GDPR

Webinar Guide

Overview and key points

Part 1 of our series on GDPR and its impact on the recruitment industry

isv.online testing and training people

Voyager RECRUITMENT SOFTWARE YOUR BEST CONNECTION

evolve

Introduction

The rules which underpin the storage of personal data have changed dramatically. The new EU-US Privacy Shield is important for firms that share data between the UK and US, but is actually far less significant than the GDPR rules that have major impact on how the recruitment (and indeed all) industry operates.

These rules, which were passed last year and will be enforced from 2018, will dramatically raise the bar on privacy standards and will come with fines that are large enough to cripple the majority of firms in the industry – and, indeed, virtually any supplier!

Technology and infrastructure suppliers could play a key role in helping recruitment firms stay within the rules.

What is GDPR?

GDPR stands for The General Data Protection Regulation. It's a set of rules designed to cover data protection for residents of Europe and is the successor to the Data Protection Directive. The rules are in place now, but they are not being enforced until May 2018. The difference in terminology is important. A Regulation is much more robust and enforceable than a Directive.

All EU citizen data is within scope of GDPR, irrespective of the geographical location of the firm responsible for the data. In other words, non-EU firms handling EU citizen data will still have to comply with GDPR. The vote for Brexit does not affect the applicability of GDPR to the UK. In addition to this the ICO recognises that the current DPA is woefully out of touch with changes in technology / data practices and have stated that they will be producing legislation of comparable strength to the GDPR.

If you store information on European citizens (referred to as Data Subjects) in a database, outlook contacts, a spreadsheet, paper files or anywhere else – you need to follow the new rules.

Can I ignore it?

Although many of the rules are similar to the current directive, the key differences are as mentioned this is a regulation rather than a directive and more importantly we have the size of the fines for infringement.

The rules allow for fines of up to 4% of the annual worldwide turnover of an organisation or EU20 Million – whichever is the higher.

Many recruitment firms may not wish to risk a fine that could destroy the business! Further, GDPR explicitly gives data subjects the rights to compensation in cases of relevant non-compliance.

Key highlights

GDPR requires all personal data collected to be gathered lawfully, and for specific purposes only. In addition, it must be used solely for the purposes for which it was collected.

Consent to store or process data has to be explicitly given by a clear, affirmative action.

Consent is not indefinite, time limits needs to be established for erasure or review and consent can be revoked at any time.

Whilst it appears that some publicly available data is exempt (where a log-in is required to access the data, it is unlikely to be defined as publicly available) any commentary or information about the candidate which goes above and beyond this (and could potentially impact on a person missing out on an opportunity) would not be.

A data subject is entitled to request access to any data held about them (and this should include any notes and comments about the data subject). They also have the right to rectify or erase the information. Typically, recruitment firms will be unable to charge for this service, and it should be provided "without undue delay and at the latest within one month of receipt of the request."

Where data has come from a source other than the person, the subject is entitled to know from where it originates. This will potentially impact on confidential sourcing. Candidates will need to be told and consent established within 30 days of the collection of the data.

Decisions based purely on automated processing are not allowed. However, so long as human intervention is involved, this should not be problematic. Technologies associated with automated "Searching and Matching" of candidates to jobs may be more problematic.

In the event of a data breach, notification should typically occur within 72 hours.

There are new rules relating to the transfer of data outside of Europe. Currently, only 11 countries are considered "adequate" from a data protection perspective. If you wish to send data overseas, you will need a legal justification for it. Data transfer to the US is covered by the "Privacy Shield" and your vendor should already be registered for it. We are on that list but unfortunately, very few recruitment solution providers are currently.

All of these rules are true for data that you may collect in future – but also for any data you have previously stored in your systems. The fact that data was stored before the rules kicked in will not be considered a justification for not treating it appropriately.

What should you be doing now?

Clearly, your database vendor can play a key role in helping you stay within the rules. However, in most firms, the database will not be the only storage tool. You may have information in spreadsheets, outlook contacts, folders and so on. Some of this may be stored in secure cloud servers, some of it may be saved on local machines or even mobile devices. This is unlikely to be sustainable – if you are storing personal data in an unsecure environment you are taking a big risk.

The end points, defined as an individual users particular workstation, laptop, phone etc, coupled with staff themselves are the greatest source of risk for any business. Staff training on GDPR and general data security principles should be provided and regularly tested.

A good initial step would be to audit your use of data, what it is, where it is kept, who has access to it and how it is stored. In addition, if your firm works in the US then you should ensure your vendor is registered under Privacy Shield.

What are we doing to support our clients?

Whilst historically the data controller (i.e. the Business) has been the primary focus of data protection rules, under the new policies, data processors (which include the companies who store the data on behalf of the controllers) are equally liable.

Controllers of data (i.e. you) are now only allowed to work with processors (i.e. suppliers like us) who guarantee support for these rules. As a result, suppliers are going to need to make very significant investments to ensure that they stay legal.

As one of the largest software groups specifically targeting the recruitment sector, our business is investing a six figure amount in 2017 into our infrastructure, with comparable investments in product development to ensure that our technology is fit for purpose.

In January 2017 we became an early adopter of the Privacy Shield rules and expect to remain at the forefront of these changes. We will provide our clients with further information on this later in 2017.

In the meantime our series of webinars are designed provide more information in bite sized chunks in conjunction with our LinkedIn group.

GDPR

Overview and key points

Part 1 of our series on GDPR and its impact on the recruitment industry

Who are we?

- Dillistone Group Plc, a public company listed on the AIM market of the London stock exchange
- Includes the brands Voyager Software Ltd, ISV Software Ltd, FCP internet Ltd, and Dillistone Systems
- Thousands of clients in over 70 countries both Recruitment and Corporate with some of the largest clients in those fields

DISCLAIMER

- This webinar is provided for information purposes and is **NOT** intended to be legal advice pertaining to the subject matter
- If you have specific questions on how this may affect your organisation you should consult a legal professional
- Guidance and member state regulator interpretation is ongoing – GDPR is dealing with a highly complex scenario and one size does not fit all
- This is the first part of a series of webinars and is therefore not designed to cover everything in one sitting!

This webinar is provided for information purposes and is NOT intended to be legal advice pertaining to the subject matter. If you have specific questions on how this may affect your organisation you should consult a legal professional.

What is it?

- General Data Protection Regulation (Regulation (EU) 2016/679)
- 99 Articles and 173 recitals
- Replaces the 1995 EU Data Protection Directive (Directive 95/46/EC)
- Adopted 27 April 2016
- Compliance to be achieved by 25 May 2018
- Some derogation to member state law – e.g. age an individual is considered a child

- To summarise a directive is more an order listing objectives to be completed, a regulation is a rule, a law. It is a legal binding force that must be followed and abided by each member state.

What is its aim?

- To standardise data legislation across the EU in common law.
- To replace the outdated legislation prevalent across EU members.
- To provide a robust level of protection to EU data subjects with individuals having 8 core rights under GDPR.
- To remove a stumbling block when trading and transferring data to other member states.
- To define “data breach” and provide rules governing what happens in the event of one.
- To provide a stringent framework of penalties to aid compliance
- To work with other legislation such as PECR and the forthcoming ePrivacy Directive

Am I impacted and what about Brexit?

- Applies to ANY organisation offering goods and services to EU Residents
- It is therefore not limited to firms in the EU
- Applies to ANY organisation who has EU staff/establishments
- The UK has not yet triggered Article 50 and will still be in the EU come May 2018
- Even if the UK were not in the EU come May 18, the ICO has stated "complimentary and comparable" legislation would have to be implemented in the UK

- "There's a lot in the GDPR you'll recognise from the current law, but make no mistake, this one's a game changer for everyone." Elizabeth Denham, Information Commissioner. Jan 17

Definitions

- Data
- ICO
- Data Controllers
- Data Processors
- Data Processing
- Data Subject
- Personally Identifiable Information (PII)

Data

- Not just 1s & 0s!
- IP Tracking*?
- B2B. Individuals who work at organisations are potentially considered “natural persons” so GDPR will likely apply to B2B and consumer data

- **Regulators and case law says yes to IP tracking but likely that further clarification will be forthcoming*

Data Controllers

- Means *the* natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data

- *This means you need to be thinking about why you have it, how long you have it, what is it being used for and why is it necessary. You are ultimately responsible for it*

Data Processors

- Means *a* natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller
- Processors can share the accountability for non-compliant processing

- Examples could be: Outsourced data cleansing companies, outsourced telesales, outsourced payroll, companies that store your data….etc.

Data Processing

- Means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including –

  (a) organisation, adaptation or alteration of the information or data,

  (b) retrieval, consultation or use of the information or data,

  (c) disclosure of the information or data by transmission, dissemination or otherwise making available, or

  (d) alignment, combination, blocking, erasure or destruction of the information or data

Data Subjects

- Natural persons who can be directly or indirectly identified by the controller or a third party using reasonably likely means

Personally Identifiable Information (PII)

- Means 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
- Sensitive data such as biometric, racial and ethnic origin, trade union membership, political opinions etc “deserve specific protection”
- Member state law will control processing of data about criminal record

GDPR – Some of the key points

- You typically will need affirmative consent to hold PII, for example, candidate data.
- Consent is NOT indefinite, data should not be retained indefinitely
- Data can be transferred from one controller to another without charge
- Subject Access Requests can only be charged for “if excessive & unreasonable”
- Data minimisation
- Integrity and confidentiality (security)
- Accountability

Fines – GDPR has some very big teeth

- Fines can be levied on both data controllers and data processors
- Can be imposed for a wide range of contraventions. Similar to employment law this includes procedural infringements
- Some contraventions will be subject to administrative fines of up to €10,000,000 or 2% of global turnover, whichever is the higher
- Others will be subject to administrative fines of up to €20,000,000 or 4% of global turnover, whichever is the higher

Data Controllers and Processors – know your obligations

- Do you hold PII data? (Staff, Clients, Candidates, Prospects……)
  - ✓ You are a Data Controller
  - ✓ You are also a Data Processor
- If a supplier hosts your recruitment CRM database they are additionally a data processor which you as controller are responsible for!
- GDPR imposes new and increased compliance obligations on Data Controllers & Processors

Controller obligations include (but are not limited to):

- Primary responsibility for ensuring that processing activities are compliant with EU data protection Law. Must be able to demonstrate compliance
- Only appoint processors that guarantee their own compliance with GDPR
- Maintain records of processing activities including:
  - Purpose of processing
  - Data Retention Periods
- Ensure data security of personal data that they process, for example data encryption, cyber security testing
- Undertake DP Impact Assessments where appropriate

Obligations – Data Breaches

- ANY breach to must be reported to the regulator within 72 Hours
- “Breach” is defined as one that leads to the accidental or unlawful destruction, loss, alteration unauthorised disclosure of, or access to PII
- Must inform data subjects under certain circumstances
  - Article doesn’t specifically oblige this but some member states have implemented reporting requirements in their respective national laws
- Excel spreadsheets, Outlook Contacts/Data in Outlook for example are potentially very problematic

Consent

- Consent is not the only method by which lawful processing of data is permitted
  - Legitimate interests – must be able to demonstrate that their legitimate interests to process personal data are not overridden by the fundamental rights and freedoms of the data subject
    - Recital 47- A legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is the client or in the service of the controller.
- In our space consent is likely to the principle method
- If the candidate approaches the Agency it is reasonable to infer consent (as noted later an audit trail should be maintained)

Consent

- Affirmative
  - Candidate **must** confirm that you can hold their PII
- Maintain audit of consent
- Verbal is OK but remember need an audit trail
- It is not indefinite and you should have a policy on data retention
- 'Renewal' may not require affirmative response from candidate
- Data subjects are entitled to require a controller to delete their personal data (Right to be Forgotten)
- ICO currently reviewing their draft guidance on the issue of consent in GDPR. Watch this space….

Transparency

- When requesting consent you must provide (amongst others) in a clear and understandable form:
  - Identity and contact details of controller
  - Purpose of processing*
  - Are legitimate interests being relied upon
  - Categories of personal data held
  - Who the recipients might be
  - If its to be transferred outside the EU how is it protected
  - Origin of personal data
  - Period to be stored or criteria used to define storage period
  - The logic of any automated processing
  - How to exercise your rights
  - The right to withdraw
  - The right to complain to a regulator

*Cannot subsequently use for another purpose without additional consent

Data Subject Access Requests

- Largely identical to current regulations
- BUT cannot charge by default anymore
- Reasonable assumption that new consent process will lead to an increase in DSARs
- There will be some debate as regards what needs to be provided – some data that is PII might be deemed commercially sensitive:
  - Comments about a candidate, correspondence about a candidate is PII
- Likely to be more requests for data rectification also

Data Portability

- Data subjects have a right to receive a copy of their personal data in a commonly used machine-readable format, and transfer their personal data from one controller to another or have the data transmitted directly between controllers

- This is likely to be highly contentious. Do you send a full data pack to a possible competitor or selectively parse data out. Database providers could assist but would require stringent control on data entry

- Further guidance is expected on this

Data currently held

- Unfortunately there is no simple transparent guidance. BUT
- It is clear that Candidate data with no audit of consent and no evidence that you have engaged with the candidate or supplied a service
  - You will need **affirmative** consent to hold the data
- If there is evidence that a service has been supplied and of engagement with the candidate this could be considered as implied consent
  - Consent is not indefinite and needs to renewed based on your retention policy
  - Best practice would be to contact these candidates

Cross Border Data Transfers/Access

- Cross-Border Data Transfers are prohibited, unless certain conditions are met
- Cross-Border Data Transfers to a recipient in a third country may take place if the third country ensures an adequate level of data protection
- The list of approved countries is very sparse at the moment http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm
- Care needs to be taken here. Accessing cloud data hosted in Europe from outside the EU is “data in transit” and hence has not been transferred. Take a laptop overseas with cached outlook data or saved phone contacts for example and the data is considered “at rest” ie its left Europe and you have transferred it!

What do I do about it?

- To recap GDPR is live now! May 2018 is the enforcement date and you have until then to get compliant
- You have a lot of obligations under GDPR eg “Controllers are obliged to engage only those processors that guarantee to implement appropriate technical and organisational measures.”
- You need to think not only about your recruitment CRM. You will hold PII on your staff, likely on your suppliers as well as your candidates and contacts
- You may need to appoint a DPO
- You will possibly need a whole stack of new policy and procedure

What else do I need to think about?

- As we said its not just about your CRM. It about the total data security of your business. For example:
  - Has every leaver had their access to all systems (and your offices) revoked?
  - Do you have a data retention policy and more importantly do you keep to it?
  - Do you know where you data goes?
  - Are you registered with the ICO?
  - Are your staff regularly trained on data security?
  - How secret/strong/rotated are your passwords?
  - Do you have a Privacy Impact Assessment?
  - How many people have access to your systems?
  - How are you protecting your local systems?
  - BYOD?
  - …..

What are some of the things we do?

- ✓ We have to be able to demonstrate that Information security is at the forefront of our developmental decisions
- ✓ Annually penetration tested
- ✓ Data encrypted
- ✓ Intrusion Detection Systems
- ✓ Data access control
- ✓ US privacy Shield
- ✓ Staff background checked
- ✓ Annual audits
- ✓ Aiming for GDPR compliance

OK, so there's a lot to this…

- Firstly, don't panic…
- Secondly, don't ignore it
- We'll be running other events including a follow up to this webinar next month where we'll be briefly recapping what we have spoken about today, looking a little more at both the "internal" and "external" facets of GDPR, as well as areas that might impact certain sectors of recruitment more than others
- We'll further be covering:
  - What makes processing legal, Controller and processor liability, DPO's and will you need one?, Impact assessments, Record keeping, Rights of Natural persons as well as Profiling

OK, so there's a lot to this…

- In addition to this webinar series there will be a Linked In group set up which will cover various articles on GDPR, the ePrivacy directive, check lists to help get you prepared along with blogs and other features
- We'll also be using this forum to keep you informed and get your feedback on some of the tools and solutions we're creating to help with some of the challenges of GDPR and potentially help keep you ahead of the competition
- https://www.linkedin.com/groups/8599770

Q & A

- Any questions we are unable to get through we'll post the answers on the LinkedIn forum.

- https://www.linkedin.com/groups/8599770