GDPR: May, 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

1. Data must be **processed lawfully**, fairly and in a transparent manner in relation to individuals.
2. It must be collected for **specified, explicit and legitimate purposes**. Further processing for archiving purposes, scientific or historical research purposes or statistical purposes are permitted if compatible with the initial purposes.
3. The data collected should be **adequate**, **relevant** and limited to the stated purposes.
4. **Accurate** and up-to-date; inaccurate or irrelevant data must be erased or rectified without delay.
5. Kept **no longer than is necessary** for the purposes for which the personal data are processed; archiving, in the public interest, scientific or historical research or statistical purposes allow a longer retention period.
6. **Securely** processed including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Controller or Processor

Prior legislation placed all the responsibilities of data processing on the "Data Controller": usually the organisation that owned and used the data. The Data Processor – unless negligent – simply did what they were told.

From May 2018, both Processor and Controller have similar duties of care and the Controller, in addition, needs to ensure that all contracts make clear the Processors responsibilities and can **prove compliance.**

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

GDPR: May, 2018

ChiasmaData

The GDPR legislation is detailed so some items, of arguably more immediate concern, are:

Consent

Consent is essential: the prior legislation would allow a "failure to opt-out" as a granting of consent. This is no longer the case. You will need **explicit and informed consent**. This means:

- No pre-ticked boxes or burying the consent in an information request form
- **Double opt-in** on all email subscriptions
- **Third party data** without proof of source and double opt-in with explicit consent to give the data to you is **not allowed**
- **Record and remember** where the consent came from
- Clear and simple methods to allow **unsubscribes**
- Let users **edit/ delete** their own data

"Fresh consent will be required after May 2018 if you cannot prove that your data acquisition methods were compliant with the new legislation."

Right to Erasure

Otherwise known as "the right to be forgotten" This right, conferred under the GDPR, requires that you can identify where any data about the subject is held and either delete it, have mechanisms in place to obfuscate the data or place it beyond use.

In particular, if the data has been shared with a third party you must know that this has happened and have processes in place to ensure the third-party's compliance.

This should be of particular concern in any organisation where you know or suspect that lists of customers and their contact details have been passed around in spreadsheets.

"If you are currently dependent on spreadsheets or similar desktop tools for data processing then you are in trouble!"

Documented Processes

GDPR requires that the organisation has documented processes to comply with the various aspects of GDPR. For example:

- If a data or security breach occurs what happens, who is informed, what safeguards are in place?
- You have 72 hours to inform the relevant supervisory authority of an identified breach – how will you achieve this?
- What process is applied to granting access to personal data within an organisation?
- How are clients to be informed?
- How are third-parties to be informed?
- Who is responsible for compliance within the organisation?

Restricted Processing

GDPR grants the right of a subject to restrict the processing of their data to only the narrow purpose of storing it without its further use.

The conditions around this can be complex but having the ability to isolate data and remove it from regular processing is required.

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.