GREATER MANCHESTER
CHAMBER OF COMMERCE
ELLIOT HOUSE
151 DEANSGATE
MANCHESTER M3 3WD

T: +44 (0) 0161 393 4321

info@gmchamber.co.uk
www.gmchamber.co.uk

A COMPANY LIMITED BY GUARANTEE
REGISTERED OFFICE: ELLIOT HOUSE
151 DEANSGATE, MANCHESTER, M3 3WD

REGISTRATION NUMBER: 05245944
VAT NUMBER: 849748168

General Data Protection Regulations

The European Commission ratified a new data protection regulation that will come into effect in May 2018. The General Data Protection Regulation will replace the current Data Protection Directive and provide a uniform date protection law across the whole of the EU. The changes brought about by the GDPR are substantial and broadens the scope of personal privacy laws to protect the data rights of EU citizens. Important measures include:

1) The introduction of the "right to be forgotten"
2) The need to document IT procedures
3) The requirements on organizations to report breaches within 72 hours
4) The requirement of privacy by design and security by design
5) Introducing new, stringent rules for obtaining consent from individuals
6) Significant penalties for a breach
7) Introducing the principle of accountability to demonstrate compliance with the provisions

The provisions in the GDPR cover capture, control and transmission of data. To attain compliance with provisions companies will need to create and demonstrate awareness of what sensitive data they control, where they store such data and who has access to it.

Data Protection Principles

The data protection principles in the GDPR remain similar to the principles – current data protection principles. Companies must process personal data in lawful, fair and transparent ways. Personal data must be collected for exactly specified and further processing that is incompatible with the previously stated purposes is prohibited. Personal data that is not relevant or in excess of the processing requirements must not be collected and where companies store personal data, they are responsible for keeping the data accurate and update. This means companies may face new challenges in ensuring that data such as CVs and records of former employees are kept up to date. In such situations, companies must evaluate whether the data needs to be kept or whether it should be erased entirely. Inaccurate data must be rectified. The confidentiality of personal data must be maintained and companies face severe penalties if there is any unauthorized or unlawful processing of personal data including accidental loss could lead to penalties.

The GDPR introduces a legal accountability obligation under which data controllers will be required to implement appropriate technical controls and data handling procedures to ensure compliance with privacy requirements. Businesses must renew and update the controls through continuous assessments. Business must also implement procedures for continuous assessments and improvements to the controls and business must determine what controls are appropriate for the scope and purposes for which they collect and process personal data. In addition, measures to objectively demonstrate compliance must be implemented. Therefore, businesses will need to maintain thorough documentation of their data protection measures. Documentation could cover inventories of personal data, processing activated privacy impact assessments, controls to preserve

GREATER MANCHESTER
CHAMBER OF COMMERCE
ELLIOT HOUSE
151 DEANSGATE
MANCHESTER M3 3WD

T: +44 (0) 0161 393 4321

info@gmchamber.co.uk
www.gmchamber.co.uk

A COMPANY LIMITED BY GUARANTEE
REGISTERED OFFICE: ELLIOT HOUSE
151 DEANSGATE, MANCHESTER, M3 3WD

REGISTRATION NUMBER: 05245944
VAT NUMBER: 849748168

confidentiality retention policies and procedures for handling data breaches. Organizations must provide adequate training to staff and foster a culture of privacy.

Data Protection Officer

Organizations are required to appoint a data protection officer in certain circumstances. These include:

1) Where the processing is carried out by public bodies including or organizations that carry out public functions or deliver public services.
2) A data protection officer must also be appointed where the core activities of the organization includes "regular and systematic monitoring of data subjects on a large scale". This includes tracking of online activity for bad forensics, marketing and email campaigns.
   The Data Protection officer could be an employee of the business and should provide advice on and monitoring of compliance. The data protection officer will be the contact point for the ICO on all matters related to data protection.

Consent

The provisions in the GDPR relating to consent have serious implications for marketing and communications activities. The regulation states that consent must be freely given by the data subject and must be specific, informed and provide an unambiguous induction of the data subject's wishes expressed through a statement or clear affirmative action. Consent cannot be assumed. The fulfillment of a service or contact cannot be conditional on providing consent if the collection and processing of personal data is not necessary for the performance of that contract.

A clear affirmative action is needed to obtain consent. Therefore, it cannot rely on silence inactivity or pre-ticked boxes. Data subjects must be informed of the purposes for which the data may be used and specific consent must be obtained for all processing activities. Separated consent must be obtained for distinct processing operations.

Finally, consent must be revocable. Data subjects must have the right to revoke their consent at any time and it must be easy to withdraw consent. In practice, this requires that organizations allow consent to be withdrawn in exactly the same manner through which it was obtained. The language of consent must be intelligible and unambiguous.

Right to be forgotten

Data subjects have the right to have their date erased where the processing fails to comply with GDPR requirements. Data must be erased fully when it is no longer required for the purpose for which it was collected, or when the data subject withdraws consent. The data controller must be able to prove that data has been erased and must inform any third party to whom the data has been disclosed.

Privacy by design

Organizations must implement technical and organizational measures to show that they have considered and integrated data compliance measures into their data processing activities where appropriate, a privacy impact assessment must be carried out to identify and minimize non-compliance. For high risk processing activities, a privacy impact assessment is mandatory.