Published on *Sydney Mitchell Solicitors* (https://www.sydneymitchell.co.uk)

General Data Protection Regulation (GDPR)

The EU's General Data Protection Regulation (**GDPR**) and related UK Data Protection Act 2018 came into force in the UK in May 2018 replacing the Data Protection Act 1998 (**DPA1998**).

The GDPR affects businesses and other organisations which are involved in the handling of personal data. It is very important to take note of the regulations as failure to comply can result in a hefty fine or penalty.

The following is a summary or reminder of some of the key features of data protection law following the changes made under the GDPR.

To help organisations to ensure compliance, we have also produced a suggested Data Protection Checklist and Action Plan.

Data Processing Principles

The 6 data processing principles set out in the GDPR are similar to those set out in the Data Protection Act 1998. The 6 principles relate to:

1. Lawfulness, fairness and transparency

In summary, personal data must be processed fairly and lawfully and in a transparent manner. There are a number of specific obligations which arise in connection with this principle, some of which are highlighted later in this summary.

2. Purpose limitation

Personal data must be collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes. This means generally that data may not be used for any purposes other than those which were notified to the individual data subject when it was collected.

3. Data minimisation

Any personal data which is processed must be adequate, relevant and limited only to what is necessary for the purposes for which it is processed. This means that data should be deleted when it is no longer appropriate to keep it.

4. Accuracy

Personal data must be accurate and up to date. Personal data which is inaccurate should be erased or rectified without delay.

5. Storage limitation

Personal data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which it is processed.

6. Integrity and confidentiality

Personal data must be processed in a way which ensures appropriate security for the data. This means protection against unauthorised or unlawful processing, accidental loss, destruction or damage using technical or organisational measures appropriate to the risk.

Accountability

The GDPR also provides for a general obligation of accountability to ensure that personal data is processed in accordance with the above principles so it is important for organisations to reflect carefully on the application of each of the six principles to their specific data processing activities to check that their processes are compliant.

Legal Basis for Processing

Any processing of personal data requires a proper legal basis to justify the processing.

Consent is often relied upon as the basis to justify processing, but in order to be relied upon must meet a number of tests. Organisations in the UK were previously able to rely on implied consent. The GDPR however now requires a very high standard of consent.

The consent must be demonstrated by a clear affirmative action establishing a freely given, specific, informed and unambiguous indication of the individual's agreement to their personal data being processed. Organisations which rely on consent as a legal basis for processing personal data must therefore ensure that any consent they obtain indicates a clear positive act of approval by the data subject.

The consent must be “informed” which means that the individual must also have been provided with all of the information required by the law to inform their decision. Unless the necessary information has not been provided, even a positive act of consent will not be sufficient to comply with the law.

The consent must also be freely given. If consent has been given by an employee in their contract of employment where there is likely to be a clear imbalance between the parties,

such consent is unlikely to be regarded as being freely given.

The onus is on the organisation to prove that it has obtained proper consent to all of its processing of an individual's data. Organisations should also be aware that consent may be withdrawn by an individual at any time.

Note that there are additional requirements in relation to consent where any processing of the personal data of children is involved.

Alternative Bases for Processing: It should be remembered that consent is not the only lawful basis for processing personal data. There are a number of other potential grounds which may be relevant where, for example, the processing is necessary for the purpose of a contract with the individual, or to protect the individual's vital interests or for the legitimate interests of the data controller.

Depending on the circumstances, it may be appropriate and more practical in many cases to rely on one of the alternative grounds for lawful processing, but it should be noted that the requirements for each of the different grounds includes safeguards, for example, to balance the rights and freedoms of the individual and so great care must be taken when considering the appropriate grounds for processing to ensure that all of the conditions in question are properly met.

Any business or organisation which controls and is responsible for the processing of personal data of individuals should check their arrangements, procedures, contracts and privacy notices to ensure that their processing can be shown to be lawful.

Special Categories of Personal Data

Organisations should be alert to the fact that there are special categories of personal data. The categories include data relating to: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health, sex life or sexual orientation.

Where data falling into any of these special categories is being processed, the grounds for lawful processing are more limited. It is more likely in practice that consent will be necessary.

Transparent processing

The requirement for transparency means that individuals need to be provided with certain information regarding the processing of their data and their rights in relation to the same. The information required to be provided has increased as a result of new rights created under the GDPR including rights in many circumstances for individuals to be able to require that their data is erased.

The necessary information will generally be set out in an organisation's privacy notice. Organisations should check that their notices have been updated to include all of the required information.

Increased obligations for data processors

The GDPR retains the concepts of Data Controllers and Data Processors which existed under

the DPA 1998 but introduced new compliance obligations for processors.

Both controllers and organisations which process data on behalf of controllers need to be aware of the obligations on processors and reflect these in the contracts between them dealing with the processing.

Technical and organisational measures

The GDPR requires organisations (both data controllers and data processors) to implement technical and organisational measures to ensure that the requirements of the GDPR are met.

In particular businesses should:

- take data protection compliance requirements into account when introducing any new technology, product or service which involves the processing of personal data referred to as “data protection by design and default”
- conduct data protection “impact assessments” where there are specific high risks to individuals (see below)
- plan these steps into future product/service cycles
- develop and implement a data breach response plan (including designating specific roles and responsibilities, training employees, and preparing template notifications) enabling the organisation to react promptly in the event of a data breach. Complying with the data breach reporting obligations in the GDPR will also entail a significant administrative burden for organisations, which may increase costs
- where appropriate, consider “pseudonymisation” of personal data (that is, the processing of personal data in such a manner that the personal data can no longer be attributed to a specific individual, without additional information). Pseudonymous data will still be treated as personal data, but may be subject to fewer restrictions on processing where the risk of harm is low. This requires that the "key" necessary to identify data subjects from the coded data is kept separately and is subject to technical and organisational security measures to prevent inadvertent re-identification of the coded data

Mandatory privacy impact assessments

For certain specified data processing operations, for example where automated decisions will be based on profiling or where there is large scale processing of special categories of data, a data protection impact assessment (PIA) will need to be carried out.

Organisations will be required to perform a PIA before carrying out any processing which, taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to data subjects. If the assessment indicates that the processing presents a high risk in the absence of measures taken by the controller to mitigate the risk, controllers must consult the ICO before carrying out the processing.

New Record Keeping obligations

The GDPR requires data controllers and data processors to maintain detailed documentation recording their processing activities and specified information relating to the processing.

These obligations do not generally apply to an organisation employing fewer than 250 people

unless the processing is likely to result in high risk to individuals; the processing is not occasional or the processing includes sensitive personal data.

In addition, in certain circumstances, controllers or processors are required to appoint a data protection officer.

New rights for individuals

The GDPR has created a number of significant new rights for individuals:

The right to erasure or “to be forgotten”

Individuals have the right to request that businesses delete their personal data in certain circumstances (for example where the data is no longer necessary for the purpose for which it was collected or the data subject withdraws their consent and the organisation has no legitimate grounds for the continued processing).

The right to object to profiling

In certain circumstances, individuals have the right to object to the processing of their personal data.

This includes where the data is to be used for “profiling". Profiling is defined broadly and includes most forms of online tracking and behavioural advertising, making it harder for businesses to use data for these activities.

The fact of profiling must be disclosed to the data subject and a PIA is required.

The right to data portability

Individuals have a new right to obtain a copy of their personal data from the data controller in a commonly used and machine readable format and have the right to transmit that data to another controller (for example, an online service provider).

In exercising this right, the data subject can request that the information is transmitted directly from one controller to another where this is technically feasible.

Data subject access requests

Individuals have the right to obtain specified information from organisations regarding the processing of their data and also to be provided with a copy of the data processed. This can be very difficult if organisations do not have systems in place ready to deal with such requests. It is important to do so because requests of this nature are often made in connection with some form of dispute with an organisation.

Under the GDPR, the organisation is no longer able generally to make any charge for responding to such requests and the time limits permitted for responding to a request have also shortened from 40 days to within one month, with limited scope to extend the timescale in some circumstances. This adds to the likelihood of receiving requests and increases the

pressure when a request is made.

Increased enforcement powers

National data protection authorities are able to impose fines on data controllers and data processors on a two-tier basis which is much more onerous than previously under the DPA 1998.

Fines may now be made of up to 2% of the annual worldwide turnover in the preceding financial year or 10 million euros (whichever is the greater) for violations relating to internal record keeping, data processor contracts, data security, breach notifications, data protection officers, and data protection by design and default.

Fines of up to 4% of the annual worldwide turnover in the preceding financial year or 20 million euros (whichever is the greater) can be made for violations relating to breaches of the data protection principles, conditions for consent, data subjects rights and international data transfers.

National data protection authorities also have power to carry out audits, to require the provision of information to them, and (subject to local law) to obtain access to premises.

Strict data breach notification rules

The GDPR requires businesses to notify national data protection authorities of all data breaches without undue delay and where feasible within 72 hours unless the data breach is unlikely to result in a risk to the individuals. If the data controller cannot do this, it will have to justify the delay to the authority.

Organisations should insofar as practicable have systems and procedures in place to identify, assess and report breaches to the authority.

If the breach is likely to result in high risk to the individuals, the GDPR, requires organisations also to inform data subjects of specific information regarding the breach "without undue delay".

Greater harmonisation across the EU

The GDPR was intended to create a single legal framework that applies across all EU member states so that businesses in different states would face a more consistent set of data protection compliance obligations across the EU with less scope for divergence arising from separate implementation in different states.

Lead enforcement authority

Under the GDPR, an organisation is able to deal with a single national data protection authority as its "lead authority" across the EU. The lead supervising authority must work with all other concerned national authorities. There is a mechanism for dealing with disagreements between the supervising authorities involved. Purely local cases continue to be handled by the supervisory authority for the local jurisdiction.

In the case of the UK, the situation is of course dependent on what happens in relation to

Brexit.

Expanded application to non-EU organisations

Non-EU data controllers and data processors are subject to the GDPR if they:

- offer goods or services to individuals in the EU regardless of whether payment is received from the individual; or
- monitor the behaviour of individuals within the EU.

This means that many non-EU businesses which were not previously required to comply with the DPA 1998 are required to comply with the GDPR. This can have implications for group companies outside the EU.

The Brexit Effect

Now that the UK has left the EU and is in the transition period until 31 December 2020, the GDPR remains enforceable in the UK by virtue of the EU European Union (Withdrawal) Act 2018.

After the transition period, the UK government will be free to repeal or amend the legislation, but seems unlikely to do so because, aside from any other political or social concerns, of the difficulty this would create for any transfers of data from the UK to the EU.

Subject to the terms of any UK-EU agreements on the future relationship, the UK will upon the end of the transition period become a "third country" for the purposes of personal data transfers to and from the EU. In this situation, the UK government has indicated that transfers of personal data into the UK from the EU will continue to be permitted. The UK will however have to demonstrate to the European Commission that it can provide an "adequate" level of protection (that is, one that offers an equivalent level of protection to that which is applicable in the EU) for personal data processed in the UK, once the UK leaves the EU.

Pending an EU finding of adequacy, transfers of data into the EU from the UK will need to be completed using an approved alternative method of protection. These include the use of standard contractual clauses or Binding Corporate Rules. The latter require approval from the supervising authority which it will often be impractical to obtain while the validity of standard clauses has also recently been challenged.

Direct Marketing – Privacy and Electronic Communications Directive

The **GDPR** is not the only relevant legislation relating to data protection and privacy. The Privacy and Electronic Communications Directive (**PECR**) which requires an individual's prior consent to electronic direct marketing such as email or text also needs to be considered and taken into account in relation to any direct marketing activities.

PECR is also currently under review.

Other developments – Guidance on use of Cookies

The ICO has also recently published updated guidance on the requirements for consent to the use of cookies.

The guidance confirms that the requirements in relation to the form of consent to be obtained from individuals for the use of cookies are as set out in this summary. Any form of passive consent cannot be relied upon.

Website operators who have not already done so are likely to need to check and update the method of obtaining consent used on their websites, the form of their cookies notices and the way in which cookies are placed when the website is used.

Contact for Advice

If your organisation is involved any processing of a personal data and would like advice on the new regulations or any of our other services, speak to **Julian Milan** [1] or **Roy Colaba** [2] in our Company and Commercial Department or fill in our online enquiry form [3].

Disclaimer: This is a summary of some of the key provisions of the GDPR only. It is provided for general information purposes only. It is not intended to be and should not be relied upon as legal advice.

Links
[1] https://www.sydneymitchell.co.uk/about-us/our-people/staff/julian-milan
[2] https://www.sydneymitchell.co.uk/about-us/our-people/staff/roy-colaba
[3] https://www.sydneymitchell.co.uk/contact