GDPR

Legalities, Policies and Process

Part 3 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
- ISO/IEC 17024 GDPR-F certified

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 third 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.

A quick recap

- **Slides will be available as a download at the end of this webinar**
- In Part 1 of our series we looked at GDPR in general
- In Part 2 we looked at Consent, Rights of data subjects, Privacy by design focussing on Data Protection Officers and Data Privacy Impact Assessments

Today

We'll look at:

- What makes Processing legal?
- Controller and Processor Liability
- What are the types of policies and processes you need to have in place (and tested!)
- Data security in general
- Enforcement and Penalties
- Certifications

What Makes Processing Legal?

- Material Scope of GDPR
  - In Scope
    - Personal data processed wholly or partly by automated means
    - Personal data that is part of a filing system, or intended to be
  - Out of Scope
    - Personal data such as boarder checks/immigration
    - Personal data for purpose of crime prevention
    - Personal data used purely for personal activity

What Makes Processing Legal?

- 6 Principles of Processing personal data
  - Processed fairly and lawfully
  - Adequate, relevant and limited to what is necessary
  - Accurate, and where necessary, kept up to date
  - Collected for specified, explicit and legitimate purposes
  - Kept for no longer than is necessary
  - Processed in a way that ensures security

- **ALL THIS MUST BE DEMONSTRABLE BY THE CONTROLLER**

What Makes Processing Legal?

- Lawfulness or processing
  - The reality is there are really 6 ways in which lawful processing of personal data can be undertaken:
    - It's necessary for the performance of a contract
    - It's necessary to protect the vital interests of the subject
    - It's in compliance with a legal obligation
    - It's in the public interests or excising official authority
    - It's with the consent of the data subject
    - It's in the legitimate interests of the controller, or 3rd party except where such interests are overridden by the rights and freedoms of the natural person

What Makes Processing Legal?

- Legitimate Interests (see recital 47)
  - Exists in the DPA
  - Processing must be in the “reasonable expectations” of the subject
  - Interpretation is vital*
  - Process data of employees or clients as there is a relevant and appropriate relationship between Subject and Controller
  - Can be used for the prevention of fraud
  - Consideration of the balance of interests
  - Needs to be fully documented. Ie can you demonstrate that you considered the subjects rights and freedoms.

Controller and Processor Liability

- **Quick recap on definitions:**
  - **Data Controller**
    - 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
  - **Data Processor**
    - Means *a* natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller
  - **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

Controller and Processor Liability

Controller obligations:

- Comply with GDPR
- Implement appropriate technical and organisational measures
- Implement data protection policies
- Demonstrate compliance
- Adhere to relevant codes of conduct

Controller and Processor Liability

Data Protection by design and default

- Implement appropriate technical and organisational measures (eg encryption)
- Personal data is restricted to only those that need it
- Data minimisation
  - The amount of data
  - The extent of the processing
  - Period of storage
  - Accessibility of data

Controller and Processor Liability

Processor obligations

- Should be contracted to:
  - Process only as per documented instruction from the Controller
  - Take appropriate security measures
  - Ensure individuals processing data observe confidentiality
  - Deletes or returns all data at the end of contract period
  - Assists the Controller by appropriate measures
  - Makes available to the Controller any appropriate information to demonstrate compliance

Policies and Process

How can I demonstrate that I comply? (from ICO)

- You must:
- Implement appropriate technical and organisational measures that ensure and demonstrate that you comply. This may include internal data protection policies such as staff training, internal audits of processing activities, and reviews of internal HR policies.
- Maintain relevant documentation on processing activities.
- Where appropriate, appoint a data protection officer.
- Implement measures that meet the principles of data protection by design and data protection by default. Measures could include:
  - Data minimisation;
  - Pseudonymisation;
  - Transparency;
  - Allowing individuals to monitor processing; and
  - Creating and improving security features on an ongoing basis.
- Use data protection impact assessments where appropriate

Policies and Process

Records of processing activities (documentation)

- As well as your obligation to provide comprehensive, clear and transparent privacy policies if your organisation has more than 250 employees, you must maintain additional internal records of your processing activities.

Be careful here if you are a temps agency

- If your organisation has less than 250 employees you are required to maintain records of activities related to higher risk processing, such as:

  • processing personal data that could result in a risk to the rights and freedoms of individual; or
  • processing of special categories of data or criminal convictions and offences.

Policies and Process

What do I need to record?

- You must maintain internal records of processing activities. You must record the following information. There are some similarities with ‘registrable particulars’ under the DPA which must be notified to the ICO.
  - Name and details of your organisation (and where applicable, of other controllers, your representative and data protection officer).
  - Purposes of the processing.
  - Description of the categories of individuals and categories of personal data.
  - Categories of recipients of personal data.
  - Details of transfers to third countries including documentation of the transfer mechanism safeguards in place.
  - Retention schedules.
  - Description of technical and organisational security measures.
- You may be required to make these records available to the relevant supervisory authority for purposes of an investigation.

Policies and Process

- The following post on our LinkedIn group details some of the policies that we are applying. Some of these are taken from ISO 27001 and some are GDPR specific

https://www.linkedin.com/groups/8599770/8599770-6263713440427184132

Policies and Process

- Lets look at two of these:

  1) Data Inventory (more physical)

  2) Impact Assessment (more flow and risk)

- Whilst these may well require a lot of time and effort to produce, as we have seen they can go a long way to helping identify any risks in your business and can cover a number of the responsibilities on you under GDPR

General Data Security

GDPR states Controllers and Processors must implement a level of security appropriate to the risk, which can include:

- pseudonymisation and encryption of personal data
- ensure the ongoing confidentiality, integrity and availability of systems
- a process for regularly testing, assessing and evaluating the effectiveness of security measures
- security measures taken need to comply with the concept of data protection by design
- take steps to ensure that any natural person working for the controller or processor only processes data under explicit instruction unless required to do so by EU or Member State law.

General Data Security

What can you be thinking about?

- End users are both the greatest asset and liability
- Undertaking a data audit will help show up vulnerabilities
- What is your BYOD policy?
- Who advises you on such matters?
- Who enforces your security policies?
- When was the last time your staff were trained on data protection and security?
- When were they last tested?
- Has your organisation been penetration tested? Has your hosted CRM/payroll/HR etc supplier?
- Who ensures that all leavers have had all system access suspended?
- Is all this audited to demonstrate compliance?

- **How would you know you have been breached??**

General Data Security

Clearly some of the things we have talked about can cost disproportionately large amounts if you are trying to do it all yourself. Multi-layered intrusion detection and countermeasures can run into 5 or 6 figures without breaking a sweat

Similarly having you or IT supplier managing security of self hosted systems with encryption etc is likely to become more expensive as more organisations become switched on to the threat

However some of the most effective security strategies can be the cheapest, although granted in some cases if you are not used to it could be perceived as an admin burden.

General Data Security

Good places to start

- Do that data inventory (yes I'm going to keep on about this)
- Check access rights to all your personal data applying GDPR principles
- Password protect your payslips
- Set domain and key system password policies
- Educate your staff (I'm going to keep on about this too!)
- Check your building security – access control and staff awareness
- Think about a BYOD policy
- Encrypt machines (something like Windows Bitlocker)
- Set 6 monthly review meetings about your general data security
- Get rid of anything you don't need
- Look at your suppliers – some can become processors and take some of the burden if they are taking security seriously. Do your due diligence.
- Always ask what else can we be doing?

Enforcement and Penalties

Conditions for imposing fines (Article 83)

- Fines to be “effective, proportionate and dissuasive”
- European Data Protection Board (EDPB) to ensure consistency in application of GDPR
- Supervisory body can in addition or instead of imposing fines:
  - Issue warning
  - Issue reprimand
  - Order compliance
  - Communicate a breach directly to the data subject

Enforcement and Penalties

Conditions for imposing fines (Article 83)

- The supervising body may consider (amongst others):
  - The nature of the infringement
  - Any action taking by the controller or processor to mitigate the damage
  - What technical and organisational measures were implemented
  - How cooperative have you been
  - The manner in which the infringement became known
  - Adherence to approved codes of conduct/certification mechanisms
  - Any previous infringements

Enforcement and Penalties

Conditions for imposing fines (Article 83)

- What attracts the largest tier of fines? (€20m or 4% TO)
  - Infringements relating to the following articles:
    - Principles of processing personal data (5)
    - Lawfulness of processing (6)
    - Conditions for consent (7)
    - Sensitive categories of data (9)
    - Subject rights (12-22)
    - 3rd country transfers (44-49)
    - Provision of access to supervisory body (58)
    - Orders on processing/suspension of data flow (58)

Enforcement and Penalties

Conditions for imposing fines (Article 83)

What about the €10m or 2% TO level?

Infringements relating to the following articles:

Childs consent(8)
Processing not requiring identification (11)
Data protection by design & default (25)
Joint controllers (26)
Controller representatives not in the EU(27)
Processing (26,28-30)
Cooperation with the supervisory body (31)
Data Security (32)
Breach notification (33 & 34)
DPIA (35)
Prior consultation (36)
DPO (37-39)
Codes of conduct (41)
Certification (42)
Certification bodies (43)

Enforcement and Penalties

Right to compensation and liability (Article 82)

Any person having suffered material or non material damage shall have the right to compensation from the Controller or Processor

Controller involved in processing is liable for damage caused by the processing

Processor liable only for damage caused by (their) processing or where it has acted contrary to lawful instruction of the Controller

Joint and several liability

Certifications

- **Under Article 42 (Certification)**
  - There will be the establishment of data protection certification mechanisms (eg ISO 27001, C GDPR-P)
  - Development of certification bodies (Eg GASQ)
  - Certification bodies must be approved by Supervisory Authorities
  - Certification voluntary
  - Certification valid for 3 years
  - Certification does not absolve controller from need to comply
  - Possible development of EU Data Protection seal

Next Time…

- Unlawful data and what can you do about it?
- Sample contract & data collection notices
- Outsourcing vs In-house from a GDPR point of view
- The GDPR vs PECR and B2B marketing debate
- Binding Corporate Rules

- Any updates from the ICO/working parties.

Reminder

- In addition to this webinar series there is 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