GDPR Compliance Guide

Confidential | August 2025

Prepared for Data Protection Officers, legal teams, and governance stakeholders

This document provides a high-level overview of how FaiceTech addresses its obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. More detailed documentation, including full Data Processing Agreements, DPIA templates, and sub-processor registers, is available on request and is shared with customers and qualified prospects only.

1. Introduction

FaiceTech provides facial recognition solutions that process biometric data — one of the most sensitive categories of personal data under UK GDPR. We take this responsibility seriously. This guide explains how we approach GDPR compliance, the safeguards we have in place, and the shared responsibilities between FaiceTech and our customers.

FaiceTech holds multiple independently audited certifications and accreditations that underpin our approach to data protection. For full details, please refer to our Security & Certification Overview document.

2. Lawful Basis for Processing

Under UK GDPR, every organisation processing personal data must have a valid lawful basis. For facial recognition deployments using FaiceTech, the relevant lawful bases are typically:

- **Article 6(1)(f)** — Legitimate interests, where the system is deployed in a retail loss-prevention or safety context. The deploying organisation must carry out a Legitimate Interests Assessment (LIA) to demonstrate that their interests are not overridden by the rights of the individuals being processed.
- **Article 9(2)** — Because facial recognition involves biometric data (special category data), an additional condition under Article 9 must be met. This is typically substantial public interest (Schedule 1 of the DPA 2018), where the processing is necessary and proportionate for purposes such as the prevention of crime.

The responsibility for establishing and documenting the lawful basis sits with the deploying organisation (the Data Controller). FaiceTech provides guidance and template documentation to support this process, but the final determination is a matter for the Controller and their legal advisors.

3. Data Controller & Processor Roles

Understanding who is responsible for what is critical to GDPR compliance. The table below outlines the typical role allocation between FaiceTech and the deploying organisation.

Responsibility	Deploying Organisation	FaiceTech
Determining lawful basis for processing	Data Controller	Guidance & templates
Deciding who is placed on watchlists	Data Controller	Platform provider
Signage and transparency obligations	Data Controller	Guidance provided
Conducting the DPIA	Data Controller (with support)	Template & consultation
Hosting and securing the platform	N/A	Data Processor
Processing biometric comparisons	N/A	Data Processor
Managing sub-processors	Informed via DPA	Data Processor
Responding to data subject requests	Data Controller	Technical support
Data retention configuration	Data Controller (sets policy)	Data Processor (enforces)
Breach notification	To the ICO (within 72 hours)	To the Controller (without undue delay)

Depending on the deployment context, FaiceTech may operate as a Data Processor or as a Joint Controller. The specific arrangement is documented in the Data Processing Agreement provided to each customer.

4. Data Subject Rights

UK GDPR grants individuals a number of rights over their personal data. FaiceTech's platform is designed to support the deploying organisation in fulfilling these rights.

- **Right of Access (Article 15):** Individuals can request confirmation of whether their data is being processed and, if so, access to that data. The platform supports this by enabling authorised users to locate and export relevant records.
- **Right to Rectification (Article 16):** If data held is inaccurate, individuals can request correction. Watchlist records can be updated or corrected by authorised users at any time.
- **Right to Erasure (Article 17):** Individuals can request deletion of their data in certain circumstances. The platform supports secure deletion of subject records, including biometric templates and associated images. Structured removal reasons are recorded in the audit trail.
- **Right to Restriction (Article 18):** The platform supports restriction of processing as required under UK GDPR, allowing processing to be paused while a request is being resolved.
- **Right to Object (Article 21):** Individuals have the right to object to processing based on legitimate interests. The deploying organisation is responsible for handling objections, but FaiceTech provides the technical tools to act on any decisions made.

Processes are in place to support data subject rights requests, including access, rectification, and erasure, subject to applicable legal exemptions.

5. Data Minimisation & Retention

5.1 Data Minimisation by Design

The FaiceTech platform is built around the principle of collecting only what is strictly necessary. Key design features include:

- **Data minimisation controls:** Data collection is limited to what is strictly necessary for the stated processing purpose. The platform enforces this through design constraints that prevent the capture of unnecessary personal data.
- **Biometric separation:** Biometric templates are stored separately from contextual subject data and cannot be reverse-engineered back into facial images.

Additional technical safeguards — including pseudonymisation, tenant isolation, and encryption measures — are detailed in our Security & Certification Overview.

5.2 Retention & Deletion

FaiceTech does not impose fixed retention periods. Instead, retention is fully customer-controlled:

- Deploying organisations set their own retention periods via the platform, aligned with their data protection policies and any legal requirements.
- The platform enforces configured retention periods and supports automatic deletion of expired records.
- Subject records can be manually deleted at any time by authorised users. Biometric templates and associated images are permanently removed.
- All watchlist changes are recorded in the audit trail, supporting accountability and compliance with data lifecycle requirements.

6. Data Protection Impact Assessments

A DPIA is a mandatory requirement before deploying facial recognition technology. Under UK GDPR Article 35, a DPIA is required when processing is likely to result in a high risk to individuals — and biometric processing at scale clearly meets this threshold.

6.1 What the DPIA Must Cover

A DPIA for a facial recognition deployment should address:

- The nature, scope, context, and purposes of the processing
- The necessity and proportionality of the processing relative to the purpose
- Risks to the rights and freedoms of individuals, including misidentification
- The safeguards and measures in place to mitigate those risks
- Consultation with a Data Protection Officer where required

6.2 How FaiceTech Supports DPIAs

FaiceTech provides template DPIAs tailored to facial recognition deployments and works with customers to complete them. Our support includes detailed descriptions of data flows, processing activities, security measures, and risk mitigations.

The DPIA remains the responsibility of the deploying organisation (as Data Controller), but FaiceTech ensures you have the technical detail needed to complete a thorough assessment.

7. Sub-Processors & International Transfers

7.1 Sub-Processor Governance

FaiceTech uses a small number of carefully vetted third-party services. All sub-processors are selected using a risk-based approach aligned with GDPR Articles 28 and 32, and are bound by contractual Data Processing Agreements. For further detail on our supplier assurance process, please refer to the Security & Certification Overview.

A complete sub-processor register is available to customers and qualified prospects under NDA. Customers are notified in advance of any changes to sub-processors.

7.2 International Data Transfers

FaiceTech's primary infrastructure is UK-based. Where any sub-processor operates outside of the UK, appropriate safeguards are in place in line with UK GDPR Chapter V requirements, including Standard Contractual Clauses (SCCs) or UK International Data Transfer Agreements (IDTAs) where applicable. For detail on our infrastructure and data sovereignty approach, see the Security & Certification Overview.

No biometric data or watchlist content is transferred outside of the UK and EU.

8. Breach Notification Procedures

FaiceTech maintains a documented incident response plan that is regularly tested. In the event of a personal data breach:

- **Notification to Controller:** FaiceTech will notify the affected customer (Data Controller) without undue delay upon becoming aware of a breach affecting their data.
- **Notification to ICO:** The Data Controller is responsible for assessing whether the breach must be reported to the ICO within 72 hours and whether affected individuals must be notified.
- **Supporting information:** FaiceTech will provide all necessary technical detail to support the Controller's assessment and reporting obligations, including the nature of the breach, categories of data affected, and remedial actions taken.

For details on the platform's preventative security controls, please refer to the Security & Certification Overview.

9. Human Review & Automated Decision-Making

Under UK GDPR Article 22, individuals have the right not to be subject to decisions based solely on automated processing that significantly affect them. FaiceTech's platform is designed with this requirement in mind:

- The system presents potential matches to human operators — it does not make enforcement, exclusion, or access decisions autonomously.
- All matches produced by the facial recognition system must be verified by a trained human before any action is taken.
- The platform does not carry out profiling, bulk search, or automated decision-making without human oversight.

This human-in-the-loop approach ensures that the system supports rather than replaces human judgement, reducing the risk of misidentification and ensuring proportionality.

10. Contact & Further Information

FaiceTech has a designated Data Protection Officer (DPO) who oversees compliance with UK GDPR. For any questions about this document, our data handling practices, or to request detailed compliance documentation, please get in touch.

Data Protection Officer: dpo@faicetech.com

General Enquiries: info@faicetech.com

Website: faicetech.com

ICO Registration Number: Available on request