Data Processing Agreement

Terms for processing personal data on a customer's behalf

REFERENCE	VERSION	DATE	CLASSIFICATION
SLL-DPA	2.1	1 November 2026	Public

This agreement applies when Secure Logiq Limited processes personal data on behalf of the customer named in Part A in connection with the customer's use of Secure Logiq products and services. It forms part of the customer's contract with us, which includes our Terms of Sale (SLL-TOS).

Part A. The parties

Secure Logiq. Secure Logiq Limited, registered in England and Wales (company number 07714764), Unit B1, Fleming Centre, Fleming Way, Crawley RH10 9NN.

The Customer.

Customer legal name	
Jurisdiction of registration	
Address and postcode	
Contact name	
Email	
Telephone	
Effective date	

1. Definitions

1.1 In this agreement:

TERM	MEANING
Customer Contract	means the contract between the Customer and Secure Logiq under which Secure Logiq provides Products or services to the Customer, including the Terms of Sale and any applicable Product Terms.
Data Protection Laws	means the UK GDPR, the Data Protection Act 2018 and, where it applies to the Customer or to the processing, the EU General Data Protection Regulation (2016/679), together with any other data protection law the parties agree in writing applies.
Controller, Processor, Data Subject, Personal Data, Processing and Special Category Data	have the meanings they have in the Data Protection Laws.
Product Terms	has the meaning given in the Terms of Sale.
Security Incident	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Submitted Data.
Submitted Data	means the Personal Data that Secure Logiq processes for the Customer under the Customer Contract. It includes Personal Data on a system that Secure Logiq sees during support or when a unit is returned, and Personal Data that Secure Logiq's software sends to Secure Logiq for health and monitoring.
Subprocessor	means a third party that Secure Logiq uses to help it process Submitted Data on the Customer's behalf.

1.2 Words defined in the Terms of Sale have the same meaning here.

2. How this agreement applies

2.1 Effect. This agreement takes effect either (a) on the Effective Date stated in Part A, once both parties have signed it; or (b) where Product Terms say that this agreement applies automatically, from the time Secure Logiq first processes Submitted Data under those Product Terms, without signature. It applies to Secure Logiq's processing of Submitted Data under the Customer Contract.

2.2 Part of the Customer Contract. This agreement forms part of the Customer Contract. If it conflicts with the Customer Contract on data protection, this agreement prevails.

2.3 Term. This agreement stays in force until the Customer Contract ends and clause 11 has been carried out.

2.4 Customer under Product Terms. Where this agreement applies under clause 2.1(b), the Customer is the Licensee under the Product Terms. In a channel sale this is the End User, which is the Controller. The Customer details in Part A are taken from the licence acceptance record, and Part A and the signature page do not need to be completed.

3. Roles

3.1 Controller and processor. The Customer is the Controller of the Submitted Data, and Secure Logiq is its Processor. The Customer appoints Secure Logiq to process the Submitted Data for the purposes in Schedule 1.

3.2 Compliance. Each party must comply with the Data Protection Laws that apply to it.

4. Processing the data

4.1 Instructions. Secure Logiq will process Submitted Data only on the Customer's documented instructions, which are this agreement, the Customer Contract and the Customer's support requests, unless the law requires otherwise. If Secure Logiq thinks an instruction breaks the Data Protection Laws, it will tell the Customer.

4.2 Details of the processing. The subject matter, duration, nature and purpose of the processing, the types of Personal Data and the categories of Data Subjects are in Schedule 1.

4.3 Special category data. The Customer must not deliberately send Special Category Data to Secure Logiq. Data that Secure Logiq sees or holds only incidentally during support or a return, such as footage on a system, is not treated as disclosed to it. Where it can, the Customer must remove footage and other data from a unit before returning it.

4.4 Confidentiality. Secure Logiq must make sure that everyone it authorises to process Submitted Data treats it as confidential and is bound by a duty of confidentiality.

5. Security

5.1 Measures. Secure Logiq must use appropriate technical and organisational measures to protect Submitted Data from unlawful destruction and from unauthorised disclosure of or access to it, based on industry practice and the Data Protection Laws.

5.2 Security incidents. If Secure Logiq becomes aware of a confirmed Security Incident, it will tell the Customer without undue delay, give the Customer reasonable information and cooperation, take reasonably necessary steps to remedy or reduce its effects, and keep the Customer informed of material developments.

5.3 Impact assessments. Secure Logiq will give reasonable cooperation, at the Customer's expense, with any data protection impact assessment or consultation with a regulator that the Data Protection Laws require.

6. Subprocessors

6.1 Consent. The Customer consents to Secure Logiq using the Subprocessors on the list published on our website at https://securelogiq.com/terms-conditions/, for the purposes in Schedule 1, provided that Secure Logiq: (a) imposes data protection terms on each Subprocessor that require it to protect Submitted Data to the standard the Data Protection Laws require and consistent with this agreement; and (b) remains liable for any breach of this clause caused by a Subprocessor.

6.2 Changes. Secure Logiq may replace a Subprocessor or appoint another by updating the list. It will tell the Customer at least 10 days before it allows a new Subprocessor to process Submitted Data.

6.3 Objections. The Customer may object to a new or replacement Subprocessor on reasonable grounds relating to data protection. The parties will try in good faith to resolve the objection. If they cannot, Secure Logiq will not appoint the Subprocessor or, if that is not possible, the Customer may suspend or end its use of the Products and the Customer Contract, and remains responsible for all fees and charges up to that point.

7. Transfers outside the UK and EEA

7.1 Transfers. Secure Logiq will not process Submitted Data outside the United Kingdom and the European Economic Area unless it has taken the steps needed to make the transfer comply with the Data Protection Laws. Those steps can include transferring to a country the UK or the European Commission has approved as adequate, using the UK International Data Transfer Agreement or Addendum or the European Commission's standard contractual clauses, or using binding corporate rules.

8. Data subjects and audits

8.1 Data subject requests. Secure Logiq will give reasonable and timely help, at the Customer's expense, so the Customer can respond to requests from Data Subjects to use their rights, and to other correspondence, enquiries or complaints from Data Subjects or regulators about the Submitted Data. If any of these reaches Secure Logiq directly, it will promptly tell the Customer, with full details.

8.2 Information and audits. On written request, and subject to confidentiality and security obligations, Secure Logiq will give the Customer the information needed to show it is complying with the Processor obligations, and will allow and contribute to audits, including inspections, by the Customer or an auditor the Customer appoints.

9. Liability

9.1 Limits. Clause 15 of the Terms of Sale applies to each party's liability under this agreement, except where the law does not allow it.

10. Notices and law

10.1 Notices. Notices under this agreement may be given by email to the contact in Part A (for the Customer) or to info@securelogiq.com (for Secure Logiq). They are treated as received on the next business day after they are sent.

10.2 Law and disputes. Clause 21 of the Terms of Sale applies to this agreement, so English law governs it and disputes go to the courts of England and Wales, or to arbitration for customers outside the United Kingdom.

11. Return or deletion

11.1 When the Customer Contract ends. Secure Logiq will delete or return, at the Customer's choice, all Submitted Data under its control when the Customer Contract ends. This does not apply to data that the law requires Secure Logiq to keep, or to data on backup systems, which Secure Logiq will keep securely isolated and protected from further processing except as the law requires.

11.2 Physical media. If the Customer asks for data on physical media to be destroyed, the Customer must pay the costs unless Secure Logiq agrees otherwise.

12. General

12.1 Independent parties. The parties are independent. Neither may make any commitment or representation for the other unless authorised in writing.

12.2 Whole agreement. This agreement, with the Customer Contract, is the whole agreement between the parties on its subject. A change takes effect only if it is in writing and signed by both parties, except that where this agreement applies under clause 2.1(b), the version in force when the Product Terms were accepted applies, and later versions apply only once the Customer accepts them. Neither party may transfer this agreement without the other's written consent.

12.3 Signature. The parties may sign this agreement electronically and in counterparts. Each party confirms that it has full power and authority to sign and to perform this agreement.

Signatures

Signed for and on behalf of Secure Logiq Limited (a director).

Signature

Date

Print name

Position

Signed for and on behalf of the Customer named in Part A.

Signature

Date

Print name

Position

Schedule 1. Details of the processing

ITEM	DETAILS
Subject matter	Providing support, handling returns under RMA, and health and monitoring for the Products.
Duration	The term of the Customer Contract.
Nature of the processing	Accessing, viewing, temporarily storing and analysing data on systems and data sent by our software.
Purpose	Diagnosing and fixing faults, handling returns, monitoring the health of Products, and providing the Products and services under the Customer Contract.
Types of Personal Data	Data on systems that Secure Logiq sees during support or a return, which can include video recordings and images, user names and account details, system and event logs, and network details such as IP addresses; and health and monitoring data that our software sends to us.
Categories of Data Subjects	The Customer's staff and users, its own customers and their staff and users, and people who appear in footage.