Newtons solicitors

GDPR Fact Sheet

3rd May 2018

What is data?

Data is 'personal data' if it contains information relating to an identified or identifiable natural person. It will include things like a name, online identifiers (such as an IP address) and location data.

'Sensitive' personal data includes information such as racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

What is the GDPR?

GDPR is the General Data Protection Regulation and represents the biggest shake-up in data protection for 20 years. It is designed to provide greater transparency and accountability for personal data. It comes into force on 25th May 2018 and the potential fines for non-compliance are significant.

What can your organisation do in simple terms?

- Review existing data you've collected and identify whether your organisation collects and processes data caught by the GDPR.
- Assuming it does, identify exactly what conditions you rely on to process personal data and sensitive personal data. Do you have a legitimate interest in processing data (if so, what is that legitimate interest?) or do you rely on consent perhaps – you need to be clear. If you rely on consent, your procedures for obtaining/ managing consent should be reviewed to ensure they meet the higher threshold under the GDPR.
- Ask whether your organisation's conditions for processing data have an effect on individuals' rights.
- If you process large amounts of genetic, biometric or health data, be extra careful of any further restrictions that might be imposed by individual Member States.

<u>The Information Commissioner's Office – 12-Step Checklist</u>

1. **Awareness and Training –** You can ensure that decision-makers and key people in your organisation know that the law is changing and understand the impact it will have on what you do, including any specific areas which may cause potential compliance issues;
2. **Information you hold -** Document what personal data you hold and where it came from as well as who you share that data with. Where you process data on more than an occasional basis you will need to document those processing activities as well as where there might be any risk to the rights and freedoms of individuals or if you process any sensitive 'special category' data;
3. **Communicating privacy information -** Update your privacy notices to comply with the GDPR. You should provide this information at the time personal data is obtained and should

also include the right for the data subject to withdraw their consent if you rely on that consent as a basis for processing their data;

4. **Individuals' rights** - Check procedures to ensure that they cover all the rights individuals have, including when and how you would delete personal data and the different formats of data used and provided by you;
5. **Subject access requests -** Update procedures and plan how you will handle requests to take account of the new rules. Individuals and customers you deal with should be able to access their personal data easily and in a concise, transparent and intelligible form;
6. **Lawful basis for processing personal data -** You should identify what lawful basis you use for processing data, you should then document that basis and update any privacy notices to explain it;
7. **Consent -** Under the GDPR, data subjects must be able to withdraw their consent to processing at any time and withdrawing that consent must be as simple as when the individual gave it in the first place. Consent should be explicit - freely given, specific, informed and unambiguous. For example, silence, pre-ticked boxes or inactivity should not constitute consent;
8. **Children -** If you process children's data you should pay particular attention to data protection by design. Privacy notices for services provided directly to children must be written in such a way that their understanding is borne in mind;
9. **Data breaches** - The correct procedures must be in place to help detect, report and investigate any breach of personal data. You should also consider pseudonymising and encrypting any personal data you hold, for example;
10. **Data protection by design** – This means that people who control data within your organisation must have in place measures to implement the GDPR's six data protection principles;
11. **Data protection officers** - Consider whether you should appoint a data protection officer (or perhaps a privacy manager) on either a mandatory or a voluntary basis. This might, for example, depend on the size of your organisation and the particular types of data that you process;
12. **International -** If you have a 'cross-border' or an international/ wider European presence you should map out who your lead data supervising authority is and what measures are in place to comply with the different jurisdictions that you may deal with.

Should you require any assistance, a member of our Commercial Department would be pleased to assist with your data protection requirements or address any specific questions you might have.

Oliver Hebdon
Solicitor
Newtons Solicitors Limited

T: 01642 711 354
E: oliver.hebdon@newtons.co.uk