THE DEFINITIVE

GDPR

GUIDE FOR RECRUITERS

THE CLOCK IS TICKING . . . Keeping your data secure may seem like a good idea, but it is not only best practice. It is your legal duty.

General Data Protection Regulation (GDPR) protects the private data of every EU citizen. The new rules comes into effect on 25th May, 2018. Every organisation that stores, processes, or manages personal data must demonstrate GDPR compliance or face fines of €20 Million, or 4% of its annual global turnover.

Learn more at eBoss.

CREATED BY eBoss RECRUITMENT SOFTWARE

CONTENTS

SECTION 1: Introduction to GDPR

The **General Data Protection Regulation (GDPR)** redefines data protection in European law. The new regulations will standardise the management and usage of digital personal data across all territories.

The process of ensuring compliance has the potential to create significant disruption for businesses. Nevertheless, it is possible to implement programs which minimise the impact of GDPR. These programs should be neither costly, nor time-consuming, for the majority of organisations.

Perhaps the greater concern for many organisations is the task of getting to grips with the regulation itself. The GDPR is an 88 page legal document, and it is not the most approachable read. Clarifying your own specific duties and obligations may not necessarily be an easy task.

That is why **eBoss** has compiled this definitive guide for recruiters. It will explain the changes that you will need to make, why you need to make them, and outline ways to implement them, without disrupting the day-to-day running of your recruitment enterprise.

Our objective is to ensure GDPR compliance while minimising disruption, costs, and workload.

1.1 What is GDPR?

GDPR is a new set of rules which govern the use of digital data relating to citizens of EU nations. The changes have been made to address developments and changes in globalised markets and networked technologies. GDPR extends the scope of regulation to include: non-EEC organisations, cloud computing services, and social media, amongst other factors.

1.2. When?

Although you may have seen little evidence of it, we are currently in a two-year transitional period of GDPR adoption. It is the responsibility of every organisation possessing the personal data of EU citizens to demonstrate compliance by the end of this period. The deadline for this transition, at which point GDPR becomes law, is **25th May, 2018**.

1.3. Why GDPR?

GDPR has been designed to achieve the following core objectives:

- Reinforce & modernise regulations as set out by the **EU Data Protection Directive**.
- Extend the rights of EU citizens as data subjects across all jurisdictions.
- Standardise legal obligations, penalties and best practice in regard to data security.

1.4. How does GDPR do this?

GDPR creates a lasting framework of standards to govern data processing in the future. The law is built around a few fundamental factors. The first of these is ***privacy by design***. Organisations must be able to demonstrate that their data management systems have been developed with security as a core consideration from their earliest stages.

GDPR introduces new rights for individuals in respect of the use and retention of their own data, including the ***right to be forgotten***. Individuals – called ***data subjects*** – can ask you to provide them with a portable copy of all information you have about them. They can ask you to refrain from collecting any further data about them, or they can withhold consent from you processing or using their data in any way in the future. They are also entitled to ask to be *forgotten*. That is: they can request you remove all information relating to them from your systems. Organisations can only dispute these requests under rare and exceptional circumstances – *most of which will never apply to a recruitment enterprise*.

GDPR introduces **higher penalties** for infractions such as failing to handle data with due care, not implementing appropriate security processes, or failing to report a security breach to authorities within the allotted time (72 hours from its discovery).

Under the new framework, non-compliant organisations are liable of fines totalling **4 per cent of annual global turnover** or **€20 million** – whichever is higher.

1.5. Who is affected?

Any organisation which supplies goods or services to EU citizens, or which processes or retains data relating to EU data subjects will fall within the GDPR framework regardless of size, sector, or location. This makes GDPR the first EU data regulation to apply to businesses based outside the EU. Businesses based globally must demonstrate compliance.

1.6. What is *'personal data'*?

GDPR defines ***'personal data'*** as any information which may be attributed to an identified, or identifiable, individual. This means that data relating to an IP address, personal identification number, or account identification number is personal data in exactly the same way as information relating to a name, identity, or physical address. GDPR defines personal data as:

> *"any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".*
> **Article 4(1), GDPR.**

1.6.1. *Special Personal Data*

Recruiters should pay special consideration to Article 9(1) of GDPR. This section outlines several new ***special categories of personal data***, which are subject to tighter regulation. Special personal data includes:

- racial and ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic or biometric data;
- health;
- sexual orientation.

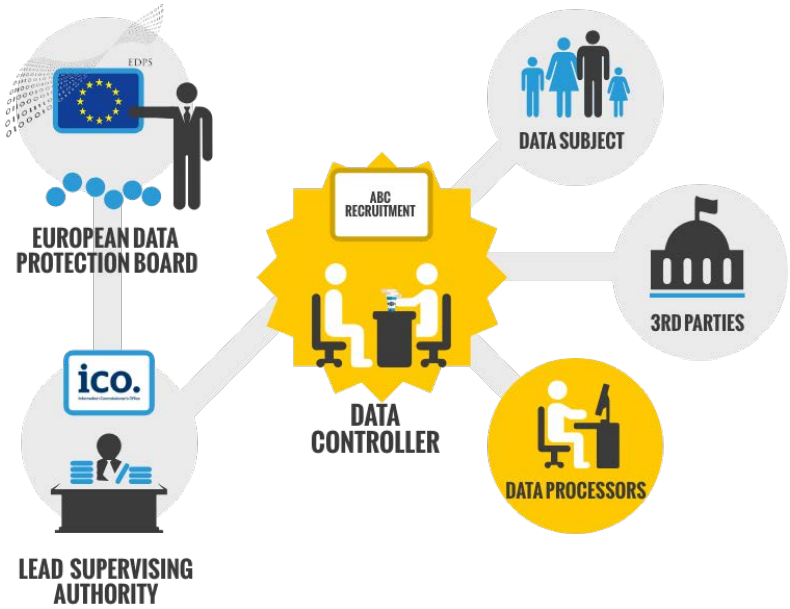
Not every recruitment organisation will control or process data in this category; but some will. If your enterprise is using this type of information, you are obliged to meet an additional set of standards (**See: 3.5.1.**). The next step is to evaluate your own activities, and assess your exposure to GDPR law.

SECTION 2: GDPR & RECRUITERS

Personal data is one of the primary resources of the recruitment sector. Without it, we would never discover new candidates or fill placements for our clients. GDPR *will* have an impact on our sector. It is our job to minimise the disruption.

This next section highlights some of the specific considerations that recruiters (and service providers within the sector) will make before implementing a compliance program.

We address the reach of **your responsibilities as a data controller**. We look at **networked technology**, and consider how some **modern approaches to recruitment** may leave you exposed to stricter elements of the GDPR regulation



2.1. Controller, or Processor?

So what are our obligations? Understanding this requires us to first determine our role in the data network. GDPR outlines the obligations of two entities: the data controller, and the data processor.

2.1.1. *The Data Processor*

A data processor is an individual or organisation which processes data on behalf of another entity, but which does **not** control the reasons for processing it, or its subsequent uses.

Examples of data processors in the recruitment industry include a cloud-based storage solution, a communications service, or a software (SaaS) provider.

The role of the data processor is newly defined in GDPR. Under previous DPD legislation, it was the responsibility of the **data controller** to ensure compliance across the entire data processing chain. This has been updated to distribute responsibility between the various elements of your data ecosystem.

These changes are intended to address the growing reliance on third-party services, like cloud storage. Under GDPR rules, if your off-site provider suffers a security breach, and fails to report it to the authorities within the correct time frame, it is they who will be penalised.

Nevertheless, it is still the responsibility of the data controller to assess the suitability of potential business partners within their network, and ensure compliance.

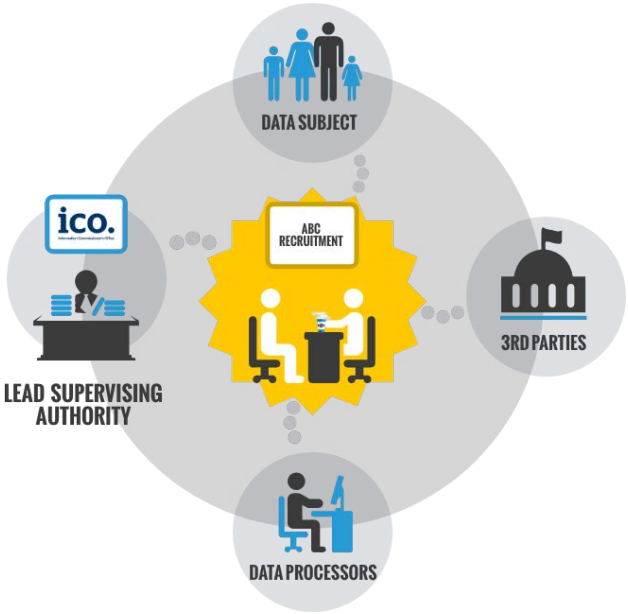
2.1.2. *The Data Controller*

A data controller, on the other hand, is an entity which determines the use or method of processing data. It is possible to be *both* a data controller in some areas of your business activities, and a processor in others. For a (very broad) method of determining your legal status, ask the following question:

''Do I own or collect data relating to living people in the European Union?''

If the answer to that question is 'Yes', then you are most likely a data controller. *(NB: If decisions on how to use data are made in collaboration with other organisations, all participating bodies will be classed as a data controller.)*

Due to the nature of the industry, it is highly likely that a recruitment firm will be a data controller. For the benefit of this guide, we will assume that your recruitment enterprise is a data controller, and therefore has to meet these responsibilities.



2.2. Duties and Responsibilities

A data controller has several duties. The first is to ensure GDPR compliance among all of your data processors, including partnered businesses, service providers and clients. However, the full list of obligations is considerably longer:

- Collect **no** new data on individuals without prior and explicit consent.
- Ensure **existing data subjects** consent to the continued processing of their information
- Clearly state the intended uses of personal data when requesting consent.
- Do not use data in any way other than those laid out in the consent form.
- Move to obtain consent within 30 days of storing new data.
- Supply data subjects with a portable digital copy of their data upon request.
- Ensure your entire data ecosystem – including use by off-site processors and subcontractors - is secured and compliant with new regulation.
- Implement adequate measures to secure personal data.
- **Store data in a secure fashion**: consider encryption, and off-site cold storage.
- Perform Data Protection Impact Assessments (DPIA) when the processing of sensitive personal data may harm the privacy or freedoms of a data subject.
- **Keep detailed records** of your security measures and data processing activities.
- **Train staff** and subcontractors to understand data security regulations and best practice.
- Stay informed about developments in EU data law, and implement processes which address any changes.
- Appoint a Data Protection Officer if required (see: **3.5.1.**)
- Notify the Information Commissioners Office (ICO), or relevant local authorities within 72 hours of a data breach.

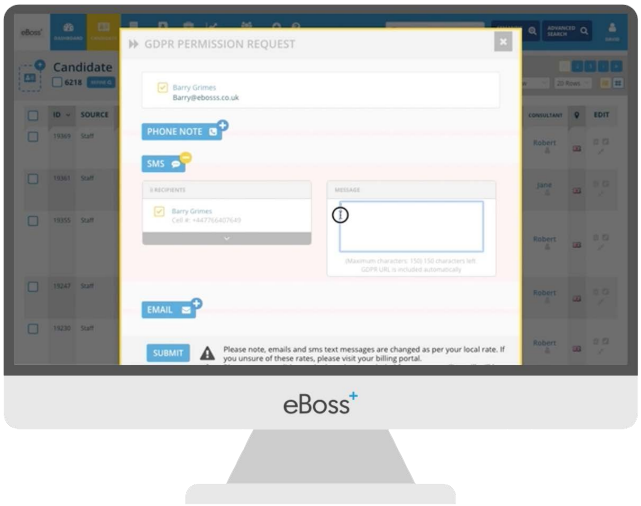
2.2.1. Priorities for recruiters

Recruitment is a sector which relies on data. In one sense, our data subjects are our product, and our value offering to clients and customers. Consider the impact on the day-to-day running of your enterprise if you were unable to access your database. That is the potential impact of failing to implement a GDPR readiness scheme.

From the 25th of May 2018, any data which does not have voluntary, explicit, and up-to-date consent provided by the data subject will be deemed non-compliant. This means you cannot use it, or process it in any way. Existing consents do not cover the new GDPR requirements, which means your enterprise must establish contact with each existing data subject, and request new consent.

The bulk of recruiters' GDPR workload therefore is unlikely to come from network management. Instead, consider prioritising ways of obtaining consent from new and existing data subjects, and complying with requests.

2.3. CASE STUDY: eBoss Software tools



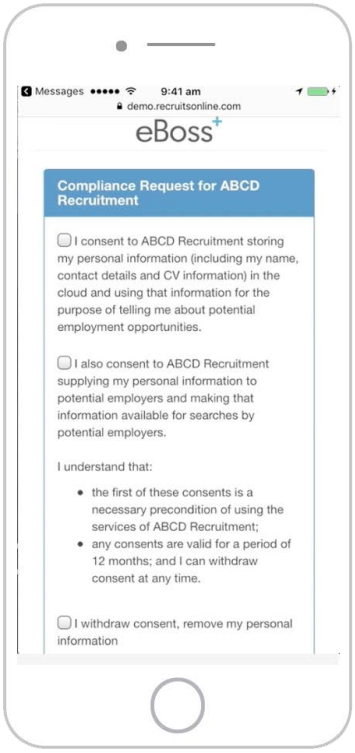
eBoss Recruitment Software is a service provider for the recruitment sector. Although we act as a **controller** of our own business data, our primary function for our clients is that of a **data processor**.

In short, we understand the needs of both sides of the GDPR discussion.

Recruitment priorities
We have developed our systems to address the priorities of the recruitment sector. We guarantee out-of-the-box GDPR compliance from day one. We have also streamlined the internal processes necessary for any GDPR readiness initiative:

- simpler consent forms,
- faster communications,
- clearer overviews of your compliance status.

Our clients have responded positively to our implementation of **privacy by design** in our software products. It is reassuring to know that every link in your data processing chain is secured by a single service. Additionally, we reduced compliance workloads by implementing concise, at-a-glance monitoring for our GDPR toolkit.

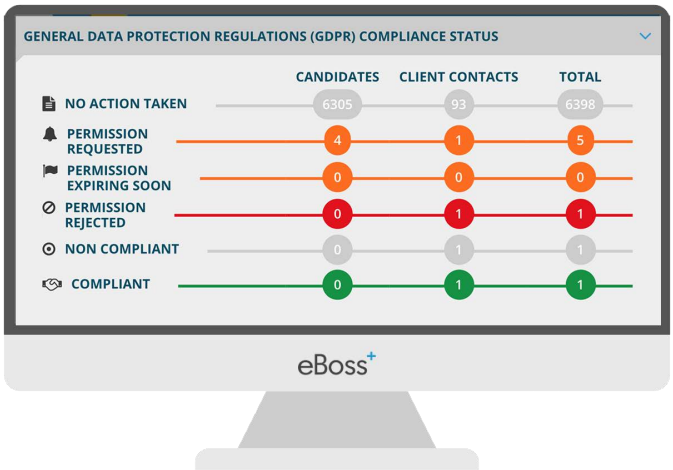


Monitor a complete overview of your database; identify and isolate any outstanding consent requests. Alternatively, view the consent status of individual data subjects from their individual profiles.

From the same screen, you can initiate a consent request. The two greatest challenges our clients face are the time constraints of establishing contact, and the need to improve rates of responses among data subjects. **eBoss** has addressed these demands by making contact easy.

Reach out via **email**, **phone**, or **SMS**, and allow your data subjects to respond instantly. Consent is granted with a single click once the data subject has followed the link to the compliance page – making the process as simple as possible, and improving your response rates. Pro package features make the process even easier, with bulk actions and targeting

eBoss generates records of every interaction: automatically and in real time. Producing compliance reports becomes quick, accurate, and effortless



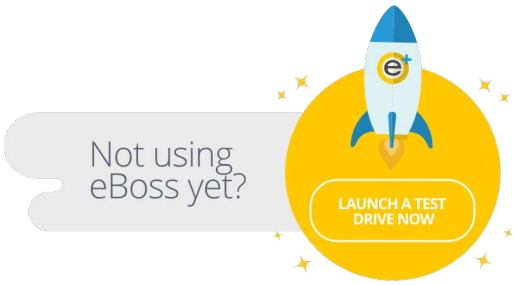
The ideal GDPR Toolkit for Recruitment professionals

Bringing your existing database into compliance is potentially the most time-consuming task for your business. GDPR does not acknowledge your current consent information, so you must request new permissions from each of your existing data subjects. Without clear and voluntary consent, you cannot use your stored data.

Any data system which implements **eBoss** tools assists your readiness initiative in several ways. You do not only have access to the GDPR compliance dashboard and toolset that we have showcased in this section. You also have a partner for your business who has demonstrated **privacy by design in all of our products** – and who remains committed to staying ahead of the regulatory curve when it comes to meeting the technical requirements of the future.

Furthermore, with storage solutions powered by the fully-compliant Amazon AWS cloud services, you have a fully-compliant ecosystem for your company data, out of the box. Working with eBoss tools means that half of your duties as a data controller are already completed – and the remaining tasks are made faster, and more efficient.

Maybe you do not use **eBoss** software; perhaps you are not even considering updating your existing system. However, if you are implementing a strategy which is not able to match these simple solutions, you are working at a disadvantage to your competitors.



2.4. Databases, social media, and automation

Today's high-tech recruiters monitor social media channels and use automated software solutions. But if you are on the cutting edge of recruitment software, you may need to be aware of the legal uncertainties surrounding some strategies under GDPR.

Take, for example, **social media** monitoring.Around 60% of UK businesses already screen the social media accounts of potential hires. The information scraped in this way is likely to contain examples of *special personal data* (see: **1.6.1.**).

There is a safeguard built into GDPR which allows the continued collection of this material. Namely, organisations are permitted to process data which meets the following criteria:

"Data manifestly made public by the data subject" **Article 9(2)(e), GDPR**

Most social media sites bind their users to a terms of service agreements. These typically require consent for the publicising of data shared within the service. In this sense, social media recruiters have some degree of legal coverage.

However, GDPR also states that a recruiter or employer must demonstrate that: (i) there is a justifiable need to collect the information from the candidate, and (ii) the collection of this data will not impact upon the privacy or freedoms.

The underlying cause for concern is in this latter point. If a candidate is unsuccessful in their application, they may cite the collection of social media data as a cause for discrimination. This would represent a *loss of freedom* .

A claim of this type could create serious legal challenges for your recruitment enterprise. Therefore, the routine screening of social media profiles may require a Data Protection Impact Assessment (and, consequently, the services of a DPO) to ensure compliance. The additional costs of these safeguards may mean it is more cost efficient to simply stop screening social media profiles altogether. You will have to evaluate this in relation to your own business model and resources.

SECTION 3: Applying Solutions

This section lays out a concise GDPR readiness initiative, which you can implement directly, or adapt to suit your company. We take you from the planning stage, to software implementation, data security, and the hiring of mission-critical personnel.

As ever, we focus on one concern:*how can I ensure GDPR compliance with a minimum of disruption to my day-to-day processes?* By the time you have carried out the following steps, your business will be at, or very close to, full compliance.

3.1. Assess

It is time to take stock of your current situation and practices. Before you go any further, complete the following self-assessment:

1. Review your existing data protection policy, and your internal codes of conduct.
2. Determine if existing standards comply with GDPR. If they do not, renew your policies.
3. If you do not have a data protection policy, establish one as soon as possible.
4. Review your ongoing service provider and supplier arrangements. Renew terms to ensure obligations for data processors are correctly established and allocated.
5. Update end-user notices and terms of service to ensure GDPR compliance.
6. Update insurance agreements & policies which have not previously covered data security.

3.2. Audit

Auditing your current database will help you to establish which data lacks the sufficient

permissions from your data subjects. It also allows you to determine any pools of obsolete data – information which is no longer needed, and which is therefore more efficient to erase (in the correct manner), rather than seek permissions to retain.

1. Audit all data processes. Log which specific categories of personal data you are processing, and why.
2. Establish your legal justification for each of these processes. If you have none, stop immediately.
3. If these processes are required for the performance of a contract, or because they represent a legitimate interest for clients or employers, then you *do* possess a legal justification.
4. Map your data processing network. Achieve a clear and accurate understanding of where your data is, who uses it, who can access it, and which processes they carry out.

3.3. Act

By assessing your processes and auditing your databases, you have the requisite information to put your compliance initiative into action. Once the following section has been completed, your existing data will have achieved compliance, new data entering your system will have the appropriate consents, and your systems will be secured.

1. Create physical back-ups of all your data. Ensure back-up storage is located at a separate physical location to live databases.
2. Improve security standards for categories of sensitive data: consider data encryption, and offline, 'cold' storage options.
3. Remain conscious of the fact that, as technology changes, compliance requirements will change, too. Data security is an ongoing process, not a one-time remedy.
4. Ensure you possess consent for all of your data subjects.
5. Seek consent for new and outstanding data subjects.
6. Consider the methods you will use to obtain or renew data subjects' consent. Seek active consent for new and existing data subjects. Opt-out or pre-filled consent forms are no longer valid under GDPR legislation.
7. Consent must be voluntary, explicit, and must relate directly to its intended usage. If existing consents do not fulfil each of these criteria, seek renewal.

3.4 Record

Recording your results and activities will not only provide evidence of best practices if you are audited or suffer a breach; they will also act as a valuable reference to guide you in future data security programs.

1. Document each step of your compliance initiative and maintain (digital) paper trails of all of your data processing, as these will be required if you are audited.
2. Retain contracts and terms of service issued by service providers and partners.
3. Conduct Data Protection Impact Assessments when required.

3.5. Train

Your staff must be conscious to the changes in legislation. Not every member of staff will use personal information, or have access to your data management system. But all should be brought up to date with their obligations under GDPR, to **minimise the risk of a data breach by human error**.

1. Staff must be trained in GDPR best practices.
2. Reduce the risk of a breach from human error by enforcing: **high strength passwords**, password **expiration dates**, the **correct disposal** of old data.
3. Train staff to spot security breaches. Explain the most common methods of launching a hostile attack (including suspect email communications and social engineering threats), and those most likely to affect your particular enterprise.

4. Customer-facing personnel must understand their obligations should they receive **a request from a data subject**. Instruct your staff on their legal duties, and make sure they know how to respond.
5. Introduce a clear command structure, so all personnel know who to report to in the event of a data request or a security breach.
6. Implement data breach response procedures; ensure staff understand the importance of the 72 hour time window for reporting an attack.
7. Don't stop. Training is an ongoing process. Update the knowledge base of your team on a regular basis.

3.5.1. ...and hire?

Not every organisation will have to recruit to attain GDPR compliance. But some businesses may find they require a **data protection officer** (DPO). A controller or processor must appoint a DPO, if:

- The nature, scope, or purposes of data processing requires the regular monitoring of data subjects on a large scale;
- The primary data processing activities include the processing of a large volume of *special categories of data*.

Small and medium sized recruiters that do require a DPO may be in the minority. However, if you do need DPO oversight, it is vital that you understand their unique duties, and your obligations to their work.

- The DPO must be an active participant in any internal process where data security is a consideration.
- Every part of your enterprise must co-operate with the DPO in their work.
- The DPO is the sole contact point for external supervisory authorities within your organisation.
- The DPO is the primary contact point for data subjects on all issues concerning the process of their data, and the exercising of their rights under GDPR.
- A DPO must be appointed for a minimum of two years.
- A DPO must be supplied with the staff and resources necessary to complete their duties
- The DPO must control of their own budget
- The DPO reports to the highest management level within the organisation only.
- The DPO is bound by confidentiality
- The duties of the DPO must not be compromised by a conflict of interest relating to any other duties they may have within the organisation.
- The DPO cannot receive instructions or guidance concerning how they carry out their duties

It is acceptable for a single data protection officer to provide oversight to an entire network of associated businesses and organisations. Providing there is **no conflict of interest** in the DPO's duties, a single data officer can ensure compliance for your business and your service providers

Section 4. GDPR: Myth Vs Reality

While we have done our best to highlight the realities of the General Data Protection Act, some common misconceptions about the laws remain. In the following section, we address some of the most common assumptions made about GDPR compliance – and put them right.

MYTH 1: ***''GDPR will not affect my business.''***
GDPR applies to all organisation which offers goods and service to EU citizens, or which possess or process their personal information.

The scope of the law virtually guarantees that all enterprises – wherever they are located –could be required to demonstrate GDPR compliance. Your business need not have a physical presence within the EU. If your customer and client base contains EU citizens, you must show compliance.

MYTH 2: ***''Our business is too small to be affected by the tougher penalties''.***
That commonly-repeated statistic - *'4 per cent of annual global turnover, or €20 million'* – applies to everybody. There is no minimum size for an organisation to be liable for fines and penalties under GDPR. The figures quoted above are the maximum penalties for the most serious breaches of data protection standards – and it is always the greater of the two which is applied.

MYTH 3: ***''We no longer collect new data, so we are already compliant.''***
Assuming that GDPR only affect new data is one of the most dangerous assumptions to make. The regulation is retroactive, and will be applied to your existing databases immediately, on 25th May, 2018. If you have not demonstrated an attempt to achieve compliance by then, you are in breach of the law. You must seek consent from each of your new and existing data subjects to continue processing their data.

MYTH 4: ***''We outsource our data processes; GDPR does not affect us.''***
As a data controller, you are charged with assuring compliance across the entire data processing network. It is your duty to select partners who demonstrate compliance, and to assess the readiness of service providers prior to May 2018.

MYTH 5: ***''We do not really need to hire a DPO.''***
In many instances, it will not be necessary to appoint a Data Protection Officer. However, this must be assessed on a case-by-case basis.

A DPO is required to conduct impact reports (DPIA). Therefore, their services are required if your business is consistently processing high volumes of data, or if the information you are processing is sensitive personal data.

Equally, if your day-to-day operations, or your data management network, may be exposed to elevated risk of breach or hostile attack, it is best practice to retain the services of a DPO. Your data protection officer will be responsible for risk assessments and for seeking special authorisations from the ICO (the Information Commissioner's Office). Check with your legal team if you are in any way unsure of your obligations concerning the recruitment of a DPO.

SECTION 5: GDPR Compliance Roadmap

1. Define your role: Data controller, data processor, or both?
2. Update your data protection procedures to meet best practices
3. Audit your existing databases and processes
4. Choose software which demonstrates **Privacy by Design**
5. Reinforce the security of your data storage solutions
6. Oversee best practices and compliance across all of your data processors
7. Inform data subjects of their new rights
8. Request fresh consents from new and existing data subjects
9. Comply with data subjects' requests, if they exercise their rights
10. Cease the processing and use of data for which you have no up-to-date permissions
11. Train staff to be aware of their new data security obligations.
12. Hire a DPO to address your GDPR requirements
13. Keep records and accounts of each stage in your compliance initiative.
14. In the case of a security breach, contact the authorities immediately.
15. Reassess your processes to ensure compliance.

About This Guide

The definitive guide to GDPR for recruiters has been compiled by the **eBoss** recruitment solutions team.

We are a specialist enterprise that develops software products for the recruitment industry. As well as providing an unequalled level of personal support for all of our services, we promote the understanding and adoption of technology-based solutions within the modern jobs market.

Although GDPR represents a significant change in the working culture of many traditional recruiters, it became apparent to us that a lot organisations in the sector were unaware of their new legal obligations, even as the transition period came to an end.

This guide has been written to help organisations such as yours achieve compliance at every step: from laying initial groundwork, to completing the final assessment. It is as relevant for a small start-up as it is for a multinational. You may choose to implement it in part, or in full. Please feel free to share this guide, or links to it. Kindly do not reproduce any part of this guide without first seeking prior consent.

David Lyons,
Director

END OF DOCUMENT

CREATED BY eBoss RECRUITMENT SOFTWARE