WHAT IS GDPR?

INTRODUCTION

Current data protection laws are almost 20 years old and are not adequate for today's digital age. The EU's General Data Protection Regulation (GDPR) raises the standards for processing personal data, to strengthen and unify protection for individuals across the EU. The new legislation comes into force in Europe (which still includes the UK) on 25th May 2018. Now with less than a year to go, organisations must prepare for the new laws, or risk heavy fines for non-compliance.

This document does not intend to provide legal advice. This document aims to provide you with a better understanding of the legislation and provide practical guidance on steps you can take on the road to compliance.

We recommend you work with your legal advisors, CRM partner and IT providers to help prepare your business for GDPR. Microdec will be making specific product enhancements to assist our clients with GDPR compliance and these will be announced on our website (www.microdec.com/gdpr) and via your account manager.

WHAT ARE THE IMPLICATIONS FOR RECRUITERS?

To be good recruiters, we need to store candidate names, addresses, career history, salary information, passport details, the list goes on. For GDPR compliance, it's vital to demonstrate that you're acting lawfully, with reason to handle personal data and with permission, control and processes in place.

GDPR doesn't mean we have to fundamentally change how we work. If you have good data protection policies and you use your CRM properly, there's a fair chance you're in good shape and compliance will be easier for you, but it's likely that you'll need to review and document your processes. Organisations must not delay. You may need to change existing company practices, policies and technologies in order to comply.

The GDPR includes the following rights for individuals:

- the requirement to give consent in certain circumstances
- the right to be informed of how their data is being processed
- the right of access to see the information you're storing on them
- the right to rectification of any errors
- the right to erasure or removal from your database
- the right to data portability
- the right to object
- the right not to be subject to automated decision-making including profiling.

There is a great opportunity to use data protection as a means of standing out from your competitors. Demonstrating that you are acting responsibly and with integrity means you will benefit from increased trust and credibility from your candidates and clients.

© Microdec Plc 2017
E&OE

THE STEPS TO GDPR COMPLIANCE

MAKE YOUR TEAM AWARE

GDPR should be a board-level topic within your organisation. You should ensure that decision makers, consultants, researchers and back office teams are aware that the law is changing. They need to understand likely impacts of the legislation on their roles. Involving them now can help you identify areas that could cause compliance problems under the new law and will help you introduce new processes if necessary.

APPOINT DATA PROTECTION OFFICER RESPONSIBILITY

The law requires that a data protection officer (DPO) should be appointed by companies passing certain thresholds of size and activity levels, although the metrics for this are unclear. For most commercial enterprises, the commission and parliament texts respectively state that companies of over 250 employees and/or companies that process the personal data of over 5000 subjects in any 12 month period, should appoint a DPO.

We recommend that regardless of your company size, someone should be given this responsibility so you have one central point of contact to coordinate the data management standards and processes in your business. In appointing this person, you must ensure they have the knowledge, support and authority to carry out their role effectively.

UNDERSTAND CONSENT AND LEGITIMATE INTEREST

It is important to recognize that consent is just one way of processing data lawfully. Another is through legitimate interest. In order to provide workfinding services, your organisation processes personal data - to assess a candidate's suitability for a role, check identity, right to work and to process pay. Therefore, it's in the legitimate interests of all parties involved that your organisation can process personal data.

If you are to rely on consent, each individual must perform a clear affirmative action to give you permission to hold and process their information. The source must be verifiable, so you'll need to keep records of what personal data you hold, where that data came from, when consent was given.

Consent must be freely given, specific, unambiguous and the individual must be informed of how you intend to process their data. Your consent request should be prominent, concise and easy to understand. There must be a positive action to opt-in – consent cannot be inferred using pre-ticked boxes or assumed through silence or inactivity. The GDPR does not specifically ban opt-out boxes but they are essentially the same as pre-ticked boxes, which are banned.

Consent must also be separate from other terms and conditions of business and must not be a requirement of doing business with your organisation.

For marketers, you will also need to obtain consent to process personal data for digital marketing.

Depending on how you communicate with candidates, you may wish to be quite granular with your consent statements, by seeking consent separately for different types of processing. For example, asking someone for consent to receive notification of job opportunities does not mean they agree to receive your monthly newsletter.

You should keep records to demonstrate what the individual has consented to, including what they were told, and when and how they consented. This should be stored and managed in your CRM, so discuss the best ways to do this with your provider.

© Microdec Plc 2017
E&OE

AUDIT YOUR DATA

We have already established that under GDPR, you must have consent or legitimate interest for processing personal data. We recommend you start by reviewing how you obtain, record and manage personal information and whether you need to make any changes.

- What information is being collected?
- How is it collected and by whom?
- Why is it being collected?
- How will it be used?
- Who will it be shared with?
- What will be the effect of this on the individuals concerned?
- Is your intended use likely to cause individuals to object or complain?

How old is your data? Decide how long you should keep personal data and take steps to cleanse your database of records which are old or out-of-date.

Look at the type of data that you hold. GDPR is very specific about 'sensitive' personal data relating to racial or ethnic origin, political opinion, religious beliefs, trade union memberships, sexual preference and health or sex life. Do you currently hold any of this information? Do you have a legitimate interest in holding it? If the answer is 'no', then you should remove it from your database. If you do need to hold sensitive information, then you will need to obtain express consent from the individual and record this in your CRM.

Don't assume that information taken from the public domain (LinkedIn, Facebook, company websites) absolves your responsibilities under GDPR. This data can also be classified as personal information and you will still need to prove legitimate interest or consent to store this information on your own systems.

Do you have data stored in different places or on separate systems? Now may be the time to consolidate your systems to help make it easier to manage going forward.

We can't stress enough, the importance of ensuring your consultants use the CRM as intended. Compliance will be so much more difficult if work is done outside the CRM. Take steps now to ensure that your consultants are engaged with the CRM and that your processes support everything being done through the software.

DOCUMENT YOUR PROCESSES

You should have defined processes in place for acquiring data, seeking consent, processing information and responding to data subject requests. Under GDPR, you cannot comply 'by accident'. You must be able to prove your business has deliberate procedures to ensure lawful processing of personal data.

Ideally, you will document the process for acquiring data; you will have defined roles and responsibilities of those handling data; and you will have processes and actions for managing requests, removals and data transfers.

ADDRESS YOUR DATA COLLECTION METHODS AND CONSENT MECHANISMS

Take a look at your website and all candidate application routes and implement 'source' recording in your CRM to give you visibility to the provenance of your data going forward. If you are relying on consent, have an opt-in consent process that agrees to you (name your company) storing an individual's data and communicating with them about employment opportunities and other relevant business information.

© Microdec Plc 2017
E&OE

CREATE A PRIVACY NOTICE

When you collect personal data under the GDPR you will need to give your identity and explain your lawful basis for processing the data. You will need to explain your data retention periods and that individuals have a right to refuse consent or be removed from the database. This can be done through a privacy notice.

The privacy notice will demonstrate that you:

- use information in a way that people would reasonably expect
- think about the impact of your processing
- are transparent and ensure that people know how their information will be used.

You should also make it clear that personal data may be shared with third-parties (such as your clients) as part of the application, selection and recruitment process.

As well as being compliant with the law, a privacy notice gives peace of mind to your candidates. Being honest and open about who you are and what you are going to do with the personal data you collect will give candidates assurances to work with you.

DEFINE TIME LIMITS

There are no specific time limits for how long consent lasts, although you may wish to set periods for reviewing your data to ensure ongoing compliance.

Consideration: Does your CRM have the facility to report on data by age (of the information) or last contact?

PREPARING YOUR CRM SYSTEM FOR GDPR

SUBJECT ACCESS REQUESTS (SAR)

Individuals have the right to access or view their data and you should update your procedures to show how you will handle such requests. You will have a month to comply with a SAR.

Consideration: Does your CRM allow you to easily extract all the data you hold on a particular individual?

Again, best practice is to have all your consultants using the CRM. If you're doing things outside the CRM, you're still obliged to provide the data – but you're making it much harder for yourselves to locate the data if it's stored on various separate email systems, folders, mobile devices etc.

RIGHT TO RECTIFICATION

If an individual feels that the information you are holding is incomplete or inaccurate, they have the right to ask for that information to be corrected. **As part of your GDPR training, induction training, or best practice guidance within your business, you need to make sure your employees understand their obligations to keep data well maintained under GDPR.**

© Microdec Plc 2017
E&OE

THE RIGHT TO WITHDRAW CONSENT

GDPR states that it must be as easy for an individual to withdraw consent as it was to give consent. This means you will need to have simple and effective withdrawal mechanisms in place. We suggest your website and other candidate communication tells people they have the right to withdraw their consent at any time, and how they can do this. **Have a documented process for updating and managing the consent mechanisms within your CRM.**

THE RIGHT TO ERASURE

Individuals have the right to be removed from your database under GDPR. You will need to have documented process in place to ensure that people are deleted from your database in a timely manner.

Consideration: Does your CRM have a mechanism for safely deleting personal data?

When you carry out an erasure request, you are obliged under GDPR to inform any third-parties of the deletion request. So, you will need to check who you have shared the information with. If your consultants are using your CRM properly, your exposure is reduced here, as there should be an audit trail that you can follow.

Consideration: How easily can you identify where a candidate's CV has been shared and when? Can you track emails from within your CRM?

RIGHT TO PORTABILITY

Legislation allows for a data subject to lift their information from one service provider to another, meaning that you need to have a process and a mechanism for extracting information from your CRM and providing it to another organization.

Consideration: Can you extract an individual's data from your CRM in a commonly used, machine readable format that allows for transfer?

SECURITY AND DATA PROCESSING

Take a look at system access within your organisation. Who can see what? Does your CRM partner offer any access management tools to allow more granular access to your data? Consider security modules to prevent or restrict users running particular reports or extracting data and look at how an audit trail can help you see who has tried to access what, and when.

Look at data security, passwords and the location of your data. What happens to your backups? Now could be the time to consider a cloud-based infrastructure over an on-premise server for improved security.

Consider how your colleagues work with data. Look at the information saved to desktops, laptops, tablets, excel spreadsheets and so on. Map the workflows and routes of data around your organisation and take steps to eradicate any ad-hoc practices from your process.

Emails play a huge role in our day-to-day transactions with candidates and clients and often contain personal information. Using email within your CRM helps maintain working standards, keeps an audit trail for the data and makes subject access requests far easier to deal with.

If your CRM has a mobile app, find out where the data is stored. For example, in the Profile mobile app, we don't store any information on the phone itself, it all goes back to the database.

© Microdec Plc 2017
E&OE

DATA BREACHES

The regulations will introduce a duty on all organisations to report certain types of data breach to the relevant supervisory authority within 72 hours, and in some cases to the individuals affected.

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

You only have to notify the relevant supervisory authority of a breach where it is likely to result in a risk to the rights and freedoms of individuals such as discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you must notify those concerned directly. A 'high risk' means the threshold for notifying individuals is higher than for notifying the relevant supervisory authority. For example, if workers bank details are accessed or stolen.

Failing to notify a breach when required to do so can result in a significant fine.

You should make sure that your employees understand what constitutes a data breach, and you should ensure that you have an internal reporting procedure in place for breaches. This will help the DPO decide whether you need to notify the relevant supervisory authority or those individuals on your database.

SUMMARY

If you have documented processes, if you use your CRM properly and already take steps to give individuals their rights now, then the transition to the GDPR should be relatively easy. This is a good time to check your procedures and to work out how you would react if someone asks to have their personal data deleted, for example. Who would deal with such a request? Would your systems help you to locate and delete the data? Who will make the decisions about deletion?

Start your data audit now. This will be the best platform for understanding how you process data and what needs to change before the deadline.

If you don't already have set workflows and recruitment processes in place, do it now.

Going forward, make sure the people in your business understand GDPR and why you have these processes in place. Make data a part of your induction process, so new starters are on-board from the beginning.

Get your consultants engaged with your CRM. The workflows it provides will set and maintain standards in your business; the quality of the information you hold will make your people better recruiters; the audit trail your CRM provides will improve your business and assist with compliance; and having everything in one place will make your role as a DPO so much easier to carry out.

Finally, don't panic about GDPR. With proper thought, planning and buy-in from your business and with input from your CRM partner, there's no reason why you won't be ready for May 2018.

© Microdec Plc 2017
E&OE

ABOUT MICRODEC

Microdec is a software and services company providing solutions exclusively for the recruitment industry around the globe.

Our award-winning Profile software uses revolutionary data intelligence to reduce admin and proactively assist the user, by actively mining and analysing the data entered by the consultant and feeding back the relevant actions and reminders to ensure you never miss a task or opportunity – it's like having a PA for every member of your team.

Profile has a modern, best-in-class user interface that is strongly influenced by social media to be popular with recruitment consultants and ensure user adoption. Clearly labelled processes guide you through all the steps necessary to manage fast and reliable recruitment processes.

Profile has integrated email and social media links that reduce admin and improve user efficiency, saving time and costs. Profile has options for integrating with back office software, analytics applications and job board distribution tools.

Microdec's software and professional services enable you to make more placements in less time, resulting in increased profits and significant advantage over your competition.

For more information on how Microdec can help your business grow, please take a look at www.microdec.com, contact sales@microdec.com or call 01277 227778.

© Microdec Plc 2017
E&OE