Guidelines on Data Protection

Introduction

As per the Data Protection Act 1998 we abide by 8 principles.

- Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –
    - at least one of the conditions in Schedule 2 is met**, and
    - in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met***.
- 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 organisational measures shall be taken against unauthorised 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.

Schedule 2

1. The data subject has given his consent to the processing.
2. The processing is necessary—
    a. for the performance of a contract to which the data subject is a party, or
    b. for the taking of steps at the request of the data subject with a view to entering into a contract.
3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.
4. The processing is necessary in order to protect the vital interests of the data subject.
5. The processing is necessary—
    a. for the administration of justice,
        i. for the exercise of any functions of either House of Parliament,]
    b. for the exercise of any functions conferred on any person by or under any enactment,
    c. for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or
    d. for the exercise of any other functions of a public nature exercised in the public interest by any person.

6. (1)The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.
   (2)The [F2 Secretary of State] may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.
7. The processing is necessary for the purposes of making a disclosure in good faith under a power conferred by—
   a. (a)section 21CA of the Terrorism Act 2000 (disclosures between certain entities within regulated sector in relation to suspicion of commission of terrorist financing offence or for purposes of identifying terrorist property), or
   b. section 339ZB of the Proceeds of Crime Act 2002 (disclosures between certain entities within regulated sector in relation to money laundering suspicion).]

Schedule 3

1. The data subject has given his explicit consent to the processing of the personal data.
2. The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.
3. The processing is necessary—
   a. in order to protect the vital interests of the data subject or another person, in a case where—
      i.)consent cannot be given by or on behalf of the data subject, or
      ii. ii)the data controller cannot reasonably be expected to obtain the consent of the data subject, or
   b. in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.
4. The processing—
   a. is carried out in the course of its legitimate activities by any body or association which
      i. is not established or conducted for profit, and
      ii. exists for political, philosophical, religious or trade-union purposes,
   b. is carried out with appropriate safeguards for the rights and freedoms of data subjects,
   c. relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes, and
   d. does not involve disclosure of the personal data to a third party without the consent of the data subject.
5. The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.
6. The processing—
   a. is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),
   b. is necessary for the purpose of obtaining legal advice, or
   c. is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

7. (1)The processing is necessary—
    a. for the administration of justice,
        i. (aa)for the exercise of any functions of either House of Parliament,]
    b. for the exercise of any functions conferred on any person by or under an enactment, or
    c. for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

    (2)The [F3 Secretary of State] may by order—
    a. exclude the application of sub-paragraph (1) in such cases as may be specified, or
    b. provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

7A. (1) The processing—

    a. is either
        i. the disclosure of sensitive personal data by a person as a member of an anti-fraud organisation or otherwise in accordance with any arrangements made by such an organisation; or
        ii. (ii)any other processing by that person or another person of sensitive personal data so disclosed; and
    b. is necessary for the purposes of preventing fraud or a particular kind of fraud

    (2) In this paragraph "an anti-fraud organisation" means any unincorporated association, body corporate or other person which enables or facilitates any sharing of information to prevent fraud or a particular kind of fraud or which has any of these functions as its purpose or one of its purposes.

7B. The processing is necessary for the purposes of making a disclosure in good faith under a power conferred by—

    a. section 21CA of the Terrorism Act 2000 (disclosures between certain entities within regulated sector in relation to suspicion of commission of terrorist financing offence or for purposes of identifying terrorist property), or
    b. section 339ZB of the Proceeds of Crime Act 2002 (disclosures within regulated sector in relation to money laundering suspicion).]

8. (1) The processing is necessary for medical purposes and is undertaken by—
    a. a health professional, or
    b. a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

(2)In this paragraph "medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

9. (1) The processing—

a. is of sensitive personal data consisting of information as to racial or ethnic origin,
b. is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and
c. is carried out with appropriate safeguards for the rights and freedoms of data subjects.

(2) The [F6 Secretary of State] may by order specify circumstances in which processing falling within sub-paragraph (1)(a) and (b) is, or is not, to be taken for the purposes of sub-paragraph (1)(c) to be carried out with appropriate safeguards for the rights and freedoms of data subjects.

10. The personal data are processed in circumstances specified in an order made by the [Secretary of State] for the purposes of this paragraph.

Definition of 'Sensitive Information'

Sensitive personal data means personal data consisting of information as to -

(a) the racial or ethnic origin of the data subject,
(b) his political opinions
(c) his religious beliefs or other beliefs of a similar nature,
(d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
(e) his physical or mental health or condition,
(f) his sexual life,
(g) the commission or alleged commission by him of any offence, or
(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

EU General Data - Protection Regulation

The EU General Data Protection Regulation (GDPR) was adopted in April 2016 and will take effect across the European Union (EU) on 25 May 2018, when it supersedes the 28 current national data protection laws based on the 1995 Data Protection Directive (DPD).

Introduced to keep pace with the modern digital landscape, the purpose of the new Regulation is twofold:

1. to improve consumer confidence in organisations that hold and process their personal data by reinforcing their privacy and security rights consistently across the EU, and

2. to simplify the free flow of personal data in the EU through a coherent and consistent data protection

Key Changes

1. Scope of the new law

Harmonisation – only one law

Guidelines on Data Protection

There are currently 28 different sets of data protection laws across the European Union. The GDPR will replace these with a pan-European regulatory framework effective from 25 May 2018. As a Regulation, it is directly effective in all member states without the need for further national legislation.

For organisations that operate across multiple member states, this harmonisation is welcome. However, some national divergences are likely to remain and further divergences may arise because member states have limited rights to amend some of the obligations under the Regulation:

 Employment - member states can introduce further restrictions on the processing of employee data.

 National security - member states can pass laws to limit rights under the Regulation in areas such as national security, crime and judicial proceedings.

Although the Regulation has been published, there is still uncertainty about what some of the provisions mean or how they should be applied. Different social and cultural attitudes to data protection will influence their interpretation, and what is regarded as "high risk" in Berlin may not also be regarded as "high risk" in Rome.

Finally, differences in the resources and attitudes of supervisory authorities may result in wide variations in enforcement. There is a wide discrepancy between the theoretical powers open to national regulatory authorities and the application of those powers in practice.

Issues of this sort will be resolved in the normal course of regulatory business. Organisations still face the 25 May 2018 compliance deadline.

Expanded territorial reach

The GDPR applies to all EU organisations – whether commercial business or public authority – that collect, store or process the personal data of EU individuals.

Organisations based outside the EU that monitor or offer goods and services to individuals in the EU will have to observe the new European rules and adhere to the same level of protection of personal data. The Regulation also requires such organisations – controllers and processors – to appoint an EU representative based in one of the member states in which the relevant individuals are based. This is unless the processing is occasional and does not include large scale processing of special categories of data or processing of data relating to criminal convictions and offences.

Single scheme "one-stop shop"

A new one-stop shop provision means that organisations will only have to deal with a single supervisory authority, not one for each of the EU's 28 member states, making it simpler and cheaper for companies to do business in the EU. An organisation that carries out cross-border processing should be primarily regulated by the supervisory authority in which it has its main establishment (the lead supervisory authority).

Obligations on processors

The Regulation also introduces obligations on data processors. These are service providers that process personal data on behalf of organisations but do not determine the purpose or means of the processing, such as call centres.

Where a controller contracts a processor to process personal data, that processor must be able to provide "sufficient guarantees to implement appropriate technical and organisational measures" to ensure that processing will comply with the GDPR and that data subjects' rights are protected. This requirement flows down the supply chain, so a processor cannot subcontract work to a second processor without the controller's explicit authorisation.

Contractual arrangements will need to be updated, and stipulating responsibilities and liabilities between the controller and processor will be imperative in future agreements. Parties will need to document their data responsibilities even more clearly and the increased risk levels may impact service costs.

2. Individuals' data rights

Core rules remain the same

Many of the core definitions from the DPD remain largely unchanged. In particular, the Regulation retains the very broad definition of personal data and processing, and organisations must comply with all six general principles when processing personal data. Some important new concepts are "high risk to individuals", "large scale processing" and "pseudonymised data" (data from which no individuals can be identified without the use of additional information).

Consent

The Regulation imposes stricter requirements on obtaining valid consent from individuals to justify the processing of their personal data. Consent must be "freely given, specific, informed and unambiguous indication of the individual's wishes". Silence, pre-ticked boxes or inactivity do not count as consent. The organisation must also keep records so it can demonstrate that consent has been given by the relevant individual. Finally, consent must be explicit when processing sensitive personal data, or transferring personal data outside the EU.

Additional protection for children

Consent from a child in relation to online services is, under the new Regulation, only valid if authorised by a parent. A child is someone below the age of 16, though member states can reduce this age to 13.

New data access rights

One of the key aims of the Regulation is to empower individuals and give them control over their personal data. While the Regulation largely preserves the existing rights of individuals to access their own personal data, require rectification of inaccurate data, object to direct marketing, and challenge automated decisions about them, it also confers significant additional new rights for individuals.

Right to be forgotten

Individuals have a new right to require the data controller to erase all personal data held about them in certain circumstances, such as where the data is no longer necessary for the purposes for which it was collected. There are a number of exemptions to this right, for example in relation to freedom of expression and compliance with legal obligations. It is likely that the limits of this right will be fought over in EU law courts for many years.

Right to data portability

This is a new concept under the Regulation. Individuals will have the right to transfer personal data from one data controller to another where processing is based on consent or necessity for the performance of a contract, or where processing is carried out by automated means.

Profiling

Data controllers must inform data subjects of the existence and consequences of any profiling activities that they carry out (including online tracking and behavioural advertising).

Organisations that collect and use personal data will need to put in place more robust privacy notices than have previously been required, providing more information in a more prescribed manner. This will involve a large-scale review of all privacy notices.

3. Data protection

Data protection by design

The Regulation does not just require 'tick- box' compliance; compliance must become part of 'business as usual'. The key to accountability is to embed compliance into the fabric of your organisation. This includes not just developing appropriate polices but also applying the principles of data protection by design and by default.

Specifically, organisations must take appropriate technical and organisational measures before data processing begins to ensure that it meets the requirements of the Regulation. Data privacy risks must be properly assessed, and controllers may use adherence to approved codes of conduct or management system certifications, such as ISO 27001, to demonstrate their compliance.

Data protection impact assessment (DPIA)

Data protection must now be designed into processing systems by default and a DPIA is now mandatory in certain circumstances. Good practice for new technologies and processes is to assess whether processing has a "high risk" of prejudicing data subjects' rights, and whether this risk can be reduced or avoided, for example by pseudonymisation. A DPIA shall "in particular" be required where there is automatic processing (including filing) and processing of special categories of data on a large scale.

Compliance standards

The GDPR encourages the adoption of certification schemes as a means to demonstrate compliance. Compliance with the international information security standard ISO 27001 – the only independent, internationally recognised data security standard – will help organisations demonstrate that they

have endeavoured to comply with the data security requirements of the GDPR. Implementing ISO 27001 involves building a holistic framework of processes, people and technologies in order to secure information.

Records of data processing

The Regulation now places the onus on organisations and data processors to keep their own records of data processing activities and make these available to the supervisory authority on request. This record needs to contain a specific set of information so that it is clear what, where, how and why data is processed. Small businesses employing fewer than 250 employees are exempt from these record-keeping requirements unless their processing activities involve a risk to the rights and freedoms of data subjects, are not occasional, or include special categories of personal data or data relating to criminal convictions or offences.

4. Accountability

Data protection officer

Many organisations will be required to appoint a data protection officer (DPO) to be responsible for monitoring compliance with the Regulation, providing information and advice, and liaising with the supervisory authority. They are an existing feature of some member states' data protection laws, such as Germany.

A DPO must be appointed where:

 the processing is carried out by a public authority;

 the organisation's core activities require regular and systematic monitoring of data subjects on a large scale; or

 the organisation's core activities consist of the large-scale processing of special categories of data and data relating to criminal convictions and offences.

In most organisations, it will be good practice to appoint a DPO anyway. The GDPR obligations are such that having readily available advice and support from a data protection specialist will be an essential risk management step, in the same way that organisations now appoint HR or health and safety managers.

The DPO, where appointed, must be independent. This does not mean you have to appoint an external person; the DPO role can be fulfilled by an employee. The post can be a part-time role or combined with other duties, but, in performing the role, the DPO must have an independent reporting line and be empowered to report directly to the board without interference. What is important is that the appointed person must be a data protection professional with "expert knowledge of data protection law and practices" to perform their duties.

 What qualification does the data protection officer need?

The data protection officer must have the right professional qualities and knowledge of data protection law. There is currently no express requirement to hold any particular qualification or certification. However, obtaining training and qualifications in GDPR compliance would be an

effective way to demonstrate expert knowledge. The IBITGQ ISO 17024-accredited EU GDPR Practitioner (EU GDPR P) is one such qualification.

Data breach notification and penalties

The increase in high-profile cyber attacks is reflected in the enhanced data security obligations in the Regulation and the parallel obligations in the Network and Information Security Directive.

It will be mandatory for an organisation to report any data breach to its supervisory authority within 72 hours of becoming aware of it. If that requirement is not met, the eventual report must be accompanied by an explanation for the delay. The notification must include specific information, including a description of the measures being taken to address the breach and mitigate its possible side effects. Where the breach may result in a high risk to the rights and freedoms of data subjects, the data subjects themselves must be contacted "without undue delay". This contact will not be necessary if appropriate protective measures – essentially encryption – are in place to eliminate danger to data subjects.

Any infringements of the new Regulation are subject to a tiered financial penalty regime with fines of up to 4% of annual global turnover or €20 million, whichever is the greater. In determining the level of the fine, the supervisory authority must consider a range of factors including the gravity of the breach, whether the breach was intentional or the result of negligence, and any steps taken to mitigate the breach. Additionally, individuals can sue organisations for compensation to cover both material and non-material damage (e.g. distress).

Given the magnitude of potential fines, the rights of individuals to bring cases and claim compensation, and the prevalence and effectiveness of cyber crime, the risk of a data breach should go straight onto the board's risk register, with compliance high on senior management's agenda.

5. Data transfers outside the EU

The Regulation prohibits the transfer of personal data outside the EU to a third country that does not have adequate data protection. The European Commission has the power to approve particular countries as providing an adequate level of data protection, taking into consideration the data protection laws in force in that country and its international commitments. At present this list is Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland and Uruguay.

For data transfers to any country not on the list, there must be a legal contract that stipulates that the non-EU recipient agrees to the data protection safeguards required. The Regulation explicitly recognises and promotes the use of binding corporate rules as a valid data transfer mechanism within groups of companies. Approved codes of conduct also can be used for data transfers.

Updated November 2017