fieldfisher

Data Protection and Information Security

October 2022

Introduction

Fieldfisher is committed to protecting the privacy and security of our IT infrastructure and the data we hold, whether this is client data or that of our employees.

Our team work to ensure that our systems and processes meet the highest standards, whilst working as a business enabler to improve agility and respond to our clients' needs.

In this note, Fieldfisher is Fieldfisher LLP and its associated entities, but not members of Fieldfisher Global, a Swiss Verein.

This document is provided in confidence as an overview of our controls when handling your data.

Certifications

Fieldfisher holds the following certifications:

- ISO27001:2013
- Cyber Essentials
- Cyber Essentials Plus

Applicable Regulations

Fieldfisher is headquartered in the UK, and is subject to the EU and UK General Data Protection Regulations (GDPR). Fieldfisher also has offices in several other countries, within the EU and outside. Irrespective of the UK's exit from the EU, Fieldfisher complies with the GDPR.

Processing Personal Data

Fieldfisher is a law firm, and provides clients with legal services across a variety of practice areas. Inevitably, in the course of providing these services to its clients, Fieldfisher will process personal data about clients who are individuals, personnel at clients that are legal entities (such as companies), and other people relevant to the legal matter in relation to which we are instructed (for example, witnesses or experts).

Categories of Personal Data

Fieldfisher collects and uses personal data which is necessary for the performance of legal services. The data could include data such as the subject's name, contact details, job information, identification and background information, ethnic origin, criminal record, medical records or financial information (among other things), depending on the nature of the legal matter.

Legal Basis for Processing

Fieldfisher's legal basis for collecting and processing personal data will depend on the personal data concerned and the context for collection. However, personal data is usually collected where it is necessary in order to perform a contract with the data subject or where the processing is in Fieldfisher's legitimate interest and not overridden by the subject's data protection interests or fundamental rights and freedoms. Fieldfisher also has a legal obligation to process personal data, or may need to process it in order to establish or defend legal claims.

Data Subject Rights

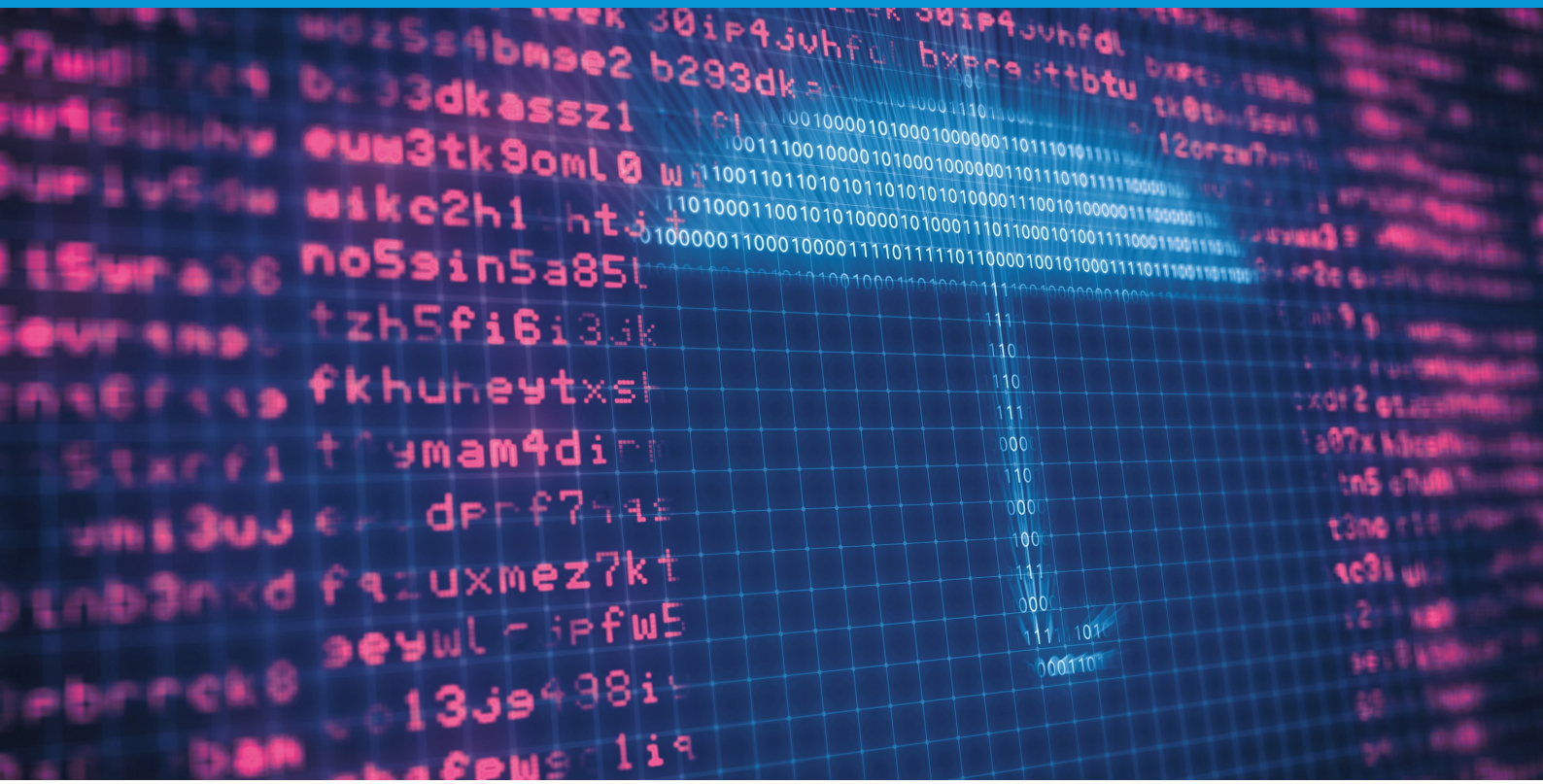
Individuals wishing to exercise their data subject rights under the GDPR should contact the team on data.protection@fieldfisher.com .

Data Protection Officer

Fieldfisher has a Data Protection Officer, Martin McElroy, who can be contacted at data.protection@fieldfisher.com .

Data Centres

Our data centres are located in the UK and are appropriately certified to handle our information. They can be accessed only by authorised persons with the requisite permissions. Access to data is controlled using a layered security process at the domain, application and server levels, allowing access to data to be granted selectively.



Data Transfer between Fieldfisher Offices

Fieldfisher has a number of offices outside of the UK. These offices are required to adhere to the same policies and procedures as the UK offices, and are subject to the European Commission's Standard Contractual Clauses and a Data Transfer Agreement.

Data Transfer Security

In the event that data needs to be taken offsite on removable media, we have software applications, policies and processes to protect the data with appropriate levels of encryption.

Where information needs to be sent to or received from external organisations, Fieldfisher uses a number of tools for secure transfers of data both internally and externally. These include Secure File Transfer Protocol (SFTP) and Hypertext Transfer Protocol Secure (HTTPS) for internet and extranets, plus a range of encryption tools. When files are required on removable media, devices are encrypted and network endpoint controls are in place to prevent the writing of any data to an unencrypted or unauthorised device.

Where the sending of hard copy documents cannot be avoided, safe transfer can be arranged by secure courier and/or secure post, depending on the nature of the information. In addition, information stored electronically which needs to be sent on removable media is encrypted to a CESG approved standard before being sent externally.

Sub-processors

As part of the provision of legal services Fieldfisher engages data processors (for example to help with storage of data). Fieldfisher may be responsible for the appointment and instruction of such data processors. Third party service providers undergo vetting procedures and the transfer of personal data to third party service providers outside of the UK and the EEA takes place on the basis of data protection adequacy decisions by the UK or the European Commission or via the implementation of EU data protection standard contractual clauses.

Staff Vetting

New staff are required to provide proof of identity, right to work, and education and professional qualification certificates at the point of acceptance (country based variations may be in place). Copies of relevant documents will be taken on their first day. In addition Fieldfisher performs background and identity checks, criminal background checks (as appropriate), including pre-employment references covering at least three years or the past two employers. Some groups such as Senior Associates, Partners, and Directors are subject to DBS checks as part of their pre-employment vetting.

Staff Awareness

All Fieldfisher staff are required to complete training on information security and data protection on a regular basis. Staff who handle sensitive information receive additional guidance and training.

Access Control

Standard provisioning and de-provisioning processes are in place for system access.

Access to data files is logged. We utilise Role Based Access Controls (RBAC) for user accounts and segregate duties to ensure that privileged users only have access to the data and systems for which they are responsible. Any requests for escalation of access rights are recorded and follow an authorisation process. Access to our IT network is controlled, with additional levels of protection for sensitive data.

Information barriers are available for a client or contractual requirement.

Monitoring

Fieldfisher proactively monitors activity on its systems in order to ensure system security, effective operation and to protect against misuse or non-compliance with the Firm's policies or other forms of suspected misconduct.

Physical Security

Access to Fieldfisher offices requires a pass and swipe card to enter non-public areas. Our premises are typically secured by a combination of 24-hour security control, CCTV and patrolling security guards although specific controls may vary by office.

Penetration Testing

Testing is undertaken by CHECK approved vendors and/or aligned to CREST standards. Tests are reviewed by the Information Security Manager and Technical Managers. Remediation is prioritised and completed in line with the risk of the identified vulnerabilities.

Vulnerability Management

Scans are performed regularly on Fieldfisher assets. Results are risk assessed and remediated based on criticality and potential impact to the firm. Patching and updates are deployed regularly to ensure software and services are within supported versions.

Network Security

Firewall protection, router configuration and rules are in place and regularly reviewed. Appropriate resilience and protection services are set across the network. Monitoring is in place to identify problems and remediate in accordance with the risk. Settings are in accordance with need, protection and the required security features.

Backup and Disaster Recovery

Our critical services are designed to be resilient in the event of various scenarios with the ability to move entire or partial services in the event of an incident.

We test systems at least annually and retain the capability to recover from backed-up data in the event of data corruption or catastrophic systems failure. A number of our critical services operate independently from our data centre meaning our operation can continue without core infrastructure services.

Business Continuity

We have a testing program which includes table top exercises focusing on business activities and threat based scenarios. The program is reviewed regularly by business leadership and senior stakeholders to ensure it is fit for business purpose and meets the firm's objectives.

Cloud Services

The firm utilises cloud services where they offer the best solution for us and our clients. Services are subject to appropriate due diligence, review and risk assessment. Services are continually reviewed to ensure they meet our legal, contractual and regulatory expectations.

Collaboration Services

We have a number of services available for collaboration. They are hosted in the Cloud and provide fully secured and encrypted data solutions.

Document and Case Management Systems

The firm combines document and email records in a single solution to ensure comprehensive management of client activities and interactions. Client matters are stored in a logical filing structure, which can be shared securely with the relevant stakeholders. All activities are auditable and restrictions can be applied by client, specific matter, or at the document level, allowing flexibility to meet our clients' needs.

Data Deletion

Fieldfisher is able to carry out the deletion of data upon request subject to statutory and regulatory obligations.

Endpoint Protection

Devices run an advanced anti-virus and firewall protection. Restrictions are in place to control USB device usage. All computers and mobile devices are encrypted as standard.

Encryption

We use a combination of protocols to safeguard data at rest and in transit to ensure data integrity and authentication. We use symmetric and public keys schemes which are managed and rotated periodically. We also use file and drive level encryption where practicable to do so.

Email

All email, inbound and outbound, is checked by our cloud -based email platform. Our email system has a number of security safeguards in place to protect our systems such as anti-virus, anti-malware, URL redirection and targeted threat protection.

We have additional protection in place to help our staff to identify misaddressed, unauthorised and phishing email.

We use TLS as standard and can move to Enforced with clients as required.

We limit email size and restrict certain file types to protect the firm.

Secured email services can be used on request.

Mobile Computer Working

All staff who are authorised for mobile computer working are able to access data through secure, auditable VPN access. All of the firm's laptops are encrypted and remote access to our network is controlled via multi-factor authentication and secure VPN. Personal mobile computers can only be used for Citrix connectivity to firm systems.

Mobile Device phones and tablets

Firm issued mobile phones are encrypted and built to a standard which includes a device management application installed to centrally manage security and provide remote tracking/wiping capabilities. Staff also benefit from threat and filter content management.

Bring Your Own Device (BYOD)

Staff may also have an encrypted mobile phone, which has a device management application installed to centrally manage security and provide remote tracking/ wiping capabilities.

Change Management

Changes are centrally recorded through a system. All changes go through a submission process which aligns to the IT Infrastructure Library (ITIL) framework.

Configuration

Devices are imaged and updated regularly with security standards and policies which are centrally enforced. Users are prevented from altering and modifying device configurations without the appropriate privileges.

Asset Management

Software and hardware is centrally managed and assets are allocated to individuals.

Audit

Fieldfisher regularly tests, assesses and evaluates the effectiveness of technical and organisational measures. We audit internally as well as obtaining independent review. We are subject to regular external surveillance audits for our certification for ISO 27001 and Cyber Essential Plus.

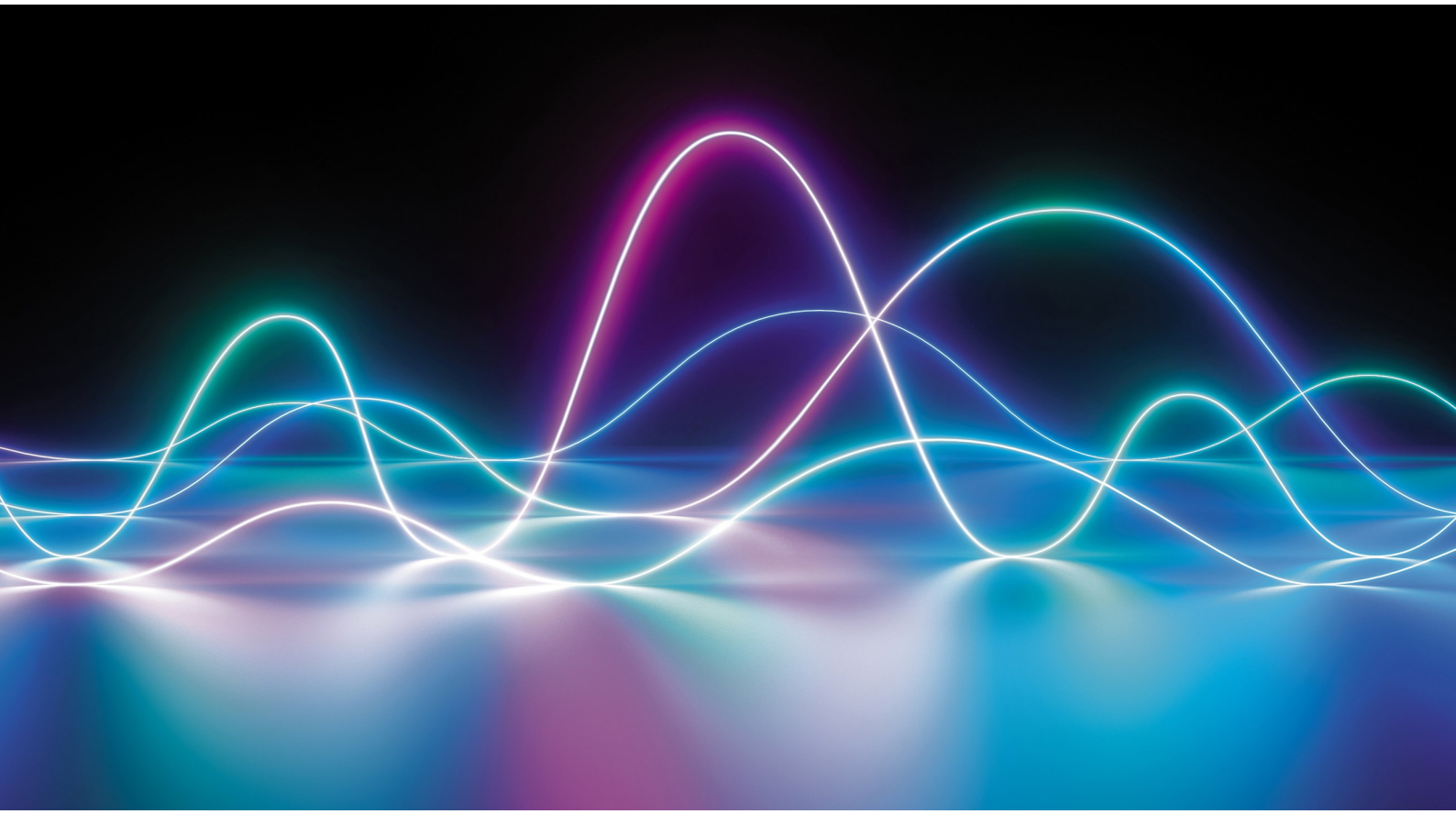
Supplier Management

Where appropriate, suppliers are assessed and credentials are validated as part of the engagement. Appropriate clauses and provisions in relation to the services being rendered are reviewed by our legal and risk teams.

As part of the supplier's contract review, we will assess the deliverables, and depending on the nature of the engagement; we request a right to audit.

Incident Management

All incidents are reported via Fieldfisher's IT Service Desk, who carry out an initial triage and will alert our Incident Response team as required. Incidents are classified and evaluated with appropriate mitigating measures. Incidents are recorded in a system. Incidents involving actual or potential breaches of data will be referred to relevant parties as necessary within our legal obligations.



fieldfisher

Contact Details

Gareth Davies
Head of Information Security, Business Services, Risk & Compliance
+44 (0)330 460 6507
Gareth.davies@fieldfisher.com

Martin McElroy
Data Protection Officer, Business Services, Risk & Compliance
+44 (0)330 460 7063
martin.mcelroy@fieldfisher.com