data is processed and used.

Measures to prevent unauthorized persons from using data processing systems (computers).

Measures to ensure that persons authorized to use a data processing system can only access data subject to their access rights and that personal data cannot be read, copied, modified or removed without authorization during processing, use and after storage.

Technical Measures	Organisational Measures
Office premises accessible only to employees	Key issuance is documented
Premises secured by locking system	No unsupervised visitors in office premises
Login with username + password (min. 10 characters - (uppercase & lowercase), min. 1 number, min. 1 special character)	Network equipment for local network is in locked network cabinet
Use of password safe (currently 1Password Cloud)	Obligation to change initial passwords after first login
Remote access to server in data center only possible via encrypted SSH access with Public/Private Key + Key via VPN	Managing user permissions
Hard drive encryption (FileVault)	Creating user profiles
Automatic desktop lock	Password policy "Secure Password" including minimum length (12 characters)
Secured access using ZeroTrust	System access lock after a defined number of failed login attempts
No storage of company data on local storage	Instructions for manual desktop lock (Windows + L)
	Minimum number of administrators
	Logging of admin activities
	Management of user rights by administrators
	Central password assignment
	Secure storage of data carriers

Technical Measures	Organisational Measures
	Use of certified service providers for file and data destruction
	Clean Desk Policy
	Defined Joiner, Mover, Leaver process for granting and adapting permissions
	Separation of conflicting permissions (Segregation of Duties)

Separation Control

Measures to ensure that data collected for different purposes can be processed separately. This can be ensured, for example, by logical and physical separation of data.

Technical Measures	Organisational Measures
Separation of production and test environment	Control via authorization concept
Logical client separation (software-side)	Production environments are managed only by selected employees
Multi-tenancy of relevant applications	Definition of database rights
Encryption of data records processed for the same purpose	Data records are provided with purpose attributes/data fields
For pseudonymized data: Separation of the assignment file and storage on a separate, secured IT system	Production environments are located on separate server instances

Pseudonymisation & Encryption

The processing of personal data in such a manner that the data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organisational measures.

Technical Measures	Organisational Measures
Data masking: Passwords are never stored in plain text	Internal instruction to anonymize/pseudonymize personal data as far as possible in case of transfer or after expiry of the legal deletion period
Customers receive a customer number for pseudonymization	
Data in Transit: TLS 1.2 encryption	

2. Integrity

Input Control

Measures to ensure that it can be subsequently checked and established whether and by whom personal data has been entered, altered, or removed from data processing systems.

Input control is achieved through logging, which can take place at various levels (e.g., operating system, network, firewall, database, application).

Technical Measures	Organisational Measures
Technical logging of data input, modification, and deletion	Overview of which programs can be used to enter, modify, or delete which data
Manual or automated control of logs	Traceability of data input, modification, and deletion by individual usernames (not user groups)
	Assignment of rights for data input, modification, and deletion based on an authorization concept
	Clear responsibilities for deletions
	Retention of forms from which data has been transferred into automated processing

Transfer Control

Measures to ensure that personal data cannot be read, copied, altered or removed without authorisation during electronic transmission or during their transport or storage on data carriers, and that it can be checked and established to which places a transmission of personal data by means of data transmission facilities is intended.

Technical Measures	Organisational Measures
Encryption of confidential information via OTS	Overview of regular retrieval and transmission processes
Email encryption (if supported by customer/recipient)	
Logging of accesses and retrievals	
Provision of encrypted connection via https	

3. Availability and Resilience

Availability Control

Measures ensuring that IT systems and (personal) data are accessible to authorized users at all times. This includes measures that prevent failures and enable quick re-access after disruptions. Personal data within the scope of this data processing agreement is stored and processed exclusively on the (cloud) systems of the following providers. As these are constantly being adapted, reference is sometimes made to the respective provider's website.

Technical Measures	Organisational Measures
Daily backup of all relevant data	Backup and Recovery Concept
Virus scanner	Patch management
SPAM filter	Separate partitions for operating system and data
Encryption programs	Hard drive mirroring
Use of uninterruptible power supply	
Emergency power generator	
Permanently active DDoS protection	
Use of software firewall and port regulations	

Procedures for regular review, assessment and evaluation Data Protection Management

Data protection management includes the systematic planning, implementation and monitoring of measures for the protection of personal data. The aim is to ensure that all data protection requirements are met and risks to the protection of personal data are minimized.

Technical Measures	Organisational Measures
Central documentation of all data protection procedures and regulations	Employees committed to confidentiality / data secrecy
	Regular employee awareness training on data protection issues
	Formalized process for handling information and data subject requests implemented
	(External) Data Protection Officer
	(External) Information Security Officer
	The organization complies with the information obligations pursuant to Art. 13, 14 GDPR

Privacy-friendly default settings

Ensuring compliance with the principles of "Privacy-by-Design" and "Privacy-by-Default"

Technical Measures	Organisational Measures
No more personal data is collected than is necessary to achieve the purpose	All data is stored in a central location to comply with logging and deletion requirements
	All used (cloud) services are operated in accordance with the requirements of the GDPR

Order Control (Outsourcing to Third Parties)

Measures that ensure that personal data processed on behalf of the client can only be processed in accordance with the client's instructions.

Technical Measures	Organisational Measures
	Prior review of the security measures taken by the Processor and their documentation
	Supplier Policy with checklist
	Selection of the Processor based on due diligence
	Conclusion of the necessary agreement for data processing or EU Standard Contractual Clauses
	Ongoing review of the Processor and its level of protection
	Documented prohibition of subcontracting by freelancers

Effectiveness Control

Measures that ensure that the intended measures are appropriate and effective for their purpose.

Technical Measures	Organisational Measures
	Regular review of compliance with all measures and validity of external certifications by the Data Protection Officer
	Regular review of processes with randomly selected employees in the form of sample checks

Development Security

Measures that ensure that development takes place in compliance with data protection and information security.

Technical Measures	Organisational Measures
Test automation for front- and backend	Use of a Secure Software Development Lifecycle
Unit tests, static tests, and regression tests	Regular monitoring of capacities
Code review during development	OWASP Top Ten comparisons
Dependency and Vulnerability Scans during development	No use of production data or personal data for testing purposes
Use of standard configurations	

Incident Response Management

Measures to support the response to security breaches.

Technical Measures	Organisational Measures
Use of spam filters and regular updates	Documented process for detecting and reporting security incidents / data protection incidents
Use of virus scanners and regular updates	Documented procedure for handling security incidents
Intrusion Detection Scanner	Involvement of DPO ensured
Intrusion Prevention Scanner	Formal process and responsibilities for post-processing security incidents and data protection incidents

HR Security

Measures that ensure that the HR department is appropriately trained to handle particularly sensitive (personal) data.

Technical Measures	Organisational Measures
	All employees have signed an NDA and a declaration of commitment to comply with data protection principles
	All employees receive regular training on data protection topics
	Employees are subject to a strict selection process to ensure their suitability
	Employees are instructed on what to do in the event of information security incidents
	There are issue and return logs for company equipment