Business Forum Mid Devon

Clyst Information Systems

GDPR – relevant even to small businesses!

William Lines
Clyst Information Systems

Why this new law?

- Replaces laws conceived in 1995
- So much has changed since then:
  - Technology available
  - How we use technology
  - (almost) Everyone uses the web
- EU worried by businesses' attitude to personal data
- Key reasons for the new law:
  - ATTITUDE
  - TECHNOLOGY


Clyst Information Systems
Under investigation
£400,000
£150,000
£70,000
£10,500
£80,000
£100,000

ICO research (Nov 2017) shows that **people simply don't trust** organisations to look after their personal data

INFORMATION COMMISSIONER'S OFFICE - TRUST AND CONFIDENCE IN DATA

An online survey of adults in the UK about trust and confidence in data.

- Only a fifth of the UK public report (20%) having trust and confidence in companies and organisation storing their personal information.

The EU's Response: GDPR

- EU legislators and officials very focussed on the rights of the individual
- Increasing sense of public distrust in organisations' attempts to safeguard personal data
- Update needed due to changes in data use, development of IT capabilities, and extensive use of social media
- Key focus of GDPR is to offer **transparency** and **accountability**

What you need to know

Personal Data - relates to a natural living person (not to a business entity) “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”

Think: staff, business partners, customers

What you need to know

Processing of personal data includes “collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction”

Think: computer, phone, cloud, paper filing, desk diary, backups, archives

What you need to know

Data controller – essentially the “owner” of the collected data

Data processor – any other organisation that has access to or works on personal data collected by or for the data controller

Think: accountant, mailing list, IT maintenance, website

What you need to know

Lawful Basis for processing personal data:

- **Consent**: the individual has given clear consent for you to process their personal data for a specific purpose.
- **Contract**: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- **Legal obligation**: the processing is necessary for you to comply with the law (not including contractual obligations).
- **Vital interests**: the processing is necessary to protect someone's life.
- **Public task**: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- **Legitimate interests**: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

What you need to do

Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now

1. **Awareness**
   You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

2. **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.

3. **Communicating privacy information**
   You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

4. **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.

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

6. **Lawful basis for processing personal data**
   You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

7. **Consent**
   You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.

8. **Children**
   You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.

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

10. **Data Protection by Design and Data Protection Impact Assessments**
    You should familiarise yourself now with the ICO's code of practice on Privacy Impact Assessments as well as the latest guidance from the Article 29 Working Party, and work out how and when to implement them in your organisation.

11. **Data Protection Officers**
    You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer.

12. **International**
    If your organisation operates in more than one EU member state (ie you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.

ico. Information Commissioner's Office

ico.org.uk

V2.0 201705

What you need to do

1. **Keep records of what you do**
2. **Know what personal data you hold**
   - **Where (IT systems, phones, paper filing, etc.)**
   - **Why (by consent or some other lawful basis)**

What you need to do

3. **Check / update and publish:**
   - **Privacy Notice**
   - **Data Protection Policy**
   - **Data Retention, etc.**
4. **How you will support Individuals' Rights**
   - **Delete data**
   - **Subject Access Request, etc.**

What you need to do

5. **Children – if processing data about children it requires special care**

6. **Security**

   - **Check your security systems**
   - **Cyber Essentials scheme**
   - **Plan how to identify and respond to data breaches**

7. **Training for staff**

Don’t delay…

Lots of advice at https://ico.org.uk

- Guidance documents
- Phone helpline for small businesses
- Checklists

Commissioner Elizabeth Denham said on 2 February 2018 “While there will be no grace period – you’ve had two years to prepare – I know that when 25 May dawns, there will be many organisations that are less than 100 per cent compliant.”

Also “if you self-report a breach, engage with us to resolve issues, can demonstrate effective accountability arrangements, you will find us to be fair.”

Questions…?

William Lines

Clyst Information Systems

william@clystis.co.uk

07743 329367