



# Data & Privacy Policy

**Lancaster**  
Alston House  
White Cross  
Lancaster  
LA1 4XQ





**Manchester**  
Empress Business Centre  
380 Chester Road  
Manchester  
M16 9EA

**London**  
15 Maddox Street  
Mayfair  
London  
W1S 2QN

**Birmingham**  
S1 The Tubeworks  
48-52 Floodgate Street  
Digbeth  
B5 5SL

**Liverpool**  
Cotton Exchange  
Old Hall Street  
Liverpool  
L3 9LQ

FGH Security Limited is a company registered in England and Wales with company number 04713843

<b>Document Owner</b>	Compliance Officer			
<b>Authorised to Approve</b>	Board/Directors			
<b>Review Schedule</b>	Annual, or until such time there is a significant change in the legislation or the organisation			
<b>Category</b>	 Legal/Critical	 Financial/High	 Reputation/Med	 Other/Low

## Revision History

Version	Date	Author	Summary of Changes	Approved by
001	Feb 24	CM	New policy created	JS
002	Aug 24	CM	Updated to FGH Group language and letterhead	JS
003	Apr 25	CM	Added organisational scope table Largely restructured	JS
004	Jul25	ML	???	JS
005	Oct25	CK	17.5 Timeline to report	JS
006				

## Organisational Scope

FGH Group				
<b>FGH Security</b>	<b>FGH Training</b>	<b>FGH Consult</b>	<b>FGH Systems</b>	<b>FGH Teoranta</b>
UK	UK	UK / UAE	UK	ROI
Yes	Yes	Yes	Yes	Yes

## Introduction

FGH Group (“the **Organisation**”) is committed to protecting the privacy of our team members, customers, and suppliers. We process personal data as part of providing services and fulfilling employment responsibilities, typically as a data controller but occasionally as a processor on behalf of others.

We maintain detailed records of data processing activities and make these available to the Information Commissioner’s Office (UK) or the Data Protection Commission (ROI) upon request. This policy explains clearly what data we collect, how it’s used and stored, and outlines your rights under GDPR.

---

*This document is strictly confidential and must not be copied, shared, or used without prior written permission from FGH Group Ltd. © All rights reserved.*

---

## 1 Purpose

- 1.1 To ensure commitment to protecting personal data and compliance with the General Data Protection Regulations.

## 2 Scope

- 2.1 This policy applies to the collection, use, transfer/sharing, handling, storage, publication and other data processing in manual and electronic records held by FGH Group and applies to all team members, former team members and applicants, customers, suppliers and any other individuals associated with FGH Group.
- 2.2 “Data processing” is defined as any operation or set of operations which is performed on personal data or on sets of personal data, whether by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- 2.3 This policy sets out the Organisation’s response to any data breach or other rights under the prevailing General Data Protection Regulation and prevailing Data Protection legislation.
- 2.4 For the purpose of this policy, personal data is defined as;
  - a) “Personal data” is information that relates to an identifiable person who can be directly or indirectly identified from that information, for example, a person’s name, identification number, location, online identifier. It can also include pseudonymised data.
  - b) “Special categories of personal data” is data which relates to an individual’s health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership. It also includes imagery and recorded footage from security and surveillance software, including but not limited to facial recognition software, CCTV and access control systems, genetic and biometric data (where used for ID purposes).
  - c) “Criminal offence data” is data which relates to an individual’s criminal convictions and offences.

## 3 Objectives

- 3.1 To ensure data is processed lawfully, fairly and in a transparent manner.
- 3.2 To outline specific, explicit and legitimate purposes for collecting and processing data.
- 3.3 To ensure data collected is relevant and limited to what is necessary in relation to its purpose, avoiding the collection of excessive or irrelevant data.
- 3.4 To ensure data is accurate and kept up to date; any inaccurate data should be erased or rectified without delay.
- 3.5 To ensure data is held for no longer than is necessary to fulfil the purpose for which it was collected.
- 3.6 To ensure data is protected by appropriate security measures including protection against unauthorised or unlawful processing, accidental loss, theft, destruction, or damage.
- 3.7 To ensure compliance with the relevant data protection procedures for international transferring of personal data.

## 4 Related Documents/Platforms

- 4.1 Legal Register (UK Data Protection Act 2018, UK GDPR, Irish Data Protection Act 2018, EU GDPR)
- 4.2 Compliance Procedure
- 4.3 GDPR & Privacy Notice
- 4.4 IT Policy
- 4.5 Cookie Policy
- 4.6 Surveillance Scheme Policy

- 4.7 Surveillance Manual Template
- 4.8 Guide to Data Privacy and Protection
- 4.9 Feedback Procedure
- 4.10 Surveillance & Data Request Form
- 4.11 Employee, Client/Patron and Supply Chain Data Tables (See Appendices)

## 5 ARC Team

- 5.1 It is the **accountability** of the of all hiring managers to ensure new team members complete Data Protection training before being granted access to any software or data.
- 5.2 It is the **responsibility** of the Data Protection Officer(s) to ensure compliance with this policy and be the main point of contact for GDPR principles.
- 5.3 It is the **responsibility** of all team members to operate within and familiarise themselves with this policy.
- 5.4 Other stakeholders **consulted** in the creation and review of this policy includes but is not limited to the significant data handlers across the organisation; training, marketing, recruitment, IT and HR.

## 6 Key Measurables

- 6.1 # of Data Protection Breaches
- 6.2 # of Subject Access Requests
- 6.3 # of team members that have completed the Guide to Data Privacy and Protection

## 7 Data Protection Officer

- 7.1 The FGH Group Data Protection Officer responsibilities are fulfilled by the Compliance team.
- 7.2 The DPO's responsibilities include but are not limited to;
  - 7.2.1 Informing and advising team members of their obligations to comply with data protection legislation.
  - 7.2.2 Monitoring compliance with data protection legislation, including managing internal data protection activities, advising on data protection impact assessments, training and conducting internal audits.
  - 7.2.3 Co-operating with and acting as the first point of contact for the ICO.
- 7.3 FGH Group will ensure that the DPO reports to the highest management level of FGH Group in respect of their DPO duties, and is not subject to any detriment for performing their duties.

## 8 Data Security & Access Controls

- 8.1 Team members are only permitted access to relevant data after reading and acknowledging the Data & Privacy Policy and data awareness training at their induction.
- 8.2 All team members have access to training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach.
- 8.3 Whether this training is mandatory or recommended is outlined in the relevant job description and/or assignment instructions.
- 8.4 The nominated data controller(s) for the Organisation are trained appropriately in their roles under data protection legislation.
- 8.5 Team members will be allocated personal user accounts with appropriate access levels and security control measures to allow action tracking. Wherever available, two-factor authentication is utilised.
- 8.6 Team members will have access to relevant data in the course of their duties.
- 8.7 Use of personal devices for work purposes, including data access or recording, is prohibited as outlined in the IT Security Policy.

- 8.8 All files or written information of a confidential nature and/or including personal data are stored in a secure manner and are only accessed by people who have a need and a right to access them.
- 8.9 Passwords meet the complexity set out in the IT Security Policy and are kept personal and confidential.
- 8.10 Use of digital solutions wherever possible and good housekeeping and safe storage of physical documents ensure that all files or written information of a confidential nature and/or including personal data are not left where they can be read by unauthorised people.
- 8.11 Failure to follow the Organisation's rules on data security may result in disciplinary action up to and including dismissal, in addition to legal consequences under data protection law.
- 8.12 Data Collection
- 8.13 Any process involving the collection, processing or storage of data is designed with privacy and data protection in mind from the outset.
- 8.14 An of employee, customer and supply chain data matrix can be found in the appendices.
- 8.15 FGH Group collects, processes and stores data on the following platforms;
  - 8.15.1 **ATS** Applicant Tracking System
  - 8.15.2 **WMS** Workforce Management System
  - 8.15.3 **IMS** Integrated Management System
  - 8.15.4 Finance and Invoicing Software
  - 8.15.5 Project Management Software
  - 8.15.6 Form Builder Software
  - 8.15.7 FGH Group Websites
- 8.16 All personal data collected is gathered openly, transparently, and with a clearly defined purpose.
- 8.17 Individuals will always be informed about what data they're providing and why, ensuring all sharing of personal data is voluntary and based on explicit consent.
- 8.18 Data Privacy Notices will be provided where appropriate and applicable.
- 8.19 Cookie Notices will be provided where appropriate and applicable.
- 8.20 Where personal data is shared with FGH Group, if this is to be utilised for communication with the data subject, the source and purpose of the data share will be clearly outlined in that communication.

## 9 Data Retention

- 9.1 Personal data is retained only as long as necessary to fulfil regulatory obligations, including compliance with GDPR, employment laws, financial regulations, insurance and personal injury statutes.
- 9.2 At the end of the retention term, data is securely deleted or anonymised. This process is automated wherever possible to avoid delays.

## 10 Data Sharing

- 10.1 Team members are strictly prohibited from sharing personal data—whether verbally, electronically or physically—without explicit authorisation and in line with one or more of the clauses set out below. This includes customer information, employee details, CCTV footage, incident reports, or any data obtained during employment.
- 10.2 Personal data may be shared contractually with customers to fulfil contractual obligations and in the necessary fulfilment of services, including but not limited to names, SIA licence numbers, qualifications, telephone, email, relevant medical and dietary needs.
- 10.3 Customers and supply chain partners may request EDI data or carbon footprint in relation to their own reporting obligations, where this is requested, it will be provided anonymously.
- 10.4 Personal data may be shared with supply chain partners in the reasonable delivery of services during the course of employment, including but not limited to payroll, finance, insurance, uniform providers.

- 10.5 Supply chain partners are audited, during which they are required to demonstrate that personal data belonging to FGH Group will be handled in compliance with data protection legislation.
- 10.6 Where appropriate, FGH Group will enter into a data sharing agreement before sharing personal data with another data controller, particularly where personal data is to be shared on a large scale and/or regularly.
- 10.7 FGH Group may be required to disclose certain data/information in the course of your employment, such disclosure include but are not limited to;
- a) any employee benefits operated by third parties
  - b) disabled individuals - whether any reasonable adjustments are required to assist them at work
  - c) health data, to comply with health and safety or occupational health obligations towards the employee
  - d) for Statutory Sick Pay purposes
  - e) People management and administration, to consider how an individual's health affects his/her/their ability to do their job
  - f) the smooth operation of any employee insurance policies or pension plans.
- These kinds of disclosures will only be made when strictly necessary for the purpose.
- 10.8 FGH Group may be required to disclose certain data/information to authorities including but not limited to the police, licensing, regulatory body or to an authority by virtue of a court order, or to comply with other legal requirements, including those relating to the prevention or detection of crime, the apprehension/prosecution of an offender, or the collection of taxation/duties. The Organisation may also, in appropriate circumstances, make discretionary disclosures of personal data to a person or organisation other than the data subject where it is permitted to do so by law. When deciding whether to exercise its discretion to disclose personal data in such circumstances FGH Group will always give proper consideration to the data subject's interests and their right to privacy.
- 10.9 Some data subject rights such as 14.4.1 are superseded where the data is to be shared in line with the reasons set out in 11.6.
- 10.10 Any unauthorised access, sharing, copying, or distribution of personal data is considered a data breach and may result in disciplinary action up to and including dismissal, in addition to legal consequences under data protection law.

## 11 International Data Sharing

- 11.1 The Organisation may transfer personal data internationally to fulfil contractual obligations and in the necessary fulfilment of services, including but not limited to names, SIA licence numbers, qualifications, telephone, email, relevant medical and dietary needs.
- 11.2 Transfers from the UK or Ireland to another country will comply with the prevailing UK and Ireland data protection laws and local data protection laws applicable within the destination country. Where necessary, we implement appropriate safeguards, including contractual clauses or adequacy agreements, to protect personal data during these transfers.

## 12 Surveillance Equipment

- 12.1 A surveillance scheme may include, but is not limited to, passive or active monitored CCTV, Body Worn Video, Facial Recognition, ID and/or Biometric Access Systems and ANPR.
- 12.2 Any surveillance scheme owned, operated, installed or maintained by FGH Group will be subject to the Surveillance Scheme Policy.
- 12.3 A Surveillance Manual Template will be completed to reflect the surveillance scheme in place.
- 12.4 Amongst other aspects, the Manual will outline the purpose, authorised uses, access and method of requesting copies of any footage.
- 12.5 Surveillance footage or data must only be viewed, accessed, duplicated and stored in line with the relevant Surveillance Manual.



- 12.6 An SIA CCTV licence is required for the active viewing or review of any recorded footage when the viewer is doing so in relation to a customer contract in the interest of monitoring members of the public or guarding against disorder, assault, trespassers, destruction, damage or theft.
- 12.7 An SIA CCTV licence is not required for the active viewing or review of any recorded footage that is 'in house' and/or is being viewed in relation to the activities of an employee or any person that has intentionally visited the surveilled space with the reasonable expectation of being surveilled.
- 12.8 Where footage is used for investigations into a complaint, incident or conduct, the footage will be obtained, redacted and watermarked (if appropriate) to share and store as evidence.
- 12.9 The unauthorised recording, duplication or sharing of CCTV is strictly prohibited.
- 12.10 The use of personal devices to record, capture, or duplicate any footage, live or playback, is strictly prohibited and may constitute a breach of data protection law and internal policy.

### **13 Automated Decision Making**

- 13.1 Automated decision making is utilised during the recruitment application process, where predetermined outcomes are linked to the answers submitted. For example, a licensed role will automatically reject applicants who are not licensed.

### **14 Data Subject Rights**

- 14.1 Individuals, known as 'Data Subjects' are protected by the following rights in regard to their personal data under GDPR regulations;
  - 14.1.1 The right to be provided with specified information about FGH Group's processing of their personal data ('the right to be informed').
  - 14.1.2 The right to access their personal data and certain supplementary information ('the right of access').
  - 14.1.3 The right to have their personal data rectified, if it is inaccurate or incomplete ('the right of rectification').
  - 14.1.4 The right to have, in certain circumstances, their personal data deleted or removed ('the right of erasure', sometimes known as 'the right to be forgotten').
  - 14.1.5 The right, in certain circumstances, to restrict the processing of their personal data ('the right to restrict processing').
  - 14.1.6 The right, in certain circumstances, to move personal data the individual has provided to FGH to another organisation ('the right of data portability').
  - 14.1.7 The right, in certain circumstances, to object to the processing of their personal data and, potentially, require FGH to stop processing that data ('the right to object').
  - 14.1.8 The right, in relevant circumstances, to not be subject to decision-making based solely on automated processing ('Rights related to automated decision making, including profiling').
  - 14.1.9 The right to withdraw their consent at any time where consent is the basis for processing their personal data ('the right to withdraw consent').
  - 14.1.10 The right to lodge a complaint with a supervisory authority such as the Information Commissioner's Office (UK) or the Data Protection Commission (ROI) if they believe their data has been handled unlawfully or unfairly ('the right to lodge a complaint').
- 14.2 Organisations are not afforded these rights, though any requests of the nature listed above will be given reasonable and fair consideration.

## 15 Accessing Your Data

- 15.1 Informal requests for copies of documents such as contracts, payslips, P60's or other standard employment documents can be emailed to [engagementteam@fghgroup.global](mailto:engagementteam@fghgroup.global) and will be responded to within 7 days. Where this is not possible, the data subject will be notified of the cause of the delay and the anticipated timeframe.
- 15.2 For a formal or more extensive requests, Data Subjects may make a Subject Access Request in writing to [compliance@fghgroup.global](mailto:compliance@fghgroup.global) or [hr@fghgroup.global](mailto:hr@fghgroup.global). Requests should specify the type of data required, date ranges, and any identifying information necessary to assist the search.
- 15.3 FGH Group may seek verification of the requesters identify, or if the request is from a third party, then written and signed consent from the Data Subject.
- 15.4 On receipt of a SAR, the DPO will assess the request and estimate a timescale for the request to be fulfilled. Where possible this will be within 30 days, where it is not likely to be possible, a reasonable timeframe will be set out and the Data Subject notified.
- 15.5 SAR findings will be provided digitally unless expressly requested as print material, in which case FGH Group reserves the right to charge reasonable cost in the time, materials and postage.
- 15.6 Where the SAR is manifestly unfounded or excessive or unreasonably frequent, FGH Group will ordinarily refuse the request(s). Or, in exceptional cases, FGH Group may instead exercise its right in such circumstances to charge a reasonable fee that considers the administrative cost of complying with the request.
- 15.7 A Data Subject will be at no detriment for making a Subject Access Request.

## 16 Updating Your Data

- 16.1 FGH Group team members wishing to update their data can do so using the Change My Details form in the Employee Portal.
- 16.2 External Data Subjects wishing to update their data can do so by contacting the DPO by emailing [compliance@fghgroup.global](mailto:compliance@fghgroup.global).
- 16.3 It may be necessary to support the request with verifiable proof of the change, if this is the case FGH Group will request that proof without delay.
- 16.4 FGH Group will endeavour to make the update within 7 days of the request. Where this is not possible, the data subject will be notified of the cause of the delay and the anticipated timeframe.

## 17 Data Breaches

- 17.1 In the event of an alleged, suspected or confirmed data breach the DPO will initiate a swift investigation to establish the facts.
- 17.2 Any parties affected by a data breach will be notified at the earliest opportunity and with transparency about how the breach happened, what was accessed, and what reactive and proactive preventative measures are being taken.
- 17.3 FGH Group holds a robust insurance policy against data breach occurrences, including Cyber Security threats.
- 17.4 Internal breaches will be investigated, and any intentional or malicious actions will be considered under the Disciplinary Policy.
- 17.5 External breaches will be declared to the ICO and/or DPC and the police notified within 72 hours.

## 18 Raising a Concern

- 18.1 Any concern about this policy, its application, the handling of personal data or FGH Group's performance in relation to its obligations can be reported;
  - 18.1.1 internally to the DPO or using the Feedback Procedure, or;
  - 18.1.2 externally to the ICO (UK) and/or DPC (ROI) in serious cases or where informal routes have been exhausted.



## Appendix 1: Employee Data Table

Data Collection	What is collected?	How is it collected?	Where is it stored?	Why is it collected?	Lawful basis of collection	Retention period	Internal access and sharing	Possible external sharing
Application for work	Contact data	Application	ATS IMS monday.com DBS Checker	Recruitment	Consent Consent Consent	13 months	Recruitment Hiring managers People Compliance	None
Screening	Address					7 years from leaver date		SIA regulator NSI auditor NSI auditor Customers
DBS Checks	EDI data Work history Criminal record Medical Dietary/allergy							
Employment	Bank account NI number Next of Kin Contract terms Performance & conduct records	Employment	WMS IMS	Employment	Consent Contract			
Employee Activity	telephone calls, e-mail and internet access		Microsoft IMS Internet		Contract		Compliance Investigations	None
Employee Services	Contact data	Shared by FGH	Wagestream EAP	Employment	Contract	Term of employment	None	Service provider(s)
Timesheets (physical)	Name SIA Licence	Signing in/out of shift	Shredded once transferred to IMS	Shift verification	Contract	7 years from deployment	Operations Payroll	Customer
Incident Reports	Details of all parties	Team member submission	JotForm monday.com	H&S Security	Contract Legal obligation	7 years from incident	Compliance Investigations	Customer
Website visitors	IP address	Cookies?		Improving user experience Market research	Consent		Marketing	None
Newsletter subscribers	Name Email	Employment	WMS monday.com Brevo	Marketing	Contract	Term of employment	Marketing	None
Payment for services	Payment details	Transaction	WordPress Amelia SumUp	Transaction	Contract	7 years from transaction	Finance	None
CCTV			Server IMS	Security		See CCTV Manual	Compliance Investigations	None

## Appendix 2: Client/Patron Data Table

Data Collection	What is collected?	How is it collected?	Where is it stored?	Why is it collected?	Lawful basis of collection	Retention period	Internal access and sharing	External access and sharing
Client				Service Provision				
Incident Reports	Details of all parties	Team member submission	JotForm monday.com	H&S Security	Contract Legal obligation	7 years from incident	Compliance Investigations	SIA regulator NSI auditor
CCTV		CCTV Scheme	Server IMS	Security		See CCTV Manual	Compliance Investigations	None
Venue Facial Recognition	Facial stills	CCTV Scheme	Server IMS	Security		See CCTV Manual	Compliance Investigations	None
Venue Patron Data	ID Name	ID Scanners Barred register	Server IMS	Security		See CCTV Manual	Compliance Investigations	None
Enhanced Search	Person's Name Contact details	Form completion	IMS	Security Safeguarding	Contract	90 days	Operations Investigations	Client
Positive Search	Person's Name Contact details	Form completion	IMS	Security	Contract Licensing	90 days	Operations Investigations	Client
Eviction Form	Person's Contact details	Form completion	IMS	Duty of care Security	Contract Duty of care Licensing	90 days	Operations Investigations	Client
Venue Documentation	DPS Name DPS Contact details			Service Provision		X years from contract term	Operations Compliance	SIA regulator NSI auditor SDP
Payment for services	Payment details	Transaction	WordPress Amelia SumUp	Transaction	Contract		Finance	None

### Appendix 3: Supply Chain Data Table

Data Collection	What is collected?	How is it collected?	Where is it stored?	Why is it collected?	Lawful basis of collection	Retention period	Internal access and sharing	External access and sharing
Application to supply	Contact details SIA licences	Application	JotForm monday.com WMS	Supplier compliance	Consent			SIA regulator NSI auditor
Suppliers	Director details Insurance Governance Finance details Screening sample Payslips sample	Audit			Contract			
Deployment details	Employee details Licence details			Employees supplied for deployment				
Enquiry form	Contact details				Consent			None
Supplier Audit					Compliance			