GROUP GOVERNANCE & COMPLIANCE

Data Protection and Privacy Policy

CONTECH Group

How we collect, use and protect personal data, and respect individuals' privacy

Document Control	
Document title	Data Protection and Privacy Policy
Owner / Group entity	CONTECH Group (CONTECH GROUP Ltd, UK and CONTECH GROUP sh.p.k., Kosovo)
Policy owner	Group Executive Management (overseen by the Group CEO)
Approved by	Gazmend Kelmendi, Group Chief Executive Officer, on behalf of the Board
Classification	Public
Version	1.0
Effective date	11 May 2026
Next review	15 April 2027

Contents

1. Policy Statement

CONTECH Group ("CONTECH", "the Group", "we") respects the privacy of the individuals whose personal data it handles and is committed to protecting that data and processing it lawfully, fairly and transparently. This Policy sets out how we comply with data protection law and the standards we expect of everyone who handles personal data on the Group's behalf.

We handle personal data belonging to our employees and job applicants, our clients and their representatives, our suppliers, subcontractors and partners, and visitors to our website and premises. We treat all such data with care and in accordance with the law.

The data protection principles we follow:

- Lawfulness, fairness and transparency — we process data lawfully and openly.
- Purpose limitation — we collect data for specified, legitimate purposes.
- Data minimisation — we collect only the data we need.
- Accuracy — we keep data correct and up to date.
- Storage limitation — we keep data no longer than necessary.
- Integrity and confidentiality — we keep data secure.
- **Accountability — we can demonstrate our compliance.**

2. Purpose

The purpose of this Policy is to explain how the Group meets its obligations under applicable data protection law, to protect the rights of individuals, and to reduce the risk of data breaches and of regulatory, legal and reputational harm.

3. Scope and Application

This Policy applies across the entire Group, including CONTECH GROUP Ltd (United Kingdom) and CONTECH GROUP sh.p.k. (Kosovo), and any subsidiary, branch or controlled joint-venture operation. It applies to all directors, officers, employees and workers who handle personal data, and to any third party that processes personal data on the Group's behalf.

It covers all personal data processed by the Group, in any format, whether held electronically or on paper.

4. Key Definitions

- **Personal data** — any information relating to an identified or identifiable living individual (a "data subject").
- **Special-category data** — more sensitive personal data, such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health, sex life, sexual orientation, or genetic or biometric data.
- **Processing** — any operation performed on personal data, including collecting, storing, using, sharing, altering and deleting it.
- **Controller and processor** — a controller decides why and how personal data is processed; a processor processes personal data on a controller's behalf.
- **Consent** — a freely given, specific, informed and unambiguous indication of the individual's wishes.
- **Personal data breach** — a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

5. Legal Framework

5.1 United Kingdom

The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025, together with the Privacy and Electronic Communications Regulations (PECR). The supervisory authority is the Information Commissioner's Office (ICO).

5.2 Kosovo

Law No. 06/L-082 on the Protection of Personal Data, which is aligned with the EU General Data Protection Regulation. The supervisory authority is the Information and Privacy Agency.

5.3 European Union

Where the Group processes the personal data of individuals in the European Union, or offers goods or services to them, Regulation (EU) 2016/679 (the EU GDPR) may also apply.

6. Data Protection Principles

We process personal data in line with the following principles:

- **Lawfulness, fairness and transparency** — we process data lawfully, fairly and in a way people would reasonably expect.
- **Purpose limitation** — we collect data for specified, explicit and legitimate purposes and do not use it in incompatible ways.
- **Data minimisation** — we collect only what is adequate, relevant and necessary.
- **Accuracy** — we take reasonable steps to keep data accurate and up to date.
- **Storage limitation** — we keep data in identifiable form no longer than necessary.
- **Integrity and confidentiality** — we protect data with appropriate security measures.
- **Accountability** — we take responsibility for compliance and can demonstrate it.

7. Lawful Basis for Processing

We process personal data only where we have a lawful basis to do so. Depending on the circumstances, this may be: the individual's consent; the performance of a contract; compliance with a legal obligation; the protection of a person's vital interests; the performance of a task in the public interest; or our legitimate interests (or those of a third party), where these are not overridden by the individual's rights and freedoms. We process special-category data only where an additional condition applies, such as an employment-law obligation or explicit consent.

8. Individuals' Rights

Subject to the conditions and exemptions in applicable law, individuals have the right:

- to be informed about how their personal data is used;
- to access their personal data;
- to have inaccurate data corrected and incomplete data completed;
- to have their data erased in certain circumstances;
- to restrict processing in certain circumstances;
- to data portability;
- to object to certain processing, including direct marketing; and
- to safeguards in relation to solely automated decision-making and profiling.

We handle requests to exercise these rights promptly and within the timescales required by law (generally one month), and we take reasonable steps to verify the identity of the person making the request.

9. Transparency and Privacy Notices

We tell individuals, through clear privacy notices, what personal data we collect, why we collect it, the lawful basis for processing, who we share it with, how long we keep it, and their rights. The Group's website privacy notice explains how we handle the personal data of website users, job applicants, clients and suppliers. Privacy notices are made available at the point at which we collect personal data.

10. Data Security and Confidentiality

We put in place appropriate technical and organisational measures to protect personal data against unauthorised or unlawful processing and against accidental loss, destruction or damage. These measures include access controls, secure storage and transmission, and confidentiality obligations on those who handle personal data. Everyone who handles personal data on the Group's behalf must keep it confidential and use it only as authorised.

11. Personal Data Breaches

We maintain arrangements to identify, report, contain and assess personal data breaches. Anyone who becomes aware of an actual or suspected breach must report it immediately to the Data Protection Contact. Where a breach is likely to result in a risk to individuals, we notify the relevant supervisory authority — the Information Commissioner's Office in the United Kingdom, or the Information and Privacy Agency in Kosovo — without undue delay and, where feasible, within 72 hours of becoming aware of it. Where a breach is likely to result in a high risk to individuals, we also inform the affected individuals.

12. Data Retention and Disposal

We keep personal data only for as long as necessary for the purposes for which it was collected, or as required by law, in accordance with the Group's retention arrangements. When personal data is no longer needed, we securely delete, destroy or anonymise it.

13. Data Sharing, Processors and International Transfers

- We share personal data only where there is a lawful basis to do so, and we disclose only what is necessary.
- Where we engage a processor to handle personal data on our behalf, we do so under a written contract that requires appropriate security and confidentiality and permits processing only on our instructions.
- We transfer personal data outside the United Kingdom, Kosovo or the European Economic Area only where appropriate safeguards are in place, as required by applicable law.

14. Accountability — Records, DPIAs and the Data Protection Contact

We take a "data protection by design and by default" approach. We keep records of our processing activities, carry out data protection impact assessments (DPIAs) for higher-risk processing, and review our practices to ensure ongoing compliance. The Group designates a Data Protection Contact — and appoints a Data Protection Officer where this is required by applicable law — responsible for advising on and monitoring compliance with this Policy and with data protection law.

15. Roles, Responsibilities and Training

- **The Board and Group CEO** are accountable for data protection compliance and approve this Policy.

- **Executive management** ensure appropriate resources, systems and controls are in place and that the Data Protection Contact is supported.
- **The Data Protection Contact** advises on compliance, maintains records, coordinates breach handling and responses to individuals' requests, and provides guidance.
- **Line managers** apply this Policy in their areas and oversee the third parties they engage.
- **All personnel** handle personal data in line with this Policy, complete required training, and report any concern or suspected breach.

16. Breaches, Governance and Review

Failure to comply with this Policy may result in disciplinary action up to and including dismissal, and — for third parties — termination of the relevant engagement. Serious breaches of data protection law can also expose the Group to significant fines and expose individuals to personal liability.

This Policy is approved by the Group Chief Executive Officer on behalf of the Board and is owned by Group Executive Management. It should be read together with the Group's website privacy notice, the Code of Conduct and Business Ethics, the information-security arrangements, and related policies. It will be reviewed at least annually, and sooner if required by changes in law — including the phased implementation of the Data (Use and Access) Act 2025 — in the Group's structure or in operating practice.

Approved on behalf of CONTECH Group

Name	Gazmend Kelmendi
Position	Group Chief Executive Officer
Date of approval	11 May 2026

Contact

Data protection questions or requests may be directed to the Data Protection Contact or to **info@contech.biz**. Concerns may also be reported in confidence to **ethics@contech.biz**.

CONTECH GROUP Ltd — 62 Camden Road, London NW1 9DR, United Kingdom
CONTECH GROUP sh.p.k. — Magjistrala Prishtinë–Lipjan, Km 10, përballë QMI, 10500 Graçanicë, Republic of Kosovo
contech.biz