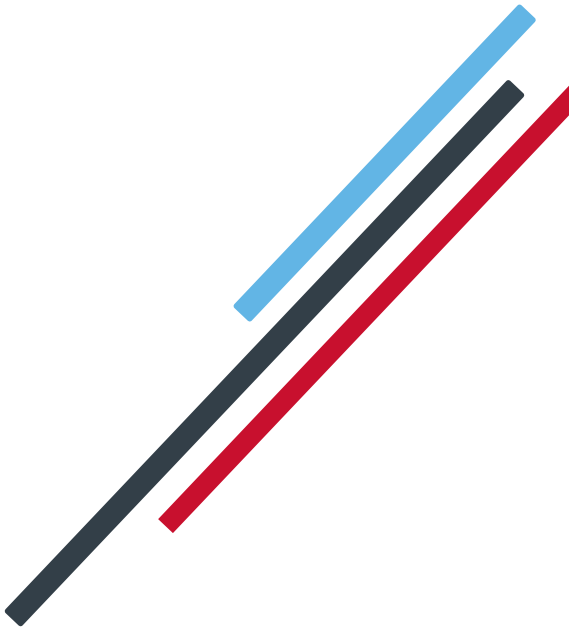
Due Diligence Questionnaire

IRIS Managed Payroll Service

25th April 2018

Version: 1.0



Document Control

Version	Date	Amendment	Amended by
1.0	25/04/2018	▪ Initial Draft	Claire Treadwell
		▪	
		▪	
		▪	
		▪	
		▪	

Contents

Introduction

For GDPR purposes the IRIS Managed Payroll Service has been identified as a Data Processor, with the client as the Data Controller. As such the client has an obligation to:

1. Choose only processors that can provide sufficient guarantees to implement appropriate technical and organisational measures to make sure that the processing will meet data protection requirements and will protect the rights of the individuals the information relates to.

2. Put in place a contract or agreement, that is binding on the processor and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the customer. That contract must include certain clauses listed in Article 28 of the General Data Protection Regulation (GDPR).

This document is designed to provide reasonable guarantees in line with above.

IRIS Managed Payroll Service commitment to data protection

The IRIS Managed Payroll Service will:

- Use personal data legally and securely
- Respect privacy and treat personal data lawfully and correctly
- Ensure that the service complies with the General Data Protection Regulations
- Adhere to the group data protection policy
- Report any breaches of data protection to the relevant channels

Click on the links to download the Standard Terms and Conditions and the Customer Data Processing Terms.

Frequently Asked Data Protection Questions

No.	Controller's Question	Processor's response
1	**Processing Data**	
1.1	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 ▪ Client contact information is held
1.2	For what purposes do you use the personal data?	As processor, to provide the contracted services i.e. payroll processing and/ or payments to employees and third parties, such as HMRC. The IRIS Managed Payroll Services ensures that the mandatory reporting requirements are met, this includes submitting data to third parties such as HMRC.
1.3	Which of your departments have access to the personal data?	Access is restricted to the IRIS Managed Payroll Team and those that support the product internally. Only personnel with authorised access can view data and access data.
1.4	What data processing activities do you undertake on our behalf (e.g. collection, recording, organisation, storage, use, disclosure, transmission or dissemination of data)?	▪ Payroll Processing ▪ Submission of BACS payments ▪ Printing or publishing payslips ▪ Submission of data to third parties such as HMRC, Pension providers, Court Authorities
1.5	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).	Data is collected from the controller via the agreed method. This will be either spreadsheet, which is password protected and uploaded to IRIS OpenSpace or using Remote Payroll Entry (timesheet entry portal). We prefer customers to submit their data to us via IRIS Remote Payroll Entry, IRIS OpenSpace or secure FTP. Customers that choose to send information to us by normal (unencrypted) internet email, must take responsibility for the security of that data as this is widely known to be insecure.
1.6	How do you collect/receive the personal data? e.g. application form, secure online portal, password protected attachment via email	▪ Via password protected spreadsheet attached to an email ▪ Via password protected spreadsheet via secure FTP ▪ Remote Payroll Entry app ▪ Data is then imported into the Earnie system

1.7	What procedures do you apply to ensure personal data is accurate and kept up to date?	See the IRIS Managed Payroll Service Data Protection Policy for more details.
2	**Policies**	
2.1	Is there a Data Protection Policy applicable to all staff who process data for us? If yes, please provide a copy.	Yes. The current data protection policy is accessible through the IRIS Data Protection Policy. This applies to all employees.
2.2	Do you have an up-to-date internal data breach register?	Yes. This is managed by the IRIS Group Data Protection Officer.
2.3	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?	HMRC state that records should be kept for 3 years, plus the current tax year. The IRIS Managed Payroll Service client data will be kept for 5 years to demonstrate compliance, should a HMRC audit take place. 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.
3	**SECURITY AND IT**	
3.1	Do you have adequate physical security procedures and measures in place to protect personal data?	Yes we have an Information Security Management System
3.2	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
3.3	Do you use encryption to protect personal data?	If using IRIS OpenEnrol, IRIS OpenPayslips or IRIS Remote Payroll entry: ▪ The data is encrypted using strong cipher suites ▪ Password security is in place for user access. Data is encrypted during transit ▪ All datacentre environments are isolated from the corporate ones. Access is provided with two factor authentications
No.	**Controller's Question**	**Processor's response**
3.4	Are all mobiles phones, laptops and tablets which contain personal data tracked in an asset register, pin or password protected, encrypted and remotely wipeable?	Our Group IT look after IRIS's asset register. Devices issued to staff by IRIS Group IT will be included in that register.
3.5	How is removable storage media recorded and managed to ensure security?	Not applicable

3.6	What protections are there against unauthorised copying, processing etc?	Not applicable
3.7	What protections are there against accidental loss, damage or destruction?	Not applicable
3.8	Do you have robust frequent data backup procedures?	Daily back-ups are taken of the data Data is backed up to tape, which is retrieve by Iron Mountain each day and taken to a secure location. Iron Mountain certifications can be viewed using the link below: http://www.ironmountain.co.uk/about-us/certifications-and-awards
No.	**Controller's Question**	**Processor's response**
3.9	What additional identification and security measures apply to any sensitive or special category data (if applicable)?	Not Applicable
4	**Sharing/Receiving data from third parties**	
4.1	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.	The IRIS Managed Payroll Service share data with the necessary agencies to ensure compliance such as HMRC, court authorities, pension providers. Employee personal data is never share with third parties for marketing purposes.
4.2	How do you audit your data processors' compliance with data protection law?	We request security guarantees in line with Schedule 1 part II of the Data Protection Act 1998 (Seventh Principle). With respect to GDPR we request guarantees relating to compliance with processor obligations under the Regulation We have Corporate guidelines on this.
4.3	Do you have a standard data processor agreement for use with third parties?	Yes
5	**Compliance programme**	
No.	**Controller's Question**	**Processor's response**

5.1	Who is responsible for data protection compliance in your organisation?	The Chief Information Officer (CIO) has ultimate responsibility but is supported by the governance structure described in Appendix 1 of the Group Data Protection Policy.
5.2	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?	We have an overarching critical incident process, supported by a personal data incident reporting procedure, which ensure any incident is promptly reported to the Group Data Protection Officer and assessed in line with the Article 29 Working Party Guidelines on Breach Reporting under GDPR.
5.3	Who is responsible for dealing with the response to data breaches in your organisation?	Group Data Protection Officer in consultation with the CIO.
5.4	Do all staff receive data protection training? Please provide details.	This is covered at induction at a corporate and local management level. Classroom based refresher training is organised for staff by local management and this is supported at a corporate level by our eLearning Platform. Our eLearning covers data security, GDPR and phishing/cyber risks. Data protection policy documentation is reviewed on an annual basis and each team member signs to state they have read and will adhere to both the IRIS Managed Payroll Service policy and the corporate policy.
5.5	To the extent not already set out above, what action have you taken to ensure compliance with data protection laws?	The IRIS Managed Payroll Service has conducted a Risk Assessment and updated its policies and procedures in accordance with the findings. IRIS has an Information Security and Governance Group, which includes members of the Executive Committee and this is supported by divisional projects to ensure ongoing compliance by 25 May 2018 and beyond.
6	**Consent and rights of individuals**	
6.1	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 (the customer).
6.2	If consent is obtained, is the consent written? If not, how will it be demonstrated that consent has been given?	As above
6.3	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

6.4	If no consent is required or obtained, which grounds for processing will be relied on?	As above
6.5	Do you have a clear and known process to deal with Subject Access Requests?	As your Data Processor we do not process Subject Access Requests on your behalf.
6.6	What is the process for you to respond to requests to rectify inaccurate personal data about an individual?	The named contact would need to contact the IRIS Managed Payroll Service and inform them of the required changes. Requests will only be accepted from named contacts.
6.7	What is the process for you to respond to a request under the right to be forgotten?	As your Data Processor we will not process the right to be forgotten, but we would assist you within the GDPR timescales.
6.8	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?	All data is stored within the UK. To implement appropriate safeguards, the IRIS approach is to include Model Contract Clauses approved the European Commissioner or as recommended by the European Article 29 Working Party.
6.9	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.
6.10	How are individuals whose personal data you process made aware of the Privacy Policy/Fair Processing Notice?	See above