What does Europe's new data protection law mean for global payroll managers?

By ***Beverley Flynn*** *head of data protection, and*
Ayesha O'Connor, *associate,* ***Stevens & Bolton LLP***

As of 25 May 2018, the European Union's new General Data Protection Regulation - widely referred to as the "GDPR"- will alter the rules for how organisations collect, store, process, use or share so-called personal data, which includes employee information. Outlined below are some of the key changes and implications for HR and payroll professionals whether located in the European Union or beyond.

What is the GDPR?

The GDPR is a European Union (EU) regulation that will replace the existing Data Protection (DP) Directive and impose new DP rules across the region and beyond. Compliance will be mandatory for businesses if they are operating in, or providing services to, the EU, whether they are located there or not.

For HR and payroll managers, the good news is that, in theory at least, the GDPR will introduce a single set of DP standards that apply in a largely uniform manner across all EU countries. But the new legislation will also introduce more stringent requirements, which means they may need to adjust their DP policies and procedures as a result.

Why is the GDPR significant?

The new rules will have a broader territorial scope than the existing DP Directive. Moreover, some of the new legal obligations will apply not only to employers that control the use of personal and

employee data, but also to third party data processors such as outsourced payroll service providers.

How is the GDPR likely to affect organisations operating in Europe?

Payroll providers offering services that affect individuals located in the EU (even if they are headquartered outside of the EU themselves) could be caught by the broad territorial scope of the new requirements. In other words, non-EU-based payroll companies that process data on behalf of EU-based and certain non-EU based customers could be just as subject to the GDPR as organisations that actually employ workers within EU countries.

It is also worth noting that, although DP regulations will be largely harmonised throughout the region, each country has the right to put in place its own additional rules on processing employees' personal data. Therefore, standards could vary. ▶

"The new regulations will impose direct legal obligations on data processors such as outsourced payroll providers, many of which are not directly subject to existing local data protection laws derived from the Directive."

How is Brexit likely to affect the situation for organisations operating in the UK?

In spite of the recent referendum decision for the UK to leave the EU, the country's legal relationship with the EU has not yet changed. EU legislation continues to apply as it did prior to the vote and will continue to do so for as long as the UK remains a member.

If the UK is still part of the EU on 25 May 2018 when the new regulations come into force, the GDPR will apply - and will continue to do so for as long as the country remains in the EU. But even if it does leave, the GDPR is likely to be replaced with equivalent legislation and many UK businesses would continue to fall within its scope because of its broad territorial application.

What key changes will GDPR bring for the payroll industry?

The new requirements will lead to several key changes:

1. New obligations on outsourced payroll providers

The new regulations will impose direct legal obligations on data processors such as outsourced payroll providers, many of which are not directly subject to existing local DP laws derived from the Directive. Data processors will be required to comply with certain legislative requirements and will become liable to fines. They will also be required to compensate individuals if they are non-compliant.

2. Registration/notification and one-stop-shop mechanism

The existing notification regime, whereby organisations register with the regulator and in some circumstances pay a fee, will be replaced with the "accountability" principle. This principle will require those dealing with personal data to take more proactive compliance steps.

Due to a new one-stop-shop mechanism, data controllers and data processors that carry out cross-border processing will generally only have to deal with the regulator in the country of their "main establishment". Therefore, payroll processors will need to ascertain where this is for the purposes of the GDPR.

3. Policies and procedures

Data controllers will be required to adopt internal policies and procedures that demonstrate compliance with the GDPR. They will also need to show that they are taking steps to implement privacy measures into projects early and by default. Where processing carries a high risk, data controllers will also need to conduct risk assessments known as "Privacy Impact Assessments" and consult with the regulator before processing starts.

4. Record-keeping

Organisations will need to document their DP activities and make their records available to the regulator upon request - although if they have fewer than 250 employees, they may be exempt from this requirement.

5. Data protection officers

In certain circumstances, organisations will be required to appoint a DP officer (DPO) with expert knowledge. DPOs will benefit from having an enhanced protected employment status. This means that they must be allowed to perform their duties independently and cannot be dismissed or penalised for simply doing their job. It will be possible to appoint a single DPO for group companies operating across the EU.

6. Mandatory breach notification

In certain circumstances, reporting data breaches will become mandatory. Data controllers will need to let the regulator know about all breaches within 72 hours of them taking place, unless they are unlikely to result in a risk to individuals.

A breach posing a high risk to their rights and freedoms will have to be reported to the individuals concerned, unless steps have already been taken to encrypt the data or otherwise minimise risk. Data processors will also need to notify data controllers of any breach without undue delay as soon as they become aware of it.

7. Increased financial penalties

Organisations, including payroll processors, will be at risk of new and larger fines if they breach the regulations. The maximum fine for some of these breaches will increase to E20 million ($21.7 million) or four per cent of the previous year's annual worldwide turnover, whichever is higher.

How can payroll departments or service providers best tackle this legislation?

- If acting as an outsourced payroll processor, be aware that the GDPR will apply directly to you for the first time
- Make decision-makers in the organisation aware that the law is changing
- Be aware of the territorial reach of the GDPR both within and outside the EU
- When appointing payroll processors, review contracts to take account of the new requirements
- Document all of the personal data that the business holds
- Identify and document the types of processing that is carried out, where personal data comes from and with whom it is shared in order to ensure accountability
- Review existing privacy policies and procedures and plan for any necessary changes
- Consider appointing a dedicated DPO, if required.

Beverley Flynn is a partner at Stevens & Bolton and leads the firm's data protection practice. She regularly advises on international transfers, data protection policies and other data issues such as freedom of information.

Ayesha O'Connor is an associate at Stevens & Bolton and regularly works on issues surrounding data protection and privacy. She also drafts and advises on commercial contracts.