TaylorWessing

Preparing for the General Data Protection Regulation

Practical guidance for job boards

9 November 2017

General Data Protection Regulation (GDPR)

- Comes into force: **25 May 2018**
- Expands the scope of European data protection
  - offering goods and services to data subjects in the EU
  - monitoring EU data subjects
- No soft landing
- Implemented in UK notwithstanding Brexit

- Directly applicable law, creates a framework: Member States to "fill in the gaps" subject to fundamental principles
  - draft UK Data Protection Bill published on 13 September 2017

- Extra-territorial scope – beyond Europe
- Enforcement: "one stop shop"

What does the GDPR mean for you?

- As data controllers, you will need to review how you collect, hold and process personal data as well as how you communicate with individuals
- New measures and principles will need to be adopted into internal processes and policies – the aim of the GDPR is a **culture shift**
- Job boards hold personal and sensitive personal data for candidates – already subject to fines (several earlier this year)
- Also need to think about your own staff and the steps you will need to take

Summary: key aspects of the GDPR

Implications for job boards

Why care?

> Under the GDPR, increased fines in two tiers:

- **Tier 1:** up to **2% of annual worldwide turnover** of the preceding financial year or **10 million Euros** (approx. $11 million) (whichever is greater) for violations relating to internal record keeping, data processor contracts, data security and breach notification, data protection officers, and data protection by design and default
- **Tier 2:** up to **4% of annual worldwide turnover** of the preceding financial year or **20 million Euros** (approx. $22 million) (whichever is greater) for violations relating to breaches of the data protection principles, conditions for consent, data subjects' rights and international data transfers

> To put this in context:

- Under the DPA 1998, maximum fine is £500,000
- In 2016, 21 fines were issued for a total of just over £2 million (average fine of around £100,000)

What stays the same?

- **Key concepts:** personal data, processing, data controllers etc.
  - definitions of “personal data” and “sensitive data” have been expanded
- **Data protection principles:** similar to what we have under DPA
  - new accountability principle (demonstrating compliance)
- **Conditions for processing:** similar under GDPR (e.g. consent, performance of a contract and legitimate interests)
  - but some changes to how these are relied upon
- **Data subject rights:** broadly recognisable (subject access, rectification, processing restrictions), but there are some new ones
- **Basic data security obligations:** basic obligations are the same but there are some increased requirements and clarification with GDPR
- **National authorities:** ICO still the UK national supervisory authority

What is changing?

- **Consent:** conditions for obtaining consent have become stricter
- **Transparency:** obligation to provide greater information to individuals
- **Access rights:** greater rights given to individuals to access their personal data
- **Privacy by design and default:** obligation to build appropriate privacy requirements into day to day operations
- **Breach notification:** mandatory breach notification to privacy regulators and affected individuals in the event of certain breaches
- **Accountability:** organisations will have to demonstrate compliance to regulators on an ongoing basis and maintain records
- **Data Protection Officer:** obligatory in some circumstances and jurisdictions
- **European Data Protection Board:** overarching authority, will adjudicate on disputes arising from national supervisory authority decisions
- **Sanctions**

Individual rights (job seekers or candidates)

- **Data rectification rights: (enhanced)**
  - entitled to have personal data rectified if it is inaccurate or incomplete
  - requests will normally have to be processed within one month
- **Data deletion rights – the right to be forgotten: (new)**
  - request deletion of personal data in certain circumstances
  - respond without undue delay and within 1 month of the request
- **Data portability right: (new)**
- **Process restriction: (enhanced)**
  - right to restrict data processing e.g. if an individual considers processing is unlawful or they contest the accuracy of the data
  - if personal data is restricted, the controller can only store the data until the restriction is lifted
- **Right to object: (enhanced)**
  - limited circumstances – no right to object to processing in general

In-depth: Individual rights and what you need to consider

What are the practical implications?

Processing personal data

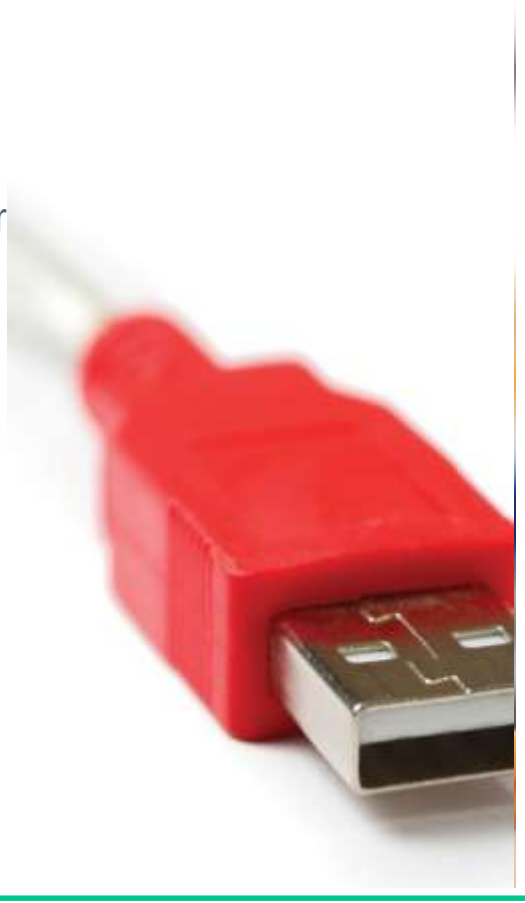
- Two grounds for processing personal data
  - consent
  - legitimate grounds for processing
- Legitimate grounds include the following:
  - for the performance of a contract
  - for compliance with a legal obligation to which the processor is subject
  - to protect the vital interests of the individual, or another individual
  - for the legitimate interests of the processor or a third party, except where overridden by the interests or rights of the individual

Consent

- Under GDPR, consent must be:
  - freely given
  - specific and informed
  - unambiguous
  - given by a statement or clear affirmative action
  - be able to be withdrawn at any time
- Not freely given if:
  - there is no genuine or free choice
  - there would be detriment if the consent was refused or withdrawn
- Reliance on contractual wording as a catch-all
- Privacy notices

Sensitive personal data

- Broadly the same as under the DPA
  - processing permitted where necessary for carrying out an obligation under a contract or a collective agreement
- Sensitive personal data includes data relating to:
  - political opinions
  - religious or philosophical beliefs
  - health
  - genetic and biometric data
- Common examples – criminal records and medical records



SARs under the GDPR

- SARs under GDPR: a growing problem
  - £10 fee removed
  - reduced timeframe for response
  - no restriction on number of requests
  - first copy provided free
  - requirements for provision of information
  - limited exemptions
  - **significantly higher penalties for non compliance (higher tier)**

- Potential pitfalls
  - onerous requests
  - requests for non-data protection related purposes
  - scope

Monitoring, personalisation and recordings

- Monitoring & personalisation
  - Personalisation – what data and where from?
    - basis for monitoring
    - monitoring carried out by non-EU entities
    - PIAs
- Informal communications (whatsapp, texts etc.)
- Social media
- Technology and recording
    - monitoring and recording staff (email trackers, CCTV etc.)
    - candidate recordings – voice / video recordings?
    - covert recordings

Overseas transfers, cloud solutions and cross border operations

> Consider international transfers of personal data, including where you:
  - use equipment, servers or resources located overseas
  - outsource database or recruitment resources
  - use cloud-based database, storage or other resources

> Inform candidates (and staff) – privacy notices

> Ensure that your staff do not allow personal data to be inadvertently transferred overseas without safeguards and process being followed

> Processing personal data in or for individuals in multiple EU jurisdictions – who is the lead regulator?

Third party providers

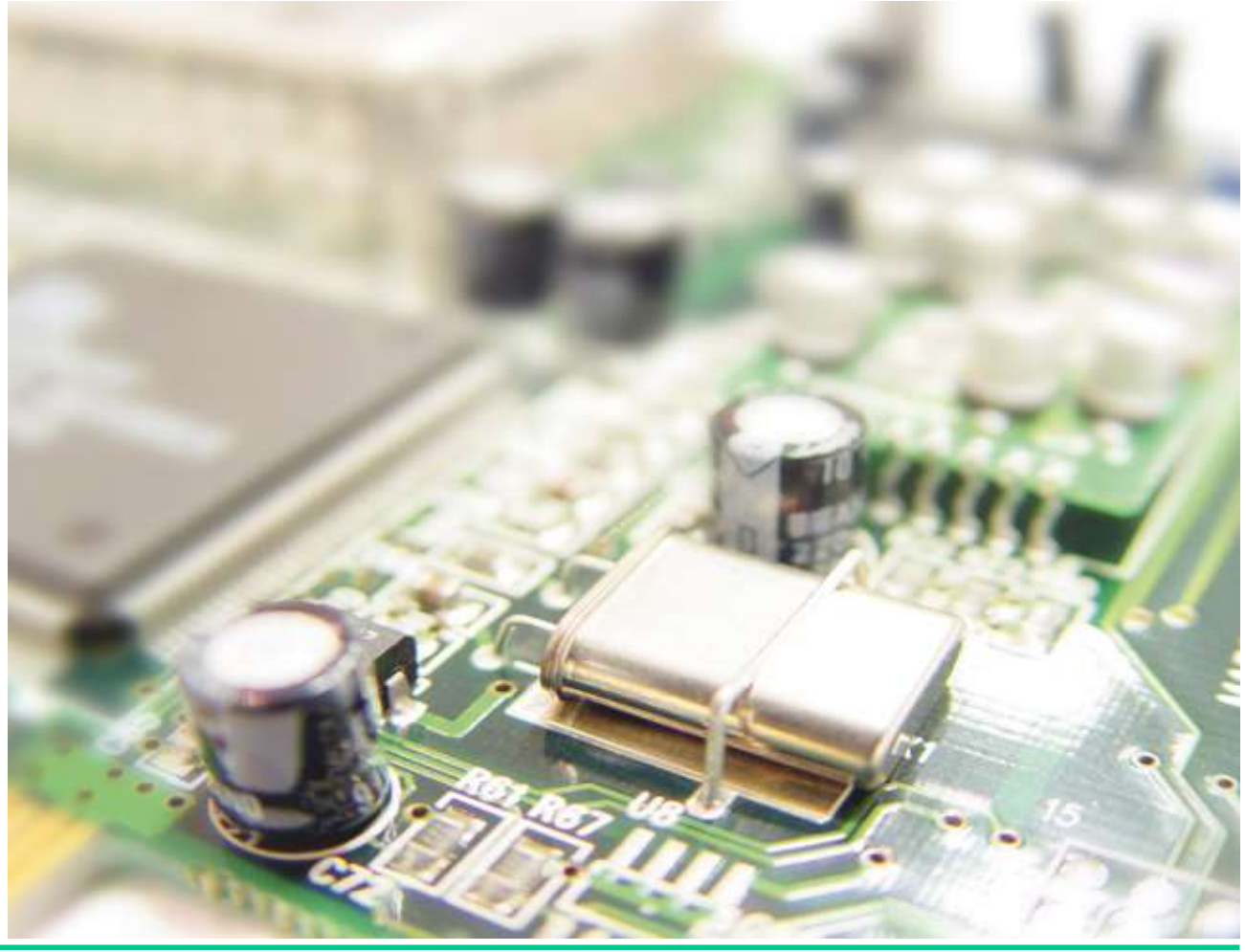
> Data is often processed by third party providers
  - data collection and storage
  - cloud-hosted systems, payroll, CRMs

> **Next steps:**
  - Review contract terms – are these GDPR compliant? Do they provide for sufficient safeguards?
  - Inform candidates / staff:
    - **what** do / have you told them?
    - **when** do you tell them?
  - Amend contract terms – to include appropriate levels of data security and instructions from you on how to process data

Data retention

- **Data retention:** data collected should be –
  - only keep what is necessary for the purpose obtained
  - do not keep for longer than is necessary for the purpose retained or as required by law
- **Record keeping:**
  - requirement to keep suitable records of data processing activities that concern high risk processing **OR** records of all data processing activities
  - records need to be clear and easily accessible
- **Data security:**
  - requirement to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk
  - review security measures regularly
  - size of your organisation and how it operates
  - volumes and nature of personal information processed and shared
  - potential harm that could result from a security breach

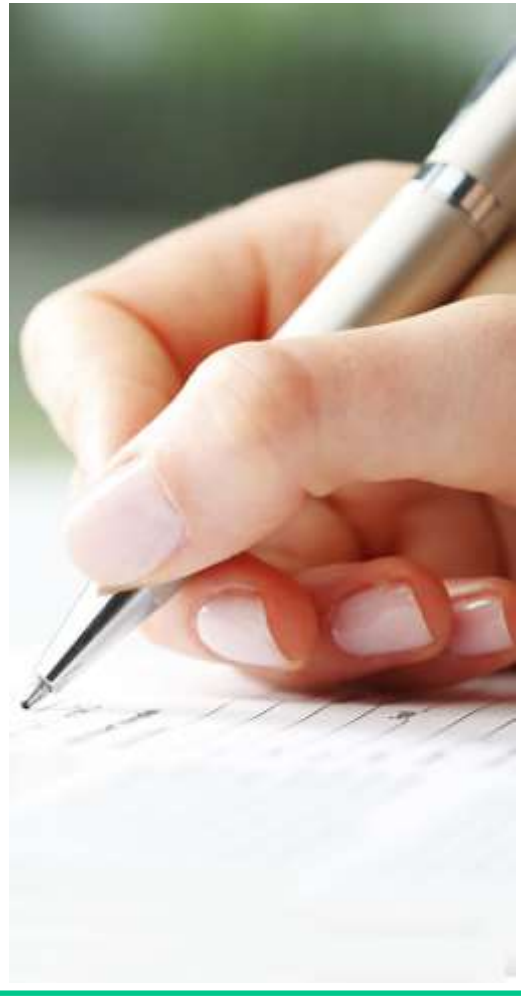
What should you be doing now?



Preparing for the GDPR: Audit and Action

> **Review and identify:**
  - what **personal** and **sensitive personal** staff data you obtain, process, store
  - how data is stored, used and accessed
  - where data is stored, used and accessed
  - the grounds on which you do so
  - what data do you obtain or share with third parties
  - monitoring – what and where

> **Rectification** – prepare an action plan
  - what, when, who?
  - internal support?
  - external support?



Policies & training

> **Think about:**
  - your audience
  - your compliance obligations and what you need to show

Candidates	Employees	Managers
• Privacy notice • Policy framework • Information on how to exercise individual rights	• Basic policy framework (to extend the privacy notice) • Information on how to exercise individual rights	• Access rules / parameters • Retention standards • Recordkeeping requirements • General communication and data processing standards

> Data protection by “design and default"
  - put policies into operation
  - reinforce by training

> Ongoing training and keep records of attendance

Evidencing compliance: documents **AND** processes

- **Policies, contract and other documentation**
  - Communications are key for candidates and staff alike
    - review template documents
    - privacy notices and informing staff and candidates
    - update contracts and handbooks for staff
    - update policies and notices for candidates
    - update policies – data protection, data retention and destruction policy
    - other related policies, e.g. disciplinary and grievance, homeworking, information and IT security, terms of use for company devices,
  - **e.g. subject access requests**
    - managing and responding to SARS
    - polices and procedures
    - training

Processes – how will you implement and support?

- Practice and processes – changing culture
  - How will you implement key GDPR requirements?
    - withdrawal of consent
    - management of deletion of records
    - notification to 3rd parties of rectified personal data
    - data portability
    - record keeping
    - internal data breach reporting
- Training
- Breaches and high impact response
    - reporting – internal escalation and external reporting obligations
    - investigations and audits
    - crisis response and breach management
    - reputation management

Where to start?

> ICO – published guidance

> Initial free resources – loads, including TW's:
  - Microsite with free HR data assessment tool
  - Global Data Hub
  - Law at Work

> Assessment tools

> Think about what support you will need, internally and externally

Any questions/other issues?

> Law at Work July 2017

> International Law at Work on Recruitment and background checks

> Global Data Hub

> HR Data Microsite

Stephanie Creed
Associate
s.creed@taylorwessing.com
02073007011