IRIS SOFTWARE GROUP
Data Protection Policy

Version number	1.1 (minor update)
Author	Vincenzo Ardilio
Date of issue	13 February 2018
Document type	Policy
Replaces	Data Protection Group Compliance Policy 2010
Approved by	Executive Committee
Approval date	27 March 2017 (confirmed)
Data Protection Impact Screening	No PIA required
Date of next review	25 May 2018

Contents

1) Introduction

IRIS acts in the capacities of controller and processor of personal data[1]

We are a processor in respect of the personal information entrusted to us by our customers in our products and solutions.

We are a controller when we make decisions on how and why we will use personal data. For example, as an employer, we hold records about our staff. Also, as a commercial organisation, we directly market our products to prospective customers – and some data used in these campaigns will be personal data.

IRIS is committed to fulfilling its obligations under the General Data Protection Regulations (GDPR) and any subsequent data protection legislation. We have produced this policy to give such assurance to our customers and staff.

Appended to this policy is an explanation of how responsibility for data protection compliance is delegated. More detailed practice notes and guidance will be provided to assist staff and to support this policy.

This document sits alongside the IRIS Information Security Management System[2] and is subject to ongoing review – at least annually - in light of changes in law, guidance and working practice.

2) 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 network or device, in filing systems, on paper, or recorded on other material such as audio or visual media.

IRIS regards the proper and good 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 ensure that:

- there is someone acting in the statutory role of Data Protection Officer on behalf of the IRIS Group of companies. This person is IRIS Software Group Ltd.'s Data Protection Officer;

- responsibility for each system or product's data protection compliance is assigned to one or more specific individuals;

- our collection and use of personal data complies with the data protection principles, data subject rights, relevant regulations and codes of practice, wherever we are acting as controller;

[1] See Appendix 4 - Definitions

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

- we provide appropriate privacy notices and explanations through whatever means we collect personal data, such as on application forms, products, web pages and via telephone wherever we are acting as controller;

- appropriate technical and organisational measures for all of our products and Group IT systems are implemented to ensure a level of security appropriate to the risks;

- 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;

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

- our privacy notices make clear to anyone that wants to make enquiries about our personal data processing, can do so through the Data Protection Officer or the product's designated data protection representative

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

- a corporate procedure is in place to report and investigate personal data breaches[3] without undue delay;

- we keep the statutory records required under GDPR as well as any further records required to demonstrate compliance, such as risk assessments, policies, working procedures, records of consent and so on.

In addition, where IRIS is acting in the capacity of data processor we will:

- provide our customers with appropriate guarantees in respect of the technical and organisational measures we have in place to protect personal data and to protect the rights of data subjects;

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

- ensure that persons authorised to process the personal data entrusted to us are under an appropriate statutory obligation of confidentiality;

- 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;

- 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 us to store the personal data for longer;

[3] See Appendix 4 - definitions

- 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;

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

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

- 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;

Appendix 1

Roles and Responsibilities

All Staff will:

- routinely assess the kind of information they use whilst carrying out their work and whether they have responsibility for any personal data.
- ensure they understand how this policy, its associated guidance notes and their local working procedures affect their work and use personal information accordingly
- follow local procedures that apply to the systems and products they have access to in order to handle personal data appropriately
- report data breaches and "near misses" in line with the corporate Critical Incident Procedure.

Senior Management Team members will:

a. identify information assets they are responsible for which involve or affect the processing of personal information.

b. act as Information Asset Owners (IAOs) – in other words

    - take ownership of information assets and the extent of compliance with data protection rules
    - lead and foster a culture that values, protects and uses personal data ethically
    - understand what information is transferred in and out of the information asset(s) they are responsible for
    - know who has access and why, and ensure that use of the asset is monitored

c. ensure that a record of processing activities is maintained in line with GDPR requirements for data controllers *(See Appendix 3 – Statutory Records)*

d. ensure that a record of the categories of processing activities carried out on behalf of each customer is maintained in line with GDPR requirements for data processors *(See Appendix 3 – Statutory Records)*

e. understand and address risks to the asset(s), provide assurance to the CIO and Data Protection Officer, and ensure that any data risk incidents are managed in line with the Corporate Critical Incident Procedure

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

g. ensure the Data Protection Officer has access to the register of information assets and all records associated with compliance

h. ensure that the Data Protection Officer is present where decisions with data protection implications are taken and that all relevant information is passed to the Data Protection Officer in a timely manner in order to allow provision of adequate advice

i. ensure that the principles of *data protection by design and default* are applied to each new or major update to projects or proposals (including product development) involving the use of personal information or with potential to affect privacy. The Data Protection Officer must be informed at an early stage of the proposal and any corporate templates provided to meet the requirements of *data protection by design and default* should be used.

j. ensure that staff (including temporary staff and contractors) that have access to personal data also have access to instructions that include the actions they must take to protect personal data and privacy.

k. In consultation with HR, to ensure that arrangements are in place to vet individuals (such as staff and contractors) to HMG Baseline Personnel Security Standards (BPSS) before giving access to financial data, payment card information and special category personal data for the first time.

l. ensure staff training needs have been communicated to the Data Protection Officer

Managers who are Information Asset Managers (IAMs) will

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

b. implement control measures as required or delegated by the IAO

c. where delegated, maintain the statutory records on behalf of the IAO (see Appendix 3 – Statutory records)

All line Managers will

a. ensure new recruits receive training - including on the job training – on local working procedures to ensure they handle personal data in a compliant and secure way

b. ensure their staff have access to training and materials including guidance, checklists and templates provided by IRIS to ensure compliance with data protection regulations

c. ensure that data breaches and “near misses” are reported in line with the Corporate Critical Incident Procedure

HR Services will be responsible for the following:

a. BPSS checks for new staff who will have access to special category personal data, financial data and payment card information before access to systems holding such data is given.

b. Ensure that new members of staff are made aware of this policy document at recruitment and induction stage and also that a specific confidentiality provision is included in contracts of employment and job descriptions.

The Data Protection Officer will

a) inform and advise the business, including any employees who carry out processing of their data protection obligations;

b) monitor data protection compliance against the relevant legislation and company policies in relation to the protection of personal data, the assignment of responsibilities, awareness raising and training of staff involved in the processing of personal data;

c) provide advice, where requested, as regards data protection impact assessments and the monitoring of the performance;

d) act as IRIS Group's contact point for the Information Commissioner's Office including consulting, where appropriate, with regard to any matter relating to the IRIS Group's data processing;

e) ensure that this Data Protection Policy, the associated documents and guidance are kept up to date and communicated to staff in an appropriate manner;

f) arrange for the provision of advice and training to staff on request;

g) manage the notification of IRIS's processing to the Information Commissioner's Office;

h) investigate personal data breaches and data security incidents in liaison with the Information Asset Owner and provide recommendations to the Chief Information Officer;

i) act in an independent manner and will not perform duties or tasks that would give rise to a conflict of interests;

Appendix 2

The Data Protection Principles and data subject rights

The Data Protection Principles

Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject *('lawfulness, fairness and transparency'*);

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (*'purpose limitation'*);

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (*'data minimisation'*);

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('*accuracy*');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (*'storage limitation'*);

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (*'integrity and confidentiality'*).

Data subject rights

1) to receive from IRIS any information relating to processing of personal data in a concise, transparent, intelligible and easily accessible form, using clear and plain language

2) the right of access: to their own personal data, a description of how it is being used, the source, how to exercise their rights and to complain etc.

3) the right to rectification

4) the right to erasure (‘right to be forgotten’)

5) right to restriction of processing

6) right to data portability

7) right to object

8) right not to be subject to automated individual decision-making and profiling:

Appendix 3 – Statutory records

Where IRIS is 'data controller'

(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 purpose(s) 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 where relevant;

(f) where possible, the envisaged time limits for erasure of the different categories of data;

(g) where possible, a general description of the technical and organisational security measures in place

(h) records that demonstrate compliance with the data protection principles (for example, data protection by design and default records, risk assessments, training records and so on)

Where IRIS is 'data processor'

Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

(a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;

(b) the categories of processing carried out on behalf of each controller;

(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, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

(d) where possible, a general description of the technical and organisational security measures

Appendix 4 – Definitions

‘information asset’ is a body of information that is defined and managed as a single entity so that it can be understood, shared, protected and exploited effectively. For example an information asset may be a product, database, IT system, file or filing system. In the context of managing personal data processing it can also be useful to classify vendors, outsourced data processors (such as cloud hosts), software and hardware as information assets

'personal data' means *any information relating to an identified or identifiable natural person ('data subject'*); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a *name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*;

'processing' means operations, such as *collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*;

'restriction of processing' means the *marking of stored personal data with the aim of limiting their processing in the future*;

'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular *to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements*;

'filing system' means *any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis*;

'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, *determines the purposes and means of the processing of personal data*;

'processor' means a natural or legal person, public authority, agency or other body which *processes personal data on behalf of the controller*;

'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.

'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

'personal data breach' means 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;

'genetic data' means personal data *relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health* of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which *allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data*;

'data concerning health' means personal data related to the *physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status*;

'representative' means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation;

'enterprise' means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;

'international organisation' means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

Third country, means a country outside of the EU