The Essence of GDPR

INTRODUCTION

This paper purports to highlight the most significant elements of the General Data Protection Regulation (GDPR) recently issued by the EU Commission, a document that runs to over 260 pages of hard reading and the regulations that run to 88 pages with 98 Articles, (http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf)

In essence the principle of the GDPR is to protect the data held by companies and organizations that relate to individuals. To ensure that the ruling is effective GDPR have set very large financial penalties for those who break the rules.

- While the GDPR is an EU directive (Law) it has been adopted by the UK Government and is therefore applicable to the UK irrespective of the outcome of Brexit.
- GDPR comes into force on 25May 2018, by which time all Organizations are expected to be fully compliant.
- GDPR not only applies to all countries in the European Economic Area including the UK but also applies to all persons and organizations that reside outside the EEA but have control or process personal data of EEA nationals.
- The penalties for failing to apply the regulations are severe being €20m (£18m) or 4% of the organization's worldwide group turnover (whichever is higher).
- The regulations will be policed by The Information Commissioners Office (ICO) from whom advice and guidance may be sort (https://ico.org.uk).

The current data protection laws in the UK will be completely dominated by the GDPR regime. These new laws are designed to provide a high level of protection for the data held about individuals and place strict guidelines for those in control of such data.

It is important to take note that GDPR differs from the current situation insofar as GDPR is a legal requirement rather than a best practices scenario. Organizations need to fully embrace the rules as those who attempt to short cut or do the minimum are likely to find themselves in trouble.

Although the GDPR brings in a number of major changes, much of it is not completely new. Instead, It adds to, reinforces and clarifies obligations that already exist under the Data Protection Act 1998.10 tin this it is very much an evolution of data protection law rather than a revolution.

PERSONAL DATA

Personal Data refers to any information that relates to any identifiable living individual. This includes name, address, telephone numbers, emails addresses, IP addresses, biometric data, and geo-location data. The GDPR applies to all processing of data including storage, use, transfer and the deletion of all data. All and any data stored must at the request of the individual be completely deleted by the holder.

What was previously known as sensitive data is also covered by GDPR and may include racial or ethnic origin, religious beliefs, trade union membership, health details, sexual orientation and practices. Some financial data may be excluded but will still require additional security due to its nature and the harm that could result from a personal data breach.

INDIVIDUALS RIGHTS

Under the GDPR the individual must have given his/her consent for an organization to hold personal data. This is in contrast to regulation currently in force, the current DPA 1998 (Data Protection Act) is not only less stringent but also carries far lower penalties, (a maximum of £500k). All requests for consent must be clearly distinguishable from other matters, intelligible, easily accessible, and in clear and plain language.

Consent must be freely given and unambiguous. The consent must be a clear statement providing an indication of understanding by a definitive positive statement. In all cases where consent is needed there must be an expressed opt-in anything less is unlikely to be sufficient.

Keep in mind that the consent given:

- Must be valid and may need to be refreshed.
- Needs to be made available for review if requested.
- Can be withdrawn without undue difficulty.
- Must be balanced, it must not be biased towards the employer.

Any existing agreement in place prior to the 25th May 2018 deadline that does not meet all of the GDPR requirements will not be valid and a new consent must be obtained. This must be specifically drafted and must be agreed by the participant. This document, known as a privacy notice must be clear, concise and satisfy the rules laid down by GDPR.

There has always been the right under the DPA 1998 for subjects to view their personal data but under GDPR there are some changes.

- The response time for a SAR (Subject Access Request) is reduced from 40 days to one month
- Fees cannot be charged unless a subject makes excessive requests
- All information held on the subject must be provided

The subject under GDPR has the right to object to their personal data being used for direct marketing or automated decision making and to have any inaccurate personal data corrected.

In addition GDPR introduces the following rights:

- the right to erasure (also known as the right to be forgotten) which allows a data subject to require his or her personal data be deleted (subject to some exceptions)
- the right to data portability entitling data subjects to a copy of any personal data he or she has provided and which is processed automatically on the basis of consent or performance of a contract.
- This data should be provided in a structured common electronic format. Where it is feasible to do so a right to restrict processing should be made available in certain situations.

PRINCIPLES OF DATA PROTECTION

The current DPA 1998 (Data Protection Act) sets out eight principles which in essence are:

- Personal data shall be processed fairly and lawfully

- Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Personal data shall be accurate and, where necessary, kept up to date.
- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- Personal data shall be processed in accordance with the rights of data subjects under this Act.
- Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

GDPR adopts these principles which can be summarized as follows:

- Only processed lawfully, fairly and transparently
- Collected and used for lawful purposes only
- Is strictly appropriate, adequate, relevant and not excessive for purpose
- Is accurate and kept up to date
- Is only stored on systems for as long as necessary
- Is kept secure, confidential and fully protected

An important change under GDPR is that any processing of personal data (e.g. by suppliers, contractors, service providers) has to be carried out under a written contract which meets the criteria set out in Article 28 of the GDPR.

Amongst other things, the contract must address:

- international transfers
- only acting on the controller's instructions
- confidentiality
- sub-processing restrictions
- security obligations
- deletion of data
- provision of information
- audits and inspections
- responding to requests by data subjects.

Any processing must be carried out pursuant to a contract which meets the requirements of Article 28 or it will be unlawful. Professionally drafted standard contracts and policies will make compliance much easier. Keep in mind that even contracts entered into before the GDPR comes into force will need to be compliant by 25 May 2018.

Over and above these principles there is another overriding GDPR principle; this is that organizations are accountable and must be able to demonstrate compliance with the principles and sprit of the regulations.

It is also important to be aware that both GDPR and the interpretations and rules imposed by the ICO (https://ico.org.uk/) may change with time and should therefore be monitored.

CONTROLS

GDPR defines organizations and others handling personal data into two categories:

- Processors – who process data under instruction from or on behalf of the Controller.
- Controller – controls how and why data is used 'means and purpose'.

The controller is principally responsible for data protection, however processors may also be liable.

Many organizations may also need to appoint a Data Protection Officer (DPO). GDPR stipulates that a DPO must be appointed if:

- It is a public authority (except for courts in their judicial capacity)
- Organizations monitoring individuals behavior
- Organizations processing sensitive data on a large scale
- While provisional documents referred to companies employing over 250 people 'Article 37' is broader and should be consulted.

The DPO may be an existing member of staff providing that appropriate qualification is established, in all cases the DPO must be an expert in data protection and shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.

ADMINISTRATION

There is a GDPR requirement for the controllers and processors of organizations to keep detailed records of all processing activities. This is a significant overhead and must include categories of personal data processed, personal data transfers, security measures and the need to demonstrate overall compliance.

Under GDPR the transfer of personal data outside the EEA (European Economic Area) remains prohibited, the same as the DPA 1998. There are exceptions to this ruling and these should be clarified with the ICO as there may be changes when GDPR comes into force.

The GDPR includes the need for organizations to put in place 'appropriate technical and organizational measures' to protect personal data against theft, unauthorized access, loss, damage and destruction. The level of protection may depend on the personal data held and may require organizations to include encryption and/or pseudonymization.

GDPR will include what is referred to as 'profiling' which is a form of automated decision marketing resulting in such elements as automatic emailing. The exact details of the ruling are to be finalized and organizations should check with the ICO to verify that they are in line with the most recent ruling.

Under GDPR the processing of any personal data by third parties (e.g. service providers, contractors, suppliers) must be covered by a written contract which meets the criteria outlines in Article 28. This agreement must address the following:

- International transfers
- Only acting on the controller's instructions
- Confidentiality

- Sub-processing restrictions
- Security obligations
- Deletion of data
- Provision of information
- Audits and inspections
- Responding to requests by data subjects

All processing of personal data must comply with the requirements of Article 28 or it will be unlawful. It is recommended that contracts should be prepared by appropriate lawyers and it should be noted that any contract written prior to 25 May 2018 will need to be compliant when GDPR comes into force.

IF THERE IS A DATA BREACH

There is a significant change between the DPA and GDPR. After 25 May 2018 the GDPR requires:

- Controllers must inform the ICO of a data breach within 72 hours unless the breach is unlikely to compromise the rights and freedoms of the data subject.
- Controllers must notify affected data subjects of any severe data breach.
- That Processors must notify Controllers of any data breach.

It is important that organizations need to put policies in place so that employees/personal will be able to act appropriately and quickly in the event of a data breach.

BREXIT

Brexit will not have any affect on the GDPR from coming into force. The UK Government and ICO have made clear their Intention that the GDPR (or an equivalent regime) will continue to apply when the UK leaves the EU.

At the moment it is not clear if and how European Union court judgments relating to data protection will be implemented in the UK. Other cross border issues (such as cooperation between data protection authorities, the UK's role in the Eli data protection board) also remain uncertain.

CONTACT

MPWA limited

mw@mpwa.co.uk