



IRIS Software Group

Global Privacy & Data Protection Policy

Version	4
Replaces	3
Release Date	15 January 2023
Author	Group Data Protection Officer
Owner	Vincenzo Ardilio
Review Period	12 months
Classification	PROTECTED

BEFORE USING THIS POLICY ALWAYS ENSURE YOU ARE USING THE MOST UP TO DATE VERSION

IRIS. Look forward

Document Control

Version History:

Version	Date	Author	Changes
3	Jul 2022	Vincenzo Ardilio – Group Data Protection Officer	<ol style="list-style-type: none"> 1. International data transfers - off-shoring criteria clarified 2. Supplier annual due diligence refresher added 3. Product annual risk assessment refresher added as PM responsibility 4. Training link to performance clarified 5. Global application rather than just UK

Reviewers

Name	Role	Date
Josiah Idowu	Data Protection Adviser	2 Nov 2022
Andrea Powers	Privacy Manager (US & Canada)	2 Nov 2022
Alex Madden	Group IT Security Director	14 Nov 2022
Bryce Tyrer	Group Compliance Manager	14 Nov 2022
Jody Donovan	Compliance Manager	14 Nov 2022

Policy made available to the following for consultation

Role	Date
Group IT Director – Alex Jack	9 Dec 2022
Development Director – Tim Johnstone	9 Dec 2022
VP Data Science – Jer Jang	9 Dec 2022
Senior Director Programmes – Stephen Chambers	9 Dec 2022

Approvers

Name	Role	Organisation	Date Approved	Signature
Alan Hartwell	Chief Technology Officer	IRIS	06 January 2023	DocuSigned by: Alan Hartwell
David Lockie	Chief Operating Officer	IRIS	06 January 2023	DocuSigned by: David Lockie

Distribution:

Name	Role	Organisation	Date
To be published on MetaCompliance			

Contents

Why is this policy needed?	4
Territorial application.....	4
Consequences to IRIS employees and contractors who do not comply with this policy	4
Roles and responsibilities	6
All IRIS employees and contractors in all territories.....	6
Executive Committee collectively and as individual Chief Officers	7
All managers.....	7
Product and service directors	8
Product Development, Engineering, Development Operations and Architecture	9
The Group IT Director.....	9
The Chief People Officer	9
The Data Protection Officer	9
Data protection policy statements	11
1. IRIS will always ensure that it has the processes, procedures and records to demonstrate that personal information is managed following the data protection principles.....	11
2. Rights of individuals	11
3. Transparency to individuals (“data subjects”)	12
4. Supplier (“processors” and “sub-processors”) due diligence	12
5. Transfers of personal data to third countries	12
6. Data Protection Officer	12
7. IRIS commitment to keep records of processing activities.....	13
8. Data mapping and process mapping	13
9. IRIS responsibilities as data processor to customers.....	13
10. Corporate procedures for reporting and investigating personal data breaches.....	13
Appendix 1 – Controls on personal data transferred to third countries for processing	14
Appendix 2 – Data Protection Officer	16
Appendix 3 – Statutory Records of Processing Activities	18
Appendix 4 - IRIS commitments when providing a service to customers, whether through a managed service or online product.....	19
Appendix 5 – IRIS Pre-employment vetting.....	21
General principles of pre-employment vetting	21
Appendix 6 - Data Protection Assessment Process (overview)	22
Appendix 7 - Definitions.....	23

Why is this policy needed?

The responsible and ethical handling of personal information¹ helps to protect the people the information relates to. Good management of personal information also helps to build trust between IRIS and its customers and employees.

On the other hand, negligent or unethical use or handling of personal information can result in unwarranted intrusion and, in more serious cases, distress, threats to personal safety, unfair treatment and financial loss for individuals. The consequences may also damage the IRIS reputation and lead to loss of sales, compensation payments to affected individuals and, in more serious cases, regulatory action including fines of up to many millions of GBP.

IRIS, its employees, contractors, employees of subcontractors and any other individual who has access to any of IRIS information, IRIS infrastructure, IRIS applications or IRIS data have a responsibility to look after our employees', contractors' and our customers' information responsibly and in line with data protection and privacy laws that apply to IRIS as data controller and in whichever territory IRIS processes personal data.

IRIS is committed to fulfilling its obligations under the Data Protection Act 2018, the GDPR (EU and UK versions as applicable) and any applicable privacy legislation in other territories in which IRIS operates, such as North America, Australia and India. IRIS has produced the *Data protection policy statements* in this policy to give more detailed assurance to IRIS customers, contractors and employees.

Territorial application

This policy applies in all territories in which IRIS operates. To ensure consistency for customers and individuals, IRIS will comply with the EU General Data Protection Regulation (EU GDPR) by default in all territories of the IRIS customer base. Where there is a conflict between the EU GDPR and local data protection laws in a particular territory, IRIS will aim to meet the highest regulatory requirement in that territory.

Consequences to IRIS employees and contractors who do not comply with this policy

This policy sets out the standards that all employees and contractors working within the IRIS Software Group must observe in relation to their use and retention of personal information.

Any employee found not to have complied with this mandatory policy (and any associated procedures for data management relevant to their role and responsibilities) may be subject to performance management and in the case of serious or deliberate violations will be subject to the IRIS disciplinary policy.

Contractors with access to IRIS information or systems found not to have complied with this policy may be considered in breach of contract and may have their contracts terminated or access to information or systems removed.

¹ "Personal information" and "personal data" are used interchangeably in this document to mean information about living individuals. A more detailed definition can be found at Appendix 7

IRIS will support the investigation of offences committed by any employee or anyone else such as those set out under S170-173 of the Data Protection Act 2018:

- Unauthorised, unlawful or negligent obtaining or disclosure of personal data¹
- Unauthorised or negligent re-identification of anonymised (“de-identified”) personal data
- Alteration or deletion of personal data following receipt of a subject access request with the purpose of preventing disclosure to the data subject (who would otherwise have been entitled to receive a copy).

Roles and responsibilities

All IRIS employees and contractors in all territories

Must:-

1. complete all mandatory privacy, data protection and security training and accept mandatory policies relevant to IRIS and to their role. This must be completed within the time frame specified on the notification issued from the learning management system. For employees eligible for the IRIS Bonus Plan or PS/CS Commission scheme, the terms and conditions of these plans (found within the documents sections of Cascade) confirm that all mandatory MyCompliance training and policies must be fully complete within 30 days of the training/policy launch and as at the end of 30th April each year to receive any annual bonus payout in the financial year. Failure to complete mandatory training by specified deadlines may impact eligibility for promotion and ultimately may lead to disciplinary procedures. Contractors risk termination of their contract.
2. Notify the following to the Group Data Protection Officer without delay:
 - 2..1. any incident that has occurred leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data;
 - 2..2. contact from an official data protection regulator in any territory
 - 2..3. non-routine requests to IRIS from any government, public authority or any other third party for the disclosure of personal data².
 - 2..4. subject access requests
 - 2..5. any other expression of rights provided by GDPR such as requests for restriction of processing, erasure, objections, data portability, profiling.
3. routinely assess whether they use or have access to any personal information when performing their job function for IRIS;
4. accept that they are responsible for the security of the personal information they use and have access to;
5. ensure that the Group Data Protection Officer, or their delegate is involved, properly and in a timely manner, in all issues that relate to the protection of personal information including but not limited to:
 - 5..1. new or changed processes or projects that impact or affect personal data
 - 5..2. new or changed vendors who may have access to or process personal data

² Under no circumstances should any disclosure be made without the approval of the Group Data Protection Officer and, where appropriate, the customer. In all territories the test for appropriate disclosures will be based on EU and UK human rights and privacy regulations.

- 5..3. new or changed assets including software applications that process or impact personal data
- 5..4. any incidents implicating or impacting personal data
- 6. follow the standard operating procedures provided to them by their manager, which sets out what steps they must routinely take in order to protect privacy and security of the systems, products and information they have access to. If their manager has not provided procedures, they should ask. In the event of a personal data breach, ignorance is not a defence;
- 7. report information security risks, incidents and “near misses” (including concerns raised by customers) to the Group Data Protection Officer via Teams or direct call, straight away;
- 8. report all requests received for personal information or for the exercise of data protection rights to the Group Data Protection Officer without delay;

Executive Committee collectively and as individual Chief Officers

Must:-

- 9. lead and foster a culture that values, protects and uses personal data ethically;
- 10. bear data controller and data processor responsibility for IRIS compliance with data protection and privacy law;
- 11. ensure the functions they are responsible for comply with this policy, related security policies and any supporting procedures;

All managers

Must:-

- 12. understand that they are responsible for the use of personal information by teams, contractors and individual employees who report to them;
- 13. identify and assess business processes they are responsible for (which involve or affect personal information) to ensure they meet the requirements of this policy (see Appendix 6). This assessment includes due diligence reviews of any vendors and assets involved in the processing activity;
- 14. understand that they are accountable for the data protection compliance of any project, proposal, process or solution they manage that will involve the processing, accessing or retention of personal data or has potential to affect the privacy of any individuals;
- 15. document the standard operating procedures that their teams (and users of systems they are responsible for) are expected to follow and provide targeted training in relation to those procedures so that their teams and users can perform their functions securely and in line with the data protection policy statements set out below;

16. understand that they are accountable in the event of a personal data breach triggered by the action of any employee they manage or the user of any system that they manage; that the absence of standard operating procedures or adequate training will be considered as the manager's performance issue – this is especially the case if the Group Data Protection Officer or any regulator considers that the provision of standard operating procedures or targeted training could have prevented or mitigated the breach;
17. be able to demonstrate that they meet the requirements of this policy;
18. ensure temporary employees and contractors who require access to personal data (or require elevated IT or system permissions) are vetted and trained to at least the same requirements as for a permanent member of staff and have accepted any relevant mandatory policies such as this one;
19. provide the product or service manager and, when requested, the Group Data Protection Officer with evidence of compliance with Appendix 4 of this policy (specifically in relation to product or service support, professional services and development).

Product and service directors

Must:-

20. register each product or service they are responsible for with the Group Data Protection Officer
21. must ensure any sub-processors that form part of the product or service supply chain have been subject to data protection and security due diligence before entering into any agreement and then at least annually after that
22. co-ordinate the assessment of each product or service they are responsible for, at least annually, in consultation with the Group Data Protection Officer and any relevant stakeholders such as Engineering, DevOps, Customer Services, Professional Services, Compliance and Group IT
23. provide evidence of their products' or services' compliance with Appendix 4 of this policy, when requested, to:
 - 23..1. Customers (via the relevant Account Manager as appropriate)
 - 23..2. The Group Data Protection Officer
 - 23..3. Senior Managers
 - 23..4. Other product and service stakeholders
24. evidence referred to in (22) above includes the completion of the Customer Security Assurance Statement in line with the template authorised for use with IRIS products and services
25. coordinate the response to the Group Data Protection Officer or Critical Incident Manager in respect of alleged personal data incidents, ensuring that relevant business leads are involved;

26. ensure that post incident actions are completed and implemented in a timely manner by the agreed target date and relevant teams are informed.

Product Development, Engineering, Development Operations and Architecture

Must:-

27. evidence that their teams follow the principles of *data protection by design and default* in the development, configuration, testing and operation of IRIS products and services. Data protection by design and default can be evidenced by documented standard operating procedures, secure software development lifecycles, testing checklists, record-keeping and training targeted at their teams.

The Group IT Director

Must:-

28. ensure that there is a nominated point of contact within the Group IT function for the provision of IT security and network security advice to IRIS Data Controller and Data Processor business functions;
29. ensure that new IT projects, and significant changes to systems and vendors have been notified to the Group Data Protection Officer for assessment to ensure compliance with this policy.

The Chief People Officer

Must:-

30. ensure employees and contractors are informed through compliant and targeted, succinct, plain language privacy statements and notices as to how and why their personal data are collected and processed by IRIS and any third parties on behalf of IRIS (such as benefits partners, employee survey vendors and so on);
31. ensure that the recruitment process for posts that will have access to customer personal data, special category personal data, financial data or payment card information are vetted to meet the requirements of Appendix 5 before a postholder is given access to the data;
32. ensure that there is a process in place to make new employees aware of this policy at recruitment and induction stage and that a specific confidentiality provision is included in contracts of employment and job descriptions as appropriate;
33. ensure that company standards are in place to vet and train temporary employees, including contractors who require access to personal data, to the same standard as permanent employees;

The Data Protection Officer

Must:-

34. perform the statutory Data Protection Officer function, without conflict of interests, as set out in Appendix 2 of this policy.

Data protection policy statements

1. IRIS will always ensure that it has the processes, procedures and records to demonstrate that personal information is managed following the data protection principles
 - 1.1. *Lawfulness, fairness and transparency*: technical and organisational controls must be in place to ensure personal information is used lawfully, fairly and transparently
 - 1.2. *Purpose limitation*: technical and organisational controls must be in place to ensure personal information is collected for specified, explicit and legitimate purposes, with protection against further incompatible use of the information (“function creep”);
 - 1.3. *Data minimisation*: when personal information is collected and used, there must be technical and organisational controls to ensure it is adequate, relevant and limited to what is necessary to achieve the specified purpose(s);
 - 1.4. *Accuracy*: technical and organisational controls must be in place to ensure personal information records are accurate and, where necessary, kept up to date. These controls must include the steps required to erase or rectify inaccurate personal information without delay;
 - 1.5. *Storage limitation*: technical and organisational controls and processes must be in place to dispose of or anonymise personal information once it is no longer required. This must be in line with the IRIS Records Retention Schedule and any applicable legislation.
 - 1.6. *Integrity and confidentiality*: appropriate and proportionate security measures (both technical and organisational) must be in place, based on an assessment of the risks. Security measures include targeted staff training and instructions, organisational and technical measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.
 - 1.7. IRIS processes for the collection and use of personal data will be subject to a data protection assessment (carried out by the relevant project manager, product or service manager, or data owner) to ensure they align with the above data protection principles and any other relevant regulations (such as the Privacy and Electronic Communications (EC Directive) Regulations 2003) and related codes of practice;
2. Rights of individuals
 - 2.1. IRIS will ensure it has the processes and procedures in place within its Group systems and products to manage the rights of individuals, including:
 - (a) Right of an individual to have access to personal information IRIS holds about them
 - (b) Right to rectification of inaccurate personal information
 - (c) The limited right to erasure (right to be forgotten)
 - (d) Right to restriction of use of an individual’s personal information
 - (e) Right to data portability
 - (f) Right to object
 - (g) Right to know about automated individual decision-making and profiling.

3. Transparency to individuals (“data subjects”)

- 3.1. In order to comply with the principle stated at 1.1, the relevant project manager, product or service manager, or data owner will ensure that any use of personal data that they are responsible for has been communicated to the individuals whose data they intend to use (this includes explanations of use by third parties and suppliers on behalf of IRIS). Transparency information should be communicated through whatever means they intend to collect personal data, such as on application forms, products, web pages and via telephone;
- 3.2. The relevant manager should ensure they follow the procedures implemented by the Group Data Protection Officer in order to achieve this.

4. Supplier (“processors” and “sub-processors”) due diligence

- 4.1. Managers who intend to engage a supplier or vendor that will host, access or otherwise process personal data on behalf of IRIS must follow the data protection due diligence procedures implemented by the Group Data Protection Officer before they enter contract negotiations with the intended supplier and must review this at least annually.
- 4.2. Managers must ensure that the use of the supplier processor is reflected in the relevant transparency information available to affected individuals and, in the case of business to business services, to the customer.
- 4.3. Product and Service Managers must ensure that the results of due diligence carried out on “sub-processors” are available to customers through the relevant customer information security assurance documentation, which must be reviewed at least annually.

5. Transfers of personal data to third countries

- 5.1. IRIS will comply with data protection law in respect of transfers of personal data from UK or EU territories to third countries for processing by observing the controls set out in Appendix 1.
- 5.2. Business customers which use a product or service involving the transfer of personal data to a third country will be expected to comply with their responsibilities as data controller under relevant data protection law.

6. Data Protection Officer

- 6.1. IRIS is required to have a Data Protection Officer because the Group’s core activities include large scale processing of special categories of personal data. The Data Protection Officer will be involved, properly and in a timely manner, in all issues which relate to the protection of personal data and will be appointed and will operate in accordance with the requirements set out in Appendix 2.
- 6.2. The Data Protection Officer will be represented in the US and Canada by the Privacy Manager (US & Canada).

7. IRIS commitment to keep records of processing activities.

7.1. IRIS will maintain records of processing activity described in Appendix 3 and will ensure that a copy of these records is available to the IRIS EU representative as required by Article 27 of the EU GDPR.

8. Data mapping and process mapping

8.1. IRIS will require data mapping and process mapping to the extent necessary to demonstrate that the requirements of this policy have been met.

9. IRIS responsibilities as data processor to customers

9.1. IRIS will ensure that it has arrangements in place at product and service level to meet the obligations to customers and clients who are data controllers as set out in Appendix 4.

10. Corporate procedures for reporting and investigating personal data breaches

10.1. All staff must follow the corporate procedure for reporting personal data breaches (and allegations of breaches) to the Group Data Protection Officer without delay. Incidents must immediately be reported by a call (Teams or phone) to the Group Data Protection Officer in addition to any written report about the incident. The full corporate procedure is published to all staff on the MetaCompliance platform.

Appendix 1 – Controls on personal data transferred to third countries for processing

1. IRIS will comply with data protection law in respect of transfers³ of personal data from UK or EU territories to third countries by observing the controls set out below:
 - (a) Where possible, IRIS will choose third party suppliers, vendors and sub-processors that can guarantee personal data will not be transferred to or accessible from third countries unless that territory meets the European Essential Guarantees requirements. The purpose is to make sure interferences with rights to privacy do not go beyond what is necessary and proportionate in a democratic society.
 - (b) Where a supplier, vendor or sub-processor cannot provide the guarantee described in (a), IRIS will either (1) pseudonymise the personal data prior to transfer so that it is not possible for any identification of individuals to take place in a third country, or (2) encrypt the personal data before transfer so that IRIS retains the encryption keys and so it is not possible for identification of any individuals to take place in a third country.
 - (c) Unless authorised by the data controller (such as a customer) or voluntarily by the data subject, IRIS will not transfer personal data from the UK or EU to any recipient in a third country including IRIS entities based outside of the EU or UK for “in the clear” processing unless the territory meets the European Essential Guarantees or is one of the territories listed below:
 - Andorra,
 - Argentina,
 - Canada (commercial organisations only),
 - Faroe Islands, Guernsey,
 - Israel,
 - Isle of Man,
 - Japan,
 - Jersey,
 - New Zealand,
 - Switzerland
 - Uruguay
2. IRIS may off-shore personal data processing to IRIS entities based in third countries provided the following controls are in place:
 - (a) technical and organisational measures provide equivalent protection to the rights and freedoms of individuals enjoyed in the EU and UK.

³ “Transfers” includes making personal data accessible in a third country even if the data remains on servers within the UK or EU. Note that this section is more concerned with the destination than the method of transfer. Whenever you send personal data – and wherever the destination is – you must do so securely and usually through encryption. Please refer to the Information Security Acceptable Use Policy Summary for more detail on secure data sharing.

- (b) Each off-shoring process will be subject to privacy assessment and regular review, and this will be the responsibility of the relevant business owner.
 - (c) All IRIS entities based in third countries are required to comply with this Policy and all related policies affecting the security of data and the privacy of individuals.
 - (d) Guidance, tools and codes of practice produced by the European Data Protection Board and the relevant UK regulator will be used as the basis to establish whether sufficient protections have been put in place.
 - (e) IRIS business entities located outside of the EU or UK which provide services to customers who are also based outside of the EU or UK will be encouraged to host data on servers outside of the EU or UK. This is to avoid transfers from the EU or UK as part of the service provision.
3. In all cases:
- (a) IRIS will ensure that the relevant Model contract clauses to safeguard personal data transferred to third countries and territories are included in supplier data processing agreements. In the case of customer agreements, it is the customer's responsibility to ensure the correct clauses are included in the contract, but IRIS will provide reasonable assistance.
 - (b) Any transfer of personal data that does not meet the standards set out in this Policy must be authorised by the relevant Chief Officer taking into account the risks posed to individuals and of any regulatory action and this decision must be notified to the Group Data Protection Officer.

Appendix 2 – Data Protection Officer

1. IRIS is required to have a Data Protection Officer because the Group's core activities include large scale processing of special categories of personal data. IRIS will ensure there is someone acting on behalf of IRIS Group of companies in the role of Data Protection Officer reporting directly to the highest management level of IRIS Group as required by Article 38 of the General Data Protection Regulation.
2. The Data Protection Officer will be:
 - involved, properly and in a timely manner, in all issues which relate to the protection of personal data;
 - supported with necessary resources in performing the tasks referred to in Article 39 of the General Data Protection Regulation by providing resources necessary to carry out those tasks;
 - given access to personal data and processing operations;
 - free of conflict of interests, independent of instructions regarding the exercise of the statutory tasks and shall not be dismissed or penalised for performing the tasks;
 - bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with the law.
3. IRIS will:
 - publish the contact details of the Data Protection Officer and communicate them to the relevant Regulator;
 - ensure data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under data protection law.
4. The data protection officer may fulfil other tasks and duties and IRIS will ensure that any additional tasks and duties do not result in a conflict of interests.
5. The data protection officer shall have at least the following tasks:
 - (a) to inform and advise IRIS employees who carry out processing of their obligations;
 - (b) to monitor compliance with data protection law and with IRIS policies in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
 - (c) to provide advice when requested as regards the data protection impact assessment and monitor its performance as required by Article 35 of the GDPR.
 - (d) to cooperate with the relevant Regulator;

- (e) to act as the contact point for Regulators on issues relating to processing
- 6. The data protection officer shall consider the risk associated with processing operations, taking into account the nature, scope, context and purposes.
- 7. The Privacy Manager (US & Canada) will be delegated to act on behalf of the Group Data Protection Officer for citizens and customers in those territories.

Appendix 3 – Statutory Records of Processing Activities

1. IRIS will maintain the following records of processing activities

1.1. Controller record of processing activity containing:

- (a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer
- (b) the purposes of the processing
- (c) a description of the categories of data subjects and of the categories of personal data
- (d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations
- (e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, the documentation of suitable safeguards
- (f) the envisaged time limits for erasure of the different categories of data
- (g) a general description of the technical and organisational security measures

1.2. Processor record of all categories of processing activities carried out on behalf of a customer, containing:

- (a) the name and contact details of the IRIS processing entity (and any sub-processors) and of each customer on behalf of which IRIS is acting, and, where applicable, the customer's data protection officer;
- (b) the categories of processing carried out on behalf of each customer;
- (c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and the documentation of suitable safeguards;
- (d) where possible, a general description of the technical and organisational security measures.

Appendix 4 - IRIS commitments when providing a service to customers, whether through a managed service or online product

1. **Responsibility for products and services compliance:** IRIS will ensure responsibility for each system or product's data protection compliance is assigned to specified individuals employed or designated by IRIS. This requirement includes "white labelled" products ("White labelled" is a term used at IRIS to describe products that are made by a third party and packaged and sold by IRIS under the IRIS brand).
2. **Customer information security assurance:** The product director or service manager will maintain customer information security assurance documentation relating to their service or product. This covers the complete lifecycle of customer data obtained as part of the service or product including implementation, support and disposal of the data. It includes assurances relating to third parties and suppliers contracted to process personal data as part of the product or service provision. This will be subject to internal audit and, in the case of certifications and standards, external audit under direction of the Compliance Manager. It is the product director or service manager's responsibility to seek advice from the Compliance Manager or Data Protection Officer when in doubt about these requirements.
3. **Records kept of customer instructions in relation to use of personal data:** The product director or service manager will ensure controls are in place to restrict the use of personal information so that it is only processed on documented instructions from the customer. Customer instructions will be retained as a record along with appropriate audit trails of the actions taken by IRIS in the provision of the service.
4. **Employee and supplier vetting and commitments to confidentiality:** All directors responsible for IRIS employees, contractors or third parties authorised to access or process customer personal information will ensure these have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
5. **Assistance with rights requests:** The product director or service manager will ensure arrangements are in place to provide reasonable assistance to customers responding to data subject rights requests. Requests received by IRIS directly from data subjects will be referred to the relevant customer without delay.
6. **Risk assessment to establish appropriate product and service security controls:** The product director or service manager will shall carry out a risk assessment in consultation with IRIS product stakeholders to implement technical and organisational measures appropriate to the risk to customer information in any given processing activity.
7. **Notification of personal data breach to customers:** IRIS will inform customers without delay of any personal data breach affecting a customer's data and will assist in providing information required for notification to the relevant regulator and affected data subjects where necessary.
8. **Assistance with Data Protection Impact Assessments:** IRIS will provide reasonable support to customers who are carrying out data protection impact assessments relating to the use of an IRIS product or service.

9. **Retention and deletion of customer data:** After the end of service provision, IRIS will delete or return all the personal data to the customer in line with customer's choice and will permanently delete existing copies unless the law requires IRIS to continue storage for a specified time. In the latter case, IRIS will identify the specific legislation that required IRIS to hold the data for a longer period and will ensure processes are in place to dispose of the data at the end of that retention period.
10. **Assistance to customers carrying out audits:** IRIS will make available to customers all information necessary to demonstrate compliance with our data protection obligations and allow for and contribute to audits, including inspections, conducted by or on behalf of the customer.

Engagement of supplier processors ("sub processors")

11. **Authorisation for the use of sub-processors:** IRIS will obtain the written authorisation of the customer for the engagement of any other processor involved in the service. This authorisation may be specific or may be general (such as through the customer agreement).
12. **Informing customers about changes to sub-processors:** IRIS shall inform the customer of any intended changes concerning the addition or replacement of sub-processors, to give the customer the opportunity to object in advance of any changes occurring.
13. **Obligations placed on sub-processors:** Where IRIS engages a sub-processor for carrying out specific activities on behalf of the customer, the same data protection obligations as set out in the agreement between the customer and IRIS shall be imposed on the sub processor through a contract or agreement. This includes providing sufficient guarantees to implement appropriate technical and organisational measures to ensure the processing will meet the requirements of data protection laws.
14. **Liability for sub-processors:** Where the sub processor fails to fulfil its data protection obligations, IRIS is fully liable to the customer for the performance of the sub processor's data protection obligations.

Transfers of customer personal data to third countries and international organisation

15. IRIS will seek to avoid the use of components or suppliers that result in the transfer of personal data to third countries. IRIS will only transfer (or provide access) to customer personal data in third countries if the following conditions apply:
 - (a) The customer has provided documented instructions authorising the transfer to take place or IRIS is under a legal obligation to do so and
 - (b) A risk assessment of surveillance laws in the recipient territory has been carried out in line current regulator guidance and;
 - (c) The product director or service manager has ensured controls are in place to demonstrate that the transfer of personal information to a third country is in line with

documented instructions from the customer.

Appendix 5 – IRIS Pre-employment vetting

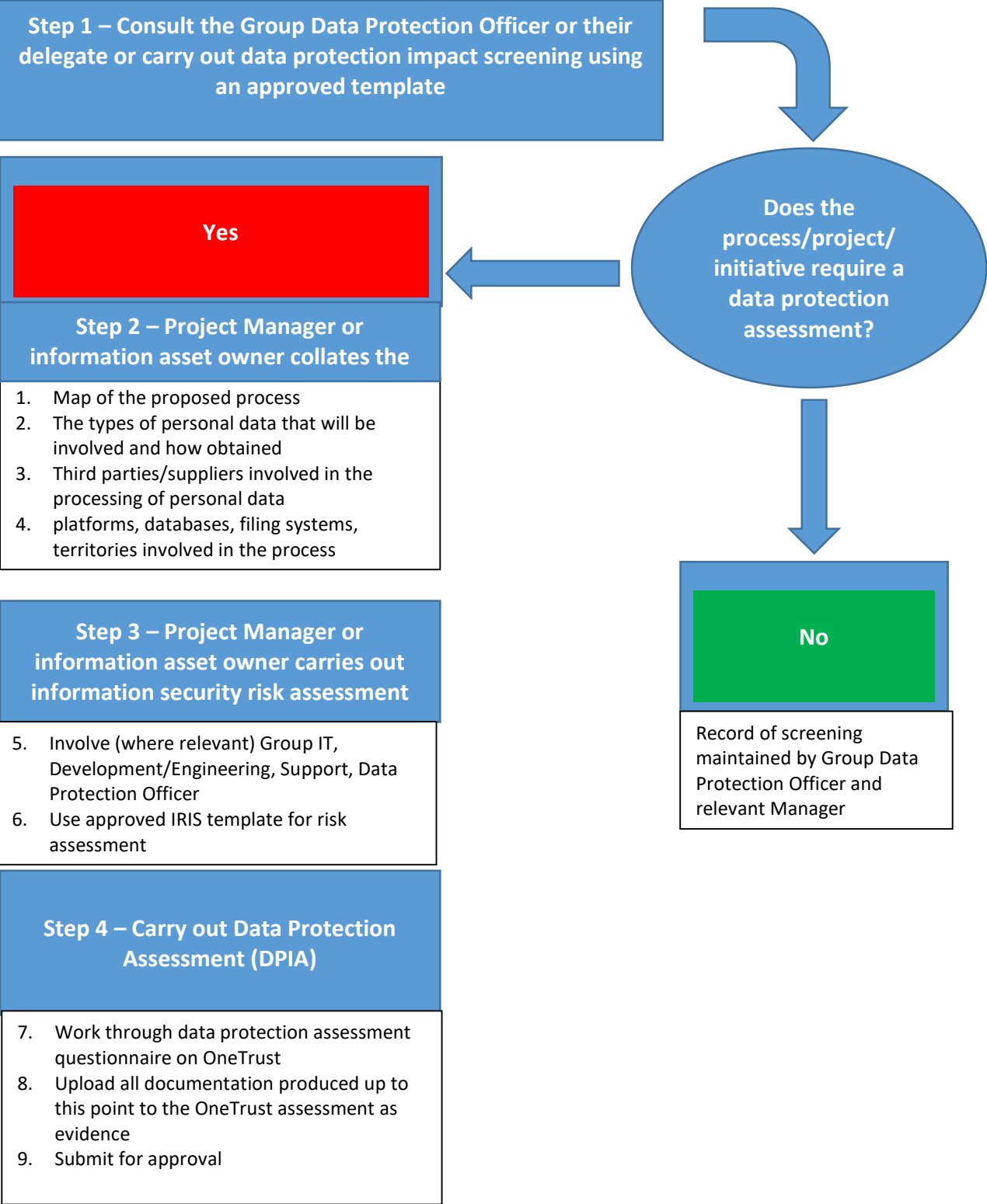
1. IRIS must ensure that the recruitment process for posts that will have access to “*sensitive data*”, allows for at least a basic DBS check before a successful applicant is allowed to access that data. This will cover most posts within the IRIS Group. IRIS defines “*Sensitive data*” as customer personal data, special category personal data, financial data and payment card information.
2. Posts that will not have access to the above data should be identified and will be exempt from the vetting process.
3. Roles that require a higher level of vetting (such as posts that fall under financial services regulations, security services regulations or require employees to work with children) must be on record to ensure all future recruitment to these posts are subject to the required level of pre-employment vetting.

General principles of pre-employment vetting

4. Pre-employment vetting will be carried out at as late a stage as is practicable in the recruitment process but before an employee is given access to sensitive data.
5. No comprehensive pre-employment vetting will take place on shortlisted applicants - only the people selected for the job will be submitted to comprehensive pre-employment vetting.
6. The requirements of pre-employment vetting and how it will be conducted will be made clear early in the recruitment process such as on application forms or other recruitment material, explaining the nature, extent and range of sources to be used to carry out the vetting.
7. Vetting will not be used as a means of general intelligence gathering – only as a means of obtaining specific information to meet clearly stated objectives and which will have a significant bearing on the employment decision.
8. Applicants will be informed of information received that would lead to the applicant not being appointed and they will be allowed to make representations.
9. The vetting process will be designed to avoid discovering information about other people unnecessarily. If substantial personal information is collected about another person and is to be retained the other person will be informed of this and of how IRIS will use the information.


Appendix 6 - Data Protection Assessment Process (overview)

(This assessment is co-ordinated by the relevant product manager/project manager and as a minimum must be reviewed annually or as a result of significant changes, whichever is more frequent)



Appendix 7 - Definitions

Definition	Meaning
Personal data/personal information	Any information relating to an identifiable living individual (“data subject”), whether they can be identified directly or indirectly.
Processing	Simply put, “processing” means “use”. It is anything that can be done with personal data including (but not limited to) collection, recording, organising, structuring, storing, adaptation, retrieval, consultation, disclosure, restriction, erasure or destruction.
Data controller	<p>This is a business or entity that determines the <i>purpose</i> for which personal data will be used and <i>how</i> this will be done.</p> <p>IRIS is data <i>controller</i> when IRIS makes decisions on how and why IRIS will use personal data. For example, as an employer, IRIS holds records about IRIS staff. Also IRIS directly markets products and services to existing and prospective customers – and some data used in these campaigns will be personal data. In this context IRIS must comply with the laws and regulations relevant to data controllers.</p> <p>IRIS is data controller when collecting or using personal data as a result of a direct legal obligation placed upon the company – for example, in government fraud prevention initiatives.</p>
Data processor	<p>This is a business or entity that processes personal data <i>on behalf of the data controller</i> (e.g. as an outsourced service)</p> <p>IRIS is data <i>processor</i> when, through our products or services, IRIS hosts or processes personal data on behalf of customers through our products, solutions and support services. Even if IRIS sub-contracts this to a third party, IRIS is responsible and must meet the requirements of data processors set out in data protection laws and regulations.</p> <p>“<i>Sub-processor</i>” is a term used at IRIS to refer to an IRIS supplier that processes customer personal data on behalf of IRIS as part of a service or product offering (for example a cloud hosting service or payroll partner).</p>
Data Protection Impact Assessment (DPIA)/Data Protection Assessment	A data protection assessment is an initial assessment to identify what actions are required to ensure a proposed or active processing operation complies with data protection rules. A <i>Data Protection Impact Assessment</i> (DPIA) is the same as a data protection assessment but fulfils a statutory function for higher risk processing activities and usually requires wider consultation. The Group Data Protection Officer will advise you when a DPIA is required.
Sensitive personal data/Special category personal data	Information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.



IRIS Software Group
Heathrow Approach 470
London Road Slough
Berkshire SL3 8QY

0344 815 5656
sales@iris.co.uk
iris.co.uk

IRIS HR is a trade mark.
© IRIS Software Group Ltd
02/2020. All rights reserved.