

CLOUDFACTORY

GDPR Compliance Statement

Who are we?

CloudFactory is a global leader in combining people and technology to provide workforce solutions for machine learning and business process optimization. As such, we are both a data controller and data processor.

CloudFactory are:

- Controllers of personnel information in relation to the operational data generated and stored at CloudFactory.
- Controllers of our customer and supplier contact information, to manage and deliver services under contract, and manage customer requests.
- Processor of our customer data.

If you have any questions about CloudFactory's GDPR compliance activities, please contact:

- Privacy@cloudfactory.com, or chris.shorthouse@cloudfactory.com

Our commitment

CloudFactory is committed to ensuring the security and protection of the personal information that we process, and to provide a compliant and consistent approach to data protection.

We demonstrate our commitment to data privacy by maintaining industry standards, certifications and accreditations, including ISO 9001:2015, ISO 27001:2013, Service

Organizational Control (SOC) 2 reporting and the Health Insurance Portability and Accountability Act (HIPAA) as a Business Associate.

Our data protection framework complies with existing laws and regulations, including the GDPR and the Data Protection Act 2018 for the U.K.

We are dedicated to safeguarding the personal information that we process, and to the continuing development of the data protection framework, that is effective, fit for purpose and demonstrates understanding and compliance to the GDPR regulations.

Our objectives and underlying principles for GDPR compliance are summarized in this statement and include the implementation of data protection roles and responsibilities, policies, procedures, controls and recording and reporting to ensure ongoing compliance.

Data Protection Officer

CloudFactory has appointed **Christopher Shorthouse** as a full-time DPO who holds responsibility for all matters relating to data privacy to ensure the GDPR principles are upheld at CloudFactory.

Should you require any further information about CloudFactory and its data protection framework, please feel free to contact us using the details below:

- Email: chris.shorthouse@cloudfactory.com (Christopher Shorthouse, Director of Compliance),
or write to:
- Privacy, CloudFactory International Limited, Fora Space, Thames Tower, Station Road, Reading, RG1 1LX, United Kingdom

Our GDPR compliance plan

Our compliance plan is subject to continuous improvement; at CloudFactory we continually seek ways of improving our data protection framework through our workers, processes and

technology. Below we have summarized our main activities associated with the GDPR Articles.

1. Appointed responsibility for data protection, compliance and information security governance.

- Appointed person to carry out the Data Protection Officer (DPO) role described in Article 38 and the DPO tasks detailed in Article 39.

2. Maintaining a record of our processing activities using a leading Governance Risk and Compliance platform.

- Record of Processing (when CloudFactory is the Controller or the Processor) described in Article 30 Records of Processing Activities.
- CloudFactory obligations as a Processor on behalf of Controllers (clients) described in Article 28 GDPR Processor.

3. Validation of our processing activities through internal audit, data mapping gap analysis and peer review.

- Compliance with Article 5 Principles relating to the processing of personal data.
- Compliance with Article 6 Lawfulness of Processing.

4. Reviewing and updating our Data Privacy and Security policies on an annual basis.

- Data Privacy Policy to encompass requirements detailed in Article 13 Information to be provided where personal data are collected from the data subject.
 - Security Policy encompassing requirements detailed in Article 32 Security of Processing obligations.

5. Establishing robust processes in support of the GDPR including, subject access requests and the right to be forgotten.

- Data Subject Access Request (DSAR) process for compliance with Article 12 Transparent information, communication and modalities for the exercise of the rights of the data subject.
- Our processes satisfy all the Data Subjects rights including:
 - Article 15 Right of access by the data subject
 - Article 16 Right to rectification

- Article 17 Right to erasure ('right to be forgotten')
- Article 18 Right to restriction of processing
- Article 19 Notification obligation regarding rectification or erasure of personal data or restriction of processing
- Article 21 Right to object
- Article 22 Automated individual decision-making, including profiling

6. Data security monitoring and reporting, which encompasses incident and event management.

Our breach management includes:

- Controller obligation under Article 33 Notification of a personal data breach to the supervisory authority.
- Controller Obligations under Article 34 Communication of a personal data breach to the data subject.
- Processor Obligations under Article 28 to notify and support the Controller (typically a client) in the event of a Breach.

7. Regular incident response exercises that focus on areas such as personal data breach and data leakage.

- Referenced as part of Article 39 Tasks of the Data Protection Officer.

8. Assessed our lawful basis for processing data to ensure all personal data is processed lawfully, fairly and in a transparent manner.

- Referenced as part of Article 39 Tasks of the Data Protection Officer.
- Compliance with Article 5 Principles relating to the processing of personal data.
- Compliance with Article 6 Lawfulness of Processing.

9. Undertake assessments of our processing activities, such as legitimate interest as the lawful basis for processing personal data.

- Compliance with Article 39.1.b Tasks of the data protection officer.
- Compliance with Article 6 Lawfulness of Processing.

10. Provision of extensive training for our workers, raising awareness and understanding of data privacy, individual responsibilities and the importance of GDPR to our business.

- Incorporated in the DPO tasks detailed in Article 39.1.a Tasks of the data protection officer.

Safeguarding and security measures

CloudFactory places a high importance on information and data security; we already hold accreditation to the international information security standard, ISO 27001:2013 and the Health Insurance Portability and Accountability Act (HIPAA) as a Business Associate. On an annual basis, CloudFactory is externally audited against the Service Organizational Control (SOC 2 Type II) standard.

Further information on our data security practices and overall compliance program can be found under the Certifications & Compliance section of CloudFactory's website.

Data subject rights

In accordance with the GDPR regulations, data subjects have eight rights that CloudFactory must uphold, these are:

- The Right to Be Informed
- The Right of Access
- The Right to Rectification
- The Right to Erasure
- The Right to Restrict Processing
- The Right to Data Portability
- The Right to Object
- The Right to Avoid Automated Decision-Making

Further detail on these rights can be found in the CloudFactory Privacy and Personal Data Protection Policy together with the types of personal data we process and its purpose.

Third-party processing

Suppliers who process personal data on behalf of CloudFactory have been identified and asked to provide details of their state of compliance with the GDPR. We will not on-board any new supplier unless we are satisfied that they comply with the appropriate data protection regulations. Further information can be found at:

[CloudFactory sub-processors](#)

International transfers

CloudFactory may transfer personal data outside the UK and EEA when product and services are provided by external third-party suppliers and the processing of personal data is necessary for the performance of a customer contract.

Whenever we transfer your personal data outside the UK and EEA, we ensure at least one of the following safeguards is implemented:

- We will only transfer your personal data to countries that have been deemed to provide an adequate level of protection of personal data by the European Commission. For further details, please reference the European Commission – Adequacy Decisions.
- Where we use certain service providers, we may use specific contracts approved by the European Commission which give personal data the same protection it has in Europe. For further details, reference the European Commission – Standard Contractual Clauses.

Useful link

Further information is available within our various policy documents, including:

- [Privacy Policy](#)

The following policies are not published but are available by request, under NDA:

- Privacy and Personal Data Protection Policy
- Data Protection Staff Responsibilities Policy
- Standard Data Processing Agreement

Published Date: 23, October 2022

Revision Date: 3, April 2024

Version 3.0. Public