IPPEX GLOBAL

GPA
global payroll association
Supporting payroll professionals around the world

Implementing EU General Data Protection Regulation (GDPR) in your global payroll operation

November 2016

Contents

Executive summary

Recently a series of stories concerning high profile and large scale data breaches in consumer based businesses have hit the press. This white paper has been specifically written for organisations with EU employees and addresses the potential data breaches that could arise from payroll processes.

The aim of General Data Protection Regulation (GDPR) is to protect all EU citizens from privacy and data breaches in a data driven world - one that is very different from the time when the 1995 Data Protection Directive was established. Many of the key principles of data privacy from the previous directive still apply, but several changes have been proposed to the former regulatory policies.

This paper will examine the key effects on payroll processes. Payroll encompasses a vast set of personal data and organisations can be too relaxed about the way they transmit this information within and outside of their organisations.

EU fines for data breaches have increased exponentially to up to 4% of global turnover, or €20 million (whichever is higher). This is applicable to both the company and their providers.

Data privacy is the responsibility of the organisation as a whole - it is not just an IT issue - as the biggest risk lies in the process and with the users in an organisation and its partners.

IPPEX Global, the author of this white paper, has had much experience of global payroll environments where the business has focused on the IT security and has not addressed the data risks posed by users and the process. With a background of delivering global payroll data systems and government security, IPPEX Global addresses the challenges presented by the new EU regulation on global payroll.

This white paper is published by Global Payroll Association (GPA), which strives to keep payroll professionals one step ahead of global and in-country developments in payroll.

A general overview of GDPR can be found at www.eugdpr.org.

Why is GDPR important to payroll?

This white paper will address the areas of risk pertaining to global payroll operations serving employees within the EU and provides guidance to prepare organisations for GDPR which comes into effect on 25 May 2018. By their very nature and because of their responsibility for handling personal information, HR and payroll organisations have to adhere to GDPR.

GDPR is applicable to all businesses within the EU and focuses on the exchange of data between employees, employers and payroll providers. This includes anyone handling the personal data of an EU-based individual from outside EU borders. .

Penalties for not complying with the current data protection regulations

Fines can be imposed on an organisation for failing to adequately manage their data. They can be considerable - up to 4% of the global turnover of a business, or 20 million (whichever is greater).

GDPR applies to a number of key personnel in payroll including:

- **The controller:** The employer who says how and why personal data is processed
- **The processor:** The person or organisation who acts on the controller's behalf, for example, the employer's payroll administrator, a payroll provider, or a company that supplies the systems which support the payroll process
- **The subject:** The employee
- **The data protection officer (DPO):** An individual who has extensive knowledge of data privacy laws and standards
- **The third party:** An individual or organisation who under the direct authority of the controller or the processor is authorised to process the data

Who is responsible for data protection within your organisation?

There are new obligations for processors under GDPR. For example, they are required to maintain records of personal data and processing activities. They will have significantly more legal obligations and liability for data breaches under GDPR.

GDPR places further obligations on controllers to ensure that contracts with the processors comply with GDPR.

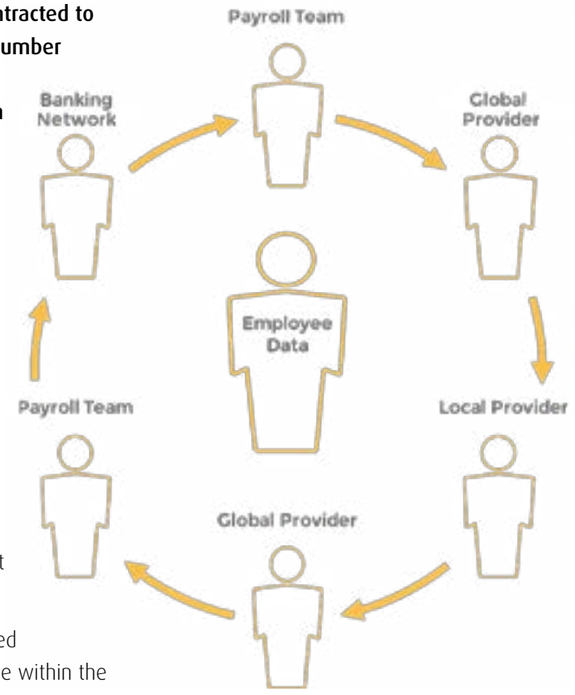
Did your payroll operations actively respond to the 1995 Data Protection Regulations and have you reviewed your processes when systems and contracts have changed over the years? If not, now is the time to address the shortfall.

How GDPR could affect a global payroll operation

Case study

This example demonstrates the potential complexity and supply chain of data events for a given employee.

The employer (controller) has a payroll team that prepares payroll data for a global payroll provider who has been contracted to deliver statutory processing. The employer uses a number of third party applications to store and manipulate data, including a document management system in the cloud. The cloud system, as a third party to the employer, has an obligation to secure that data.



The global payroll provider will also utilise third party systems to manage and store data, such as document management systems. These may also be held in the cloud.

The global payroll provider may use country specific payroll companies to undertake the statutory calculations for the payroll processing. These organisations employ local payroll processing engines and allow document storage. Payments to employees are made through banking portals, which could be housed outside of the EU, even if the recipient is within the EU.

The employer and global payroll provider could be based outside of the EU, yet the final processing point could be within the EU, managing payroll affairs for EU citizens.

The notification of a data breach may have to travel from the end of that data chain through to the data controller within a 72-hour time period. The data controller has the responsibility to ensure that the necessary measures have been taken to minimise the risk of a data breach for the entire data chain.

The employer has to understand all of the data touchpoints by person, end-to-end process and systems in the entire payroll process. Contracts with any third party organisations need to be reviewed and adjusted to take the regulations and penalties into consideration.

“Do you really know who all of the organisations accessing your data are, and how often should you audit them?”

Areas of risk for payroll

Users

GDPR Article 33 has significantly strengthened the Data Protection Impact Assessment stating that the "entire lifecycle of the data must be accounted for". One of the new requirements is "an explanation of which data protection by design practices have been implemented". Whilst this applies to all aspects of the payroll process, the users are a significant risk within the data lifecycle, where a user could become inadvertently compromised by an 'outside' organisation.

The majority of the risks arise from business users (processing users). Some are accidental and others are targeted - the outside user becomes an 'insider'. A significant proportion of these outside users who are gaining access are doing so via the forced human error of an insider user. Investments in firewalls, intrusion detection and other IT security measures do not necessarily prevent a third party accessing systems by impersonating an internal user.

An outsider could also move from one user to another and eventually gain access to the systems that hold personal data, for example. This could be done by using malware to obtain user and password credentials.

Developments are being made at present into software to detect unusual user activity, time of login, systems being used and the behaviour of users. For example, allowing for security threats to be detected whilst a user is away on annual leave.

The risks of lone users breaching data privacy still exists. This can be partly addressed with role segregation, privileges and controlled access rights. Adding workflow controls and other measures, such as an audit trail of access and changes to data and managing the exposure of a data breach, can improve compliance.

This area of insider risk cascades through the data chain, from the employer to the global payroll provider and sub-contract local payroll vendor level. Hiding behind an organisation's international standards accreditation, such as ISAE 3402 or ISO 27001, is no longer enough when it comes to GDPR.

Processes

GDPR Article 30 ***Security of Processing***, has been expanded to focus on the security policies, stating that the "the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing".

One of the new requirements is that the security policy shall include "the ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data".

It is surprising how many users do have access to payroll data. A good starting point is to map out the end-to-end payroll process, listing all of the personnel and systems at each stage of the process.

GDPR talks about minimising the data needed for a given task. The initial focus here is minimising the number of people who may have access to some or all of the payroll data. This is easier to achieve within the employer organisation, but is harder to achieve externally when there is a dependency on provider partners to enforce the same rigour when minimising the access to data. They too have to share their detailed processes and justify why specific users have the need to access personal information about employees. They also have to exhibit the same controls when it comes to employee data.

The handling and transfer of data

One of the biggest risks in the payroll process is associated with moving data outside the boundaries of the company to third party payroll providers and banking institutions. In many organisations the data is transferred by email and spreadsheet files may not be encrypted or password protected. The exchange of information should ideally take place through a portal or document storage system where the data is encrypted on transfer.

Offshoring of payroll processing has to be reviewed in light of the broadening scope of GDPR in Chapter 5: ***Transfer of Personal Data to Third Countries or International Organisations.*** Of the many new clauses and requirements, the commission addresses a new requirement for "contractual clauses between the controller and the recipient of the data authorised by a supervisory authority" in Section 42 on the ***Transfers by way of Appropriate Safeguards.***

Section 43: ***Transfer by way of Binding Corporate Rules*** lists what must be contained in the binding corporate rules. The onus is on the controller to ensure the contracts with any third party organisation are appropriate for GDPR.

Manipulation of data

During the preparation of payroll changes data, multiple data sources may be merged together or re-keyed into another template. Too often a temporary copy of the file is stored locally on the hard drive of a user's computer, resulting in the duplication of personal information which is unmanaged and often forgotten. Enforcing the use of a secure document store or file system is essential for minimising data duplication.

Article 23 on ***Data Protection by Design and by Default*** introduces a new requirement for data minimisation and the minimum length of time data is held. Whilst payroll is constrained by legislative rules regarding access to payroll history, a review of this area is important.

Assessing the minimum data set needed for a provider to process the payroll is the first step to addressing data minimisation. For example, if the provider is not making employee payments then they do not need the employees bank details.

Redundant data

It is important to remove data from systems when it is no longer needed, although it is important to strike a balance when holding payroll data for a period of time, especially to meet each countries statutory requirements. A judgement has to be made on how much historic information should be held by the organisation and consideration should be given to how easily data can be removed, as it will become an obligation.

Systems

Data is held in systems and systems have to be secure. GDPR Chapter 4 Section 2 on ***Data Security*** addresses the security of processing, notification and communication of a data breach.

IT services provision should take care of firewalls, intrusion detection systems, intrusion prevention systems, security testing and every other measure associated with cyber attacks. But who is examining the weaknesses in the payroll systems and associated processes? These areas of risk are as relevant to the employer organisation as they are to a third party, so any assessment of risk should cascade down through the systems and organisations that participate in the end-to-end payroll process.

There are a significant number of areas to address. Ultimately an organisation has to take a practical approach to understand, evaluate, mitigate risk and to assess the risk in any given scenario. To completely lock down system access could inhibit the process or add significant cost to the service.

Password protection

There are a number of important areas to address when it comes to password protection:

- **Individual user accounts:** The processes in place for user accounts in some global providers' subcontract partners may not be as rigorous as those of a corporate organisation.
- **Process for leavers:** The processes in many corporate organisations are strong and follow a number of steps to disable access to systems. There is a risk that when users interact with third party providers, accounts and privileges may persist after that user has left the organisation.
- **Single sign on:** Extending the use of single sign-on to internal and external systems is a good way to reduce the burden of disabling access rights to multiple systems.
- **Enforcement of password complexity and frequency of password change:** Significant progress has been made in many organisations in this area. However, it is important to review all of the systems being used by the controller organisation as well as the third parties

Encryption

This has become a complex topic in the world of transactional systems. Information almost never travels from point to point. It is routed from server to server around the internet until it reaches its destination, not always taking the same route. If data isn't encrypted it is available for anyone and everyone to read along the way.

There are many types of encryption and many different points where it should be implemented including the transport layer, the web, email, data at rest encryption and multi-tenant databases. Unfortunately, there are no 'one size fits all' scenarios, but it does need to be considered, or it could be the weak link in the chain.

Privilege access control

Most payroll systems offer the facility to limit the access and rights to specific functions and data within the system. All too often, users are given more rights than they need, to reduce the burden of managing the user access controls. GDPR will push organisations to review the current user rights management and whether it is sufficient to reduce the risk of a data breach or provide the highest level of compliance.

Conclusions

In this white paper, a number of areas for consideration have been highlighted. The process of preparing an organisation for GDPR will take time, therefore it is advisable to make an initial assessment as soon as possible.

Many of the steps are logical, although detailed knowledge is required of the entire payroll process environment. The global payroll and finance leadership should set out a programme to assess the readiness for GDPR and to have a continuous process of reviewing the organisations GDPR compliance.

Next steps

- Assess the risks associated with users, processes and systems for both your organisation and your providing partners and put an action plan together to mitigate those risks
- Establish a payroll data breach reporting process escalation plan compatible with the corporate reporting process which includes third party payroll partners
- Review your partner agreements in light of the regulations ensuring that they adequately cover the responsibilities and liabilities of the third party provider organisations
- Establish a communication process for your employees addressing the rights to the subject (employee) to request access and information about the personal data held by the employer. This includes the employer (controller) who has an obligation to address corrective requests from the employee where there is a potential risk of a data breach

All businesses operating with subjects in the EU should establish a corporate process for monitoring and detecting data breaches. The goal is to integrate your payroll organisation with the corporate monitoring and detecting process.

“The key is to understand the risks, plan for the unexpected and be prepared”

About us

IPPEX Global

IPPEX Global delivers independent consulting to businesses with global payroll portfolios. Helping businesses to understand how to manage, own and deliver global payroll, utilising industry best practice and technology. IPPEX Global was formed of global practitioners who have operated in the provider environment serving Fortune 500 businesses.

Our services include pre-procurement and procurement consultancy, project management, process improvement, data security and GDPR readiness. Our step by step, internal information security evaluation will help ensure your business meets both the requirements of partner organisations and industry compliance standards. We help prepare your organisations payroll facility for GDPR. Determining business readiness, recommending compliance improvement changes and helping to set-up the processes for data breach notifications, monitoring and risk assessment.

www.ippexglobal.com

Global Payroll Association

Global Payroll Association is the first international payroll association of its kind. It is a central hub for 'all-things payroll' and a one-stop-shop supplying comprehensive directories, interactive training and in-depth country resources.

It is here to help payroll and HR professionals with their international payroll needs, no matter how complex, connecting them with the world's leading experts and offering a forum to network with other like-minded global professionals. The Global Payroll Association welcomes international payroll, HR and financial professionals of all levels.

www.gpa-global.org

Contact us

Kevin Tonner
Chief Security Office
IPPEX Global Limited
+44 (0)203 287 1234
kevin.tonner@ippexglobal.com

Melanie Pizzey
CEO
Global Payroll Association
+44 (0)203 871 8870
melanie@globalpayrollassociation.com

Sources

- GDPR Portal: www.eugdpr.org
- International Organisation for Standardisation: www.iso.org/iso/home.html
- ISO/IEC 27001:2013: www.iso.org/iso/catalogue_detail?csnumber=54534
- ISAE 3402: http://isae3402.com/ISAE3402_overview.html

www.adworksdesign.co.uk

Written by IPPEX Global
Published by Global Payroll Association