GDPR: May 25, 2018

ChiasmaData

GDPR – It's serious

The General Data Protection Regulation (GDPR) will be adopted into the UK on May 25, 2018. The UK Government has confirmed that this legislation will be unaffected by the decision to leave the EU.

While many of the principles of data protection remain the same, the processes and procedures that must be in place to achieve compliance have been significantly tightened.

The maximum fines that can now be applied by the ICO (Information Commissioner's Office) for non-compliance or data miss-use have increased to £20m or 4% of global turnover – whichever is the higher.

GDPR, the Principles

Acquiring Data

Data is collected with a specific purpose in mind and in accord with the following principles:

1. **Consent**: positive, explicit, informed and freely given
2. **Legitimate Interest**: the data is need in the fulfilment of a contract or activity.
3. **Legally Required**: to comply with legislation the data is needed.

Data must be processed in a manner consistent with the consent given. A data subject must be able to:

1. View their own data
2. Change their data
3. Require that it be deleted (the right to be forgotten)

Consent is not forever. If the consent was granted in the past and there has been no recorded interaction with the subject then the consent must be refreshed or lapsed. The length of time depends on context and is a judgement.

Restricted Data

Certain data is proscribed. Explicit consent is required if you are collecting information that reveals a subject's:

1. Racial or ethnic origin
2. Political opinions
3. Religious or philosophical beliefs
4. Trade union membership
5. Genetic data or biometric data
6. Medical status, health or sex life
7. Sexual orientation.

Securely Processed: the data must be processed in a secure manner. Including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

- In a smaller company a spreadsheet of customer details on a laptop is not secure.
- Sending email lists to colleagues via email is not secure.
- Leaving email lists on FTP sites is not secure.
- Leaving a yellow sticky with your password on the computer is not secure.

Not Just Marketing

There is a tendency to think that data protection is primarily about marketing consent and permission. It also applies, with equal force, to data collected in the transacting of business or in recording information about employees.

Business Processes

You need them!

If you cannot identify an audit trail showing where a consent was acquired and how that data has subsequently been used you are in breach.

You need to be able to identify and notify a data breach when it occurs within 72 hours of the event.

You need to have a named individual who is responsible for seeing that all this happens.

When does GDPR NOT apply?

The intent of GDPR is to make the use of automated communications and the storing of bulk data more secure and responsible. If it's just you and your personal contacts on an outlook file for one-to-one communications – you're not the target of this legislation.

GDPR: May 25, 2018

ChiasmaData

Some Practical Examples

1. You need to market your business, you buy a list from "The Big List Company". Is this legal?
    a. 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?
    a. 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.
    a. 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.
    a. 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.
    a. 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.
    a. 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.
    a. Do you have to comply?

8. We will sometimes share your details with selected third parties – tick here if you agree…
    a. Is this GDPR compliant?

What Next?

Take a close look at your processes and make sure it is somebody's day job to understand the implications for the organisation. You have to demonstrate compliance – so review, design and document the processes by which you acquire and manage consent.

"Specifically, audit your consent procedures now and seek refreshed consent if you are unsure – by May next year it will be too late"

ChiasmaData designs, builds and manages databases, reporting and business intelligence solutions. If you would like to discuss how we might help you make more of your information, simply email paul@chiasmadata.com or call 07880 706162.

Chiasma Data Limited·info@chiasmadata.com·+44 (0)1276 919819
Basepoint Business Centre·377-399 London Road·Camberley·Surrey·GU15 3HL