IRIS Cascade

Information Security Assurance Statement of Cascade HRi

Document control
Version number: 1.1
Owner: Chris Kerridge – Senior Manager, Product Management
Date of last update: 12/08/2024
Document type: Assurance Statement
Replaces: N/A
Approved by: Julian Musson – Senior Product Director
Approval date: 21/05/2024
Data protection impact screening: N/A
Date of next formal review: 20/12/2024

Contents

Information security assurance statement

Objective of this document

The purpose of this information security assurance statement is to provide customers of IRIS Cascade with transparency as to the security and personal data compliance of this product 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 Cascade as a thoroughly secure software and service provider.

Description of the data processing carried out by IRIS Cascade

IRIS Cascade is a Human Resources Information System which allows companies to manage people and organisational data. Personal details of employees are held so that the company can manage HR and Talent processes and in many cases, Cascade acts as the system of record for starters, leavers and changes through an employee's career, as well as holding salary data to ensure they are correctly and accurately paid.

The objective of the software is to:

- Support Compliance: Keep your business ahead of regulatory change with a comprehensive solution that mitigates any risks.
- Drive Productivity: Automate both mundane and complex operational tasks, whilst also providing new data and insights to drive business success, saving you time and money.
- Improve Engagement: Build a culture of employee engagement by providing a user-friendly experience that unifies services and software and eliminates duplication

The IRIS Cascade Payroll solution provides various types of payroll related services such as employee record maintenance, payroll calculations, HMRC reporting, BACS processing to employees and 3rd parties, payslip distribution and payroll queries.

Statement of assurance

IRIS Cascade 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 Cascade Organisational Security

IRIS Cascade 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 Privacy, Security and Compliance Steering Group*. This group 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
- IRIS Group Compliance Manager
- Other key security leads within the company

The Privacy, Security and Compliance Steering Group 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 Cascade HRi

At IRIS Cascade, 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 Cascade to ensure IRIS Cascade 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 Cascade, the team with responsibility for ensuring your data remains secure and in compliance with IRIS Group Policies and ISMS are:

Employee Name	Department	Designation
Julian Musson	Product	Senior Director, Product
Chris Kerridge	Product	Senior Manager, Product Management
Mohammad Othman	Engineering	Director, Engineering
Tim Johnstone	DevOps	Director, DevOps Engineering
Thomas Derbyshire	Customer Service/Support	Senior Manager, Customer Services
Yellie P Williams	Professional Services	Professional Services Director
Tarka Duhalde	Finance and Accounts	VP, Financial Controller
Rob Brough	Sales Order Processing	Director, Revenue Operations
Vincenzo Ardilio	Central Compliance	Data Protection Officer – Group

The IRIS Cascade 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 Cascade.

Measures are "appropriate" if they have been identified through risk assessment.
Date of last IRIS Cascade risk assessment review: October 2023

The IRIS Cascade 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 Cascade 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 are responsible for the operation and integrity of IRIS Cascade's IT systems and for keeping systems reasonably up to date.

IRIS Cascade's Development systems are managed by local development team and Cybage.

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

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

Human resource security for Cascade HRi

IRIS Cascade staff will have access to your [customer's] 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 Cascade 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 KnowBe4 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 Cascade places the onus on the employee for their adherence to security protocols and a disciplinary procedure is enforced for non-compliance. 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
IRIS Cascade 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 access).

Upon instruction from HR of a person leaving IRIS Cascade, 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 Cascade Access Control

Question	Answer
Is there a documented procedure to revoke leaver access to data, physical access to premises and information systems	Yes
Is there a documented procedure to recover all computer equipment, access tokens, key etc prior to an employee leaving?	Yes
Upon termination, is there a documented procedure to for the immediate revoking of physical access to premises and the logical access to computer systems?	Yes
Are privileged user accounts only used for performing specific functions that require administrator or other privileged access, and are not used day to day work?	Yes
Are your password settings configured to ensure that passwords meet a minimum length of 8 characters, are complex*, and are required to be changed at least every 90 days? *Complex passwords must contain characters from three of the following five categories: • Uppercase characters (A through Z) • Lowercase characters (a through z • Base 10 digits (0 through 9) • Non-alphanumeric characters: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/ • Any Unicode character that is categorised as an alphabetic character but is not uppercase or lowercase. This can include Unicode characters from Asian languages	Customers are in control of their password policies, which can be configured within the application. Customers can control password complexity and history. Note that this applies only to users logging in against simple username/password combinations in IRIS Cascade – customers may choose to instead/also authenticate their users against an external provider such as ADFS or Azure AD. In this instance, password policies are the responsibility of the customer's external provider.
What technical measures are implemented in relation to passwords being stored in the database?	Passwords in the Cascade database are salted and hashed, with a unique salt per user.
Can Azure authentication but used in scenarios where users share terminals?	Azure authentication (and any other external providers) can be used for shared devices, however users must sign out of Azure before leaving their machine for others to access.
Can you use Cascade Modern Authentication with 3rd party authentication libraries?	Modern Authentication was designed to work with 3rd Party authentication providers - It is designed to work with OIDC/OAuth 2.0 only - SAML is not supported. You must remember that when signing in and out of Cascade, you must

	also sign in and out of your chosen 3rd party authentication provider.
Are shared (generic) accounts used for any privileged / sensitive access or functions?	No
How is data separation managed between your different customers?	IRIS Cascade is a multi tenanted SaaS with customers databases separated logically. User cannot access any database other than their own.

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

Processing data

Question	Answer
Who do you hold personal data about as part of the services you provide to us? e.g. employees, customers	Employee personal data is held regarding your employees, dependent upon the modules you have purchased
For what purposes do you use the personal data?	As processor, to provide the contracted services i.e. an HR and Payroll System
Which of your departments have access to the personal data?	Only the necessary departments at IRIS can access the cloud services' data including Support, Development/QA and Admin. We do have a role-based access policy in place for these departments
What data processing activities do you undertake on our behalf (e.g. collection, recording, organisation, storage, use, disclosure, transmission, or dissemination of data)?	IRIS Cascade allows the employee to view their own personal HR records Your internal HR Team can send communication directly to the employee via email; this may contain personal data All communication between client browsers and IRIS Cascade is protected by TLS 1.2 encryption IRIS Cascade uses UK data centres exclusively for storing data, currently provided by Rackspace You and each individual employee can access that individual's personal data

Where is the personal data collected from? e.g. direct from data subject, from us (customer), passed by a third party. If the latter, please state which third party(ies)	The data is entered directly into the system by your employees. No data is passed to a third party unless you have enabled third-party API links. You would be in control of this process
How do you collect/receive the personal data? e.g. application form, secure online portal, password protected attachment via email	Personal data can be entered into the system via: • Employee self-service • You control who has access to the system to view and enter personal data • You control what fields are visible in the system for each employee level • Data can be imported into the system – this is done on your instruction
What procedures do you apply to ensure personal data is accurate and kept up to date?	The responsibility for collecting information lies with the person processing the data in the software. Customers should ensure they have adequate standard operating procedures to ensure the accuracy of data entered into the system
Do you automatically profile individuals? If yes, do you make decisions solely based on such automated processing, including profiling?	No
What procedures do you apply to ensure that no more than the personal data required is collected?	The responsibility for collecting information lies with the person processing the data in the software. Customers should ensure they have standard operating procedures in place to ensure data minimisation
What processes do you have in place to prevent the ex-filtration of sensitive data?	All actions in IRIS Cascade are bound by role based access control (RBAC) and profiles, which are fully configured by the customer's admins to control who sees what, and what they can do, down to the field level.

Encryption (cryptology)

Question	Answer
Do you have adequate physical security procedures and measures in place to protect personal data?	Yes, IRIS Cascade is BS EN ISO/IEC 27001:2013 compliant
Do any staff who do not need access to any personal data have access to it? Consider both physically and via a computer network	No
Do you use encryption to protect personal data?	Data is encrypted at rest using the storage device to encrypt the data as it's written to disk.

	Encryption is AES-256 and the encryption keys are managed by Rackspace but are unique to IRIS Cascade's dedicated platform.
Are all mobiles phones, laptops and tablets which contain personal data tracked in an asset register, pin or password protected, encrypted and remotely wipeable?	No customer data is stored on staff equipment. Our Group IT look after IRIS's asset register. Devices issued to staff by IRIS Group IT will be included in that register
How is removable storage media recorded and managed to ensure security?	Use of removable storage is minimal; no customer data may be downloaded from production environments
What protections are there against unauthorised copying, processing etc?	Password security is in place for user access, encryption for data in transit, limited IRIS employee access only given to those employees that are necessary. All datacentre environments are isolated from corporate ones – access is via an VPN with two-factor authentication. Backup procedures by Azure and Rackspace are also in place.
What protections are there against accidental loss, damage or destruction?	We work with the principle of least privilege – developers and administrators are not allowed to work directly with live customer data, data is geo-replicated where possible.
Do you have robust frequent data backup procedures?	Data is fully backed up offsite weekly, with differentials happening every few hours and transaction logs every 30 minutes. The internal Recovery Point Objective (RPO) is 4 hours. The target Recovery Time Objective (RTO) is 72 hours
How are Back-up failures identified?	RackSpace Managed Backup produces a report that we can query and see when there's been a failure. Also, RackSpace generate a ticket when MBU fails.
How are Back up failures remediated?	At IRIS we review the MBU output every morning and follow up with any backup failure to understand why it might have failed, and also to decide whether it is appropriate to trigger an immediate further attempt at a backup, or whether it is more appropriate to ensure the subsequent backup definitely succeeds. All effort is focused on ensuring there are no sequential backup failures for the same device.
What additional identification and security measures apply to any sensitive or special category data (if applicable)?	Not Applicable.

Operations security

Question	Answer
Is there a formally documented change management procedure in place that requires	Yes. Changes are documented.

that all changes to applications, systems, databases and all network components are documented and require management approval?	Software changes require approval from a Change Advisory Board Technical Development requires approval from the Architectural Review Board
Is there a process in place to ensure that only secure and approved hardware and software is procured for use in providing services within your organisation?	Rackspace provide the hardware used in the IRIS Cascade service
Are all systems required to have active anti-malware installed and running?	Yes
Are anti-malware signature updates deployed across the production environment, including servers, email servers and end users' devices, within 24 hours of updates being made available?	The production environment anti-malware is a managed service provided by eSentire Rackspace. Updates are deployed when available
Is there an internal vulnerability scanning process this is performed on at least a quarterly basis?	Vulnerability scanning for IRIS Cascade is performed on a regular basis and when significant platform/software changes are made
Are findings from vulnerability scans tracked, and are rescans performed until no findings are identified?	Yes
Is there patch management process in place to ensure that all systems are kept up to date with the latest patch levels?	Patching is managed by IRIS on a schedule multiple times weekly
Is there a process to ensure that critical security patches for hardware and software are implemented within 30 days of patch release?	Yes. Patching matches the IRIS Group Policies
Are penetration tests of critical applications or networks with Internet connectivity performed at least every 12 months and after significant changes?	Yes. We pen test the applications. Infrastructure is tested as part of those pen tests. External penetration tests are conducted annually by an independent penetration tester. Internal penetration tests are also conducted.
Is customer data physically and logically separated from data of other clients?	Customer data is stored in separate databases.

Communications security

Question	Answer
Is there a process or a system in place to ensure that all systems and networks used to deliver services to Client configured in a consistent and secure manner, with approved security settings applied?	Yes, systems use hardened images and configurations. Configuration management is used to ensure consistency
Are the computer systems and networks that will be used to provide services to Client configured	Yes. All systems are at least N+1

to prevent single points of failure, in order to provide business as usual services in the event of a systems failure?	
Are the computer systems and networks that will be used to provide services to Client monitored in real time, or have alerting that is responded to in a timely manner?	Yes
Are network intruder detection systems (NIDS) or network intruder prevention systems (NIPS) installed and configured to monitor all external perimeter network connections?	Yes, an IDS is in place to detect suspected activity
Is there technology in place to encrypt, point to point, all customer data that travels over public networks, including email, instant messaging and voice over IP (VoIP), using an industry standard encryption algorithm?	Data encryption in transit uses certificates. Data is also encrypted at rest
If wireless networks are used, are technical controls in place to protect connections to it using WPA2/PSK at a minimum?	No wi-fi networks exist on the production systems
Are controls in place to segregate guest wireless networks from the corporate network?	Yes

System acquisition, development and maintenance

Question	Answer
Are controls in place to prohibit the use of customer live data within the development and testing environments?	Yes
Does the system development lifecycle (SDLC) include information security requirements to support development of secure systems?	Yes – security is considered during Architecture Review Board (ARB) stage for major projects; all code changes are subject to automated analysis against the OWASP top 10 and SANS top 25 lists. In addition, the codebase is scanned at least once a week by an automated vulnerability scan tool. Any issues found during any of these stages are fixed straight away, before release. The SDLC emphasises shifting security testing left so that the master branch remains secure, stable and releasable
Are Penetration tests conducted? How often are they conducted?	Yes – at least annually
Does the change management process require the security team to authentication, authorisation, and access control mechanisms?	Yes

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.

Processing locations and international data transfers

On occasion, IRIS may use engineers and third parties located in India for production environment support, deployment activities, access management and security & 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.

Supplier relationships

Question	Answer
Do you have a complete list of data processors used by your organisation in respect of the personal data you process or control as part of the services you provide to us? If so, please provide a copy.	Hosting: Rackspace (UK) Emails SendGrid (Emails) Amazon SES (Emails) IRIS Cascade's production hosting environment is supported with a team that includes engineers from Cybage. IRIS Cascade's Development systems are managed by local development team and Cybage
How do you audit your data processors' compliance with Data protection law?	We request security guarantees in line with Article 28 Of the General Data Protection Regulation (GDPR); there are Corporate procedures in place in relation to this.
Do you have a standard data processor agreement for use with third parties?	Yes

Does the client have any control over the use of the third parties listed?	Rackspace is essential to the successful use of IRIS Cascade and cannot be controlled on a customer by customer basis. SendGrid is the default email service for IRIS Cascade however Cascade customers can opt for a UK-pinned service via Amazon SES which IRIS Cascade will configure for the customer. Alternatively Cascade can be configured to route emails via the customer's email relay of choice including their own email server.
What is SendGrid and what does SendGrid do with our data?	SendGrid is a US provider of cloud-based transactional and marketing email delivery, management and analytics services. These services will consist primarily of sending and delivering e-mail communications on behalf of customers to their recipients. The personal data transferred concern anyone who is a sender, recipient or copy recipient of an email which the Customer instructs SendGrid to deliver and manage. Data subjects may also include individuals who are mentioned within the body of emails sent by the Customer using SendGrid's services. The categories of personal data transferred: Sender, recipient and copy recipient identification information (first and last name), contact information (address, telephone number (fixed and mobile), e-mail address, fax number), employment information (job title); and Any other personal data that the Customer chooses to include within the body of an e-mail that it sends using SendGrid's services. The personal data transferred to SendGrid for processing is determined and controlled by the Customer in its sole discretion. As such, SendGrid has no control over the volume and sensitivity of personal data processed through its service by the Customer.
Where is our data held?	Rackspace data centre.
What and where is Rackspace?	Rackspace is a UK data centre based in London.

	We use 2 different Rackspace centres: London LON3 London LON5

Information security incident management

Question	Answer
Who is responsible for data protection compliance in your organisation?	All IRIS staff are responsible for compliance with data protection in line with IRIS policies and procedures. The Chief Information Officer (CIO) has ultimate responsibility for enforcement of policies and procedures and is supported by the governance structure described in Appendix 1 of the Group Data Protection Policy.
What processes do you have in place to ensure identification of and prompt reporting of data breaches to us and (if appropriate) the Information Commissioner's Office?	IRIS Software Group has an overarching critical incident process. The IRIS Personal Data Incident Reporting Procedure falls under that process to ensure any incident is promptly reported to the Group Data Protection Officer and assessed in line with the regulatory guidelines on Breach Reporting under current data protection laws. The IRIS Cascade Product Manager is responsible for ensuring that all staff involved in providing the IRIS Cascade service have the means to escalate incidents in line with the above corporate procedures. As your Data Processor, IRIS Cascade will not report personal data breaches to a regulator on your behalf. However, IRIS Cascade will report incidents to you without undue delay so that you can report the matter to the ICO if you believe it is necessary to do so.
Who is responsible for dealing with the response to data breaches in your organisation?	Group Data Protection Officer in consultation with the CIO.
To the extent not already set out above, what action have you taken to ensure compliance with data protection laws?	IRIS has an Information Security and Governance Group, which includes members of the Executive Committee. The IRIS Cascade Management Review Group leads on IRIS Cascade.

	IRIS Cascade has carried out a gap analysis and risk assessment in line with current data protection regulations
Do all staff receive data protection training? Please provide details.	IRIS use KnowBe4 compliance to hold all Policies and procedures in relation to data protection. The compliance software tracks, records and enforces employees to: Read company policies Conduct assessments to record understanding Conduct e-learning activities in relation to data security, information security and managing incidents The group also provides onsite training to key areas to support this knowledge and understanding of the subject matter: Training Confidentiality Training - Annually GDPR Training - Annually

Business continuity – Information security aspects

Question	Answer
Do you have a Business Continuity Plan?	Yes
Does the plan include Business and technical Recovery, so that services can be resumed to clients, within acceptable timescales?	Yes
How often is the BCP tested?	We test our Business Continuity planning yearly
Are you certified to any recognised Business Continuity Standard for the full range of products and services you provide to Client	ISO Compliant
Do you have a clearly defined Incident Response Structure which ensure incidents are identified, escalated and effectively managed?	Yes

Data Protection Systems

Question	Answer
Is your company compliant with the notification requirements of the Data Protection Act 2018 or equivalent legislation?	Yes
In the last 2 years, has your company been the subject of any data protection information notices, enforcement notices, decision notices, undertakings, or any equivalent regulatory notices/actions again? If yes, attach a copy of the document and explain what you have done to ensure that the situation does not occur again.	No
Does your organisation conduct regular compliance audits to ensure that data protection policy is compliant with relevant laws and regulations?	Yes, annual audits take place

Policies

Question	Answer
Is there a Data Protection Policy applicable to all staff who process data for us? If yes, please provide a copy.	IRIS has a Group Data Protection Policy. Staff who may have access to your data – for example in relation to Support or Professional Services are required to operate to standard operating procedures
Do you have an up-to-date internal data breach register	Yes. This is managed by the IRIS Group Data Protection Officer
Do you have a Data Retention/Archive Policy? How long do you store data in relation to the service you provide to us and what criteria are applied to determine how long data is retained?	In the context of our function as a data processor, we are required to keep customer data for the retention period agreed in the contract, which represents the customer's instructions to us. However, after the end of the provision of services relating to processing we must, at the choice of the customer, delete or return all the personal data to the customer and delete existing copies. It is up to the customer to ensure they instruct IRIS during any notice period of the end of the contract
Do you have an internal data breach register or central record of processing activities?	es, this is reviewed annually or if a breach occurs, a review takes place of the issue and how to prevent it from occurring again

Consent and rights of individuals

Question	Answer
On what basis is consent obtained by your organisation (if at all) to process an individual's personal data, i.e. for which categories of data do you rely upon the consent of the data subject?	This is only relevant to data controllers. In the context of our processor activity this would be the customer's responsibility.

If consent is obtained, is the consent written? If not, how will it be demonstrated that consent has been given?	As above
Are there processes in place to allow an individual to withdraw their consent? If so, how can they do this and is it as easy as their initial giving of consent?	As above
If no consent is required or obtained, which grounds for processing will be relied on?	As above
Do you have a clear and known process to deal with Subject Access Requests?	As above
What is the process for you to respond to requests to rectify inaccurate personal data about an individual?	As above
What is the process for you to respond to a request under the right to be forgotten?	As above
Is personal data processed or accessed outside the European Economic Area (EEA)? If so, what measures are in place for such transfers e.g. binding corporate rules, adequacy decision or appropriate safeguards including data processor contracts?	Where SendGrid is used: IRIS Cascade uses SendGrid for the sending of system generated emails. To enable this process, email header information is transferred to the USA. Email header information may contain limited personal data (employee name/email address). This process is covered by the EU Standard contract clause for data transfers to third countries. For the purposes of Schrems II: no additional safeguards are deemed necessary as the data transferred is only email header and not the email content
Do you have a Privacy Policy/Fair Processing Notice?	It is the Controller's (customer's) responsibility to provide data subjects with a privacy/fair processing explanation
How are individuals whose personal data you process made aware of the Privacy Policy/Fair Processing Notice?	It is the Controller's (customer's) responsibility to provide data subjects with this information.

Scalability

Question	Answer

Please provide an overview of your platform in terms of the tech stack, key architectural components and the dependant third party services	The tech stack at the time of writing uses Windows Server 2019 and 2022 with IIS and SQL Server 2019 as the base layer, although software versions are subject to change for patch management and operational requirements. Software is mostly written in ASP.NET, and at the time of writing is running against version 6 of the runtime. Some components remain in classic ASP, and newer components are written in Angular 8. The application is split between the distributed, multi-tenant web tier, with data housed in single-tenant databases distributed across our SQL clusters. Back-office or asynchronous services are provided by dedicated services running on headless servers. Inter-process messaging is currently handled by RabbitMQ, with caching performed using Redis. All components are installed on servers within our Rackspace network, and no external communication is required
How does your platform scale to accommodate spikes in traffic? (specify the level that can be accommodated)	The system is built to handle peak traffic. Some scaling is in place for busy periods
Please provide an overview of the monitoring solution that you have in place for the platform?	Various monitoring systems are in place, from infrastructure monitoring, APM, logs and alerting systems
Has the platform been load tested? If so, at what levels?	No
Are there any known bottlenecks (with respect to platform performance and stability) in the platform?	The system is known to be slower when employee numbers go above 14,000 – we are working to improve this, but at the time of writing this is the only known performance bottleneck
What dependencies does the platform have on licensed third-party components?	At the time of writing – Aspose Words, Aspose Cells, DevExpress, FusionCharts, Voiceflow (AI Bot)
What process is in place to ensure that all dependant third party components are upgraded when and as required particularly with respect to security patches?	Third party components are integrated using the .NET package manager, NuGet. New versions are apparent here, and development teams review every release for new versions
What level of availability has been achieved by the platform in the last 6 months?	Latest availability stats can be provided on request, typically availability if 99.9% or above over a given period.
Are there any specific areas of the platform that have not achieved the overall level of availability within the last 6 months?	No

What internal alerting and escalation process is in place within the organisation to ensure that action is taken when part of, or the entire system becomes unavailable?	The alerting and monitoring processes are managed by the Operations team. This is followed up by an incident management process.

Data Protection – quick reference

Contact	Details
IRIS Group Data Protection Officer	Vincenzo Ardilio – dataprotection@IRIS.co.uk
Data protection owner for Cascade HRi	Chris Kerridge – Christopher.kerridge@IRIS.co.uk

Retention of data

The IRIS Cascade platform will retain data indefinitely (or until removed by an admin user) and will delete it in accordance of IRIS Cascade terms & conditions, with appropriate notifications prior to deletion.

"**What happens to data when a customer terminates their contract?**

Terminated customers have 30 days to extract or request a copy of their data from the Cascade system. The 30 day window begins on the date the contract has terminated and/or service provision has ended. After 30 days IRIS will permanently delete the data."