



IRIS FMP International

Information Security Assurance Statement

Document control

Version number: 1.3

Owners: Lee-Anne Watt/Charlotte Hobson

Date of last update: 18/10/2023

Document type: Assurance Statement

Replaces: 1.2

Approved by: David Munn

Approval date: 25/10/2023

Data protection impact screening: N/A

Date of next formal review: 17/10/2024

Contents

1. Information Security Assurance Statement
2. IRIS FMP International organisational security
3. IRIS FMP International human resource security
4. IRIS FMP International physical/environmental security
5. IRIS FMP International Operation security
6. IRIS FMP International Communications security
7. System acquisition, development, and maintenance
8. Security in development and support processes
9. Supplier relationships
10. Information security incident management
11. Business continuity – Information security aspects
12. Compliance

Information Security Assurance Statement

Objective of this document

The purpose of this information security assurance statement is to provide customers of IRIS FMP International with transparency as to the security and personal data compliance of this service from all threats, whether internal or external, deliberate, or accidental. This document also aims to ensure legal compliance, business continuity, minimise business damage and maximise client confidence in IRIS FMP International as a thoroughly secure service provider.

Description of the data processing conducted by IRIS FMP International

IRIS FMP International is a payroll outsourcing department under the IRIS family. We offer end-to-end payroll processing ensuring we deliver payroll accurately and compliantly, on time, every time. The objective of the service is to reduce cost and increase profit of our clients. IRIS FMP International provide various payroll related services such as payroll calculations, statutory reporting, accounts journal output, funds transfer to employees and 3rd parties, payslip distribution and payroll queries. We have robust data security measures in place to ensure that our customers' data is protected in every way.

Statement of Assurance

IRIS FMP International will ensure that:

1. We will put in place measures to protect customer information from a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.
2. We will meet our regulatory and legislative requirements.
3. We will produce, maintain, and test Business continuity plans.
4. We will provide information security training to all our staff.
5. We will report and investigate information incidents (whether actual or suspected), in line with our Incident reporting procedure.
6. We will monitor compliance with our Information Security Policy.

IRIS FMP International ensures that all employees comply with corporate standards and procedures. These include incident handling, information backup, system access, virus controls, passwords-authentication, communication, and encryption. These policies are communicated to all employees via the company compliance portal and intranet.

IRIS FMP International Organisational Security

IRIS FMP International is committed to fulfilling its obligations under the Data Protection Act 2018, General Data Protection and Regulation (GDPR – European Union Law) and any associated privacy legislation that affects how we use or handles personal data. IRIS FMP International has produced the Statement of data protection policy to give this assurance to our customers and staff.

In addition to the IRIS FMP International Statement of data protection policy, this document sets out how responsibility for data protection and information security is designated. It includes high-level descriptions of the procedures in place that must be followed to ensure personal data is handled in a responsible, accountable, and secure manner

IRIS FMP International will use personal data legally and securely regardless of the method by which it is collected, recorded, and used and whether we hold it within our products, on a Group or third-party network or device, in filing systems, on paper, or recorded on other material such as audio or visual media.

IRIS FMP International regards the proper management of personal data as crucial to the success of our business. Observing good data protection practice plays a huge role in maintaining customer confidence. We ensure that IRIS FMP International respects privacy and treats personal data lawfully and correctly.

We employ the use of a Secure File Transfer Protocol (SFTP) service and IRIS FMP Engage platform to store and transfer sensitive documents and files with our customers.

The SFTP Service is hosted in a UK datacentre and is protected by a Managed Detect and Response Service (MDR) which has a 24 by 7 Security Operations Centre (SOC) monitoring the service and the network. Customers can securely connect through a modern browser with a complex

password/passphrase with a password reset mechanism based on a sole use one time password. Once connected customers and IRIS service staff can share files that are transferred over an https 256bit Encrypted connection.

Client data stored within the 'IRIS FMP Engage' application databases and document repositories is hosted on Microsoft Azure PaaS at the following locations: Microsoft Azure PaaS Europe West (Ireland) Microsoft Azure PaaS Europe north (Netherlands).

Customers can securely connect through a modern browser with their own unique username and password/passphrase with a password reset mechanism. These passwords have the following controls: configurable min password lengths, reset durations, passwords must contain upper, lower-case letters, number, and special character. Auto lockout after failed login attempts, captcha implemented.

Once connected customers and IRIS service staff can share files that are encrypted in transit (SSL/TLS) to and from the application and at rest using AES256bit encryption. All files uploaded to the application are scanned for malware at the point of ingestion.

IRIS FMP International is part of the IRIS Software Group.

Organisational Security at IRIS Group Level

Data protection and information security at IRIS Software Group is controlled by the IRIS Information Security and Governance Forum. This forum meets at least quarterly and includes:

- Members of the Executive Committee
- The Chief information Officer (CIO)
- IRIS Group IT Director
- IRIS Group Data Protection Officer
- Other key security leads within the company

The Information Security and Governance Forum approves IRIS Group level policies relating to information security and data protection, which IRIS products must comply with. There are three Group policies and a detailed Information Security Management System (ISMS). The three Group level policies are:

- [IRIS Group Data Protection Policy](#) - this sets out the roles and responsibilities for data protection compliance within the IRIS Group. It also sets out the requirement for risk assessment and data protection assessment for all projects and proposals that will change or impact on the handling or use of personal data.
- [Information Security and Acceptable Use Policy Summary](#) - this sets out the basic information security and acceptable use standards that all staff within the IRIS Group are required to adhere to.
- [IRIS Personal Data Incident Reporting and Investigation Procedure](#) - this indicates the reporting and investigation procedure for all security incidents that become known or are reported to anyone within the IRIS Software Group.

The above policies are communicated to all staff and relevant external staff within the IRIS Group at least annually, using a dedicated training and policy management platform. Managers responsible for

delivering IRIS products and services are required to ensure local arrangements are in place to comply with those policies and to evidence this.

- **IRIS ISMS** - This is the default security system for IRIS Software Group. All IRIS products must meet or be working towards meeting the standards of the IRIS ISMS except for those which already have their own certification under ISO27001 or any other standard relating to information security and data protection.

Organisational Security for IRIS FMP International

At IRIS FMP International, the product manager is the single point of contact for routine security and data protection enquiries. They work with the managers involved in delivering our services to ensure compliance with the IRIS Group policies and ISMS or any other information security standard – as well as any other regulatory requirements relevant to the service.

For IRIS FMP International, the team with responsibility for ensuring your data remains secure and in compliance with IRIS Group Policies and ISMS are:

Employee Name	Department	Designation
David Munn	Senior Management	Senior Director, Managed Services
Vincenzo Ardilio	Central Compliance	Data Protection Officer – Group
Lee-Anne Watt	Managed Services	Senior Manager, International Client Payroll
Charlotte Hobson	Managed Services	Senior Manager, International Client Payroll & Payments

The IRIS FMP International team keep your data secure by ensuring that appropriate measures are implemented to protect your data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to your data while being stored, transmitted, or otherwise processed by or on behalf of IRIS FMP International.

Measures are “appropriate” if they have been identified through risk assessment. Date of last IRIS FMP International risk assessment review: 20th September 2023

The IRIS FMP International team will ensure adequate records are created and maintained to support compliance verification and inspections and incident response (subject to any limitations set out in our Terms and Conditions).

The IRIS Group Data Protection Officer is responsible for providing advice and guidance to the IRIS FMP International team and for monitoring our compliance on all security policies and related issues. The IRIS Group Data Protection Officer is also the designated contact for the Information Commissioner’s Office.

IRIS Group IT are responsible for the operation and integrity of IRIS FMP International IT systems and for keeping systems up to date.

Asset Register - IRIS Group IT records and maintains a register of all assets, relevant to IRIS FMP International in a fixed assets system.

Client Defined Classifications - Client information and materials processed, stored, or transmitted by IRIS FMP International shall be handled strictly in line with the customer’s prior advised classification policies and standards, subject only to legal compliance.

IRIS FMP International Human Resource Security

IRIS FMP International staff will have access to your data.

Prior to employment

- Staff and contractors are subject to background checks and verifiable references to ensure suitability for any given job role.
- All staff are required to accept our Group Data Protection Policy, Incident Reporting Procedure, and Information Security & Acceptable Use Policy.

During employment

The responsibility for ensuring that processes and procedures are both established and maintained are held with IRIS FMP International Managers. Employees, third parties and contractors are mandated to read, and sign a document to confirm understanding of their responsibilities. In the event of the use of an external party, controls are put in place to restrict the level of data they have access to in line with group policy and this activity is supervised and relevant risk assessments have taken place.

In addition to local procedure, IRIS Group also require the completion of corporate policy training and the subsequent testing of this knowledge through the MetaCompliance portal. This testing is repeated as frequently as is reasonable for all employees, third parties and contractors.

In the unlikely event of a security breach, the governing policy or procedure would be re-reviewed and amended to ensure stricter compliance moving forwards. IRIS Group places the onus on the employee for their adherence to security protocols and a disciplinary procedure is enforced for noncompliance. If no improvement is found to employee performance under the afore mentioned disciplinary, employment is terminated as set out in the terms of the procedure.

Termination and change of employment

In the event of an employee terminating their employment contract with IRIS Group, the following departments are notified, and the following actions take place:

Department	Action
Managed Services Management	To notify Group HR and Group IT, revoke log in credentials from internal systems required for role.
Group HR	To restrict access to internal systems, HR portal and notify Payroll
Group IT	To close off network access, organise recovery of assets, revoke other access (Office 365 account, Cloud accounts, VPN (Virtual Private Network) access)

Upon instruction from HR of a person leaving IRIS FMP international, that person's access to confidential areas shall be restricted immediately, culminating in:

- full removal of access to any part of the corporate network prior to departure.
- all corporate assets in that person's possession having been returned and or been collected by the relevant Department manager or the Information asset Owner as appropriate.
- In the event of a person transferring from one department to another within IRIS Software Group that person's access will be varied accordingly.

All employees have been contracted to a non-disclosure clause in their contracts that remains applicable after termination.

IRIS FMP International Access Control

The purpose of the Access Control Policy is to ensure that information systems resources and electronic information assets owned or managed by IRIS are available to all authorised personnel. The Policy also deals with the prevention of unauthorised access through managed controls to create a secure computing environment.

Access controls to network, operating system and applications shall be set at an appropriate level on a need to use basis, which minimizes information security risks yet allows the business activities to be carried without undue hindrance. This is managed as per the Organisational Security section in conjunction with the IT Manager and Information Asset Owner and in accordance with the IRIS Group Access Control Policy.

Access is granted on the least privileged rule basis consistent with an individual's job/role responsibilities. For IRIS FMP International user login, system enforced Password complexity rules ensure that strong passwords are used, and Users are responsible for keeping them confidential. Systems and information should be secured whenever left unattended.

All static user equipment must be kept in good order and used responsibly; all laptops shall be subject to the IRIS Group's Acceptable usage policy. Passwords must not be disclosed to colleagues or any third parties. As set out in IRIS Group's standard HR Policies all personnel must maintain full conformance with company undertakings in respect of confidentiality.

Access to cloud-based administration consoles for privileged IRIS' IT Department and IRIS users is mandated with password authentication.

Server Operating System Access Control along with change and patch management shall always adhere to Microsoft's best practice and shall be administered by the IRIS IT team in conjunction with the infrastructure managers in respect of their individual department's development and support environments.

All administration systems are monitored, and audit trails produced together with email notification to the System Manager of any unauthorised attempts to access the corporate network.

Remote access to a client's network shall always be subject to client's prior written (or otherwise validated) consent or request and must be controlled either by using clients provided VPN and or remote assistance software which utilises SSL and provides a full audit trail.

Password and Authentication Policy

This policy describes the authentication requirements for accessing internal computers, networks and includes those working in-house as well as those connecting remotely. Every person, organisation or device connecting to internal IT resources and networks must be authenticated as a valid user before gaining access to IRIS's computer systems, networks, and information resources.

For the avoidance of doubt, IRIS FMP International warrants to Clients that it will not seek to circumvent, compromise, or change the Client's security controls, and IRIS FMP International will not change the Client's software configurations (without proper authorisation); and no 'back door' password or other method of remote access shall exist.

IRIS FMP International Physical and Environmental Security

IRIS FMP International follows guidance set out in our group Physical Access policy.

Physical entry controls - Entry to the site is restricted to key fob or keypad entry. Only IRIS employees have access to the area payroll is completed in.

Securing offices, rooms, and facilities - Physical security is employed at greater levels where higher risk or classification of a more sensitive nature of data is identified.

Protecting against external and environmental threats - IRIS FMP International has a robust business continuity plan; however, we also place an immense importance on our first defence. We are protected by a failover line in the event we lose connectivity due to environmental damage, we also can move the entire site remote or transfer ownership to a satellite office at a moment's notice.

IRIS Group have invested heavily into our cyber defences, these are controlled by IRIS Group IT. We have also moved customer data into an ISO-secure cloud-based environment which adds additional layers of security to your information.

Working in Secure Areas – In the event a third party needs access to a secure area within the physical site, they are always escorted by facilities. Additional measures are covered under the topic "Human Resources Security."

Delivery and loading areas – Deliveries are taken at reception with no access granted to unauthorised people.

Equipment

Equipment siting and protection - Access to critical computing resources or infrastructure is physically restricted to authorised personnel with access controlled by keys, swipe cards or a keypad lock.

Protection against power failures and disruptions - The physical site has taken adequate measures to prevent disruption. Installation of a failover line in the event of loss of connectivity.

Equipment maintenance - Regular maintenance is conducted on equipment as per the recommendations of the manufacturer. A maintenance log is held on site and maintained by designated Facilities personnel.

Removal of assets - Any physical assets to be moved from one place to another place within the office and outside the office must require prior approval from Senior Management. A register of all assets taken off site is kept and maintained by the Site Leader and shared with Group IT.

Security of equipment and assets off-premises - Guidance is outlined in mandatory policy document

Group IT Working from home manual with considerations on Information security, use of the Group's VPN. 2 Factor Authentication is implemented for access to all secure area of the network.

Unattended user-equipment – IRIS FMP International enforces a clear desk policy. Staff laptops & IT assets are sited in a secure office area, information displayed on screen may be confidential. All computers revert to screen saver mode at timely intervals and staff are mandated to logoff from sessions and ensure any paper

Clear desk and screen policy – IRIS FMP International went paperless in January 2020. In line with our Clear Desk Policy, employees and contractors are made aware of their responsibilities to ensure that data is always protected. All employees and contractors are expected to lock their computer screens, as a redundancy procedure, IRIS Group IT set screens to auto lock after 5 minutes and will require a password from the user to unlock.

Media handling

Management of removable media – IRIS FMP International sets out the acceptable usage of removable media in Information security and acceptable use summary Policy. It is not permitted to create a copy of protected data on unauthorised devices.

Disposal of media – IRIS FMP International sets out responsible use of data in our IRIS Data Protection Policy, including secure disposal and audit of media.

Operations Security

Documented operating procedures – Backups, transmission of information between environments and equipment maintenance are all fully managed services by suppliers listed in this document. All suppliers are independently audited against ISO 27001 standards.

Change management - Change management controls have been implemented to ensure satisfactory control of all changes. Major architectural changes are reviewed by an architecture review board (ARB) to discuss security, service level and complexity issues.

Capacity management - Resources are monitored, tuned and protections made of future capacity requirements to ensure systems continue to perform at optimum levels.

Separation of development, testing and operational environments - Development and production environments are separated and managed through documented and automated deployment pipelines. Access to infrastructure is restricted through IP restriction lists. Desktop payroll developers do not have access to production environments, unless authorised for a specific purpose i.e., Product Support.

Protection from malware – IRIS FMP International utilises Kaspersky, to protect against malicious software and this is centrally monitored. All client machines are auto updated on connection to the network or via internet. Firewalls are in place. Mimecast is used to provide comprehensive email filtering (not only to preclude spam but also to scan attachments more effectively to counteract viruses and other malware).

Back-ups - The backup of all processing server systems falls under the remit of the Group IT Director. All data is backed up nightly and transmitted to a secure UK-based cloud back-up location. Restoration tests are made and documented on a regular basis, not less than annually.

Event logging – Both environment and software products have independent audit logs of activities conducted within each. Environment audit is maintained and monitored at Group IT and Infrastructure level and Product is reviewed by IRIS FMP International Management.

Protection of log information – Log information and Audit trails are managed at Group IT level in line with outlined roles and responsibilities to prevent tampering of data. On a software product level, these controls have been locked at development stage, no user can manipulate information held within.

Clock synchronisation - IRIS Group IT controls clock settings, ensuring that synchronisation is enabled to a real time clock set at local standard time

Control of operational software – Installation of software on desktop payroll production systems is managed through package managers to minimise the risk of corruption of operational systems

Management of technical vulnerabilities - Penetration testing for integrated web-applications is planned annually to be undertaken by a third party. Security is considered during backlog refinement and discussed as part of the overall product backlog and workload. Any changes which have security implications are reviewed by the Architecture Review Board.

Restrictions on software installations – Group IT regularly review acceptable use and monitor or restrict installations that have not yet been deemed safe. Requests to install new software must be authorised by Group IT if not already placed on a safe list.

Communications Security

Network security – All integrated web-applications are maintained and tested to a high standard of security. The integrity of client data is ensured through a quality hosted environment that holds more than appropriate accreditation outlined within this document

Security of network services – We employ the use of Cloud-Based Technology that houses personal data in UK Data Centres hosted by 6degrees, that uses world class security protocols to ensure security compliance. 6degrees hold SOC Type I and SOC Type II, their credentials are:

- ISO27001
- National Cyber Security Centre (a part of GCHQ)
- Crest
- Cyber Essentials Plus
- Member of Microsoft Intelligent Security association

As an additional layer of complexity, only employees granted access to view this data can only do so using an internal group VPN. These controls are reviewed annually.

Segregation of networks – The network client data and software used to process this data are held in separate networks to mitigate risk. These networks are independent of all other business IRIS transacts and controls are in place to ensure that only authorised persons have access to these drives.

Electronic messaging – IRIS employees are subject to audited training on appropriate use of electronic communication, particularly with sensitive and/or personal information. In cases where customer information needs to be shared for fault finding purposes (such as support / develop liaison), these are controlled through restricted access Customer Relationship Management (CRM) systems requiring multi factor authentication.

Confidentiality or non-disclosure agreements - As required, IRIS FMP International uses Non-Disclosure Agreements (NDA) and maintains signed agreements to protect confidentiality. The requirements for

confidentiality or non-disclosure are identified, reviewed, documented regularly by IRIS, and communicated through training plans.

How we transmit confidential information to customers

We employ the use of a Secure File Transfer Protocol (SFTP) service and IRIS FMP Engage platform to store and transfer sensitive documents and files with our customers.

The SFTP service is hosted in a UK datacentre and is protected by a Managed Detect and Response Service (MDR) which has a 24 by 7 Security Operations Centre (SOC) monitoring the service and the network.

Customers can securely connect through a modern browser with a complex password/passphrase with a password reset mechanism based on a sole use one time password. Once connected customers and IRIS service staff can share files that are transferred over an https 256bit Encrypted connection.

Client data stored within the 'IRIS FMP Engage' application databases and document repositories are hosted on Microsoft Azure PaaS at the following locations: Microsoft Azure PaaS Europe West (Ireland) Microsoft Azure PaaS Europe north (Netherlands).

Customers can securely connect through a modern browser with their own unique username and password/passphrase with a password reset mechanism. These passwords have the following controls: configurable min password lengths, reset durations, passwords must contain upper, lower-case letters, number, and special character. Auto lockout after failed login attempts, captcha implemented.

Once connected customers and IRIS service staff can share files that are encrypted in transit (SSL/TLS) to and from the application and at rest using AES256bit encryption. All files uploaded to the application are scanned for malware at the point of ingestion.

CRM is used for all queries and all personal identifiable data is removed from the contents of email transactions in direct reply to a query. All employees receive audited training against this requirement.

Information transfer policies and procedures – IRIS FMP International clearly outlines the procedures within the IRIS Data Protection Policy held at local level for the teams. It is meticulous in the process that must be followed to prevent risk occurring when transferring information between IRIS FMP International and Client.

System acquisition, development, and maintenance

Securing application services on public networks - Where possible, integrated web-applications enforce the use of Transport Layer Security (TLS) 1.2 as a communication protocol.

Security in development and support processes

System changes control procedures – Major system changes are reviewed by the Architectural Review Board (ARB) mentioned previously in this document.

Technical review of applications after operating platform changes - IRIS test all product updates against a range of supported environments and software. Regression testing is completed to review the overall product impact of any system changes.

Restrictions on changes to software packages - Changes to software development inhouse is subject to change control procedures.

Secure system engineering principles - Principles for engineering secure systems have been established, documented, and maintained by the IRIS architecture team and are used as part of an internal training plan for all developers (Architecture Corpus).

System testing - All system and application changes are subject to an appropriate combination of manual, automated and regression testing comprised of testing suits managed by the internal quality engineers on the desktop payroll team. All features are tested before being accepted through a series of environments before they enter the production environment.

Secure development environment - The organisation has appropriately assessed the risks associated with individual system development and integration efforts that cover the entire system development lifecycle. Development environments are assessed for suitability and security by the Architectural Review Board.

Test data

Protection of test data - Copies of production databases are not used, and live production data is not used for testing purposes. Development, QA, and staging environments have a series of stock / dummy data and manually entered data of fictitious companies and employees for the use of testing.

Supplier Relationships

Supplier Service Delivery Management

Monitoring and review of supplier services – Suppliers are independently audited by third parties against ISO 27001/9001 standards. IRIS review these audits and SOC reports annually to assess if supplier relationships meet the standards for continuation.

Managing changes to supplier services – In addition to the assessment of supplier audits, if a new supplier needs to be selected for any reason, the IRIS internal compliance team are responsible for choosing an appropriate supplier based on ISO 27001 standards. After appropriate assessment, the Group Compliance Manager is responsible for such decisions.

List of third parties and sub-processors involved in IRIS FMP International processing customer data

Internal 3rd Parties

IRIS Cerberus – Hosted environment to act as a secure document transfer system. Access is restricted and appropriate ISO controls exist. Data contained in the system is held within UK Data Warehouses and clients have full control over deletion of data.

IRIS KPO India – provides additional support for our international payroll service. IRIS KPO use our internal secure IRIS VPN connection alongside the security architecture 6Degrees provides to process data within UK Servers. A detailed risk assessment is conducted annually to ensure continued process review of security requirements. A full Customer Assurance document is also available.

External 3rd Parties:

- Western Union Business Solutions
- ZOHO
- Payzaar Limited

Please get in touch for more information on our partners in specific territories.

Security Sub-Processors:

- eSentire (as part of our Managed Detect and Response service)

Other vendors used by IRIS Group

- Veeam
- Microsoft
- Kaspersky

Information Security Incident Management

Management of information security incidents and improvements

In all instances, any desktop or cloud payroll critical incidents (whether relating to information security or not) are managed through the “Critical Incident Management Process,” handled, and coordinated by the IRIS Critical Incident Manager. Incidents are prioritised and classified as part of this process. The process outlines stakeholder communication with a focus on customer communication during an incident resolution. A post incident review is then drawn up by the software manager and / or product manager and corrective actions are logged and tracked to execution.

Information security incidents must follow this process, but in addition will be triggered by the Group Data Protection Officer. The IRIS Group Data Protection Officer will report a summary of all data protection incidents to the IRIS Information & Security Governance Group and maintain a list of learning outcomes and actions arising from incidents with the aim of ensuring Information Asset Owners follow through on those actions. This process will also be used internally for any issues discovered during development, and training is provided for staff to promote awareness of this process.

Business continuity - Information Security Aspects Information security continuity

Planning information security continuity – During adverse situations, IRIS FMP International have several secure ways to ensure the continuity work carried out. All processors and managers are laptop users with access to the IRIS secure VPN. The installation of 3rd party software is strictly controlled with appropriate auditing in place detailed throughout this document.

Implementing information security continuity – IRIS FMP International continues its use of the Local Data Protection Policy in the event of a Business Continuity Plan (BCP) scenario. We also utilise the Working from Home Procedures policy and Acceptable Usage policy.

Verify, review, and evaluate information security continuity – IRIS FMP International review all policies as often as required but no less than once per year.

Compliance

Compliance with legal and contractual requirements

Identification of legislation and contractual requirements applicable to IRIS FMP International – Within the scope of the role performed, processors, managers and software provisions will defer to country specific statutory regulations and terms and conditions with client. IRIS FMP International makes every effort reasonable to inform its clients of any major changes to legislation within these areas.

Protection of records – Covered in the Business Continuity Plan Document

Privacy and protection of personally identifiable information – Covered within IRIS FMP International’s Data Protection Policy both at local and group level.

Regulation of Cryptographic Controls – IRIS FMP International utilises an online Payslip Portal which has been developed using market leading encryption methods. These fall well inside the scope of existing

legislation and additional security measures such as 2 Factor Authentication (2FA) have been built into the existing framework.

Information security reviews

Compliance with security policies and standards – Local policies are reviewed as regularly as required but no less than annually. This is to ensure that all relevant standards are being met and have been implemented in full. Group level compliance reviewed annually.

Data Protection – quick reference

IRIS Group Data Protection Officer - Vincenzo Ardillio dataprotection@iris.co.uk

Data protection owners for IRIS FMP International - Lee-Anne Watt lee-anne.watt@irisglobal.co.uk

Charlotte Hobson Charlotte.Hobson@irisglobal.co.uk

Categories of personal data processed as part of the IRIS FMP International provision:

- Trade Union Membership – identifiable through deductions made to employees
- Information relating to criminal convictions and offences – identifiable through court order fines processed through payroll

Categories of data subjects under the IRIS FMP International provision:

- Employees – identifiable through payroll processing

Location of personal data processing

All personal data is held within payroll software databases and on electronic documents from client communicating this data to IRIS FMP International. In all instances, information is held on secured network drives held in the UK and only accessible by those authorised to process it.

A full risk assessment is conducted annually to ensure that client data is always protected.

Retention of data

Data will be retained for a period of no more than 6 years for the purpose of assisting in any Anti Money Laundering (AML) audit that may take place. At the termination of an agreement between IRIS FMP International and client data is retained for the purposes of AML audit within the 6-year window.

In the event a client wishes IRIS FMP International to delete their data, their Right to Erasure applies. We are unable to delete anything that we are required to keep legally, however we will anonymise data, where possible and exclude from any marketing programmes. To apply the Right to Erasure, the client would need to send the request via email to the IRIS FMP International support inbox.

Data subject rights

Clients wishing to submit a Data Subject Rights request can do so by email to the IRIS FMP International support inbox. A response will be received within 2 working days. Where subject matter is comprehensive or more time is required to deliver the requested data, a client will be updated with realistic timescales to satisfy their request.

Further Information

If you would like further information relating to the FMP International service, please contact internationalpayrollsupport@irisglobal.com