SME SOLICITORS

Stallard March & Edwards LLP

Data Protection

General Data Protection Regulation

The General Data Protection Regulation (GDPR) is due to come into force in the UK from May 2018. Here we summarise some of the key points of GDPR for our business and employer clients:

1. **Subject Access Requests –** the 40 day period for complying with a request is reduced to a month under the GDPR. In most cases you will no longer be able to charge a fee, although you may be able to charge a "reasonable fee" for excessive or repetitive requests or for further copies of the same information.

2. **Data Protection officer –** the GDPR requires you to appoint a Data Protection Officer if you are a public authority, carry out regular and systematic monitoring of individuals on a large scale, or are an organisation that carries out large scale processing of special categories of data or data relating to criminal convictions and offences. In any event you may wish to appoint somebody within your business to be responsible for data protection compliance given the greater responsibilities that may apply to you under the GDPR.

3. **Processors –** data protection requirements will apply to Processors as well as Controllers. The Data Controller is the person (or organisation) who decides the purpose for which and manner in which personal data is processed. A Processor is any person (or organisation) which processes personal data on behalf of a Controller. Processors will now have to maintain records of personal data and processing activities and will become liable for breaches. This will apply to employers of 250 or more people, or for those with less than 250 people, those who deal with sensitive, high risk or more than occasional processing. This could catch many employers, and businesses that process information about customers, employees or suppliers. Processors face fines or other penalties, which they did not generally face under the Data Protection Act.

4. **Consent**- requirements for processing data based on consent have been tightened up. If your business relies on consent for processing people's data, you must get clear affirmative consent for each purpose of processing. In most cases, this is more than just ticking a box to say a customer understands their data will be processed. Burying consent provisions for data processing within a large contract such as a contract of employment, or a parent contract for a school, is not likely to satisfy the higher criteria for consent. Consent needs to be expressly and freely given and it may be appropriate for it to be dealt separately within its own document. There are other grounds on which you are authorised to process data however, including carrying out legal obligations or where it is necessary to perform a contract with the person whose data you are using.

5. **Privacy by design** – When bringing in new technologies (such as a computer system), or carrying out high risk processing, businesses will need to conduct a Data Protection Impact Statement.

6. **Strict notification rules** – these will apply for breaches of the GDPR and data protection rules. If a breach results in a high risk to an individual, then it will need to be reported within 72 hours in most cases. A breach is more than just losing data, and would include destruction, loss, alteration, unauthorised disclosure or access to the data. A breach that could lead to financial loss, damage to reputation, lead to discrimination, loss of confidentiality or other disadvantage would normally be notifiable. Loss of customer details where a breach could leave them open to identify theft would be notifiable, for example.

7. **The Right to be Forgotten –** this will apply in some circumstances. Individuals can ask you to delete their personal data in some cases, including where they withdraw consent, and where it is no longer necessary for the purpose for which it applies. You can refuse in some cases, including such as where you need to hold onto it for a legal obligation, or where it is used in exercising the right of freedom of expression and information. However the rights of individuals to be forgotten are expanded under the new GDPR.

8. **Children's personal data –** the GDPR enhances children's rights under data protection law. If services are offered directly to children, then a privacy notice must be written in a clear and plain way. If you target online information services at children, you will ordinarily need to obtain the consent from a parent or guardian of the child, in a fair and reasonable way, to process the child's data.

9. **Stricter penalties for breaches -** the GDPR significantly increases the penalties for breaches of data protection law. For violations relating to internal record keeping, data processor contracts, data security and breach notification, the fine could be up to 2% of annual worldwide turnover (of the last financial year), or if higher, 10 million Euros. For some other more serious breaches, this increases to 4% of annual turnover and 20 million Euros.

10. **Data Portability –** the GDPR creates a right to data portability. This applies to data which a personal individual has provided to a controller, and the processing is based on that person's consent or to fulfil a contract, and is carried out by automated means. In those circumstances, if requested, you would have to provide the data in a structured, commonly used and machine readable form, which would include a csv. file which can be created through excel and is excel compatible. This information must be provided free of charge.

What to do now

Consider your data

We would recommend you consider what personal data you hold, why you hold it and how you are using it. Make an itinerary of all personal data you hold and for what purpose. Then give consideration to whether you are a Controller or Processor of data. We can help you clarify if you are a Controller or Processor and what your obligations may be going forward.

Consider your contracts with other businesses

You may have contracts in place with third parties who process data for you – such as a payroll company, suppliers or sub-contractors. Alternatively you may be a data Processor for another business. If so we would recommend these contracts or terms being reviewed with a view to new contracts being put in place in readiness of the new laws. We can help you with this.

Consider your website

Consider how you collect data on your website. Your method of getting consent for processing data may need to be reviewed. Do you need express consent forms? Your website privacy notice and terms and conditions may well need an update. We can assist in reviewing your website terms and conditions and amending them for you.

Consider your employer obligations

Review how you collect and store employee data and for what purpose. Consider your personnel files. Prepare a data protection policy that complies with the new law. You may also need to review your handbooks, contracts and other policies to ensure compliance. We can help you with this.

Consider your customer contracts/terms of business

We can help review and amend your terms of business or standard contracts to incorporate the changing legal requirements.

This information is published on 12th June 2017 and reflects the published guidance of the Information Commissioner's Office as at that date. This may change prior to implementation of the GDPR and we recommend that you contact us before the implementation date if you require advice on how to meet your obligations under the GDPR.

For further information about the forthcoming GDPR data protection laws, please contact Louise Adams in our Business Services team on:

Louise Adams, Solicitor – Business Services

Email **louise.adams@smesolicitors.co.uk**

Direct Dial **01905 727 201**