IRIS Payroll Professional

Information Security Assurance Statement

Document control		
Version number:	V1.50 2024	
Owner:	Nigel Francis	
Date of last update:	04/04/2024	
Document type:	Information Security Assurance Statement	
Replaces:	V1.40 2023	
Approved by:	Fran Williams	
Approval date:	30/04/2024	
Data protection impact screening:		No PIA required
Date of next formal review:		April 2025

Contents

Information security assurance statement

Objective of this document

This information security assurance statement is to provide customers of IRIS Payroll Professional with transparency as to the security and personal data compliance of this product and the associated My ePay Window service from all threats, whether internal or external, deliberate or accidental. Also, this document aims to ensure legal compliance, business continuity, minimise business damage and maximise client confidence in IRIS Payroll Professional as a thoroughly secure software and service provider.

Description of the data processing carried out by IRIS Payroll Professional / My ePay Window

- Software development and support for Payroll processing, auto enrolment, and cloud Payroll data self-service
- IRIS Payroll Professional software can be hosted on the client's own IT infrastructure in which case payroll data is held and processed by the client, if required, the software and data can be hosted on the IRIS hosting service or a third-party hosting service in which case software, data and processing is at the specified hosting service.
- The IRIS Payroll Professional software whether hosted locally by the client or at a hosting service, transmits data securely to the IRIS My ePay Window self-service cloud portal service for information distribution to users/employees.
- The IRIS Payroll Professional software whether hosted locally by the client or at a hosting service, can transmit data securely to IRIS's EVC connector on IRIS's MS Azure tenant. This to support employee online salary verification in conjunction with the Experian work report service. Clients can opt out their company and all or individual employees from the IRIS EVC connector from IRIS payroll professional as required. See more details here
- Personal data may be shared by clients from time to time with the IRIS Payroll Professional Support team/service or Professional services team for software application support and product implementation.
- IRIS Payroll Professional software and services are designed to support customers in providing payroll services for themselves or their clients and to fulfil their obligations as a UK Employer.
- Personal data is held in IRIS Payroll Professional sufficient for the purposes of payroll processing in accordance with HMRC requirements. Please see our My ePay Window privacy statement that details the specific information held on our My ePay Window cloud service and also the IRIS global privacy policy that details the information we hold when you make contact with us or use one of our services.

Statement of assurance

IRIS Payroll Professional 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 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 Payroll Professional Organisational Security

IRIS Payroll Professional is part of the IRIS Software Group and its operations are ISO27001 certified.

Please refer to the IRIS ISO27001 Statement of Applicability (SoA) for a summary of controls for each information security aspect as per the clarifications on the pages that follow:.

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)
- The IRIS Group IT Director
- The IRIS Group Data Protection Officer

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 at IRIS Payroll Professional

The product manager is the single point of contact for routine security and data protection enquiries. They work with the managers involved in delivering IRIS Payroll Professional to ensure IRIS Payroll Professional complies 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 Payroll Professional, the team with responsibility for ensuring your data remains secure and in compliance with IRIS Group Policies and ISMS are:

- The Product Director – IRIS Information Asset Owner and Product Manager
- The Development Manager – IRIS Information Asset Manager
- The Customer Support Manager– IRIS Information Asset Manager

The IRIS Payroll Professional 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 Payroll Professional.

Measures are "appropriate" if they have been identified through risk assessment. IRIS payroll Professional is ISO27001 certified and as such carries out bi-annual information security risk assessments in accordance with this standard.

The IRIS Payroll Professional 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 together with the IRIS Compliance Team are responsible for providing advice and guidance to the IRIS Payroll Professional 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.

Group IT, IT Operations and the IRIS Payroll Professional team are responsible for the operation and integrity of IRIS Payroll Professional's IT systems and for keeping systems reasonably up to date.

IRIS Payroll Professional's Development systems are managed by IRIS Group IT, supported by the local development team.

Asset register: IRIS Group IT records and maintains a register of all assets, relevant to IRIS Payroll Professional (including acquired software licences) in a fixed assets system.

Client defined classifications: Client information and materials processed, stored or transmitted by IRIS Payroll Professional shall be handled strictly in line with the customer's prior advised classification policies and standards, subject only to legal compliance.

IRIS Payroll Professional human resource security

IRIS Payroll Professional staff specialise in the development and support of software systems for payroll and is privy to confidential information, not least to personal data which is subject to the General Data Protection Regulation we ensure that:

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 IRIS Payroll Professional Information Asset Owner is responsible for ensuring that Information Asset managers are made aware of their responsibilities to ensure that established policies and procedures are adhered to by external parties, contractors and employees.
- IRIS Payroll Professional employees, third parties and contractors receive appropriate awareness training and regular updates in organisational policies and procedures as relevant for their job function by their designated IRIS Payroll Professional Information Asset manager. Corporate policies and training are administered via the IRIS KnowBe4 portal.
- IRIS Payroll Professional 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, the following departments are notified and the following actions take place:

Department	Action
All – Inc. Development, Support, Professional services, Sales, Administration & finance	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 access

- Upon instruction from HR of a person leaving IRIS Payroll Professional, 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 still remains applicable after termination.

IRIS Payroll Professional Access Control

Users are granted access to network, systems and information therein on a need to know basis by role

and department. This is managed, as per the Organisational Security section, in conjunction with the Group 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 Payroll Professional and My ePay Window, 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 Laptop and Tablet policy and group acceptable use policy. Passwords must not be disclosed to colleagues or any third parties. As set out in IRIS Payroll Professional'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 Payroll Professional and IRIS users (including My ePay Window) is mandated with multi-factor authentication.

Server Operating System Access Control along with change and patch management shall at all times adhere to Microsoft's best practice and shall be administered by the Group IT team in conjunction with the Development 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.

All IRIS Payroll Professional personnel involved in the delivery, installation and implementation of IRIS Payroll Professional software or product for a Client must comply with the Client's security policy and access control mechanisms. In all cases Microsoft's best practices should be followed.

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

Encryption (cryptology)

IRIS IT policy ensures that encryption keys are securely managed throughout their lifecycle and in accordance with the IRIS Group encryption policy.

All IRIS Payroll professional employee laptops are protected with BitLocker encryption.

When exchanging files with IRIS Payroll Professional support team (for the sole purposes of IRIS Payroll Professional's implementation, data transfer, bespoke development, testing, maintenance or support) clients are advised to use the Egress encryption service and/or via the IRIS SFTP service. All files on the SFTP server are automatically deleted after 3 days.

Remote support sessions with IRIS Payroll Professional Support staff are with client consent, utilise SSL encryption and have a full audit trail.

Data is encrypted in transit via SSL (AES256) & TLS 1.2 protocol between the IRIS Payroll Professional desktop software application and the My ePay Window self-service portal and Data and documents on the My ePay Window service are encrypted at rest to AES256.

IRIS Payroll Professional physical and environmental security

IRIS Payroll Professional follows guidance set out in our group Physical Access policy.

Processing servers are located in the secure IRIS Woking Data Centre. Access to the data centre is subject to security guard clearance and in accordance with SOC2, PCI-DSS and ISO27001 certification. Servers are therefore protected from unauthorised access, damage, loss or compromise.

All IT equipment shall be properly maintained. 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. Any disposals of equipment or media handling devices shall be in strict accordance with WEEE recycling standards and undertaken by appropriately certified contractors.

IRIS Payroll Professional enforces a clear desk policy and access to office locations is restricted to IRIS employees. Remote workers and all staff are bound by the IRIS ISMS and specifically the Home working manual, acceptable use and Mobile device policies. Information displayed on screen (or on paper) 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 documents are stored in locked filing/cupboards when their workplace is unattended.

Media handling

IRIS Payroll Professional staff may only use prior authorised removable media supplied by Group IT and as per the IRIS acceptable use policies. Removable media containing confidential information must be encrypted.

All staff should store Corporate and other information on secure shared drives rather than on local devices.

Operations security

The operation and integrity of IRIS Payroll Professional's IT systems fall under the responsibility of the Group IT department and IT Operations team in consultation with the Information Asset Owner and Development and Support Information Asset Managers.

All purchases of additional or replacement processing resource shall be subject to a capital expenditure approval at senior management level.

Documented operating procedures - Documented operating procedures are in place to support key processes and staff in customer support and development and accessible through file repositories, IRIS intranet, the CRM system and development management system. Major architectural changes are reviewed by an architecture review board (ARB) for security, service level and complexity issues.

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) for security, service level and complexity issues. All versions due for release to any client must have prior undergone IRIS Payroll Professional's QA and release management process to ensure that changes to issued software are controlled, have been thoroughly tested and are to a high quality.

My ePay Window Service window - IRIS anticipates the period of greatest use of My ePay Window is between 21st of the month and 5th of the following month. IRIS will ensure that routine maintenance and, wherever practicable, upgrades avoid this critical period so that such work is undertaken between 6th and 20th of any month. Customers will be informed at least 5 days' in advance of such maintenance.

My ePay Window Service availability - Save during routine maintenance and upgrades IRIS will use reasonable endeavours to ensure that My ePay Window will be available at least 98% of the time within each calendar month between the hours of 8.00am and 8.00pm.

Capacity management - Information Asset Managers are responsible for monitoring and projecting required usage of processing resources and or storage together with the Group IT infrastructure team and IT Operations teams. Group IT shall be responsible for keeping systems up to date and the IT Operations team ensure that cloud facing infrastructure is monitored for performance and capacity and patched according to latest security advisories and so that systems continue to perform at optimum levels.

Separation of development, testing and operational environments - Development and testing facilities are isolated from production facilities and on segregated networks and managed through documented and deployment pipelines.

Protection from malware – IRIS Payroll Professional utilises anti-malware software, 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. Email filtering software is used to provide comprehensive 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 IRIS Payroll Professional 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. Note that Clients are responsible for ensuring that they backup their own on-premise data on a regular basis.

Event logging – IRIS Group IT maintain and access logs of user activities, exceptions, faults and information security events on IRIS Payroll Professional IT hosted systems. The IRIS Payroll Professional team and IT Operations teams maintain logs on all user activities for the My ePay Window service and for

client's data located in IRIS provided hosted environments. Only authorised users have access to logging information and in accordance with the IRIS access control policy.

Control of operational software – IRIS Payroll Professional staff must abide by IRIS Group IT policy and procedures and this means no unauthorised software is permitted to be installed. An approved-safe software list is maintained by Group IT and published on Intranet.

Management of technical vulnerabilities – IRIS Group IT and the IRIS Payrite Team ensure that internal systems are regularly patched with operating system and software updates. Annual Penetration testing for integrated cloud service applications is undertaken by a third party and appropriate action taken on the findings within specified maximum timescales. 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 and IRIS Group IT.

Communications security

Network Controls, Security and Network Segregation - IRIS Group IT are responsible for the implementation and management of Firewalls and segregation of network services to ensure the protection of IRIS Payroll Professional's networks and connected services. The IRIS hosted operations team are responsible for ensuring that appropriate security mechanisms and segregation is in place, together with appropriate service levels for cloud hosted services such as My ePay Window.

Electronic messaging – IRIS Payroll Professional staff must comply with the IRIS group IT Acceptable use policy. The IRIS Payroll Professional support team procedures & this security policy mandate that any PII must be sent via encrypted (Egress) email.

Confidentiality or non-disclosure agreements – As required, IRIS Payroll Professional uses NDAs and maintains signed agreements to protect confidentiality.

Agreements on information transfer – IRIS Standard terms of business contain agreements on information transfer between IRIS and the customer and the parties' roles/responsibilities under data protection legislation. Additional data processing agreements with sub-processors are maintained to ensure compliance with regulations.

System acquisition, development and maintenance

IRIS Group IT are responsible for the implementation and management of VPN access, Firewalls and the use of encryption and other security measures to ensure the protection of IRIS Payroll Professional's systems and connected services when new systems are implemented or changed. The IRIS hosted operations team are responsible for ensuring that appropriate security mechanisms and segregation is in place, together with appropriate service levels for cloud hosted services such as My ePay Window.

Security in development and support processes

IRIS Payroll Professional staff specialise in the development and support of software systems for payroll and is privy to confidential information, not least to personal data which is subject to the General Data Protection Regulation we ensure that our software and services are designed with robust information security at their core. This includes coding for security for both desktop and cloud services and in particular with reference to OWASP security guidelines.

The IRIS My ePay Window cloud service is subject to annual 3rd party security penetration testing and weekly vulnerability scanning to ensure it remains secure and we act on the findings within pre-determined time-scales to remediate any issues.

All IRIS Payroll Professional developed software must incorporate appropriate controls and audit trails or activity logs, and validation of input data, internal processing and output data.

All source code for Iris Payroll Professional products must be treated as highly confidential and all personnel with authorised access must strictly adhere to the use of the appropriate IRIS development tooling for the purposes of checking code in and out. The Development managers are responsible for controlling access to the respective department's development and support environments.

All versions due for release to any client must have prior undergone IRIS Payroll Professional's QA and release management process to ensure that changes to issued software are controlled, have been thoroughly tested and are to a high quality.

Test data is based on sample test data as a rule. Occasionally, production derived data may be used but its use is carefully protected and controlled and any such data is destroyed once testing is completed.

Clients must always be advised to maintain suitable facilities for testing and training purposes separately from their live environment. System changes must be reviewed and tested as agreed between IRIS Payroll Professional and Client.

IRIS Payroll Professional's servers and all other equipment containing confidential information, personal data or source code must be ring fenced. All source code must be stored in central repositories to which physical and logical access is closely monitored. All desktops and laptops, whether static or mobile, shall be fully encrypted using BitLocker and only authorised encrypted media handling devices can be used.

External Supplier relationships which are data processors

As part of IRIS Software Group, IRIS Payroll Professional abides by the group supplier data protection assessment policy. This policy ensures that suppliers who may have access to customer data are properly & regularly assessed, published to those customers whose data may be involved and engaged under a data protection compliant contract.

On occasion, IRIS may use engineers and third parties located in India for production environment support, deployment activities, access management and security and vulnerability management. In all these instances, information is held on secured network drives held in the UK and only accessible by those authorised to process it. All relevant security requirements have been addressed and further information is available on request. A full risk assessment is carried out annually to ensure that client data is always protected.

SUPPLEMENTARY MEASURES FOR PERSONAL DATA PROCESSED IN INDIA

IRIS and its engineers in India adhere to the standards of ISO 27001 and uses privileged access management controls to audit activity of engineers. VPNs and Bastions are used where appropriate and all communications are over encrypted channels. IRIS has an international data transfer agreement in place with all sub-processors used that are based in India. This requires them to comply with IRIS data protection and security policies and standards, particularly in relation to handling requests from official sources.

External Data Processors	Data Location	Description
Rackspace Ltd	UK	Hosting services for the IRIS My ePay Window service
Microsoft Azure Hosting	UK	IRIS EVC Connector service, to allow employee earning verification via Experian work report
Sales Cloud via Salesforce	UK	Our support function uses Sales Cloud to provide customer ticketing, communication, live chat and query resolution management.
Mailgun (Sinch)	US	Mailgun is used by IRIS My ePay Window for system generated email delivery. This process is covered by the EU Standard contract clauses for data transfers to third countries.
Brevo	EEA	Brevo is used by IRIS My ePay Window for system generated email delivery (No Payroll data is transmitted in email content or attachment). Brevo will fully replace Mailgun as it is progressively retired.

Information security incident management

The IRIS Payroll Professional support team have documented procedures in place to handle information security support cases:

Personal data incidents are investigated by the IRIS Payroll Professional Support & Development Information Asset Managers and in accordance with the IRIS group Incident Reporting and investigation procedure. The investigation will involve and be validated by the Group Data Protection Officer who will inform and advise the IRIS Payroll Professional Information asset Owner regarding communication to the affected Client or Clients directly without any undue delay and also will inform the Information Commissioner's Office as appropriate.

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.

Where continuity of Support Services may be at risk, all primary contacts at the affected Clients will be alerted by email together with all relevant information including contact details for emergency relief whilst normal Support Services are in process of being resumed.

Business continuity – Information security aspects

IRIS Payroll Professional, as per the Group IRIS Business Continuity management system has a Business continuity plan(BCP). The BCP is designed to ensure timely recovery of support Services to clients as well as all other internal operational systems and is reviewed on at least an annual basis.

Our Business Continuity plans must facilitate recovery of Development and Support Services of any IRIS Payroll Professional product as quickly as practicable but, in any event, within 24 hours. IPP's full business operations must be recovered within 7 days.

In the event of service failure, the Information Asset owner or Information asset managers shall be responsible for invoking the IRIS Critical Incident reporting process and this may invoke the Payroll Professional's Business Continuity Plan with the support and assistance of all relevant department heads involved.

The backup of all processing server systems falls under the remit of IRIS Group IT, utilising nightly disk backup. These nightly backups are securely transmitted to UK based cloud backup. Backups must be subject to verification testing by the Group IT team at least annually and duly documented as such together with details of any issues arising.

My ePay Window Service - business continuity procedures include daily incremental and full weekly backups(weekly backups are retained offsite for 4 weeks) and separate physical servers using virtual server technology with failover in the event of an individual virtual machine or hardware failure (through virtual machine Clustering and SAN technology) IRIS service level agreement terms provided by Rackspace Limited, provides 100% availability of the network and repair of any problem hardware component within one hour of identification, additional time may be required to rebuild a RAID array or to reload operating systems and or applications.

Compliance and Information Security reviews

Compliance with legal and contractual requirements

As a developer and implementer of Software and provider of Support Services and, as part the IRIS software group, IRIS Payroll Professional will have access to personal data and or other confidential information. This may be held on Clients' systems or on media transmitted or otherwise made available to IRIS Payroll Professional from time to time.

IRIS Payroll Professional and IRIS Group complies with industry, legal and contract requirements and maintains and protects information records compliant with Companies House, HMRC and IRIS group document retention policy.

Personal data is at the heart of the General Data Protection Regulation ("GDPR").

Article 5 of the GDPR sets out six key principles. These specify that personal data must be:

1 Processed lawfully, fairly and transparently in relation to the data subjects.
2 Obtained for specified and lawful purposes.
3 Adequate, relevant and not excessive.
4 Accurate and up to date.
5 Not kept any longer than necessary.
6 Processed securely, with integrity and confidentiality.

Principles 2, 5 and 6 especially apply in respect of IRIS Payroll Professional's access to personal data which shall be for the sole purposes of implementation, support and maintenance of Software supplied to Clients ("IRIS Payroll Professional's Services").

Where IRIS Payroll Professional is in possession of information about, held by or belonging to a Client that is by its nature confidential, or is designated as such by the Client (whether in writing or orally), IRIS Payroll Professional is obliged to (i) keep it confidential; (ii) use it only in connection with IRIS Payroll Professional's Services; and (iii) not disclose it to any other person without the Client's prior written consent.

IRIS Payroll Professional warrants to its clients that their use of IRIS Payroll Professional's software will not infringe any copyright, patent or trademark right, or any other proprietary right, or constitute a misappropriation of any trade secret, of any third party. IRIS Payroll Professional also warrants that its software will be free of any harmful code.

Encryption is used to ensure security of PII in all public data transmissions (TLS 1.2 protocol). Encrypted file and email services are used (Egress & SFTP), https plus VPN for access to networks is enforced. Cryptographic keys are maintained securely throughout the lifecycle in accordance with the IRIS encryption policy.

Information security reviews

ISO27001 certification is audited annually by an external assessor. Internal compliance with Group ISMS is also annually reviewed by the Group Compliance team. Annual external 3rd Party Penetration testing is carried out for cloud services with weekly vulnerability scanning.

Data Protection – quick reference

IRIS Group Data Protection Officer – *Vincenzo Ardilio* - dataprotection@iris.co.uk

Data protection owner for IRIS Payroll Professional – *Nigel Francis*

Categories of personal data processed as part of the IRIS Payroll Professional service provision relate to Personal Data related to Payroll Processing (please note that no special categories of personal data are processed by IRIS Payroll Professional)

Location of personal data processing

Personal data is processed in Payroll data files and these may be held by clients by virtue of their use of IRIS Payroll Professional in a number of locations depending upon the client's preference: either the client's own network Infrastructure or on IRIS UK hosted infrastructure or on another 3rd party hosting provider's infrastructure. Additionally, payslip and payroll data is shared from these locations to client employees and users via the IRIS My ePay Window cloud service hosted in the UK at Rackspace Ltd.

Retention of data

IRIS Payroll Professional desktop Software:

The IRIS Payroll Professional payroll data files retain payroll data for 6 years plus the current tax-year and data older than this is auto-deleted each year through the Year End process.

The IRIS My ePay Window cloud service retains data as follows:

- Payslips,P60s, P11Ds, P45s, CIS statements are retained for at least 12 months and for the duration of processing of the client's data on My ePay Window
- Auto enrolment letters are retained for 12 months after which they are auto-deleted
- Any documents uploaded to My ePay Window will be available for at least 3 months and the Website will warn you in advance of any deletions so that you can download information in advance.
- If an Employee leaves an Employer their data and access to it will be maintained for 15 months, during which information can be downloaded as required. After 15 months their account will be disabled and after a further 1 month their data will be anonymised.
- Client's who have not accessed or uploaded new data in the preceding 12 months will be deemed to be no longer using the IRIS My ePay Window service and will have their accounts blocked and their data will be anonymised after a further 3 months.
- We may use aggregated information for the purposes of monitoring use of the Website. Such aggregated information may be provided to third parties. These statistics will not include information which can be used to identify any individual, Client Company or client entity or the nature of its employment or business.
- For the avoidance of doubt, we shall not use any personal data held on the Website for any marketing purposes.

IRIS EVC Connector used with IRIS payroll Professional retains data as follows: (See EVC details here)

- For the contracted or agreed duration of processing using IRIS software, employee pay details are uploaded per period to IRIS's MS Azure EVC connector environment sufficient to support income verification for between 3 to 12 months prior employment. Data is auto-deleted after a rolling 15 months.
- If an Employee leaves their employer, their data will be auto-deleted after 15 months.
- Each Employer's opt-in/out status is retained on IRIS's EVC connector so that Employees of participating employers can be processed accordingly or informed to verify their income by other means.

- Data is permanently erased from IRIS's EVC connector when Employees or Employers opt out the service from IRIS Payroll Professional

Data subject rights

IRIS Payroll Professional processes personal data lawfully and for the purposes of payroll processing and to allow our clients to provide various payroll statements relating to their employees according to UK employment legislation.

All users of IRIS My ePay Window, must consent to their information being available on the service as part of the site registration process and with sight of the My ePay Window service privacy policy. Any users declining consent are referred to their 'Employers' and their account registration is stopped.

The IRIS Payroll Professional support team can be contacted regarding data subject information requests.

Available Appendices

IRIS Payroll Professional's My ePay Window Service description - Available from customer support site
Other IRIS Group policies – Available on Request