The GDPR: What does it mean for executive search?



invenias
powering your search for talent

“At Invenias, we are committed to working in partnership with our customers to ensure a streamlined journey to compliance.

Our customers benefit from data protection being at the heart of the design, build and operation of our technologies.”

Introduction from David Grundy

From May 2018, all organisations that handle the data of EU citizens will be required to comply with a single set of rules in relation to data governance, regardless of where the organisation is located. The introduction of the General Data Protection Regulation (GDPR) will materially impact the way in which data is stored, shared and moved and this will have a significant impact on the working practices of the executive search professional.

Organisations have to be fully prepared by the May 2018 deadline and it is critical that we invest time in developing an awareness and understanding of the GDPR, so that we can plan and implement changes and ensure compliance with the new legislation.

The implications of failing to comply with the changes are considerable and well documented. However, whilst meeting the new requirements will require significant investment, we believe that the GDPR also presents opportunities for the executive search profession.

We recognise our role in compliance is critical. As the provider of the platform on which you run your business, you will look to us to bring solutions for you to manage the risks, and simplify complexity. At Invenias, we are committed to working in partnership with our customers to ensure a streamlined journey to compliance. Our customers benefit from data protection being at the heart of the design, build and operation of our technologies.

This guide should not be taken as a substitute for legal advice, but I hope it will provide a useful point of reference as you prepare for the May 2018 deadline.



David Grundy
CEO



An overview of the GDPR and its impact on executive search

The GDPR or the General Data Protection Regulation will come into force in May 2018 and will safeguard European Union citizens with respect to their data privacy rights. The legislation will impact all organisations that are either based in, or do business with, the EU. In essence, the legislation will give individuals greater rights and control over their data by way of consent as well as the power to access, rectify or erase information held and the right to be informed.

There is no doubt the changes in the GDPR will have a significant impact on the executive search profession. Any firm that operates in the EU, has clients that operate in the EU, or that processes data on EU citizens are subject to these changes in legislation, regardless of where information is stored, whether it is held in emails, a database or in spreadsheets.

The rules will have a similar impact on technology suppliers to the industry, with those who act as a data controller or data processor both bound by and required to comply with the changes to the GDPR. Executive search firms will have to demonstrate that their systems and technology are compliant.

With severe non-compliance penalties of EUR20 million or 4% of worldwide turnover, the GDPR will make organisations more accountable for their approach to data and the changes must be given appropriate consideration.



It’s not all doom and gloom

However, whilst there are significant financial and reputational implications for failing to comply with the changes, it is not all doom and gloom. Instead, rather than focusing on the burden of preparing for the GDPR and the penalties associated with breaches, the new rules can be viewed as an opportunity to enhance working practices and the quality of data stored.

Compliance with the GDPR will foster a culture of data confidence amongst an organisation’s clients and candidates. Moreover, a greater level of transparency and accountability for information held and transferred will enhance working practices. The GDPR is an opportunity to enhance the quality of data held as the changes will ensure businesses invest more time in thinking about the data that they capture, its future use and how it is stored and transferred. Adhering to the GDPR is a demonstration of the quality of your operations and will strengthen relationships with clients and candidates through a greater level of transparency and increased confidence that you adhere to the highest standards.

Our commitment to the GDPR

Invenias is committed to full compliance with the GDPR. In addition, we are equally committed to providing access to the tools and services necessary for our customers to ensure compliance with the legislation on their own terms.

Whilst the formal date for the legislation has been set as 25 May 2018, we know and understand that we need to ensure compliance well in advance of the deadline. Our customers can have confidence that they are on the right platform and are fully supported in their compliance journey.

Privacy has always been at the heart of our business and is an essential part of what we do. Our customers rely on us to take care of their sensitive and confidential data, and that of their candidates and clients, as carefully as we would our own.

We have been on an ongoing journey of developing and improving our security procedures, processes and systems throughout the business and we see this as a process of continuous improvement.

The GDPR brings an awareness and responsibility to the wider market which we welcome and support. Our customers and partners will rightly expect us to demonstrate full compliance in ample time for the deadlines and we can confidently commit to this objective.

To date, in line with many of the most forward looking companies across the EU and beyond, we have been focussed on raising awareness and gathering information. We have undertaken training and orientation for our Executive Team and across the company and validated how our service provides compliance to our customers. We have also begun a series of publications, webinars and workshops for our customers and prospective customers to ensure they are informed and aware of the GDPR requirements and are supported in their compliance process.



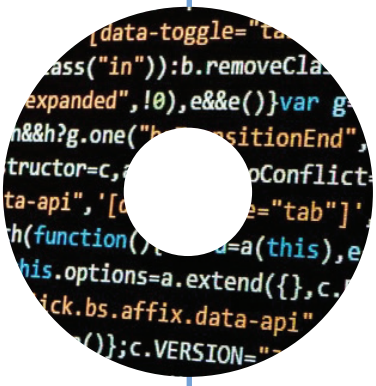
Andy Warren
Chief Information Security Officer and CFO

GDPR in 3 Words: The Three Cs

The forthcoming changes to data protection legislation are complex and must be given appropriate consideration. However, when thinking about the personal data held within your organisation, we believe that consideration of the Compliance, Consent, and Communication obligations of the GDPR is a good place to start.



Compliance



Consent



Communication

Compliance



Compliance

Under the GDPR, you are accountable for complying with the principles that personal data is:

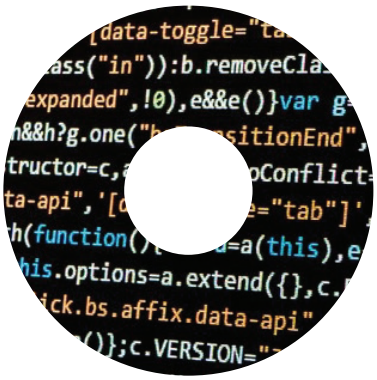
- processed lawfully, fairly and in a transparent manner
- collected for a specified explicit and legitimate purpose
- adequate, relevant and limited to what is necessary and kept for no longer than necessary
- accurate and up to date
- secure

Although the principles of accountability and transparency have previously been implicit requirements of data protection law, the GDPR's emphasis elevates their significance. Under the new legislation, you must be able to demonstrate and prove your compliance. You are obliged to implement technical and organisational measures to provide evidence that you have considered and integrated data protection into your processing activities and data protection must be at the heart of everything you do. In addition, data can only be transferred to organisations with adequate safeguards.

Article 5(2) requires that:

"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

Consent



Consent

The move to the GDPR will require organisations to review their current consent practices and audit their existing consents. Under the new legislation, consent will mean offering individuals the opportunity to positively opt-in. Under the GDPR, silence, pre-ticked boxes or inactivity is presumed inadequate to confer consent and indeed, organisations must also ensure that a transparent opt-out option is readily available.

Under the GDPR consent must be:

- freely given, specific, informed and unambiguous
- a statement or clear affirmative action

In addition to obtaining consent, organisations must keep clear records and be able to demonstrate evidence of consent if required.

Under the new legislation, organisations must inform individuals of their right to withdraw consent at any time and their rights to be forgotten; to have access to their personal data and their right to be informed.

Organisations should review their existing consents and check they comply with the new GDPR, if they do not fresh consent must be obtained.



Communication

In order to ensure compliance with the communication obligations of the GDPR, there are two key areas for consideration.

Rights to access

Under the GDPR, individuals will have the right to obtain:

- confirmation that their data is being processed
- access to their personal data and other supplementary information

In addition, if you are transferring personal data to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards relating to the transfer.

Right to be informed

The information you supply about the processing of personal data must be:

- concise, transparent, intelligible, easily accessible
- written in clear and plain language
- and free of charge

Organisations must inform individuals at the time of obtaining data directly from them or within a reasonable period (a month) in the case of data obtained from other sources; or if the data are used to communicate with the individual, at the latest, when the first communication takes place.

FAQ

Q. What impact will the GDPR have on companies based outside of the EU?

The GDPR is focused on the rights and freedoms of EU citizens. If you are processing data on, or providing goods or services to, EU citizens, then you will need to comply, regardless of your location.

Q. Will Britain's decision to leave the EU impact on the GDPR?

The UK Government has committed to complying with the GDPR by 25 May 2018, under the same timescales as the EU. So, Brexit makes no real difference assuming that post Brexit, the UK will have implemented the GDPR and will be deemed an adequate jurisdiction for data privacy.

Q. How will the GDPR be enforced?

The EU Commission will increase the powers of Supervisory Authorities (SAs), the local geographic data protection bodies. These will include investigative powers (audits, reviews, notifications) and supervisory powers (warnings, compliance orders, fines) and will be supported and underpinned by the rule of European Law. Member States will have individual discretion to decide the rules on criminal sanctions for infringements of the GDPR.

Q. Will the new legislation be applied to information we already have stored within our systems?

Yes. Once the act is in force it will apply to all personal data relating to EU citizens regardless of when it was acquired.

Q. What are the financial implications for non-compliance?

Fines imposed could be up to the greater of EUR20 million or 4% of worldwide turnover.

Checklist: what do you need to do right now?

The list below, provides a number of areas for consideration prior to the May 2018 deadline. A review of these items will ensure that the processes and policies you have in place will minimise risk of non-compliance.

- [ ] **Awareness**
  You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR.

- [ ] **Information you hold**
  You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit across the organisation or within particular business areas.

- [ ] **Communicating privacy information**
  You should review your current privacy notices and put a plan in place.

- [ ] **Individuals' rights**
  You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

- [ ] **Subject access requests**
  You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

- [ ] **Processing software**
  You should review your applications and tools to ensure that your systems, access rights and documentation processes are adequate for compliance.

Legal basis for processing personal data

You should look at the various types of data processing you carry out, identify your legal basis for carrying it out and document it.

Consent

You should review how you are seeking, obtaining and recording consent and whether you need to make any changes.

Data breaches

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

Data Protection by Design and Data Protection Impact Assessments

You should familiarise yourself now with the guidance the ICO has produced on Privacy Impact Assessments (PIAs) and consider how to implement them.

Data Protection Officers

You should designate a Data Protection Officer, if required, or someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements.

International

If your organisation operates internationally, you should determine which data protection supervisory authority you come under.

Extracts from Information Commissioner's Office, Preparing for the General Data Protection Regulation (GDPR) 14/3/16, licensed under the Open Government Licence.

Checklist: specific questions to consider

- [ ] **Candidate placement**
  What are the trigger points for informing and consent?

- [ ] **Candidate assessment**
  Where are the risks in recording opinion?
  What are the privacy rights of referees?
  Could information held be detrimental to the candidate in future?

- [ ] **Role research**
  What are the informing/consent obligations regarding existing candidate databases?
  What is the risk of non-compliance?

- [ ] **Candidate tracking**
  At what point should you inform a potential candidate?
  What are the levels of consent?

- [ ] **Candidate/contact history**
  For how long should you maintain history?
  What data is necessary?

- [ ] **How long are records kept?**
  What are the requirements of audit, discrimination and privacy?
  How could they conflict?

☐ **Purging non-relevant data**

How is this done/decided?

☐ **Access to information**

Who has access to information?

Where are they located? This is particularly relevant for cross border processing (especially via mobile devices).

If/when transferring data to other organisations, do they have adequate safeguards?

☐ **Current data and where it came from**

What data do you currently hold?

Where did it come from?

Can you evidence consent?

☐ **Record keeping**

Can you prove that processes were followed?

Can you provide evidence if required?

For additional resources and more information regarding the GDPR requirements and how they will impact the executive search profession visit www.invenias.com/gdpr.

About Invenias

Invenias is the world's leading provider of cloud-based software solutions to the executive search profession. With offices and hosting centres across Europe, the US and Asia, Invenias has over 800 customers globally and supports thousands of users across sixty countries. Customers include global executive search firms, strategic recruitment firms, in-house executive recruitment teams, and executive talent organisations within Private Equity and VC firms.

Invenias has a strategic global alliance with the AESC, and customers include leading searchs firms such as Norman Broadbent, Sheffield Haworth, Stanton Chase, The Miles Partnership and Zygos Partnership as well as leading organisations such as Expedia, General Atlantic, Royal Bank of Canada, Samsung, Tesco and Tesla Motors.

For further information on Invenias please visit www.invenias.com or email insight@invenias.com.

This guide should not be taken as a substitute for legal advice.
Copyright © 2017 Invenias. All Rights Reserved.