GDPR

What's it all about?

Declan McMahon

VP Client Services, OrangeHRM

GDPR - What's it all about?

General Data Protection Regulation (GDPR) comes into force in Europe from 25 May 2018. This is all about strengthening and unifying data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU, enforces penalties for breach and defines stronger conditions for consent. As a HR department, you're storing personal data on your employees – and job vacancy candidates – so if you have staff in Europe, you have a legal responsibility for how you process this personal data.

HR Management software solutions provide you with the tools to effectively manage personal data and assist with adherence to GDPR – but your processes are just as important as the tool that you use. This white paper looks to provide you with some background on GDPR and to provide you with some pointers on what you need to look for in your own processes and procedures to ensure you remain compliant.

Your First Steps

The core concepts of GDPR are straight-forward – you're holding personal information about individuals and you have a responsibility when you do that.
Someone within your organisation needs to have responsibility for this. Certain organisations even need to go further than this and appoint a person with very specific responsibilities – the Data Protection Officer (DPO).

If you're reading this article, you may well be the person in your organisation that needs to take this responsibility – or perhaps you need to speak with management to ensure someone is assigned. In either case, we've included some links to reference material below that might help.

Every GDPR compliance journey is likely to start with a review of what personal data exists within the business, coupled with the analysis of where it might be stored. Make an inventory of the personal data your organisation holds on its employees – or on candidates that have applied for jobs at your company. Remember that this information may be scattered across different systems from HRM to payroll to legacy systems; from paper-based files to electronic spreadsheets. If you're a geographically distributed organisation, there may be implications with personal data being sent to other locations – and the concepts of GDPR still apply if data breaches occur at secondary locations.

Consent

To process personal data, you need to have the consent of the individual. GDPR is very clear that consent cannot be implied – it must be "freely given, specific, informed and unambiguous".
For most organisations, this is already in place through existing processes for employees. But perhaps the introduction of these new guidelines is a timely reminder to re-validate that

this is the case. For example, the traditional response to an unsuccessful job application frequently includes the statement "… but we'll keep your CV on file". This could well have you in breach of GDPR consent requirements– has the individual provided proactive consent to allow you to keep the personal data included in their CV on file?

Individual Rights

At its heart, GDPR is about protecting the rights of individuals (think employees and job candidates). GDPR provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

This is as much process as technology – technology just provides a central management framework to control and aid compliance. You need to think about the processes you've defined for your business both to instruct staff who are handling personal data and to inform employees of how their personal data is being managed (and for what purposes).

Questions to ask

- Have you correctly informed people why you are collecting data and what you are doing with it?
- Do you have a process by which an individual can get access the personal data you store?
- How do you provide employees with the right to be forgotten?
- Are you using any automated tools for staff profiling and have you informed staff and provided them with a right to object?

When it comes to employee data, you need to balance the regulatory requirements to retain historical employee data for a period of time with the employee's right to be forgotten. It's key that you clearly define your policies and procedures, understand your regulatory requirements and select the technology solutions that best enable you to execute your policies.

Key Pointers

Governance & Best Practices

The core principles of accountability and governance have already been present in data protection regulations but GDPR puts a firmer focus on them. Organisations must be able to

show that they're taking steps to ensure compliance – from data audits, policy definitions and staff training.

Transfer of Data

GDPR recognises that personal data may be transferred outside the EU and it defines certain restrictions and requirements when this occurs. In an electronic world, data transfer is no longer about a physical document – sometimes organisations forget about international offices and the access they may have to EU-employee personal data. All this must be reviewed and considered in the definition of the policies and procedures.

Breach Notification & Penalties

GDPR enforces clear responsibility in relation to the reporting of data breaches – whether this is to the supervisory authority or the individual. Organisations can no longer "bury their heads in the sand" if a problem arises.

Non-compliance with GDPR can result in significant implications:

- Written warning for first and non-intentional non-compliance
- Official audits
- A fine of up to €10 million or 2% of annual worldwide turnover (whichever is greater) for serious breaches
- A fine of up to €20 million or 4% of annual worldwide turnover (whichever is greater) for very serious breaches

How OrangeHRM Can Help You?

The very act of deploying a new HR Management solution forces your organisation to think about its data protection policy. Perhaps today your personal data is scattered across different systems or servers, in unsecure systems.

Not only is it necessary to think of the data, it's also necessary to re-evaluate the business processes in place in your organisation and the way in which your staff handle personal data. Consolidating to a commercial-grade HR management solution will require a full data audit and a re-evaluation of your HR business process – and will enable you to take advantage of the industry best practices that these HR management solutions provide. The technology choices alone are insufficient to enable GDPR compliance – GDPR requires strong process definition and adherence coupled with clear corporate policies and precise communication.

OrangeHRM can provide you with the technology infrastructure to support your HR management needs. We offer a state-of-the-art HR management solution with a ten year track record, a global footprint and a history of professionalism. One of our key strengths is our global reach with a comparable customer-base in Europe and North America.

While OrangeHRM already provides an extensive range of data protection capabilities – from role-based access control to data encryption; from tools publishing corporate policies to data management with extensive audit logs – OrangeHRM continues to extend and expand our capabilities to provide state-of-the-art functionality around data protection.

Recently, we have introduced a series of new capabilities, including:

- The ability to request explicit acknowledgement from employees to published policies and procedures to ensure you have a record that employees have proactively consented to your corporate policies.

- Job application consent where you can outline your data policy and require an explicit check in the checkbox before allowing a candidate to apply.

OrangeHRM is committed to not only aiding your organisation in GDPR compliance but in providing value-added functionality to minimise your investment costs to ensure ongoing compliance. Look out for the introduction of new and exciting features from OrangeHRM in the lead-up to May 28, 2018.

Beyond Your Employees

While this white paper focuses on the implications of GDPR on your employees and job vacancy candidates, your organisation may well be storing personal data on your customers and your partners. Be sure to inform the right people in your organisation of their responsibilities related to GDPR.

More information?

If you require more information on what steps your organization should take, please contact Lucy French at lucy@orangehrm.com

Reference Material

- http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf
- http://www.eugdpr.org/
- https://en.wikipedia.org/wiki/General_Data_Protection_Regulation
- https://www.dataprotection.ie/docimages/documents/The%20GDPR%20and%20You.pdf
- https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

Please note: The content of this whitepaper provided is for information purposes only and does not contain or constitute legal advice. Please seek appropriate legal guidance and advice for future steps.