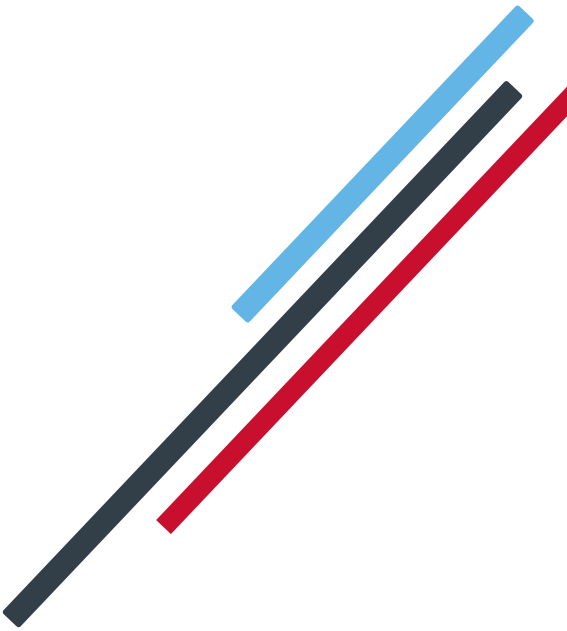
Data Protection after 25 May 2018

Helping you remain compliant using your Desktop Payroll

18th May 2018

Version: 1.0



Document Control

Version	Date	Amendment	Amended by
1.0	17/05/2018	▪ Initial Draft	Claire Treadwell
		▪	
		▪	
		▪	
		▪	
		▪	

Contents

Document Control **2**

Terminology and definitions **4**

Introduction **5**

Information you hold **5**

Who has access to the Desktop Payroll data? 5

Communicating payroll information to your employees **6**

For bureau / multi payroll company clients 7

How long do you retain personal data? 8

Subject access requests (SARs) **8**

Data breaches **9**

Data protection by design **9**

Data protection officers **9**

Useful links and resources **10**

IRIS 10

Information Commissioner's Office (ICO) 10

European Commission 10

Advisory, Conciliation and Arbitration Service (ACAS) 10

Chartered Institute of Personnel and Development (CIPD) 10

HMRC 11

Terminology and definitions

The definitions in this table may not be the official definitions given in the current legislation. It is your responsibility to seek legal advice relevant to your specific business circumstances. You can also find official advice from the Information Commissioner's Office www.ico.org.uk.

Term	Abbreviation	Definition and examples
Data breach	-	A breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data
Data Controller	-	Person or organisation responsible for determining the purposes and means of processing personal data and demonstrating compliance with data protection principles
Data processing	-	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
Data Processor	-	Person or organisation responsible for processing personal data on behalf of a data controller
Data Protection Impact Assessment	DPIA	A process to help you identify and minimise the data protection risks of a project.
Data Protection Officer	DPO	Officer responsible for informing and advising organisations about data protection, and monitoring compliance.
Information Commissioner's Office	ICO	The UK's independent authority set up to uphold information rights https://ico.org.uk/
Personal data	-	Any information relating to an identifiable person who can be directly or indirectly identified, for example, name, identification number, online identifier
Sensitive personal data	-	Special categories of personal data; for example, information revealing a person's health condition, sexual orientation or ethnic origin. It also includes genetic data and biometric data processed to uniquely identify an individual
Subject Access Request	SAR	A written request that entitles an individual to be: • Told whether any of their personal data is being processed • Given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people • Given a copy of the information comprising the data and details of the source of the data (if available)

Introduction

Data protection law is changing after 25 May 2018, beginning with the introduction of the General Data Protection Regulation (GDPR). GDPR expands on the Data Protection Act 1998, providing organisations with more accountability.

IRIS offer training courses regarding GDPR for both employers and employees. Click here for more information.

IRIS provides desktop payroll software, which is installed locally on your standalone PC or network. This means for data protection purposes, the company (i.e. the company you work for) is the Data Controller.

For desktop software, IRIS has developed functionality that will help you comply with your data protection obligations. However, you are responsible for complying with data protection laws. If you have other IRIS products, there are separate documents for each product which explain our responsibility in terms of data protection.

This guide will review the key areas you may wish to consider. This guide doesn't provide detailed information about data protection itself, nor advice on processes and legal issues, as this information is widely available from other sources (see Useful links and resources on page 10).

Information you hold

In your payroll, you hold information regarding your employees, which is classed as Personal Data. You may hold data in paper files or provided payroll data to other areas of the business. You may wish to review:

- How do you receive data?
- Where is it stored?
- Who do you send data to?
- How do you delete it?
- If it is accurate

Who has access to the Desktop Payroll data?

The personal data is stored on your standalone PC or network. It is important to ensure that only those who need access to the personal data can access the desktop payroll software and any folders that payroll information is stored in. For example, you could have a payroll folder on your network. You may need to speak to your IT department to establish who can access the payroll folders and the installation of your desktop payroll software along with their access privileges. Your IT department may need to update their IT security policy.

In the same folder as your desktop payroll software installation, there is the following information:

- Copies of RTI submissions made to HMRC in XML file format
- BACS files (if applicable)
- Pension files
- Any reports you save to the network

- You may wish to consider where your personal data is held. If it is outside the UK, data protection places restrictions on the transfer of data outside the EU. The ICO has detailed guidance surrounding this subject, click here to view

Communicating payroll information to your employees

You may wish to consider:

- Who do you provide payroll data to?
- Are you providing too much information?
- Do you provide personal data to third parties?
- How do you verify calls / communications from third parties are real?
- How do you provide personal data and in what format?
- How do you prevent personal data from getting into the wrong hands?

Payroll delivers personal data to employees, for example, payslips, P45s, P60s and Pensions communications.

IRIS have products available that can help deliver payroll information to employees in a secure environment:

Data items deliver	Product available	Key Benefits	Product Summary
Payslips, P60s and P45s	IRIS OpenPayslips	▪ Data is sent directly to the employee via a secure method – preventing delivery of personal data to the wrong person ▪ Data is encrypted ▪ No password information is visible to the payroll user ▪ Employees are responsible for their own account	▪ Payslips, P60s and P45s are delivered directly to the employee via an app to their phone or an online web portal ▪ Information is sent from the desktop payroll using Secure Socket Layer (SSL) and Advanced Encryption Standard (AES), to the cloud service and published for the employee to view ▪ Personal data is stored on the Microsoft Azure platform
Pensions communications	IRIS OpenEnrol		▪ Pension communications are delivered directly to the employee via an app to their phone or an online web portal ▪ Information is sent from the desktop payroll using Secure Socket Layer (SSL) and Advanced Encryption Standard (AES), to the cloud service and published for the employee to view ▪ Personal data is stored on Rackspace

For bureau / multi payroll company clients

When working in a payroll bureau, you have additional responsibilities in terms of delivery of client data, for example clients need to sign off payroll information and BACS.

From a bureau perspective you may wish to review how you send personal data to your clients, such as reports, and how you receive information. You could consider:

- How do you communicate with your clients?
- How do you prevent entering incorrect personal data?
- Are documents password protected and is the password strong enough?
- Do you send and receive data via email? Is this secure?
- How do your clients authorise payroll?
- How do you deal with third party requests?

Data items deliver	Product available	Key Benefits	Product Summary
Receiving client information, such as timesheets, variable pay data and static pay data	IRIS Remote Payroll Entry	▪ Prevents incorrect entry of data ▪ Data is sent directly to payroll via a secure method – preventing delivery of data to the wrong person ▪ Data is encrypted	▪ Clients enter payroll information into a desktop application ▪ Information is sent from the desktop app to payroll using Secure Socket Layer (SSL) and Advanced Encryption Standard (AES), to the cloud service and published for the employee to view ▪ Personal data is stored on the Microsoft Azure platform
Delivery and authorisation of client reports	IRIS OpenSpace	▪ Payroll allows delivery of reports directly to the secure portal – personal data can't be sent to the wrong client ▪ Data is encrypted Data can be approved online	▪ Information is sent from the desktop payroll using Secure Socket Layer (SSL) and Advanced Encryption Standard (AES), to the cloud service and published for the client to view ▪ Personal data is stored on the Microsoft Azure platform

How long do you retain personal data?

You may wish to consider how long you retain data for. Are you retaining it longer than necessary? HMRC stipulate:

'You must collect and keep records of:

- What you pay your employees and the deductions you make
- Reports and payments you make to HM Revenue and Customs (HMRC)
- Employee leave and sickness absences
- Tax code notices
- Taxable expenses or benefits
- Payroll Giving Scheme documents, including the agency contract and employee authorisation forms

Your records must show you've reported accurately, and you need to keep them for 3 years from the end of the tax year they relate to. HMRC may check your records to make sure you're paying the right amount of tax.'

Failure to comply with the HMRC legislation may result to fines of up to £3,000.

You could review how you manage and maintain your data:

- Do you keep paper records?
- How do you keep them?
- How many tax years of data have you retained?
- How often do you dispose of the data?
- How do you dispose of data? Do you use a secure supplier to dispose of data?

Subject access requests (SARs)

Individuals have a right to see the information an organisation holds about them. According to the ICO, they are entitled to know:

- If any personal data is being processed
- A description of the personal data, the reason it is being processed, and whether it will be given to any other organisation or people
- Given a copy of the information comprising the data; and give the details of the source of data (where this is available)

In most cases SARs need to be responded to within 1 calendar month. There some exemptions to SARs the ICO website provides further details on this and a SAR checklist.

You may wish to consider how to provide data to individuals should you receive a SAR. You could review the standard reports available in your system and note which ones you could use.

Data breaches

Employers must report any breach personal data breach, which would result in a risk to your data subject (such as your employees) to the relevant supervisory authority within 72 hours of becoming aware of the breach, where feasible.

For more information on reporting data breaches refer to the official guidance from the regulators.

To help you review your procedures, you could use the following areas of your IRIS system:

- Audit features
- Standard Reports

Data protection by design

Data protection by design means that you protect your data as part of your everyday processes. You may wish to think about the activities you conduct as part of your role and how you could incorporate data protection. You could conduct a risk assessment of your current processes and review your use of personal data against the data protection principals and data subject rights. The ICO has more information about this subject.

Data protection officers

Certain organisations require a Data Protection Officer. Consult official advice to see if your organisation is required one. Further guidance on the subject can be found here.

Useful links and resources

You can find more information about data protection online via the links listed below:

IRIS

- Getting Ready: https://www.iris.co.uk/insight/blog/payroll/2017/may/how-are-iris-getting-ready-for-the-introduction-of-gdpr/
- What is GDPR?: https://www.iris.co.uk/insight/gdpr-hub/
- IRIS GDPR Training Course: https://www.iris.co.uk/insight/gdpr-overview-training-and-guidance/
- GDPR health check: https://www.iris.co.uk/campaigns-sme/free-iris-gdpr-health-check/
- IRIS Group Data Protection Policy: https://www.iris.co.uk/assets/Terms/DATA-PROTECTION-POLICY-v1-1.pdf
- IRIS OpenPayslips: https://www.iris.co.uk/cloud-solution/iris-openpayslips/
- IRIS OpenEnrol: https://www.iris.co.uk/cloud-solution/iris-openenrol-and-automatic-enrolment-module/
- IRIS Remote Payroll Entry: https://www.iris.co.uk/cloud-solution/iris-remote-payroll-entry/
- IRIS OpenSpace: https://www.iris.co.uk/cloud-solution/iris-openspace/

Information Commissioner's Office (ICO)

- Guide to GDPR: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
- Preparing for the GDPR: https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf
- Getting ready for the GDPR: https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/getting-ready-for-the-gdpr/
- Exemptions: https://ico.org.uk/for-organisations/guide-to-data-protection/exemptions/
- SAR Checklist: https://ico.org.uk/for-organisations/subject-access-request-checklist/
- Data Protection Officers: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/
- Conducting Impact assessments: https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf
- International Transfers: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/

European Commission

- Article 29 working Group: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358

Advisory, Conciliation and Arbitration Service (ACAS)

- GDPR is coming for you!: http://www.acas.org.uk/index.aspx?articleid=6083

Chartered Institute of Personnel and Development (CIPD)

- GDPR in the work place: https://www.cipd.co.uk/knowledge/fundamentals/emp-law/data-protection/gdpr-factsheet

HMRC

- PAYE and payroll for employers: https://www.gov.uk/paye-for-employers/keeping-records