GDPR

General Data Protection Regulations

Principles and Practice

Paul Lethbridge

ChiasmaData

paul@chiasmadata.com

t: +44(0)7880 706162

ChiasmaData

Principles

- **Proportionality**
  - *The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality.*
- **Objectives**
  - *The objectives and principles of Directive 95/46/EC remain sound, but it has not prevented fragmentation in the implementation of data protection across the Union, legal uncertainty or a widespread public perception that there are significant risks to the protection of natural persons, in particular with regard to online activity.*
- **Access**
  - *Where personal data are processed for the purposes of direct marketing, the data subject should have the right to object to such processing, including profiling to the extent that it is related to such direct marketing, whether with regard to initial or further processing, at any time and free of charge. That right should be explicitly brought to the attention of the data subject and presented clearly and separately from any other information.*

Automation & Scale

- **Automated Processing**
  - *The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention.*
- **Scale**
  - *The processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer. In such cases, a data protection impact assessment should not be mandatory.*

Process

- The major difference between current and proposed legislation is “Process”
  - *The principles remain very similar but now you have to prove that you can do it.*
- If you receive a data subject request can you?
  - *Explain exactly how and when you got the consent*
  - *Explain what the consent covers*
  - *Demonstrate that you have adhered to it*
  - *Show that the consent is still valid*
  - *Explain where the data is stored and the protocols for its access*
  - *Show how you monitor for data breaches and who the **responsible person** is.*

Controller and Processor

- Under current legislation the Processor is only liable for errors – the Controller is responsible for compliance
- Under GDPR both Controller and Processor are equally liable.
  - As fines are large it is likely that Controllers may carry a larger risk if a small agency is managing your data.
  - Maximum fines are 4% of turnover or €20m (whichever is the larger)

Consent vs Legitimate Interest

- Consent
  - Freely given, explicit and informed
    - Clear processing notices
    - No pre-ticked boxes
    - Double opt-in for email
  - More difficult in the context of a large differential in power between the data subject and controller
    - Companies acquiring consent to access your Facebook page as part of an employment process would be construed as a consent not freely given
- Legitimate Interest
  - It is likely to be most appropriate where you use people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.
  - If you choose to rely on legitimate interests, you are taking on extra responsibility for considering and protecting people's rights and interests.
    - I need your DoB before selling you alcohol
    - I need your medical history before administering chiropracty
    - I need your address to deliver x
    - I need your email address to send an invoice

Access, Rectification & Erasure

- **Access**
  - The data subject should be able to see what information you hold
  - What consents are held
  - The basis of processing where automated decision making or profiling are involved
- **Rectification**
  - A change of consent
  - The altering of a material fact
- **Erasure:** “The right to be forgotten”
  - A difficult one as you need to have a good view of where the data is held
  - Balance “forgetting” against retaining records required for audit, contractual or regulatory compliance
  - Remembering that you forgot them.

…and the Practice

1. You need to market your business, you buy a list from “The Big List Company”. Is this legal? What are your responsibilities?
2. You don’t have an in-house marketing function – you ask an agency to email a target audience and create the campaign? What are your responsibilities?
3. You put a bowl on the table at an event to gather email addresses. You put these into a mailing list and start emailing them. What do you need to do to comply?
4. Your marketing manager stores your contact list in a spreadsheet and uses it to email clients with her latest offers. How would you respond to a Freedom of Information request or a GDPR subject access request?
5. Your new employee signs a non-disclosure form that says the company has permission to read his email on the company’s server. Is this reasonable and compliant?
6. A client negotiates a mortgage through you and you communicate the progress of the mortgage through a series of emails. Can the emails contain marketing promotions?
7. An employee is unhappy with their treatment and requires that you send all of the information you hold on them to their solicitor. Do you have to comply?
8. We will sometimes share your details with selected third parties – tick here if you agree… Is this GDPR compliant?

Q & A