IRIS SOFTWARE GROUP
Data Protection Policy

Version number	2
Owner	Group Data Protection Officer
Document type	Policy
Replaces	IRIS Software Group Data Protection Policy Version 1
Data Protection Impact Screening	Not required
Approved by	Information Security and Governance Forum
Approval date	14 May 2019
Date of last DPO review	N/A
Date of next DPO review	14 May 2020

Contents

Introduction

IRIS is a growing, market leading software group that supplies business-critical data processing services to a diverse range of customers. Our staff have a huge responsibility to look after our customers' information responsibly and in line with data protection and privacy laws.

The Data Protection Act 2018 and associated Regulations specify two key roles that are relevant to data protection compliance:

Data controller: This is a business or entity that determines the *purpose* for which personal data will be used and *how* this will be done.

Data processor: This is a business or entity that processes personal data *on behalf of the data controll*er

IRIS acts in both of the above capacities

IRIS as 'data processor'

IRIS is data *processo*r 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 must meet the requirements of data processors set out in data protection laws and regulations.

IRIS as 'data controller'

IRIS is data *controller* when we make decisions on how and why we will use personal data. For example, as an employer, IRIS holds records about 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.

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.

IRIS commitment to data protection

IRIS is committed to fulfilling its obligations under the Data Protection Act 2018 and any associated privacy legislation that affects how IRIS uses or handles personal data. IRIS has produced the S*tatement of data protection policy* to give this assurance to our customers and staff.

Purpose of this policy document

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

Detailed practice notes and guidance are provided to assist staff and to support this policy. These are made available on the corporate Intranet and on MyCompliance. Procedures and

guidance targetted at specific teams and groups of staff will be made available through local management and training.

Consequences of not complying with this policy

Failure to comply with this mandatory policy and any associated procedures (where relevant) is a disciplinary matter.

Status of the Group Data Protection Policy

This document sits alongside the IRIS Information Security Management System[1] and is subject to ongoing review – at least annually – taking into consideration changes in law, guidance and working practice. This document is supported by local working procedures produced by senior managers but where there is a conflict, this policy takes precedence.

[1] This is IRIS' comprehensive set of information security standards

Statement of Data Protection Policy

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

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

We will always ensure that:

1. there is someone acting on behalf of the IRIS Group of companies in the statutory role of Data Protection Officer, which directly reports to the highest management level of IRIS[2]. This person is the IRIS Software Group Ltd Data Protection Officer ("Group Data Protection Officer");

2. responsibility for each system or product's data protection compliance is assigned to one or more specified individuals;

3. we will risk-assess our products and Group IT systems to ensure that appropriate technical and organisational security measures are implemented which are proportionate to the risks;

4. everyone managing and handling personal data understands that they are contractually responsible for following the good data protection practice set out in this policy and the supporting guidance and standards;

5. everyone managing and handling personal data is appropriately trained, supervised and audited;

6. our handling and processing of personal information are regularly risk-assessed and evaluated;

Where IRIS is acting in the capacity of Data Controller, we will ensure that:

7. a Data Protection Impact Assessment is carried out, where required;

8. our collection and use of personal data align with the data protection principles, data subject rights, relevant regulations (such as the Privacy and Electronic Communications (EC Directive) Regulations 2003) and codes of practice;

9. we provide appropriate transparency explanations through whatever means we collect personal data, such as on application forms, products, web pages and via telephone;

10. our transparency notices make clear that anyone who wants to make enquiries about our personal data processing, can do so through the Data Protection Officer or another designated data protection representative;

[2] GDPR Article 38(3)

11. a corporate procedure is in place to report and investigate personal data breaches[1] without undue delay;

12. we keep the statutory records required under relevant laws as well as any further records required to demonstrate compliance, such as risk assessments, policies, working procedures, records of consent (where necessary) and so on.

Where IRIS is acting in the capacity of data processor we will:

13. provide our customers with appropriate guarantees (relevant to the product or service) in respect of the technical and organisational measures we have in place to protect personal data and to protect the rights of individuals;

14. process the personal data only on documented instructions from the customer, including with regard to transfers to a third country or an international organisation;

15. ensure that persons authorised to process the personal data entrusted to us are under an obligation of confidentiality;

16. assist the customer, as far as possible, by appropriate technical and organisational measures, to fulfil the customer's obligation to respond to data subjects exercising their rights as set out in the data protection legislation;

17. at the choice of the customer, delete or return all the personal data after the end of the processing contract, and delete copies, unless the law requires IRIS to store the personal data for longer;

18. make available all information necessary to demonstrate compliance with our data protection obligations and allow for and contribute to audits, including inspections, conducted by the customer's auditor;

19. not engage another processor except as authorised by the customer under the processing agreement;

20. notify the customer of any intended changes concerning the addition or replacement of other processors, to give the customer the opportunity to object to the changes;

21. ensure that any other processors we engage to process the customer's data adhere to the same standards imposed on IRIS in respect of data protection and security;

22. notify customers of security breaches that affect their data without undue delay;

Roles and Responsibilities

All Staff will:

1. routinely assess whether they use or have access to any personal data when performing their job function for IRIS;

2. accept that they are responsible for the security of the personal data they use and have access to;

3. ensure they understand how this policy, its associated guidance notes and their local working procedures affect their work and use personal information accordingly;

4. follow the working procedures provided to them by their manager, which set 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 such working procedures, they should ask. In the event of a breach, ignorance is not a defence;

5. if their manager has not made local working procedures available, staff should feel empowered to report this to the Group Data Protection Officer or their local data protection single point of contact ("DP SPOC");

6. report security risks, incidents and "near misses" in line with the corporate *Personal Data Incident Reporting and Investigation Procedure*. This includes concerns raised by customers;

7. 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 will

8. lead and foster a culture that values, protects and uses personal data ethically;

9. collectively bear data controller and data processor responsibility for IRIS compliance with data protection and privacy law;

10. ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data[3];

11. support the data protection officer in performing his or her statutory tasks by providing the resources necessary to carry out those tasks and (1) access to personal data and processing operations and (2) to maintain his or her expert knowledge[4];

12. ensure that information security and data protection compliance are included in the IRIS approach to risk management;

[3] GDPR Article 38(1)
[4] GDPR Article 38(2)

Senior Management Team members will

13. individually take responsibility for information assets and personal data processing activities carried out within the business functions they manage i.e. SMT members will be "Information Asset Owners"[5] ("IAO");

14. identify information assets/business processes they are responsible for which involve or affect personal information, ensure all are subject to data protection assessment and that a record is kept of each assessment using corporate templates;

15. ensure their business unit(s) maintain records of processing activities carried out as required under Article 30 of the General Data Protection Regulation (see separate guidance document);

16. ensure suppliers and vendors involved in the processing have been identified and the correct supplier due diligence processes are established in their business unit(s);

17. appoint one or more Information Asset Managers (IAMs) to have routine responsibility for the data protection compliance of information assets within the business unit. The aim is for clear and documented accountability for all information assets;

18. appoint data protection single points of contact ("DP SPOCs"[6]) for each business unit they are responsible for, ensuring they are given the time and resources to attend data protection steering groups and to coordinate a business unit's response to any actions or recommendations arising from meetings, from personal data incidents or from specific management instructions;

19. provide a written judgement of the security and use of their asset(s) at least annually to the Group Information Security and Governance Forum using authorised templates to support the audit process;

Information Asset Managers will

20. have day to day responsibility for the compliance of information assets assigned to them by the IAO;

21. implement control measures as required or delegated by the IAO;

22. where delegated, maintain the statutory records[7] on behalf of the IAO;

Line managers will

23. take ownership of data processing carried out by staff who are their direct reports;

[5] See under the heading *Definitions*
[6] See under the headings *Definitions* and *Data Protection Single Points of Contact*
[7] See separate guidance *Statutory Records required under GDPR*

24. ensure that direct reports have adequate training in data protection and security before being given access to customer data and any other IRIS personal data;

25. ensure that their direct reports are made aware of all procedures they are required to follow and ensure this awareness activity is documented for audit purposes;

26. ensure temps 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

Product managers will

27. act as information asset managers in respect of the products they manage (the information asset owner is the relevant member of SMT);

28. in consultation with the Group Data Protection Officer, lead on the product risk assessment and data protection assessment and ensure this is evidenced;

29. in respect of a product's compliance with data protection law and related regulations, ensure they have arrangements in place and are able to provide evidence-based assurance to:

29..1. Customers
29..2. The Group Data Protection Officer
29..3. Senior Managers
29..4. Other product stakeholders

30. ensure product-specific collateral, policies and procedures are in line with the minimum requirements of this data protection policy and the IRIS Information Security Management System;

31. coordinate the response to the Group Data Protection Officer in respect of alleged personal data incidents, ensuring that the relevant leads from Development, IT and Support and others are involved where relevant;

32. ensure arrangements are in place to assist customers to deal with rights requests from data subjects in the context of the product or service provision under their management;

Product Development will

33. follow the principles of data protection by design and default in the development and provision of IRIS software;

34. evidence that information security is a key consideration in all product development;

35. demonstrate that the OWASP secure coding checklist (or a similar industry standard) has been observed for all new developments and significant updates involving, affecting or with the potential to affect personal data;

The Group IT Director will:

36. 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;

37. ensure that new IT projects and significant changes are subject to Data Protection Impact Assessment screening and are risk assessed in respect of information security using agreed templates;

The Chief People Officer will:

38. ensure that staff who will have access to special category personal data, financial data and payment card information are vetted to accepted industry standards before being given access to such data;

39. ensure that there is a process in place to make new members of staff 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;

40. ensure that company standards are in place to make sure temporary staff, including contractors who require access to personal data, are vetted and trained to the same standard as permanent members of staff;

The Data Protection Officer will:

41. perform the statutory Data Protection Officer tasks as set out in relevant data protection law;

42. not receive any instructions regarding the exercise of those tasks, where such instructions would give rise to a conflict of interests[8];

43. be bound by confidentiality concerning the performance of those tasks[9];

44. directly report to members of the Group Information Security and Governance Forum, which includes members of the Executive Committee (thereby fulfilling the requirement to report to the highest management level within IRIS);

45. make his or her contact details available to the public so that data subjects (living individuals) can contact the Data Protection Officer on all issues related to the processing of their personal data by IRIS and to the exercise of their rights under data protection laws and regulations[10];

[8] GDPR Article 38(3)
[9] GDPR Article 38(5)
[10] GDPR Article 38(4)

46. inform and advise IRIS management and employees who carry out processing of their obligations under data protection and related privacy law[11];

47. provide advice where requested regarding the data protection impact assessment[12];

48. monitor compliance with data protection and related privacy law and with IRIS data protection policies[13]. This includes monitoring:-

48..1. the assignment of responsibilities,
48..2. awareness-raising and training of staff involved in processing operations,
48..3. related audits;
48..4. the performance of data protection impact assessments

49. have due regard to the risk associated with processing operations, considering the nature, scope, context and purposes of processing[14];

50. act as the contact point for the supervisory authority on issues relating to processing. This includes any consultations necessary for data protection impact assessments[15];

51. cooperate with the supervisory authority[16];

52. In addition to the statutory role, the Data Protection Officer will record information security incidents and support their containment and resolution. As necessary, the Data Protection Officer will produce interim and final outcome reports to the Chief Information Officer and ensure learning outcomes are followed up by the relevant Information Asset Owner(s);

Data Protection Single Points of Contact ("DP SPOCS") will:

53. act as first point of contact for other staff within the department or business unit in relation to data protection issues;

54. help to build a "privacy aware" culture by ensuring privacy and data protection is on the agenda within the departmental management and team meetings;

55. ensure personal data incidents are escalated in line with the corporate and divisional personal data reporting procedures;

56. ensure the company data protection response is communicated to the relevant managers and staff within the department;

[11] GDPR Article 39(1)(a)
[12] GDPR Article 39(1)(c)
[13] GDPR Article 39(1)(b)
[14] GDPR Article 39(2)
[15] GDPR Article 39(1)(e)
[16] GDPR Article 39(1)(d)

57. coordinate escalation of data protection issues raised by staff to the Group Data Protection Officer, the steering group or relevant managers as necessary;

58. Follow up with the relevant staff/managers where staff within the department or business unit have not completed mandatory training or accepted mandatory policies;

59. help to bring the right people together within the department or business unit to contain and deal with a data protection or security incident;

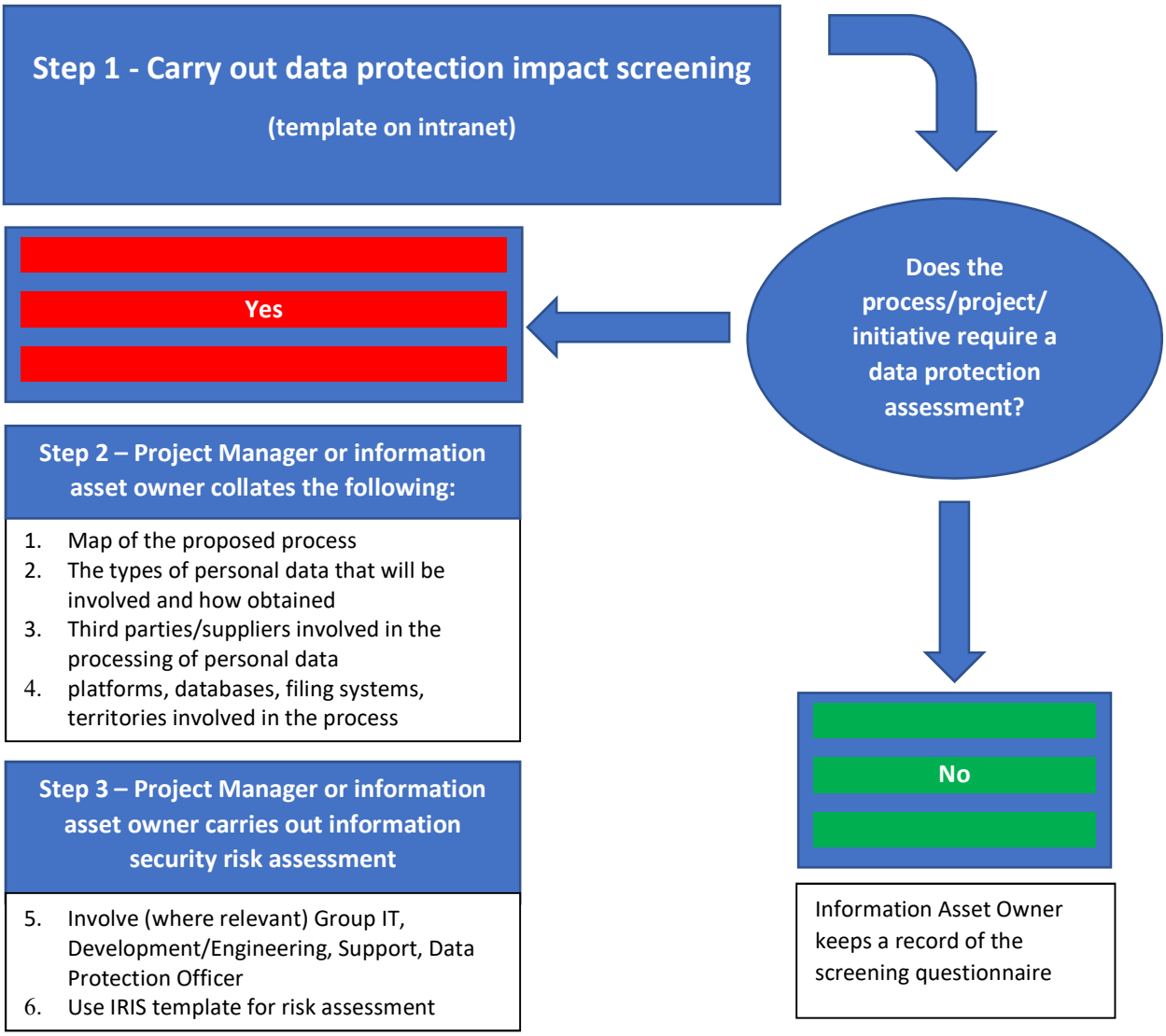
60. ensure actions identified following an incident are communicated to the right parts of the department or business unit and take the initiative to follow up to make sure the actions are implemented;

61. represent their department or business unit at Data Protection Steering Group meetings;

62. coordinate with the other departmental DP SPoCs to ensure documentation/audit trails are kept up to date in relation to data protection;

Data Protection Assessment Process (overview)

(This assessment is owned by the Information Asset Owner, project manager or process owner as applicable and as a minimum must be reviewed annually or as a result of significant changes)



Step 2 – Project Manager or information asset owner collates the following:

1. Map of the proposed process
2. The types of personal data that will be involved and how obtained
3. Third parties/suppliers involved in the processing of personal data
4. platforms, databases, filing systems, territories involved in the process

Step 3 – Project Manager or information asset owner carries out information security risk assessment

5. Involve (where relevant) Group IT, Development/Engineering, Support, Data Protection Officer
6. Use IRIS template for risk assessment

Step 4 – Carry out Data Protection Impact Assessment (DPIA) or data protection assessment, using MetaPrivacy software

7. Work through data protection assessment questionnaire on MetaPrivacy
8. Upload all documentation produced up to this point to the MetaPrivacy assessment as evidence
9. Submit for approval

Definitions

Data Protection Impact Assessment (DPIA)/Data Protection Assessment

All processes involving the use of personal data must comply with the 7 data protection principles and with data subject rights – therefore all are subject to a 'data protection assessment'.

A *Data Protection Impact Assessment* (DPIA) is the same as a data protection assessment but is likely to require wider consultation with stakeholders and in some cases requires approval by the Information Commissioner. DPIAs are a legal requirement for certain types of personal data processing – especially when new technologies will be involved and there is a high risk to the rights and freedom of the people subject to the processing (the full circumstances that require a DPIA are set out in Article 35 of the GDPR). At IRIS, the process for carrying out DPIAs is the same as for Data Protection Assessments – the Data Protection Officer will advise on a case by case basis when further consultation is required.

Data Protection Single Point of Contact (DP-SPOC)

This is a member of staff, usually a manager, which the relevant member of Senior Management Team has appointed as the first point of contact for data protection matters for the relevant department. Not necessarily a data protection specialist but someone with enough seniority to influence staff behaviour and working practice, where necessary, and with a good knowledge of local working practices that involve the use of personal data.

Information Asset

An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited efficiently. Information assets have recognisable and manageable value, risk, content and lifecycles (detailed guidance on information assets is available on the IRIS Corporate Intranet site (see Data protection FAQs)

Information Asset Owner

Information Asset Owners (IAOs) are senior/responsible individuals involved in running the relevant business. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. As a result, they are able to understand and address risks to the information and ensure that information is fully used within the law for the public good. They will provide a written judgement of the security and use of their asset annually to support the audit process.

Information Asset Manager

Although there is no official definition of Information Asset Manager, the purpose of this role is to Support the Information Asset Owner by providing day to day management of information assets under the direction of the Information Asset Owner.

Personal data

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’s anything that can be done with personal data including (but not limited to) collection, recording, organizing, structuring, storing, adaptation, retrieval, consultation, disclosure, restriction, erasure or destruction

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.

Related policies, guidance and templates

The following list is not exhaustive so you should check the Intranet for the latest documentation and guidance.

Group policies and procedures are available to all staff through the MetaCompliance system. The Intranet Data Protection pages contain further guidance, good practice and templates

	Document name	Status
1	Acceptable use and information security summary	Mandatory group policy
2	Personal data incidents – reporting and investigation procedure	Mandatory group procedure
3	Group records retention schedule	Default group procedure
4	Transparency and the right to know	Legal requirements
5	Supplier due diligence procedure	Group procedure
6	DPIA screening questions	Group template/workflow
7	MetaPrivacy DPIA and data protection assessments	Group template/workflow
8	Information risk assessment (light touch)	Group template
9	IRIS Information Security Management System (ISMS)	Group information security standards
10	Statutory records of processing	Legal requirements
	Development-specific	
11	OWASP secure coding practices checklist	Good practice/standards
	Marketing-specific	
12	Marketing and sales supplier and product due diligence for bought in prospect lists	Summary of data protection requirements
13	Various external checklists and guidance such as DMA and ICO	Good practice/standards
	Website-specific	
14	ICO cookies guidance and various standards	Good practice/standards