THE CLARUS NETWORKS GROUP

Privacy
And
Personal Data Protection Policy

Versioning History

DOCUMENT CLASSIFICATION	Protected
DOCUMENT REF	ISMS-DOC-A05-34-1
VERSION	5
DATED	02 February 2026
DOCUMENT AUTHOR	Emma Gartland
DOCUMENT OWNER	Derek Phillips

Revision history

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES	DISTRIBUTION
1	Dec 2020	Jacqui Dalgleish	First publication	All staff, suppliers etc on request
2	Dec 2021	Jacqui Dalgleish	Review	All staff, suppliers etc on request
3	15 May 2023	Kathryn Andrews	Review, update and clarify	All staff, suppliers etc on request
4	4 Feb 2025	Scott Rowley	Review and bring inline with ISO 27001	All staff, suppliers etc on request
5	30 Jan 2026	Emma Gartland	Review	All staff, suppliers etc on request

Approval

NAME	POSITION	SIGNATURE	DATE
Derek Phillips	Managing Director		Dec 2020
Derek Phillips	Managing Director		Dec 2021
Derek Phillips	Managing Director		18 May 2023
Derek Phillips	Managing Director		6 Feb 2025
Derek Phillips	Managing Director		2 Feb 2026

THE CLARUS NETWORKS GROUP

Contents

1. Introduction 3
2. Privacy and personal data protection policy 4
   2.1. Applicable privacy legislation 4
   2.2. Definitions 4
      2.2.1. Personally identifiable information (PII) 4
      2.2.2. PII principal 4
      2.2.3. Processing of PII 4
      2.2.4. PII Controller 4
      2.2.5. PII Processor 4
   2.3. Principles relating to processing of PII 5
   2.4. Rights of the individual 5
   2.5. Lawfulness of processing 6
      2.5.1. Consent 6
      2.5.2. Performance of a contract 6
      2.5.3. Legal obligation 6
      2.5.4. Vital interests of the PII principal 6
      2.5.5. Task carried out in the public interest 6
      2.5.6. Legitimate interests 6
   2.6. Privacy by design 6
   2.7. Contracts involving the processing of PII 7
   2.8. International transfers of PII 7
   2.9. Data protection officer 7
   2.10. Breach notification 7
   2.11. Addressing compliance to applicable privacy legislation 7

1. Introduction

The Clarus Networks Group is a provider of specialist connectivity solutions.

The Group operates within the UK, EU, USA and Middle East and exports globally.

This policy forms part of the Integrated Management System for Clarus Networks Limited.

In its everyday business operations Clarus makes use of a variety of data about identifiable individuals, including data about:

- Current, past and prospective employees
- Customers
- Users of its websites
- Subscribers
- Other stakeholders

In collecting and using this data, the Organisation is subject to a variety of legislation controlling how such activities may be carried out and the safeguards that must be put in place to protect it.

The purpose of this policy is to set out the relevant legislation and to describe the steps Clarus is taking to ensure that it complies with it.

This control applies to all systems, people and processes that constitute the organization's information systems, including board members, directors, employees, suppliers and other third parties who have access to Clarus systems.

The intended audience for this policy is employees responsible for designing and managing systems using personal data within Clarus.

Failure to comply with the contents of this policy may result in disciplinary action being taken by Clarus against the individual(s) concerned.

Terms used in this policy are defined within the body of the policy and as follows:

- *Data pseudonymisation* is a data management and de-identification procedure by which personally identifiable information fields within a data record are replaced by one or more artificial identifiers, or pseudonyms.

The following ISMS documents and external references are relevant to this document:

- *Information Classification Procedure*
- *Information Labelling Procedure*
- *Records Retention and Protection Policy*
- *Acceptable Use policy*
- *Electronic Messaging Policy*
- *Social Media Policy*
- *Information Security Incident Response Procedure*
- *Information Security Roles, Responsibilities and Authorities*

2. Privacy and personal data protection policy

2.1. Applicable privacy legislation

The table below shows the main items of privacy legislation that apply to the countries (or groups of countries) and states within which Clarus operates.

BLOC/COUNTRY/STATE	APPLICABLE LEGISLATION
European Union	General Data Protection Regulation (GDPR)
United Kingdom	UK GDPR Data Protection Act

Table 1: Applicable privacy legislation

Clarus has a legal obligation to comply with the provisions of this legislation at all times. Whilst there will be variations in these provisions, this policy establishes the key principles that are commonly required to be observed in such legislation.

Significant fines may be applicable if a breach is deemed to have occurred under the relevant privacy legislation, which is designed to protect the PII of citizens of the country (or state, region or countries) involved. It is Clarus's policy to ensure that our compliance with applicable legislation is clear and demonstrable at all times.

2.2. Definitions

The definitions used within privacy legislation vary and it is not appropriate to reproduce them all here. However, the common terms used within this policy are defined by the ISO/IEC 29100 Privacy Framework international standard as follows:

2.2.1. Personally identifiable information (PII)

"any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal."

2.2.2. PII principal

"natural person to whom the personally identifiable information (PII) relates."

2.2.3. Processing of PII

"operation or set of operations performed upon personally identifiable information (PII)

Note 1 to entry: Examples of processing operations of PII include, but are not limited to, the collection, storage, alteration, retrieval, consultation, disclosure, anonymization, pseudonymization, dissemination or otherwise making available, deletion or destruction of PII."

2.2.4. PII Controller

"privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing personally identifiable information (PII) other than natural persons who use data for personal purposes."

2.2.5. PII Processor

"privacy stakeholder that processes personally identifiable information (PII) on behalf of and in accordance with the instructions of a PII controller."

2.3. Principles relating to processing of PII

There are a number of fundamental principles upon which most privacy legislation is based. These are summarised as follows:

1. **Lawfulness, fairness and transparency** - PII shall be processed lawfully, fairly and in a transparent manner in relation to the PII principal
2. **Purpose limitation** – PII shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
3. **Data minimisation** – the PII collected and stored shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed
4. **Accuracy** – PII shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that PII that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay
5. **Storage limitation** – PII shall be kept in a form which permits identification of PII principals for no longer than is necessary for the purposes for which the PII is processed
6. **Integrity and confidentiality** – PII shall be processed in a manner that ensures appropriate security of the PII, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures

Clarus will ensure that it complies with all these principles both in the processing it currently carries out and as part of the introduction of new methods of processing such as new IT systems.

2.4. Rights of the individual

The PII principal also has rights with regard to their PII. These will generally consist of:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

Each of these rights are supported by appropriate procedures within Clarus that allow the required action to be taken within the timescales stated in the applicable privacy legislation.

These timescales are shown in Table 2

PII PRINCIPAL REQUEST	TIMESCALE
The right to be informed	When data is collected (if supplied by PII principal) or within one month (if not supplied by PII principal)
The right of access	One month
The right to rectification	One month
The right to erasure	Without undue delay
The right to restrict processing	Without undue delay
The right to data portability	One month
The right to object	On receipt of objection
Rights in relation to automated decision making and profiling.	Not specified

Table 2: Timescales for PII principal requests

2.5. Lawfulness of processing

Depending on the legislation involved, there may be a number of alternative ways in which the lawfulness of a specific case of processing of PII may be established. It is Clarus policy to identify the appropriate basis for processing and to document it, in accordance with the applicable legislation. The main options are described in brief in the following sections.

2.5.1. Consent

Where appropriate, Clarus will obtain consent from a PII principal to collect and process their data. In case of children below the age specified in applicable legislation parental consent will be obtained. Transparent information about our usage of their PII will be provided to PII principals at the time that consent is obtained and their rights regarding their data explained, such as the right to withdraw consent. This information will be provided in an accessible form, written in clear language and free of charge.

If the PII is not obtained directly from the PII principal, then this information will be provided to the PII principal within a reasonable period after the data is obtained and definitely within one month.

2.5.2. Performance of a contract

Where the PII collected and processed is required to fulfil a contract with the PII principal, consent is not required. This will often be the case where the contract cannot be completed without the PII in question, for example, a delivery cannot be made without an address.

2.5.3. Legal obligation

If the PII is required to be collected and processed in order to comply with applicable law, then consent is not required. This may be the case for some data related to employment and taxation for example, and for many areas addressed by the public sector.

2.5.4. Vital interests of the PII principal

In a case where the PII is required to protect the vital interests of the PII principal or of another natural person, then this may be used as the lawful basis of the processing. Clarus will retain reasonable, documented evidence that this is the case, whenever this reason is used as the lawful basis of the processing of PII. As an example, this may be used in aspects of social care, particularly in the public sector.

2.5.5. Task carried out in the public interest

Where Clarus needs to perform a task that it believes is in the public interest or as part of an official duty then the PII principal's consent will not be requested. The assessment of the public interest or official duty will be documented and made available as evidence where required.

2.5.6. Legitimate interests

If the processing of specific PII is in the legitimate interests of Clarus and is judged not to affect the rights and freedoms of the PII principal in a significant way, then this may be defined as the lawful reason for the processing. Again, the reasoning behind this view will be documented.

2.6. Privacy by design

Clarus has adopted the principle of privacy by design and will ensure that the definition and planning of all new or significantly changed systems that collect, or process PII will be subject to due consideration of privacy issues, including the completion of one or more privacy impact assessments.

The privacy impact assessment will include:

- Consideration of how PII will be processed and for what purposes

- Assessment of whether the proposed processing of PII is both necessary and proportionate to the purpose(s)
- Assessment of the risks to individuals in processing the PII
- What controls are necessary to address the identified risks and demonstrate compliance with applicable legislation

Use of techniques such as data minimization and pseudonymisation will be considered where applicable and appropriate, including at the end of processing, and the mechanisms used to achieve them will be documented.

2.7. Contracts involving the processing of PII

Clarus will ensure that all relationships it enters that involve the processing of PII are subject to a documented contract that includes the specific information and terms required by the applicable legislation.

2.8. International transfers of PII

Transfers of PII between countries will be carefully reviewed prior to the transfer taking place to ensure that they fall within the limits imposed by the applicable legislation. This depends partly on the relevant authority's judgement (for example in the case of the GDPR, the European Commission) as to the adequacy of the safeguards for PII applicable in the receiving country and this may change over time.

Where an adequacy decision (or similar statement) does not exist for a destination country, an appropriate safeguard such as standard contractual clauses will be used, or a relevant exception identified as permitted under the applicable legislation.

2.9. Data protection officer

A defined role of Data Protection Officer (DPO) is generally required under privacy legislation if an Organisation is a public authority, if it performs large scale monitoring or if it processes particularly sensitive types of data on a large scale. The DPO is required to have an appropriate level of knowledge and can either be an in-house resource or outsourced to an appropriate service provider.

Based on these criteria, Clarus does not require a Data Protection Officer to be appointed.

2.10. Breach notification

It is Clarus's policy to be fair and proportionate when considering the actions to be taken to inform affected parties regarding breaches of PII. In line with the applicable legislation, where a breach is known to have occurred, which is likely to result in a risk to the rights and freedoms of individuals, where required the relevant supervisory authority will be informed within the specified timeframe (for example, for the GDPR within 72 hours). This will be managed in accordance with our *Information Security Incident Response Procedure* which sets out the overall process of handling information security incidents and our *Personal Data Breach Notification Procedure*, which sets out the specific actions to be taken in reporting the incident.

Under privacy legislation the relevant authority may have the right to impose a range of fines, often based on a percentage of annual worldwide turnover or a specific amount, for infringements of the regulations.

2.11. Addressing compliance to applicable privacy legislation

The following actions are undertaken to ensure that Clarus complies at all times with the accountability principle of privacy legislation within the countries in which it operates:

- The legal basis for processing PII is clear and unambiguous

- All staff involved in handling PII understand their responsibilities for following good data protection practice
- Training in data protection has been provided to all staff
- Rules regarding consent are followed
- Routes are available to PII principals wishing to exercise their rights regarding PII and such enquiries are handled effectively
- Regular reviews of procedures involving PII are carried out
- Privacy by design is adopted for all new or changed systems and processes
- The following documentation of processing activities is recorded:
    - Organisation name and relevant details
    - Purposes of the PII processing
    - Categories of individuals and PII processed
    - Categories of PII recipients
    - Agreements and mechanisms for transfers of PII to other countries including details of controls in place
    - PII retention schedules
    - Relevant technical and organizational controls in place

These actions are reviewed on a regular basis as part of the management process concerned with privacy and data protection.