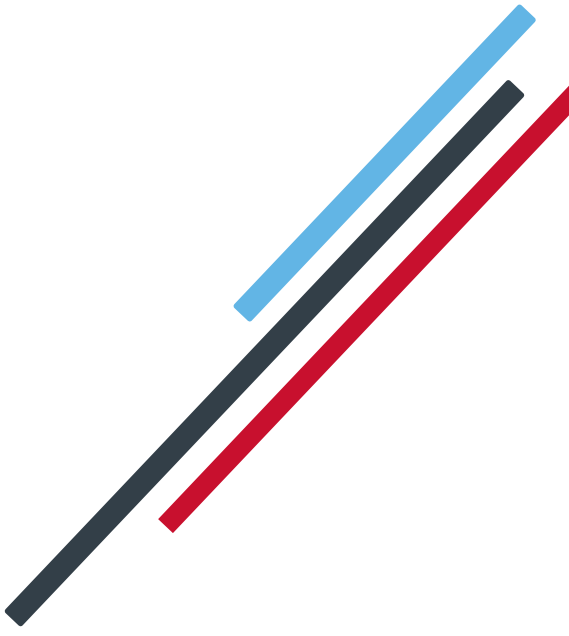
Due Diligence Questionnaire

IRIS OpenPayslips and IRIS OpenEnrol

14th May 2018

Version: 1.0



Document Control

Version	Date	Amendment	Amended by
1.0	14/05/2018	▪ Initial Draft	Claire Treadwell
		▪	
		▪	
		▪	
		▪	
		▪	

Contents

Introduction

For GDPR purposes the IRIS OpenPayslips and IRIS OpenEnrol 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 OpenPayslips and IRIS OpenEnrol commitment to data protection

The IRIS OpenPayslips and IRIS OpenEnrol 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 regarding payroll and pensions communication
1.2	For what purposes do you use the personal data?	As processor, to provide the contracted services i.e. delivery of payslips, P45s, P60s and pensions communications via mobile application or the IRIS OpenPayslips/OpenEnrol website
1.3	Which of your departments have access to the personal data?	Only the necessary departments at IRIS can access the cloud services data including Support, Development/QA and Admin. Within these departments we do have a role-based access policy in place
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)?	▪ IRIS OpenPayslips allows the employee to view payslips, P60s and P45s ▪ IRIS OpenEnrol sends pensions communication directly to the employee via email, this contains personal data ▪ Data is sent from desktop software securely, using Secure Socket Layer (SSL) and Advanced Encryption Standard (AES), to the cloud service and published for the employee to view ▪ IRIS OpenPayslips stores data in Azure platform ▪ IRIS OpenEnrol stores data in Rackspace ▪ You and each individual employee can access that individual's personal data
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).	
1.6	How do you collect/receive the personal data? e.g. application form, secure online portal, password protected attachment via email	Personal Data is collected from the desktop payroll application and sent directly to the cloud platform For IRIS OpenEnrol, employees receive a copy of their pensions communications directly to their inbox. This is a TPR compliance requirement that the communications are not password protected. This is to prevent any 'barriers' to receiving communications
1.7	What procedures do you apply to ensure personal data is accurate and kept up to date?	Changes to personal data are complete in the desktop payroll application. No changes to personal data are processed via the IRIS OpenPayslips software. The responsibility for collecting

		information to publish lies with the person processing the data in the desktop software.
1.8	Do you automatically profile individuals? If yes, do you make decisions solely based on such automated processing, including profiling?	No
1.9	What procedures do you apply to ensure that no more than the personal data required is collected?	We only collect data that is essential for publishing payslips and pension letters in accordance with legislation and compliance
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?	In the context of our function as a data processor, we are required to keep customer data for the retention period agreed in the contract, which represents the customer's instructions to us. However, after the end of the provision of services relating to processing we must, at the choice of the customer, delete or return all the personal data to the customer and delete existing copies.
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?	▪ 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
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?	Use of removable storage minimal, no customer data is allowed to be downloaded from production environments
3.6	What protections are there against unauthorised copying, processing etc?	Password security is in place for user access, encryption for data in transit, limited IRIS employee access only given to those employees that are necessary. All datacentre environments are isolated from corporate ones – access is via an VPN with two-factor authentication. Backup procedures by Azure and Rackspace are also in place
3.7	What protections are there against accidental loss, damage or destruction?	We work with the principle of least privilege – developers and administrators are not allowed to work directly with live customer data, data is geo-replicated where possible
3.8	Do you have robust frequent data backup procedures?	Database data is fully backed up weekly, with differentials happening every few hours and transaction logs every 5-10 minutes. Object storage is geo-replicated to another Azure region. The internal Recovery Point Objective (RPO) is 6 hours. The Recovery Time Objective (RTO) is 48 hours. Note: backups are for disaster recovery only, we do not support individual customer restores
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.	▪ Microsoft Azure (primary location is Netherlands and secondary is Ireland) ▪ Rackspace (UK)
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**	
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. (Note: Product Managers ensure local procedures are in place to identify and escalate incidents in line with the above procedures)
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
5.5	To the extent not already set out above, what action have you taken to ensure compliance with data protection laws?	IRIS has an Information Security and Governance Group, which includes members of the Executive Committee and this is supported by divisional projects to ensure ongoing compliance by 25 May 2018 and beyond. We have conducted a gap analysis of all our products followed by a risk assessment
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. In the context of our processor activity this would be the customer's responsibility
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 above
6.6	What is the process for you to respond to requests to	As above

	rectify inaccurate personal data about an individual?	
6.7	What is the process for you to respond to a request under the right to be forgotten?	As above
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?	As above
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?	As above