Ashtons LEGAL

overview of the gdpr

Useful information about the new Data Protection law - GDPR - in effect from 25th May 2018.

Data Protection Principles

Personal data must be:

- Processed lawfully, fairly and transparently
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary
- Accurate and kept up to date
- Kept no longer than necessary
- Processed with appropriate security.

Accountability Principles

There are new obligations to implement appropriate measures to ensure and demonstrate that you comply with the GDPR including undertaking and documenting privacy impact assessments. Some organisations will be required to appoint a Data Protection Officer. Organisations with more than 250 employees have additional internal record keeping obligations.

Lawful Basis of Processing

The lawful basis for processing personal data is more important under GDPR. The lawful processing conditions are:

- Consent of the data subject (there is a greater emphasis on consent being freely given, specific, informed and unambiguous)
- Necessary for the performance of a contract
- Necessary for compliance with a legal obligation
- Necessary to protect the vital interests of a data subject or other person
- Necessary for the purposes of legitimate interests pursued by the controller.

Individual's Rights

The GDPR codifies existing rights of data subjects and creates new rights:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure or ‘right to be forgotten’
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

Fair Processing Information

Data subjects must be provided with certain information when data is first collected probably through more detailed privacy notices.

Subject Access Requests

Similar to existing rights but with the time to respond reduced to one month (with the ability to extend for complex requests) and the removal of the £10 fee.

Breach Notifications

The GDPR incorporates new obligations to notify data subjects and the ICO of certain data breaches within 72 hours of the breach.

steps to take to comply with gdpr

1. Plan

Create a project team reporting to senior management team to oversee compliance to ensure that have a coordinated approach to prepare for May 2018.

2. Data Protection Officer

Consider if you are required to appoint a DPO or if it would be helpful to do so. Identify appropriate candidate with necessary authority, skills and experience.

3. Audit

Identify what categories of personal data you hold or process and consider as a starting point in relation to each category:

- Why was the data collected and what is it used for?
- What will be the appropriate legal basis of processing under GDPR?
- If relying on consent consider whether way in which consent is obtained complies with GDPR.
- Is any of the personal data passed to any third parties?
- Is any of the personal data ever transferred outside the country?

4. Data Processor Agreements

Review agreements with third parties who process personal data on your behalf. In particular consider stronger breach notification requirements.

5. Privacy Impact Assessments

Start adopting a 'privacy by design' approach and consider privacy impact assessments in respect of existing processing of personal data and put in place process for considering and recording decisions in respect of future data processing plans.

6. Privacy Notices

Review existing notices and prepare to update or replace to make GDPR compliant. You will almost certainly need different notices to be issued to different data subjects.

7. Data Breaches

Establish procedures to detect, report and investigate personal data breaches.

8. Staff Awareness

Consider updating policies and guidance and rolling out a training programme to bring staff up-to-date with the changes in the law and how your organisation has responded.

James Tarling

PARTNER

T: 01603 703233
E: james.tarling@ashtonslegal.co.uk
Norwich

James specialises in corporate finance transactions and advising innovative technology companies. He has a wealth of experience in leading corporate transactions and guiding businesses through complex intellectual property, data protection and privacy issues. James also has particular experience within the motorsport industry with clients valuing his detailed under-standing of the technical and sporting regulations governing the sport.