General Data Protection Regulations - Recruitment Consultant Guide

Securing business and client data is a responsibility that goes beyond best practice: it is a legal obligation. In 2018, **new legislation** comes into effect which governs the standards for processing, protecting, and storing personal data throughout the European Union.

This initial paper examines the legal implications of the new **EU General Data Protection Regulations (GDPR)**, and identifies the best practices for handling data and responding to security breaches.

In the next paper, we'll also considers some of the ways recruiters will be able to remain compliant with the new laws.

Section 1: What is GDPR?

The European Commission created GDPR to unify regulatory standards relating to the use of digital data within the EU nations. GDPR **comes into effect on 25th May, 2018**.

The new framework has a broader scope than its predecessor, the EU Data Protection Directive (DPD). The new standards take into consideration recent developments in **globalised markets** and technologies, and will address factors as diverse as non-EEC enterprises, social media, and **cloud computing** services. GDPR will affect not only organisations that operate within the European Union, but also their trading partners across the globe. For recruiters, understanding the terms of the new regulations before they become law will avoid disruptions to business activity.

New responsibilities for data managers and processors under GDPR will include:

- Implementation of **privacy by design**
- Completion of privacy impact assessments
- Transparency and willingness to submit to independent audit
- the mandatory reporting of security breaches

GDPR is applied to all data managers, controllers and processors who use or retain information relating to a living person, who is known as a **data subject**. Any organisation that must currently demonstrate EU DPD or UK Data Protection Act (DPA) compliance will also be required to implement the new GDPR standards.

1.1 Global reach

For the first time, EU data regulation will also apply to business partners and service providers of **EU businesses and citizens** based outside the EU. For example, this means that organisations that are domiciled in the United States of America and provide goods or services to EU citizens must also demonstrate GDPR compliance.

1.2 Requirements and obligations

Regulated organisations will now be expected to undertake a **Privacy Impact Assessment** whenever they choose to implement changes to their data management systems and processes, or when processing large volumes of data. Assessments are also required when the use of personal data may pose a risk to the freedoms and rights of individual data subjects.

The **reporting of security breaches to a relevant authority** will become mandatory under GDPR. As the commercial value of personal data increases, so too does the threat of malicious attacks. GDPR seeks to encourage a rapid response from data handlers whenever a system may have been compromised.

One of the key changes introduced by GDPR is the concept of **privacy by design** planning. This means that software developers and service providers will be required to demonstrate that elements of data protection and security are built into products and services throughout the developmental phase.

A key concept of privacy by design is removing the need to transfer the control of private data from the individual to the processor or manager. This allows data subjects to control which elements of personal information can be accessed – and by whom. Cryptography and two-factor authentication are some of the technologies enabling businesses to achieve this objective.

1.3 Penalties for non-compliance

GDPR provides Office of Data Protection Commissioner (ODPC) regulators with increased powers to enforce standards. These include stiffer penalties for non-compliance.

Businesses that are shown to be non-compliant with GDPR standards are liable for increased fines and penalties. Some of the changes will already be standard practice for many commercial entities; others will require new approaches to the way companies manage their databases.

Penalties for non-compliance with GDPR are progressive, and the most serious or intentional infractions are punishable with the highest fines. Breaching the data handling standards of GDPR will incur a penalty of €10M or 2% of global turnover – whichever is higher. A failure to keep sufficient records of data usage - or failing to notify authorities of a security breach - would result in a €10M (2% of turnover) fine.

Where serious infractions have occurred a fine of up to €20M or 4% of global turnover may be imposed. Again, the higher of the two figures applies. This higher tier of penalty may be used when organisations violate core concepts of GDPR, such as neglecting privacy by design obligations, or by failing to obtain data subject consent before storing, managing or processing personal information.

Section 2: GDPR and recruitment

In section two, we look at how updated GDPR rules will help to shape **data usage and digital security within the recruitment industry** through the coming years.

2.1 Why data protection?

Securing data is one of the primary responsibilities of businesses in the twenty-first century. Few working in the recruitment industry will be surprised to learn that **security factors as one of the top considerations for firms** across all sectors, when procuring a new software product.

As recruiters, we conduct our business affairs in a world of ever-expanding interconnectivity: where individuals and organisations seek candidates, contracts, and services across both technological and geographical boundaries.

Often, we use personal data to authenticate our commercial interactions. This personal data is stored by our clients and service providers, and may then be used to inform their own commercial strategies and planning.

Data has become a valuable commodity in its own right.

As recruiters, we specialise in understanding the value of people. Our core duty is to connect people with positions, to achieve improved outcomes. Many recruiters will consider their client data as the lifeblood of this process, and of the entire industry. Most firms retain vast databases, often containing many thousands of data subjects at any time. It is therefore imperative that businesses understand the new rights afforded to their data subjects before they come into effect in 2018.

2.2 Managing and processing data: what role do recruiters play?

EU regulation distinguishes between the management and processing of data; where *management* is the collection, storage and accessing of data, and where *processing* is the act of extracting value from raw data, and transforming it into information which businesses may act upon.

A modern recruiter is part data manager, part data processor. Understanding the responsibilities of each is important.

It is the responsibility of each organisation to manage its own data in a secure fashion: either in-house, or by utilising **a trusted off-site service provider**. Regulation compels businesses to take appropriate measures and remain compliant with the current data protection standards, yet how one can accomplish this is not solved by a

single approach, because technologies are constantly evolving. Increasingly, recruiters are outsourcing data management duties while accepting the duties of data processors.

GDPR will have a far-reaching effect on the recruitment sector. Understanding the regulatory changes will help every enterprise to remain secure, and allow them to begin implementing strategies for the next generation of data management.

2.3 Who is protected?

Every EU citizen is considered a data subject under GDPR regulation. The new rights for data subjects include:

- Access and portability: individuals may request a copy of their own data in any digital format
- the **right to be forgotten**: individuals can require any organisation erases their personal data, if they are unable to demonstrate a legitimate reason for its retention.
- Right to information: **individuals must be notified if their data is the subject of a security breach**.
- Ability to restrict or prevent the processing of one's own data

2.4 Achieving GDPR Compliance

The new regulations have been devised as the next step in an evolutionary development, rather than a top-down reformation. As such, most organisations will already be wholly or partially GDPR compliant thanks to existing data security laws. For many recruiters, compliance may require little more than changes to client contracts and terms of service agreements, and the willingness to submit reports when required.

However, **where firms have delayed implementing modernisation strategies, the requirements may be more wide ranging**. GDPR represents an ideal time for enterprises to update their systems for a modern, interconnected workplace. The benefits of using an up-to-date software service will go beyond either legal requirements or data security concerns. Efficiency and added functionality will aid the day-to-day activities of any business, and conserve both time and resources.

In the final part of this report, we detail specific operational and cost benefits which are available to recruitment specialists, and how an integrated software solution can assure every business that it will achieve GDPR compliance.

Section 3: Software solutions

Every enterprise plays a small part in a much larger ecosystem. The modern business is a service provider that has learned to integrate itself within a complex and decentralised network of organisations. Digital technologies allow organisations of all sizes to compete and collaborate on an even footing, and on a global scale.

The internal structures of a modern organisation reflect this outward environment. Enterprises are changing: even our most fundamental services - from filing to mailing - can be outsourced to an off-site service provider. In section 2.2, we discussed the distinct roles of data managers and data processors. We concluded that it can be problematic to try and distinguish between the two roles.

Similarly, when we are considering a company with a less formal internal structure, how can we assure ourselves of data security compliance? When more than one service provider is undertaking tasks concerning aspects of data management and processing, who is responsible when a breach occurs?

These are some of the questions that have helped to formulate the GDPR regulations as they will appear, and which will be explained in the final part of this paper. The complexities of unpicking an integrated relationship such as that shared by a Software as a Service (SaaS) provider, a client company, and their data subjects is such that GDPR regulates the entire system as a whole. This is what is known as **the shared responsibility model of data protection**.

3.1 The shared responsibility model of data protection

The shared responsibility model ensures that each process within the software system is robust and compliant with current standards. Responsibilities are delegated at each stage of the service supply chain: from software publisher, all the way through to the end-user.

It is important that recruiters acknowledge the different data security liabilities that may occur within a shared responsibility model. For instance, a **cloud storage provider** must ensure that security of the cloud is compliant with legal standards. However, the cloud service provider is **not** liable for the security of activities or processes which occur within its cloud architecture: these are the responsibility of the SaaS enterprise, or the data processor end-user.

3.2 Case study: The eBoss Recruitment experience

At eBoss, we have established a robust and DPA-compliant suite of recruitment tools, partnered with Amazon Web Services (AWS). We deliver time and resource-saving services to recruitment specialists, enabling clients to improve outcomes in a results-driven industry.

In our business model, we draw upon the scalability of AWS cloud storage facilities. AWS is wholly responsible for any vulnerability which occurs within the architecture of its cloud storage system. (AWS has an exemplary track record in this respect). This ensures that our clients at this date are covered by the existing data protection regulations.

To date, eBoss is responsible for ensuring that each of the software services that we deploy are robust and meet with the highest digital standards of security. If a vulnerability is discovered within the processing software, it is the responsibility of the SaaS provider to remedy.

As the end-user, our **clients are responsible for implementing and using these recruitment tools in a way that does not put data subjects' information at risk**.

3.3 GDPR compliance: Your next step

At eBoss recruitment software, we are working towards developing a compliance dashboard which will clearly direct the end user towards any steps that need to be taken in order to maintain the integrity and security required by the GDPR.

The details of this will be published in our next paper scheduled for the June 2017.

In the above we have discussed some aspects of the changes to data security regulations. From this analysis, we can assert that this is not a complete re-writing of the rulebook nor does it require immediate complex changes on the day to day running of your business, indeed GDPR is conceived as an improvement of existing directives, while more measures are specified for non-compliance.

However, business leaders will be required to ensure compliance over the space of the next twelve months, and it can prove beneficial to consult recruitment software providers to learn about how to begin this process.

At eBoss recruitment software, for example, will be more than happy to provide initial consultation services for recruiters who are unsure of their compliance status, and establish what they need to do or assess if their existing systems will remain fit for purpose under the new data protection laws in the coming years.

In the next paper scheduled for the June 2017, we propose to give further information about the eBoss recruitment software **compliance dashboard**, and we will explain the practical steps needed to implement and maintain compliance.

We hope that this paper has motivated you to become acquainted with the forthcoming regulations and if and when you want to find out further particulars, please let us have your comments.

Thank you

David Lyons
Managing Director

david@ebossrecruitment.com