General Data Protection Regulations (GDPR)

Group Compliance Statement – September 2025

Fusion Business Solutions (UK) Ltd

Approved By: Jeremy Bowman

Chief Information Security Officer

Signed: DocuSigned by: Jeremy Bowman BE81CC7B6C484F4...

8/10/2025 | 12:07 PM BST

1 Introduction

The EU General Data Protection Regulation ("GDPR") came into force across the European Union on 25th May 2018 and brings with it the most significant changes to data protection law in two decades. Based on privacy by design and taking a risk-based approach, the GDPR has been designed to meet the requirements of the digital age.

The 21st Century brings with it broader use of technology, new definitions of what constitutes personal data, and a vast increase in cross-border processing. The Regulation standardises data protection laws and processing across the EU and UK; affording individuals stronger, more consistent rights to access and control their personal information.

1.1 Our Commitment

Fusion Business Solutions (UK) Ltd [Fusion] 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 have always had a robust and effective data protection program in place which complies with existing law and abides by the data protection principles. However, we recognise our obligations in maintaining and expanding this program to meet the changing demands of the GDPR and other data protection legislation as it's implemented, adapted, and updated over time.

Fusion are dedicated to safeguarding the personal information under our remit and in developing a data protection regime that is effective, fit for purpose and demonstrates an understanding of the GDPR. Our objectives for GDPR compliance have been summarised in this statement and include the development and implementation of data protection roles, policies, procedures, controls and measures to ensure maximum and ongoing compliance.

1.2 Demonstrating GDPR Compliance

Fusion already has a consistent level of data protection and security across our organisation. Our compliance in meeting GDPR requirements includes:

- **ISO Standards** – Fusion has chosen to implement ISO/IEC 27701:2019 in partnership with BSI to demonstrate our ongoing compliance with our international legal and best practice handling of data to meet the needs of the UK DPA 2018 and the EU GDPR. Our ISO certification provides external independent verification of our controls and practices to meet the expectations of our clients, staff, suppliers, and third parties.

- ***Information Audit*** - carrying out a company-wide information audit to identify and assess what personal information we hold, where it comes from, how and why it is processed and if and to whom it is disclosed.

- ***Policies & Procedures -*** implementing new and updating existing data protection policies and procedures to meet the requirements and standards of the GDPR and any relevant data protection laws, including:

    - ***Data Protection*** – our main policy and procedure document for data protection has been overhauled to meet the standards and requirements of the GDPR. Accountability and governance measures are in place to ensure that we understand and adequately disseminate and evidence our obligations and responsibilities; with a dedicated focus on privacy by design and the rights of individuals.

    - ***Data Retention & Erasure*** – we have updated our retention policy and schedule to ensure that we meet the *'data minimization'* and *'storage limitation'* principles and that personal information is stored, archived and destroyed compliantly and ethically. We have dedicated erasure procedures in place to meet the new *'Right to Erasure'* obligation and are aware of when this and other data subject's rights apply; along with any exemptions, response timeframes and notification responsibilities.

    - ***Data Breaches*** – our breach procedures ensure that we have safeguards and measures in place to identify, assess, investigate and report any personal data breach at the earliest possible time. Our procedures are robust and have been disseminated to all employees, making them aware of the reporting lines and steps to follow.

    - ***International Data Transfers & Third-Party Disclosures*** – where Fusion stores or transfers personal information outside the EU, we have robust procedures and safeguarding measures in place to secure, encrypt and maintain the integrity of the data. Our procedures include a continual review of the countries with sufficient adequacy decisions, as well as provisions for binding corporate rules; standard data protection clauses or approved codes of conduct for those countries without. We carry out strict due diligence checks with all recipients of personal data to assess and verify that they have appropriate safeguards in place to protect the information, ensure enforceable data subject rights and have effective legal remedies for data subjects where applicable.

    - ***Subject Access Request (SAR)*** – we have revised our SAR procedures to accommodate the 30-day timeframe for providing the requested information and

for making this provision free of charge. Our new procedures detail how to verify the data subject, what steps to take for processing an access request, what exemptions apply and a suite of response templates to ensure that communications with data subjects are compliant, consistent and adequate.

- ***Legal Basis for Processing*** - we are reviewing all processing activities to identify the legal basis for processing and ensuring that each basis is appropriate for the activity it relates to. Where applicable, we also maintain records of our processing activities, ensuring that our obligations under Article 30 of the GDPR and Schedule 1 of the Data Protection Bill are met.

- ***Privacy Notice/Policy*** – we regularly review our Privacy Notice(s) to ensure compliance with the GDPR, ensuring that all individuals whose personal information we process have been informed of why we need it, how it is used, what their rights are, who the information is disclosed to and what safeguarding measures are in place to protect their information.

- ***Obtaining Consent*** – we have revised our consent mechanisms for obtaining personal data, ensuring that individuals understand what they are providing, why and how we use it and giving clear, defined ways to consent to us processing their information. We have developed stringent processes for recording consent, making sure that we can evidence an affirmative opt-in, along with time and date records; and an easy to see and access way to withdraw consent at any time.

- ***Direct Marketing*** – we have revised and continue to review the wording and processes for direct marketing, including clear opt-in mechanisms for marketing subscriptions; a clear notice and method for opting out and providing unsubscribe features on all subsequent marketing materials.

- ***Data Protection Impact Assessments (DPIA)*** – where we process personal information that is considered high risk, involves large scale processing or includes special category/criminal conviction data; we have developed stringent procedures and assessment templates for carrying out impact assessments that comply fully with the GDPR's Article 35 requirements. We have implemented documentation processes that record each assessment, allow us to rate the risk posed by the processing activity and implement mitigating measures to reduce the risk posed to the data subject(s).

- ***Processor Agreements*** – where we use any third-party to process personal information on our behalf (*i.e. Payroll, Recruitment, Hosting etc*), we have drafted compliant Processor Agreements and due diligence procedures for ensuring that they (*as well as we*), meet and understand their/our GDPR obligations. These measures

include initial and ongoing reviews of the service provided, the necessity of the processing activity, the technical and organizational measures in place and compliance with the GDPR.

- ***Special Categories Data*** **-** where we obtain and process any special category information, we do so in complete compliance with the Article 9 requirements and have high-level encryptions and protections on all such data. Special category data is only processed where necessary and is only processed where we have first identified the appropriate Article 9(2) basis or the Data Protection Bill Schedule 1 condition. Where we rely on consent for processing, this is explicit and is verified by a signature, with the right to modify or remove consent being clearly signposted.

2 Data Subject Rights

In addition to the policies and procedures mentioned above that ensure individuals can enforce their data protection rights, we provide easy to access information via our website, access to policies from a central shared location, in the office environments, during induction etc of an individual's right to access any personal information that Fusion's processes about them and to request information about:

- What personal data we hold about them.
- The purposes of the processing.
- The categories of personal data concerned.
- The recipients to whom the personal data has/will be disclosed.
- How long we intend to store your personal data for.
- If we did not collect the data directly from them, information about the source.
- The right to have incomplete or inaccurate data about them corrected or completed and the process for requesting this.
- The right to request erasure of personal data (where applicable) or to restrict processing in accordance with data protection laws, as well as to object to any direct marketing from us and to be informed about any automated decision-making that we use.
- The right to lodge a complaint or seek judicial remedy and who to contact in such instances.

.

3 Information Security & Technical and Organisational Measures (TOMs)

Fusion takes the privacy and security of individuals and their personal information very seriously and takes every reasonable measure and precaution to protect and secure the personal data that we process. We have robust information security policies and procedures in place to protect personal information from unauthorized access, alteration, disclosure or destruction and have several layers of security measures to meet provisions of GDPR Article 32, including (but not limited to):

- Wide use of SSL certificates from a trusted authority.
- Network and role-based access controls to systems and data.
- Strong password policy as part of Acceptable Use Policy.
- Extensive use of strong encryption of data both in transit and at rest.
- Secure network links using VPNs.
- Use of pseudonymization – especially in the context of handling customer data.
- Secure operational practices and policies around use and handling of data.
- Multi-factor authentication standards.

A copy of the Fusion Group TOMs is available on request. Please contact your Fusion Account Manager or email info@fusiongbs.com to place your request.

4 GDPR Roles and Employees

Fusion have appointed **Robert Wassall (Director of Legal Services, Norm Cyber)** as our qualified and independent Data Protection Officer (DPO) and **Jeremy Bowman (Fusion Group CISO)** to represent GDPR and data privacy for Fusion's Executive Leadership Team. Their objectives are to maintain our continued compliance with the global data protection regulation, as well as specific UK and European implementations of GDPR. They are also responsible for promoting awareness of the GDPR across the organization, assessing our GDPR readiness, identifying any gap areas and implementing the new policies, procedures and measures.

Fusion understands that continuous employee awareness and understanding is vital to the continued compliance of the GDPR and involves our employees in on-going compliance. Fusion has a robust and mandatory employee training program (based on an extended implementation of the UK National Cyber Security Center / NCSC curriculum), which also forms part of our staff induction and required annual cyber and data protection training and refresher program.

If you have any questions about our GDPR or data protection arrangements, please contact privacy@fusiongbs.com.

Document Change Control

Author	Version	Change Details	Date
J. Bowman	1.0	Issued version following internal review and MISG approval.	28/08/2018
J. Bowman	1.1	Revisions, wording updates following feedback, and annual MISG review & approval.	05/08/2019
J. Bowman	1.2	Updated DPO details. Annual MISG review & approval.	19/08/2020
J. Bowman	1.3	Annual MISG review & approval.	12/08/2020
J. Bowman	2.0	Major new document revision following updates. MISG review & approval for release.	18/04/2020
J. Bowman	2.1	Updated roles section with new details. Annual MISG review & approval.	02/05/2021
J. Bowman	2.2	Annual MISG review & approval.	11/04/2022
J. Bowman	2.3	Annual MISG review & approval.	22/04/2023
J. Bowman	2.4	Updated TOMs comments. Annual MISG review & approval.	16/05/2024
J. Bowman	2.5	Annual MISG review & approval.	02/05/2025
J. Bowman	2.6	DPO Review / Commented Updates	08/10/2025