HR & GDPR 1 YEAR ON

WITH REBECCA LABRAM

www.signalbizhub.org

GDPR one year on

Rebecca Labram

June 2019

peopleclever
practical hr solutions

Where are we now?

- As of 3rd July 2018, complaints to the ICO had increased by 160% from pre-25th May 2018 levels. In real terms that was 6281 complaints.
- Over a quarter of complaints were about large organisations processing large volumes of sensitive data.
- Many small organisations still working towards compliance, employees often overlooked as a group of data subjects.

peopleclever
practical hr solutions

GDPR – common terms

- **Data subject -** a **living** individual who is the **subject** of personal data**;**
- **Personal data** - any information about a **data subject;**
- **Data processing** means doing anything with personal data!
- **Special categories of data** –(previously referred to as sensitive data) personal data where there are **significant risks to individual's rights and freedoms**, includes genetic data and biometric data (not criminal data which is handled separately under Article 10);

peopleclever
practical hr solutions

Overview

- GDPR (Data Protection Bill) came into effect 25 May 2018 in the new Data Protection Act (2018)
- Previous cap on fines of £500,000 for serious data breaches under old DPA replaced with maximum **£20m Euro or 4% of global turnover**, whichever is the **greater.**
- Subject Access Requests now free (unless excessive) and response must be without undue delay and within a month.

peopleclever
practical hr solutions

GDPR – key principles

- **Accountability** - organisations must be able to **demonstrate** they are compliant, this is not a box ticking exercise
- **Enhanced rights for data subjects** - more control over their data and how it is used
- **Transparency** - Privacy notices and policies written in clear and concise language - notices must be **accessible**
- **Privacy by design and default** – considering security first in all data processing

peopleclever
practical hr solutions

Who does it apply to?

- Sole traders, micro-entities, businesses of every size from 1 person plus.
- If you are a business dealing with personal data you must be compliant and you may need to be registered with the Information Commissioner's Office.

peopleclever
practical hr solutions

Lawful bases

Under the GDPR all personal data that is processed by a business must be processed lawfully under one of the following bases:

- Consent
- Contract
- Legal obligation
- Vital interests
- Public task
- Legitimate interests

You must tell data subjects at the point of collecting their data:

What you are doing with it, how long your are keeping it, who and where you might transfer it to (share it with) via a Privacy Notice.

peopleclever
practical hr solutions

Enhanced rights for Data Subjects

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Rights re automated decision making including profiling

*Not all rights are absolute and depend on **lawful basis***

peopleclever
practical hr solutions

The right to be informed

Privacy Notice – the notice(s) provided to data subjects at the point of collecting personal data, both external and internal. Best practice is to split notices into concise versions for different groups of data subjects: eg employees, applicants, clients.

- consider the audience, use visual aids/icons
- Break it down into layered notices/just in time

Privacy Policy – sometimes combined with notice depending on size of organisation. This is usually an internal document detailing:

- your security arrangements;
- organisational guidelines for employees when handling personal data.

peopleclever
practical hr solutions

Special Categories of data

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation

Organisations need an **appropriate policy document** if they are processing special categories of data. Special categories also need an Article 9 condition as well as a lawful basis.

peopleclever
practical hr solutions

Data processing – Consent

- if you cannot offer a genuine choice, consent is not appropriate and you must use a different lawful basis;
- must be **freely given**; not part of terms or conditions;
- can be withdrawn at any time without detriment;
- must be granular, specific to each process;
- must keep clear records of all consent;
- Existing consent is unlikely to be adequate where organisations are in a position of power such as employers in the employment relationship.

peopleclever
practical hr solutions

Data processing – employees

Employees are data subjects too!

That means that all employees must receive privacy notice information when they commence employment, as well as when there is any change to how their information is processed.

It is no longer appropriate to use consent within the employee contract as it is tied to terms and conditions.

peopleclever
practical hr solutions

Exercises

1. You take on a supplier to help you with your marketing. The supplier is a sole trader and based at home. She sends you an invoice at the end of the month.

Is this personal data or commercial data? Does the GDPR apply?

2. An ex-employee contacts you and asks you to provide them with a copy of their file and for you to delete their HR file from your records. Do you need to comply with their request?

peopleclever
practical hr solutions

Exercises

3. You are collecting business to business data via a form on your website so you can tailor your services. Do you need to provide privacy information on the form?

4. You hold a very successful event promoting your business, lots of clients attend and you upload a series of photos to your company Facebook page. A client contacts you to complain that her photo has been uploaded without her consent and asks for you to remove it. There are several other people in the photo and you really like it. Does she have the right to complain and what do you need to do?

peopleclever
practical hr solutions

Security

Follow the principle of Privacy by Design and Default

Ensure good practice:

- Do **not** share email addresses or passwords
- Run antivirus software regularly
- Do not use personal devices for company business
- Ensure passwords are updated regularly and are alphanumeric with special characters for extra security
- Keep hard copies of personal data in locked cabinets
- Clean desk policy
- Safe disposal of hard copies

peopleclever
practical hr solutions

It’s not too late!

- Identify data protection lead
- Carry out a Data Audit and map your data to the appropriate lawful basis
- Document your findings in your Privacy Notices and Policy
- Carry out Data Impact Assessments and Legitimate Interests Assessments where needed.
- Design appropriate policy document for special categories
- Privacy notice(s)/Policy communicated to all data subjects
- Ensure you have appropriate security measures in place
- Empower your employees to use best practice
- Update consent where consent is lawful basis
- GDPR compliant contracts in place with all your data processors (suppliers)

peopleclever
practical hr solutions

In summary

- Do I need it?
- How will I use it?
- What lawful basis applies?
- Where will I store it?
- Is it secure?
- How long will I keep it?
- How will I safely dispose of it?
- Have I given the data subject privacy information via a notice?
- Am I following Data Protection Policy?

peopleclever
practical hr solutions

GDPR – free resources

- Visit www.ico.org.uk for codes of conduct, checklists and detailed guidance.
- Visit www.acas.org.uk for how GDPR relates to employees

Thank you and questions?

Questions about this presentation can also be emailed to me at rebeccalabram@peopleclever.com.

peopleclever
practical hr solutions