The General Data Protection Regulation (GDPR)

How to find the perfect blend of people, process and technology

White Paper

Contents

1.0 Introduction and Background

The EU General Data Protection Regulation (GDPR) has come into force. The purpose of this white paper is to assess the impact of the regulation, primarily from an information technology (IT) perspective - examining the role that IT can, will and has to play in the implementation of the requirements.

IT offers many solutions that will help address the challenges presented by the GDPR, and vendors have been working hard to develop their products so that they enable, facilitate and support their customers' GDPR compliance efforts. However, it is clear there is no one silver bullet or golden ticket solution that will meet all requirements. To comprehensively address the requirements of the regulation, a blend of people, processes and multiple technologies will be necessary to provide a holistic solution.

The GDPR supersedes the EU Data Protection Directive and was adopted by the European Parliament and European Council in April 2016. The GDPR forms part of the data protection regime in the UK, together with the new Data Protection Act 2018 (DPA 2018). The new DPA (replacing the 1998 version) will add clarity on how the UK will apply statutory controls to areas of the GDPR where member states have been given some flexibility i.e. the 'derogations'*. As and when the UK leaves the EU, the new DPA would replace the GDPR.

In addition, the regulation applies globally to any organisation that processes the data of anyone residing in the EU. The GDPR has been introduced to assist the free flow of information between countries and organisations, whilst protecting the privacy of individuals. It is intended to simplify the regulatory environment by harmonising data protection legislation across the EU.

Failure to comply with the GDPR could result in fines of up to €20 million or 4% of global annual turnover, whichever is the greater. The scale of potential fines and liability for personal prosecutions is making compliance with the GDPR a hot topic at board meetings. It is essential that IT quickly forms alliances with organisational compliance functions to assist in providing pragmatic solutions to ensure regulatory compliance. It should be noted that the UK's supervisory authority, the Information Commissioner's Office (ICO), has made it clear that businesses must be compliant with the GDPR, irrespective of Brexit. The UK government has also signalled its intention to implement the GDPR fully to ensure there is no interruption in the free flow of data between the UK and the EU post Brexit.

*The GDPR provides EU member countries with flexibility to make modifications to the requirements where this is necessary to reflect other in-country laws. It is envisaged that when enacted, the UK Data Protection Bill will achieve endorsement from the EU Data Protection Board that the UK has implemented the GDPR to a sufficient level. This will enable the UK to be white-listed as a country that provides 'adequate' safeguards for the protection of the rights and freedoms of individuals, in relation to the processing in the UK of EU residents' personal data. If this does not materialise, UK organisations may be required to appoint a representative in an EU/EEA (European Economic Area) member state.

2.0 What the GDPR Means in Practice

The GDPR applies to both data controllers and data processors. A data controller is the person (or more typically organisation) who determines how and why personal data is processed. A data processor is the person (or organisation) who processes data on behalf of a data controller. Under the DPA, the controller carries full responsibility, even when a processor is responsible for a data breach. However, under the GDPR, whilst data controllers still remain ultimately accountable, data processors also become liable and can attract penalties of up to €10m or 2% of global annual turnover.

It is possible that an organisation could be both a controller and a processor. Whatever the role, it is essential that organisations understand exactly what data they are processing - and who else is processing

it on their behalf. GDPR compliance requirements must be clearly defined and understood by everyone processing the data. In addition, international companies processing the data of EU residents must have a 'main establishment' or appoint a representative in the EU, even if they do not have offices in the region and irrespective of whether the data itself is not held (or processed) in the EU directly. This represents an increase in risk for global companies, as the designated main establishment may find itself responsible for carrying the risk relating to each entity in a group of undertakings.

The GDPR expands the definition of personal data, strengthens the rights of individuals, introduces new accountability requirements, extends its geographical scope and enforces harsh penalties on those who fail to comply.

2.1 What is Personal Data?

Personal data is any information that can identify a living individual. The GDPR relates to any individual resident in the EU and applies to any organisation which processes their data, wherever that organisation is located.

A name is no longer required for data to be classified as personal data. For example, IP addresses, cookies and RFID (radio-frequency identification) tags can all be classified as personal data. Equally, a name alone can be personal data depending upon the context in which it is used.

The definition of 'special category' (sensitive personal) data has also been expanded. In addition to data relating to racial or ethnic origin, political opinions, religious beliefs, trade union activities, physical or mental health and sexual orientation, the GDPR adds genetic and biometric data. This data may only be processed where there are lawful grounds for that processing. A data breach involving special category data will attract the highest fines, especially if it relates to children.

The DPA definition of sensitive personal data includes criminal convictions and alleged criminal offences. The GDPR deals with this type of data separately.

2.2 What is Processing?

As with current law, the definition of processing is very broad and covers everything organisations do with personal data, including:

- Obtaining and collecting
- Maintaining
- Storing and archiving
- Duplicating (backups)
- Encrypting and decrypting
- Analysing or profiling
- Reading or viewing
- Sharing or disclosing
- Deleting or destroying
- Transferring or transmitting (e.g. system to system or country to country, even if the data remains in the UK)

2.3 Identifying and Processing Personal Data

The GDPR mandates that an organisation must identify and document all personal data that it collects, as well as the processing activities that relate to that data. Depending on the size of the organisation, the amount of

data collected and the amount of processing performed, this exercise can be a straightforward or complex task.

Although not mandated, it is strongly recommended by the ICO that organisations draw up data flow diagrams to chart the life cycle of any data set, to better understand processing activities, data storage, transmission, archiving and destruction.

In addition, it is essential to understand how technical and physical systems access, process and store data in order to ensure full data life cycle management.

2.4 Think About:

- Data discovery tools to identify all personal data on your network
- Data flow mapping tools (including mapping organisational processes as they flow across technical systems)
- Detailed architecture diagrams defining systems interfaces
- Configuration management to ensure the impact of re-configuring systems is understood
- Change management processes and tools
- Information and IT asset registers that classify systems and components governed by the regulation

3.0 GDPR Principles

While the principles setting out the main responsibilities under the GDPR are broadly similar to those in the DPA, details have been expanded and a new accountability principle has been introduced.

Requirements involving individual's rights and overseas transfers are no longer stated in the principles, but are embedded within the body of the regulation.

The GDPR principles require that personal data is:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes and not further processed without consent if the additional processing is incompatible with the original purpose
- Adequate, relevant and limited to what is necessary
- Accurate and, where necessary, kept up to date
- Kept in a form which permits identification of data subjects for no longer than is necessary
- Processed in a manner that ensures appropriate security of the personal data

In addition, the data controller is responsible for, and must be able to demonstrate, compliance with the above principles. This is known as the 'accountability' principle.

3.1 Lawful Processing of Personal Data

Information may be collected and processed for the purposes of an organisation's legitimate business activity, or where required by law. Legitimate interest grounds cannot be used by a public authority and must not be used where there is an imbalance between the interests of an organisation and the rights and freedoms of the data subject. Organisations must document these processing activities and legal grounds, ensuring that

information relating to processing is communicated to data subjects in a way that is easily accessible, using clear and plain language and in the latter case, not including any unfair terms.

Gaining the consent of the individual for processing his or her personal data is also a valid means of providing legal grounds for the processing, but should only be used where there are no other lawful grounds available.

If an organisation can only rely on consent to justify their processing, this can no longer be gathered through pre-ticked consent boxes, hidden within lengthy online privacy policies or bundled within other terms and conditions. An explanation of the reasons for collecting personal information must be provided at the point of entry (e.g. using a so-called layered approach) and individuals must be provided with a means to supply consent that is:

"Freely given, specific, informed and an unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."

The controller must also be able to demonstrate that the data subject has consented to the processing of his or her data. As such, 'consent' records will need to be kept which can be verified, i.e. with evidence retained as to when consent was provided and the purposes for which consent was given.

The data subject must be able to withdraw his or her consent at any time, and the process for withdrawing consent must be as easy as that for giving consent.

3.1.1 Think About:

- Web page designs that provide customer-focused information, explaining how data will be processed
- Utilising a centralised consent and preferences database
- Web interfaces to manage user preferences
- Implementing a straightforward 'unsubscribe' function appended to all electronic marketing material
- Means of identifying whether the data subject is a child at the point where data is submitted

3.2 Collecting Personal Data for Specified Purposes

The processing of personal data for purposes other than those for which it was initially collected must be allowed, only where the processing is compatible with the purposes for which the personal data was initially collected.

If data is to be used for a purpose other than that for which it was originally gathered, or for which an individual provided their consent, then additional fully informed consent must be sought prior to this extra processing. The only exception to this is where processing is for purposes required by law.

3.2.1 Think About:

- Documenting your lawful purposes for collecting data so that you understand when you need to collect consent and when you do not
- Documenting any processing requirements that you are required to carry out by law
- Ensuring clarity in data protection or privacy policies
- Online privacy policies may only cover personal data collected online – internal privacy policies governing data collection within business processes are usually required
- At the point of data collection, providing consent options for all purposes for which you may wish to process data

- If you are likely to use data for other unspecified purposes in the future, ensure that users consent to future permission requests

3.3 Ensuring Data Processing is 'Adequate'

Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means.

Personal data should be limited to that which is required for the stated purpose. Information should not be collected or stored unless there is a specific reason for holding that personal data.

3.3.1 Think About:

- Data rationalisation - delete all data that you have no requirement for
- Reviewing data collection - do you collect data that is irrelevant to processing purposes?
- What data is necessary throughout the lifetime of the processing - can the same outcome be achieved by minimising or anonymising the data at a later stage in the process?

3.4 Keeping Personal Data Accurate and Up to Date

Every reasonable step must be taken to ensure that any personal data which is inaccurate is rectified or deleted.

The data subject shall have the right to obtain from the controller, without undue delay, the rectification of inaccurate personal data concerning him or her. Considering the purposes of the processing, the data subject shall hold the right to have incomplete personal data completed, including by means of providing a supplementary statement.

3.4.1 Think About:

- Securing a web interface to permit users to change their personal details (self-service)
- Identifying data duplication and merging to a single repository
- Automated online requests for data change / rectification
- Tracking of change requests and date processed
- A mechanism for flagging and/or suppressing the processing of personal data where accuracy is under dispute or investigation

3.5 Not Keeping Data Longer Than Necessary

Organisations must ensure that the storage period for personal data is kept to an absolute minimum. In order to ensure that personal data is not kept longer than necessary, time limits should be established by the data controller for erasure, or for a periodic review.

3.5.1 Think About:

- Automated data archiving
- Automated data deletion
- Backups and disaster recovery instances
- Statutory retention periods

- Mechanisms for purging unnecessary personal data from archives
- Tools and procedures for permanent destruction

3.6 Keeping Data Secure

Personal data must be processed in a manner that ensures its security (confidentiality, integrity and availability), including the prevention of unauthorised access to, destruction, disclosure or use of personal data and the equipment used for the processing. The GDPR specifies that data controllers and processors have a duty to implement and be able to demonstrate appropriate technical and organisational controls. Organisations, as appropriate, need to consider measures such as:

- Conducting a formal information security risk assessment which defines the controls to be applied commensurate with the risks identified from such an assessment
- Ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- Maintaining the availability and access to personal data in a timely manner, in the event of a physical or technical incident
- Implementing a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures, to ensure the security of data processing
- Ensuring that third party organisations (e.g. suppliers) and third party data processors who have access to personal data provide equivalent measures and security guarantees that deliver flow-down of security and compliance obligations throughout the supply chain

Organisations and suppliers will need to think about how they can 'demonstrate' compliance with their security obligations and commitments. One solution may be to implement best practice security controls and certify to BS EN ISO/IEC 27001:2017, the International Standard for Information Security Management, as well as implementing or utilising complementary ISO standards such as:

- ISO 27002: Code of practice for information security controls
- ISO 27004: Monitoring, measurement, analysis and evaluation
- ISO 27005 and ISO 31000: Information security risk management
- ISO 27014 / BS 10012:2017: Governance of information security / Personal information management
- ISO 27017: Security controls for cloud services
- ISO 27018: Code of practice for protection of personally identifiable information (PII) in public clouds
- ISO 22301 / ISO 27031: Business continuity management / Information/communication technology readiness
- ISO 27032: Guidelines for cybersecurity
- ISO 27033: Network security
- ISO 27034: Application security
- ISO 27035: Security incident management
- ISO 27036: Information security for supplier relationships
- ISO 27038: Specification for digital redaction
- ISO 27039: Deployment and operations of intrusion detection and prevention systems (IDPS)
- ISO 27040: Storage security

- ISO 27041: Guidance on assuring suitability and adequacy of incident investigative methods
- ISO 27042: Guidelines for the analysis and interpretation of digital evidence

Equally, organisations may wish to adopt/certify or comply against other standards and protocols, such as UK Cyber Security Essentials/Essentials Plus, or industry sector standards such as the Payment Card Industry Data Security Standard (PCI-DSS).

3.6.1 Think About:

- Information and IT asset management
- Document scanning and management tools
- Mobile devices, smart phones and external cloud storage
- Role-based access control
- Two-factor authentication for remote access
- Securing remote devices
- Data encryption, including removable media
- Pseudonymisation or anonymisation of data to be used for analytical, statistical, historical or research purposes (big data, profiling and monitoring)
- Authentication of user access
- Regular reviews of access permissions
- Malware protection
- Boundary firewalls, intrusion prevention and detection solutions
- Secure network architecture and network segregation
- Segregation of sensitive data
- Logging and monitoring tools
- Business continuity and disaster recovery
- External penetration testing of web interfaces
- Regular internal vulnerability checks
- Physical security and entry controls

The GDPR also encourages the drawing up of codes of conduct/practice and the establishment of data protection certification schemes. Adherence to an approved code of conduct, or an EU approved certification scheme, may be used to demonstrate compliance with the security requirements of the GDPR. While not obligatory, adhering to an approved code of conduct or certification scheme offers benefits beyond mere compliance including:

- Differentiating your organisation and building trust in your handling of personal data
- Mitigation in the event of enforcement action
- Improved standards of operating
- Reduction in insurance costs

3.7 Ensuring Accountability

In order to demonstrate compliance with the GDPR, the controller or processor must maintain records of processing activities under its responsibility. Each controller and processor is obliged to cooperate with the supervisory authority and make available those records in electronic form so that it might serve for monitoring those processing operations.

3.7.1 Think About:

- Data processing registers
- Record management
- Change history
- Workflow management

3.8 Providing Evidence

In order to demonstrate compliance with the GDPR principles, organisations must ensure that they have, and retain, extensive bodies of evidence. The GDPR grants supervisory authorities significant powers of investigation, audit and access, to both premises and data. (In the UK, the supervisory body is the ICO.) Supervisory authorities can compel controllers or processors to provide any information they require for the performance of their tasks. As such it is imperative that organisations implement mechanisms to capture and retain evidence of compliance to respond effectively to requests from the supervisory authority.

3.8.1 Think About:

- Activity logs and records
- Backups and business continuity plans to prevent loss of evidence and retain integrity of data

4.0 Governance, Accountability and Management Review

The GDPR has been designed to promote both accountability and governance. These principles have always been implicit requirements of data protection legislation, however the GDPR places much greater emphasis on them.

Organisations will need to design and implement comprehensive, albeit proportionate, governance measures where responsibility starts 'at the top'. Executive management must ensure that responsibilities for lawful processing and protection of personal data are understood and implemented at every level. Regular reporting and evidence retention will help to demonstrate whether the organisation is compliant. The 'accountability' principle states explicitly that the data controller (typically represented by the executive management team) shall be responsible for, and be able to, demonstrate compliance with all other principles detailed.

Under the GDPR, failure to ensure compliance can lead to personal prosecutions, with the Chief Executive Officer (CEO) being ultimately accountable.

Measures to demonstrate compliance include:

- Regular, minuted, management meetings to review data protection arrangements and provide management support to compliance activities
- Allocation of specific data protection roles and responsibilities, including appointment of a data protection officer (DPO)

- Assessment and review of privacy risk
- Implementation of privacy impact assessments (PIAs)
- Providing evidence that measures have been implemented to mitigate privacy risk
- Maintenance of documentation containing information registers and grounds for processing
- Implementation and communication of data protection policies
- Regular staff training and awareness
- Ensuring data protection by design and by default

4.1 Think About:

- Implementing a formal document management system
- Risk assessment tools, particularly those integrating with information security and corporate risk
- Privacy impact assessment tools
- Workflow management to address management actions and ensure completion
- Internal compliance auditing
- Preventative and corrective action
- Implementing a privacy information management system (as defined in BS 10012), integrated with ISO 27001

4.2 Appointing a Data Protection Officer (DPO)

The GDPR requires the appointment of a Data Protection Officer (DPO) where the:

- Processing is carried out by a public authority or body, except for courts acting in their judicial capacity
- Core activities of the controller or the processor consist of processing operations which require regular and systematic monitoring of data subjects on a large scale
- Core activities of the controller or the processor consist of processing on a large scale of special categories of data and personal data relating to criminal convictions and offences

Organisations are permitted to work together and form an undertaking (or group of undertakings). They may appoint a single DPO, providing they are easily accessible from each establishment.

Organisations have a duty to ensure that the designated DPO is appointed based on their professional competency and, in particular, in-depth knowledge of data protection law and practices. The DPO must be appointed to be the single representative and point of contact with the supervisory authority, but may be supported by a team. Multiple DPOs covering different processing activities are not permitted.

DPOs must be independent and have direct reporting to the executive management team. In order to prevent any conflict of interest, those prohibited from DPO roles include the CEO, COO, CFO, Chief Medical Officers, Head of Marketing, HR or IT.

4.2.1 Think About:

- An assessment of whether a formally appointed DPO is mandatory and retention of that assessment as an evidential record
- How senior roles interact with the DPO to ensure organisational compliance

- Empowerment, authority, seniority and jurisdiction of the DPO role
- Information flow to the DPO to inform them of breaches or privacy concerns, including complaint handling
- The provision of secure and unmonitored communications to data subjects (other employees)

5.0 Data Protection by Design and by Default

'Data protection by design' means that, both at the time of determining how data is going to be processed and the time when processing is taking place, organisations must implement appropriate technical and operational measures which adhere to data protection principles, such as data minimisation. By including privacy by design, the legislators are aiming to make data protection a fundamental component in the design and maintenance of information processing systems and procedures, rather than just an afterthought.

With 'data protection by default', organisations are required to implement technical and organisational measures to ensure that, by default, only personal data which is necessary for each specific purpose of the processing is processed. An example would be ensuring that the privacy setting on a social media platform is set to 'high' by default.

By default, in order to implement privacy by design, organisations will need to ensure that risks to the rights of data subjects are integrated into the design and implementation of processing systems and procedures, i.e. specification of privacy and security requirements within the systems' acquisition and development life cycle. The GDPR does provide data controllers with some flexibility, allowing them to take into account 'the state of the art', cost of implementation, nature, scope and purposes of processing, as well as the likelihood and impact of risks posed to the rights and freedoms of data subjects.

As the legislation does not specify the required level of compliance, organisations must consider conducting regular pre-screening to determine whether privacy impact assessments (PIAs) are required, as well as maintaining an awareness of the published guidance and expectations of the regulators.

5.1 Privacy Risk and Privacy Impact Assessments (PIAs)

PIAs are mandated under the GDPR for all new business projects, new technologies or major organisational changes involving the processing of personal data. PIAs must consider whether changes will impact personal information and, if so, what steps must be taken to protect that data. This includes evaluating relationships between the data controller and data processor, both in terms of outsourcing of business processing and, vitally, outsourcing of IT infrastructure management, hosting, systems development and support.

Where a type of data processing is likely to result in a high risk to the rights and freedoms of data subjects, the GDPR requires that the data controller carries out an assessment of the impact of the planned processing operations on the protection of the rights and freedoms of individuals prior to carrying out the processing. The regulation does allow controllers to use a single assessment to address a set of similar processing operations that present similar high risks.

At minimum, PIAs must contain:

- A systematic description of the envisaged processing operations and the purposes of the processing including, where applicable, the legitimate interest pursued by the controller
- An assessment of the necessity and proportionality of the processing operations in relation to the purposes
- An assessment of the risks to the rights and freedoms of data subjects

- The measures envisaged to address the risks, including safeguards, security processes and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR, considering the rights and legitimate interests of data subjects and other persons concerned

5.1.1 Think About:

- Incorporating PIAs in IT project management and change management processes
- The relationship with IT system release management and IT operations processes
- Engagement with business process owners as part of the acquisition, specification, development and deployment of new systems, suppliers or technologies
- Developing workflows to ensure that privacy concerns are addressed wherever a project or change interfaces with other systems or services that contain personal data
- Conducting PIAs for existing personal data to ensure appropriate protection mechanisms are in place
- The contribution that IT representatives (e.g. system developers, administrators, webmasters, infrastructure and IT asset managers, database administrators, system owners, IT asset managers etc.) will be required to make to PIAs and the knowledge needed
- Formal PIA reporting, sign off and authority levels (e.g. right for the DPO to veto) and retention of PIA evidence

5.2 Data Protection and Privacy Policies

The requirements for providing privacy information to data subjects are broader than those in the DPA. Data protection and privacy policies must reflect these requirements and ensure that both technical and processing information is appropriately communicated.

Organisations are required to review all privacy notices to confirm they are compliant with the requirements of the GDPR. In order to comply, organisations will need to ensure that the information they provide is:

- Concise, transparent, intelligible and easily accessible
- Available to non-online users (e.g. call centres/telephony and customer services)
- Written in clear and plain language, particularly if addressed to a child
- Unbundled from other terms and conditions
- Evidenced and verified

5.2.1 Think About:

- Maintaining records of privacy notices and information so that consent can always be linked to the notice in force at the time that information was provided
- How shared third party hosted systems will handle or publish/update your privacy notices
- Aligning with published information notice codes of practice
- Existing professional and common law expectations or obligations for confidentiality (e.g. doctor/patient, teacher/pupil, lawyer/client)
- Employer/employee expectations of privacy in the workplace and implications for monitoring communications (internet, email, telephony, IT access and usage logs)
- Application data transfers

- Data sources and the additional information to be provided when the data is not collected directly from the individual
- Providing information notices to mobile apps

5.3 Training and Awareness

To ensure organisations remain compliant with the GDPR, staff must be provided with appropriate awareness, education and training, as well as regular updates on organisational policies and procedures as a means of establishing trustworthiness and reliability. One of the tasks of the DPO is to monitor training and awareness of staff involved in processing operations. Records of the training provided, along with completion and success/failure rates, need to be maintained in order to evidence compliance under the accountability provisions introduced by the GDPR.

5.3.1 Think About:

- Conducting a training needs analysis, including targeted training for IT roles
- General staff awareness campaigns, including formal training, posters and electronic messaging
- Introducing e-learning to ensure training is provided for new joiners and regular refresher training for all staff
- E-learning tests to demonstrate understanding of requirements
- Monitoring of completion rates and effectiveness

6.0 Rights of Data Subjects

One of the primary aims of the GDPR is to give data subjects more control over the processing of their data. With this in mind, the GDPR introduces some new rights for individuals and strengthens some rights that already exist under the DPA. These rights are:

- To be informed – encompassing what information should be supplied to individuals and when they should be informed
- To access – including confirmation that their data is being processed, access to their personal data and other information which largely corresponds to the contents of privacy notices
- To rectify inaccurate or incomplete data
- To erase – also known as the right to be forgotten (but only applicable if the grounds for processing relies on consent and if there are no other statutory or legal reasons why the data is retained)
- To restrict processing – allowing the controller/processor to store, but not further process the data
- To data portability – receiving a copy of the data in a commonly used and machine-readable language, and to transmit data to another controller without hindrance
- To object to processing based on legitimate interests, the performance of a task in the public interest/exercise of official authority, to direct marketing or processing for purposes of scientific/historical research and statistics
- To safeguard against automated decision making and profiling – particularly against the risk that a damaging decision affecting an individual is made without human intervention

6.1 Think About:

- Handling and responding to subject access requests in terms of finding and assembling the data records
- Accessibility of data held in backups and archives
- Personal data held locally by staff, spreadsheets and non-centralised collections of data
- Mobile computing and the ability to decrypt legacy data
- Voice recordings and CCTV images
- Network drives and permitted storage locations
- Database extraction and incidental storage of additional data sets and reports

7.0 Breach Notification

The GDPR introduces a duty on all organisations to report data breaches that are likely to result in a risk to the rights and freedoms of individuals to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it. Breaches will also need to be notified to affected individuals without undue delay. Article 34(3c) also requires that where communication of the breach to the data subject involves undue effort, there shall be a public communication or similar measure.

A personal data breach is defined as a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Where a breach occurs, there is an expectation that the supervisory authority will receive the following information:

- The nature of the personal data breach including, where possible:
- The categories and approximate number of individuals and personal data records concerned
- The name and contact details of the DPO (if the organisation has one), or another contact point where more information can be obtained
- A description of the likely consequences of the personal data breach
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, the measures taken to mitigate any possible adverse effects

Due to the demanding notification timescales, organisations must implement an effective internal breach reporting process and comprehensive breach management procedures to ensure a consistent and effective approach to the management of information security incidents. The process/procedures will need to include communication of security events and weaknesses, including the need to notify the supervisory authority or the affected data subjects.

7.1 Think About:

- Mechanisms for security breach reporting - how are they received? Where do they go?
- Mandatory internal reporting and consequences of failing to report an incident
- Who is responsible for conducting an initial evaluation - assess if it is a real incident or suspected, as well as if any data has been lost, destroyed or disclosed
- Assembling emergency response teams and containment actions
- Training for response teams (business and IT)

- A root cause analysis to identify what caused the breach
- Preventative and corrective action and record keeping
- The role of IT support in identifying a security cause or effect arising from an IT support request
- IT incident management processes versus security incident management processes
- Incident classification; internal/external, accidental/deliberate etc.
- Whether a formal notification to the supervisory authority or forensic investigation is required
- Authority to notify the incident to external regulators and approved external communications
- Whether employees are implicated in the breach and their rights to privacy
- Integration with disciplinary procedures
- Security and retention of investigation reports
- Collection and preservation of admissible electronic evidence
- IT supplier contractual obligations for incident reporting

8.0 Use of Third Parties, Cloud Solutions and Hosted Applications

8.1 Outsourcing

Where the processing of personal data has been outsourced to a third party, one of the key changes under the GDPR is that data processors, which are currently not subject to the DPA, must comply with certain requirements of the GDPR. In addition, the legal risk will no longer sit solely with the data controllers, as data processors will become directly liable for fines - and for compensating individuals in the event of their non-compliance.

The nature of new technologies, such as platform as a service (PaaS) and software as a service (SaaS), has resulted in many third parties being captured by, and having obligations under, the GDPR (who would have previously been out of scope).

Outsourcing takes many forms; it may cover full business process outsourcing, or the outsourcing of IT infrastructure and application system development, hosting and support that involves on premise or remote services. Any service provider or supplier (whether authorised or not) is likely to be considered a third party data processor.

8.2 Boundaries of Responsibility/Accountability

The GDPR makes both data controllers and processors responsible for compliance. The increased statutory obligations on data processors include:

- Data processing agreements – processors may only process personal data on behalf of a controller where a written contract is in place. The contract must contain certain mandatory terms which are set out in Article 28 of the GDPR.
- Sub-processors may not be engaged without the prior written authorisation of the controller, and the processor must flow-down the applicable terms of a data processor agreement or service contract to its own suppliers.

- Processing agreements (contracts) must permit processing of personal data only in accordance with the instructions of the controller.
- Data processors are required to demonstrate accountability and governance by maintaining records of data processing activities and the controller's DPO contact details. PIAs must also be performed when introducing new technologies and third parties, and these records must be made available to the supervisory authority on request.
- Processors must co-operate with the supervisory authority (Article 31 of the GDPR).
- Data security – data processors must implement appropriate technical and organisational measures, and inform data controllers of any data breaches.
- Where applicable, designate a Data Protection Officer (DPO).
- Cross-border transfers – processors must comply with conditions regarding transfers of personal data outside the EEA.
- Sanctions – non-compliant processors risk fines of up to 4% of global annual turnover.

It can be difficult to determine whether you are a controller or processor and, if you are unsure, it is recommended that you conduct and document a thorough review to establish and agree your role with your client/third party provider.

8.3 PaaS Providers

Providers of platforms are certainly data processors, as they store data or host applications in which data resides. However, if they merely provide a platform onto which the customer installs their own applications, then the provider will not be a controller in respect of that data.

PaaS providers should prepare for the GDPR by:

- Anticipating what evidence controllers might seek from their organisation to ensure they are able to provide 'sufficient guarantees'. Preparing and collating the evidence in advance and maintaining it over time is much simpler than trying to respond to each customer request in isolation.
- Implementing appropriate technical and organisational measures to secure the platform, taking into account that they may not know exactly what data their customers will be processing.
- Ensuring they have versions of the data protection impact assessment for their platform/systems that they are happy to share with their customers.
- Considering how their system meets the requirements of privacy by design and privacy by default.
- Identifying what they need from data controllers so that they can meet their GDPR obligations as a processor. Controller and processor obligations must be set out clearly.
- Preparing to negotiate around the mandatory contractual clauses. Unlike the model contract clauses used to legitimise international data transfers, the mandatory contract clauses do not need to be used verbatim providing the data processor with an opportunity to tailor them to customer context.
- Carrying out, and documenting evidence of, due diligence on their supply chain.

8.4 SaaS/Application Hosting Service Providers

If an organisation provides access to a software application as a cloud service provider, then they would be classed as a data processor under the GDPR. Their responsibilities will be similar to those set out above for platform providers. However, as the service providers are closer to the data, the level of assistance they will need to provide to the data controller in relation to fulfilling subject access requests, and the requirements in

respect of ensuring the security of data, will be more significant. The parties should, therefore, consider how the cost overhead associated with maintaining GDPR compliance, and the nature of warranties and liabilities for non-compliance, will be stated within the data processing agreement (contract).

Careful consideration should also be given to how they are going to respond to the enhanced data subject rights that the GDPR introduces. Can the application offer self-service portals to data subjects, or will the data controller need to implement processes for the data processor to support their staff to field requests?

Finally, an organisation will need to agree how joint obligations (e.g. security and international transfers) are going to be dealt with contractually between the data controller and the data processor, or vice versa.

In some cases, more than one party to a data processor agreement (contract) may determine the purposes, and the manner in which, the personal data is processed for all or parts of the processing. In this case, the parties would be considered joint controllers and contracts would need to specify those obligations and set boundaries around who performs which parts of the processing.

8.5 Supplier Management and Supplier Service Delivery Management

In order to prepare for the GDPR, controllers will need to clarify the duties and responsibilities in the respective data controller and data processor, or sub-processor, contracts. Chapter IV of the GDPR deals with the requirements in respect of controllers and processors. While the burden of personal data protection rests primarily with the controllers, processors face enhanced liability for failing to comply with the applicable legislation. Controllers are responsible for ensuring that any processing activities are performed in compliance with the GDPR, and the relationship between controllers and processors must be governed by a contract that details the tasks and responsibilities of each party.

Data controllers and processors with sub-contracts are advised to ensure they have a right to audit their respective suppliers to verify their compliance with the requirements of the GDPR. Also, mandating that suppliers have achieved certification to the ISO 27001 international security standards (or equivalent standards) is common and, increasingly, includes contractual commitments in relation to Cyber Security Essentials. In addition, many cloud service providers are seeking to include the controls and assurance relating to cloud security set out in ISO 27018 within their ISO 27001 certifications, to cover the processing of personal information. Cloud service providers offering PaaS and SaaS are also increasingly offering to share their PIA results and security risk assessments, and a statement of security capability to customers and potential customers as a means of assurance. Where these are not provided, data controllers must rely upon their own due diligence/PIA evaluation within their supplier selection processes and retain the outcomes as evidential records.

8.6 Think About:

- Processes for the evaluation or re-evaluation of new and existing suppliers/service providers
- Development of pro-forma contractual clauses for use in supplier contracts
- The role of procurement in supplier selection
- Register of data processors

9.0 Role Played by Tools

Tools can play a major role in easing the burden of complying with the GDPR. In this section there will be an assessment of the role played by tools in the following areas:

- Data discovery
- Data mapping
- Encryption
- Protection of information in transit
- Hosted solutions
- Data management
- Document management
- Logging, monitoring, alerting and reporting
- Backup and restore
- Automated deletion
- Asset tracking
- Data retrieval
- Data destruction

9.1 Data Discovery

The GDPR requires both controllers and processors to maintain records of processing activities. Understanding what data is flowing through an organisation and where it is, assuming it is not always where you expect it to be, is a prerequisite for assessing the risks to the data. Modern data discovery tools not only help organisations identify unstructured personal data, but also offer the analytics, tracking and reporting necessary to deliver organisational accountability for file use and security. Designed to manage the needs of organisations with petabytes of data and billions of files, the tools can be integrated with archiving and security solutions to prevent data loss and ensure policy-based data retention. This allows organisations to:

- Automate governance through workflows and customisation
- Drive efficiencies and cost savings
- Maintain regulatory compliance for information access, use, and retention
- Protect confidential information from unauthorised use and exposure

9.2 Data Mapping

While data mapping is not a specific requirement of the GDPR, meeting the requirements of the regulation would be extremely difficult without having a clear picture of the life cycle of personal data in the organisation. This can be extremely challenging for organisations and something that requires ongoing maintenance, so it is worth considering using a tool to help manage the process. The objective of the exercise is to identify areas where there is a risk to the rights and freedoms of data subjects in order to specify and implement appropriate technical and organisational measures to mitigate the risk. A tool will help to collate the findings of the data mapping exercise, including:

- The location of in-scope data

- What format the data is stored in/on e.g. hard copy, USB, cloud etc.
- How the data is moved between applications e.g. email, SFTP, courier etc.
- The physical locations where data is processed/stored

9.3 Encryption

Where the DPA was largely technology agnostic, the GDPR makes a number of explicit references to encryption as a means of protecting data, but encryption does not represent a panacea. Encryption tools can be used in a variety of ways, such as to protect data in transit or at rest, provide verification of data integrity and authenticity, and even offer a means of secure destruction.

Encryption solutions can be applied to collective data (e.g. database encryption), at the file or database field/column level. However, the encryption may need to be reversible and data controllers must ensure that the technologies selected are appropriate for the formats needed. Controllers also need to ensure that the encryption keys are properly managed to enable decryption of the data when necessary, particularly in relation to older technologies and legacy data.

For communications systems, the latest cloud-based secure messaging and email encryption tools do not suffer from the substantial administrative burden or end user client installation. Previously, this compromised the effectiveness of typical email encryption solutions, such as enforced server-to-server transport layer security (TLS) or public key infrastructure (PKI), however the new tools enable organisations to protect sensitive information without additional hardware and software for senders or recipients.

9.4 Protection of Information in Transit

Best practice stipulates that organisations should implement adequate technical measures to protect personal data during transmission, over and between networks, to further safeguard confidentiality and integrity. This is achieved through a combination of network protection (ensuring attackers are unable to intercept data) and encryption (to render the data unintelligible). Data controllers must apply appropriate controls to ensure that data is protected:

- Between endpoints and the service
- Internally within the service
- Between the service and other services

Controls could include the use of virtual private network (VPN) solutions, disabling insecure protocols, supporting strong protocols and even private point-to-point connections between data centres.

9.5 Hosted Solutions

Hosted solutions offer smaller organisations the use of security tools that were previously the preserve of large organisations, thereby supporting their efforts to comply with the secure processing requirements of the GDPR. These could include robust firewalls, enterprise quality antivirus and web filtering, encryption of emails and management of all endpoints. By outsourcing the storage, backups, security and processing of data - and provided they meet the requirements for appointing a processor - organisations can significantly reduce their compliance burden.

9.6 Data Management, Backup and Archiving Solutions

With some estimates suggesting that 90% of all the data in the world has been generated over the last two years, effective data management i.e. the use of architectures, policies and procedures to manage the information life cycle needs of organisations, is becoming increasingly challenging. Easy-to-use data

visualisation tools can help uncover hidden personal data, identify risks and accurately classify all personal data, providing organisations the intelligence to demonstrate many obligations for GDPR compliance.

9.7 Logging, Monitoring, Alerting and Reporting

The data breach notification requirements oblige organisations to notify the supervisory authority (ICO) without undue delay and, where feasible, not later than 72 hours after having become aware of a data breach*. With the time involved in detecting a breach typically being measured in months, this requirement presents a significant challenge to organisations. Tools that monitor and log the environment, create alerts when anomalous events are detected and support reporting both for the purpose of breach notification and continuous improvement, should be considered. Tools that provide forensic analysis of events and the management of breach investigation evidence are also of value.

*May be 72 hours from actual breach with Data Protection Bill.

9.8 Asset Tracking

The capability to track assets is a fundamental building block of an effective data protection and information security management system. However, the ability to identify assets and define appropriate protection responsibilities can be challenging. Organisations should consider tools that support:

- Identification of assets and creation of an asset inventory
- Assignment of ownership of assets
- Enforcement of acceptable use rules
- Tracking of assets
- Return of assets upon termination of employment, contract or agreement

9.9 Data Retrieval

The GDPR confers a number of rights on data subjects which are dependent on the organisation being able to locate and retrieve personal data at the request of the data subject, such as the right of access or the right to data portability. As the EU is planning to promote these rights to individuals, it is reasonable to assume that data subjects will exercise these rights more frequently and controllers/processors will need to be able to respond to them in the prescribed timescales. Tools that support the effective retrieval of data from systems in common machine-readable formats should be considered, in order to minimise the overheads that might be incurred as individuals exercise their rights.

9.10 Data Destruction

Tools that enable the sanitisation and disposal of IT equipment previously used for the processing of personal data, such as electronic file shredding programs, should be deployed to ensure permanent erasure if the organisation performs this activity internally.

10.0 Likely Impacts of the Regulation on Working Practices

10.1 Data Breach Notification Case Study

Currently under the DPA there is no legal obligation on data controllers to report breaches of security to the ICO. Similarly, there is no legal obligation, although there is arguably a moral obligation, to inform potentially

affected individuals (e.g. staff or customers) of a data breach. This has meant that under the DPA, many organisations took the decision not to report breaches of security to either the regulator or the data subjects. However, the GDPR requires that, unless the breach is unlikely to result in a risk to the rights and freedoms of the data subject, it must be reported to the supervisory authority (ICO) and prescribes the information that the notification to both the regulator and the data subject must contain. Nonetheless, UK public sector data controllers have been required to notify the UK Information Commissioner, and the following case study illustrates the approach taken:

A local authority (council) received information from a journalist stating that, whilst searching online for information about his family, his search results displayed personal information about other members of the public in the guise of questions they had submitted to the council via their website. The email pointing out this fact was directed to the customer service team who did not recognise the issue as a security breach (indicating a lack of effective training), and was not made available to the legal department for a number of weeks (lack of process and awareness of roles/responsibilities).

An initial investigation into the website disclosure confirmed that approximately 3,000 records had been disclosed, or at least potentially disclosed, but no information was available as to whether anyone had actually seen those search results. The following possible causes were identified:

- The website component receiving questions from the public was a legacy application managed by a webmaster who had recently left the organisation. There was suspicion of a deliberate malicious action by a disgruntled employee. No evidence was available to support this theory, however, a single point of failure and lack of segregation of duties was evident, as the webmaster in question was the only person who had knowledge of the legacy application.
- The legacy website component used a script to poll for new questions and import them into a database. The questions were then monitored and specific questions extracted for publication on the council's 'frequently asked questions' web page hosted on another web server after all personal identifiers had been removed. No administrator log information was available to evidence that the script had been altered or removed.
- The legacy application had recently undergone a software upgrade. The investigation and consultation with the third party who managed the application did not evidence that the software upgrade was responsible.

The council suspected that external intrusion was responsible for the compromise and arranged for penetration testing and a vulnerability assessment, together with computer forensic examination. Cyber attack and the presence of malware was ruled out. However, the lack of date and time stamped audit logs hampered the forensic examination.

A data protection specialist was then engaged to conduct an analysis of the data loss and perform an evaluation of the potential harm caused to individuals by the breach. The analysis considered how many of the 3,000 records contained personal data (1,200) and, of those, how many records contained sensitive personal data (less than 100).

Subsequently, the authority notified the ICO and provided a copy of the investigation report, which included the timeline and actions taken, together with evidence of its breach management procedures and the actions taken to inform those individuals who were considered at risk of being caused harm and distress from the breach. The council elected to offer support to the individuals concerned should they suffer any consequences from the disclosure, e.g. attempted identity theft, unsolicited marketing, financial loss etc. The breach notification was submitted using the published process and forms available on the ICO's website.

Outcome:

Further root cause analysis and lessons learned activities identified that the breach was caused primarily by the security architecture applied to the legacy website, specifically, that the database collecting the submitted questions was located on the same host as the web server application. Best practice recommends that the database should have been hosted on a back office or separate server protected by an internal (DMZ) firewall. The architecture was corrected. Formal change management was applied, encompassing approval for changes made by the software supplier. Cross training was implemented to remove the single point of failure/ webmaster dependency.

Additional corrective action was taken to remove the offending data from the search engine cache to ensure that the original results would remain unavailable to future searches.

Appropriate security measures (architecture, segregation of duties, separation of database from internet facing host, firewall deployment, administrator and date/time stamped event logs/log management tools) would have prevented the considerable costs incurred in relation to specialist forensic examination, penetration testing and professional data protection consulting services. Fines levied by the ICO and the identity of the council have been deliberately omitted from this case study.

10.2 Cross Border Transfer Case Study

Background to the GDPR requirements

Chapter V (Articles 44 - 49) of the GDPR governs cross border transfers. The growing complexity of IT systems and increased use of PaaS and SaaS has seen an increasing number of organisations introducing, often unwittingly, transfers of personal data to third countries or international organisations into their operating model. The US is often where ideas and money combine and, thus, it is not uncommon for a closer inspection of the privacy notices of well known online applications to reveal that data is both transferred to, and stored, in US based infrastructure. There are several ways of legitimising transfers outside the European Economic Area (EEA). Controllers and processors will need to determine the most appropriate mechanism for their circumstances and ensure they apply the appropriate safeguards mandated by the GDPR. This could see them adopting binding corporate rules, relying on finding an adequate level of protection by the EU Commission, adherence to a code of conduct or certification scheme, or using standard data protection contractual clauses. There are also several derogations available for legitimising a transfer to a third country including:

- The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards
- The transfer is necessary for the performance of a contract between the data subject and the controller, or the implementation of pre-contractual measures taken at the data subject's request
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person
- The transfer is necessary for important reasons of public interest
- The transfer is necessary for the establishment, exercise or defense of legal claims
- The transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent

- The transfer is made from a register that, according to EU or member state law, is intended to provide information to the public and that is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case

A final derogation (under Article 49) provides that where a transfer could not be based on standard contractual clauses, Binding Corporate Rules (BCRs) or any of the other derogations, "a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data." If relied upon, the justification as to why this derogation was deemed applicable must be subject to meticulous and consistent internal documentation.

Cross-Border Data Transfer

A global online gambling group utilised a single, enterprise customer support application in conjunction with its gaming platform. The application was used by customer support agents across the organisation, including those located in regional offices where player support required local language skills. The application and supporting databases were hosted and managed within the UK HQ, replicated in real-time to a disaster recovery mirror system located in Dublin, Ireland. The organisation had acquired the company who had originally commissioned and deployed the application and specified the security requirements. Following the acquisition, the organisation commissioned a system audit.

The audit revealed that the application was used by customer support teams in Brazil to offer Portuguese language capability, provided by a third party organisation, with directly employed (internal) customer support teams using the application via a call centre in Asia, the US and Europe. The application was developed and supported by an outsourcing agreement with a third party organisation located in a non-EEA member state in Eastern Europe. The application gave access to customer support agents to all individual betting accounts, bank account data, credit and debit card data, betting history, and customers who had self-excluded on the grounds of gambling addiction. The same application included a capability to alert customer support agents to any attempted fraudulent activity.

Access control and security measures were found to be diligently applied and the organisation had established formal change management procedures within the UK IT function appropriate to a highly regulated sector, including over the IT disaster recovery system. However, data protection requirements had not been specified in the original design and development project, including the legitimisation of the international transfers of the personal data processed by the system. The organisation had made a common assumption that because the application and databases resided (data at rest) within the UK and Ireland, that no transfer of data was taking place.

No formal agreement or evaluation of the developer third party had been performed that specified the use of real/live personal data for testing purposes, and no anonymisation was applied to that test data. The local firm was storing test data sets on their own internal development systems. No contractual clauses or safeguards were in place to ensure the rights and freedoms of individuals were upheld by the recipient external third party as a means to legitimise the transfer of data to them, including administrator access to the system production environment for application support purposes. Consequently, administrator access was not logged and administrator password creation and authorisation granting remote access was available to the third party. No two-factor authentication for administrator level access was implemented.

Similarly, event logging on the live system was not fully enabled for directly employed customer support agents, leaving the organisation unable to provide reliable evidence of who did what and when. The

application log-on screen did not inform internal, authorised users, that their use of the system would be monitored.

For those countries where the group had directly employed customer support agents, no inter-group model contractual clauses were in place to legitimise the data transfers (via access) to the non-EEA countries involved. In addition, access permissions granted access to all regions' data, not limited to those customers located within the respective local regions (need to know principles).

Outcome

The resulting audit report was provided to the Head of Legal, who quickly grasped the situation and implemented inter-company/inter-group data transfer agreements for all international entities using the application, and ensured that their US entity was fully signed into the EU Privacy Shield (formerly Safe Harbour Scheme) to legitimise the international transfers. A two-factor authentication solution was identified and deployed for all technical administrator remote access, and centralised log management tools were identified and approved as a capital expenditure within the IT budget. Re-negotiation of the application support and development contract to include additional security requirements proved difficult as this represented additional expense for the supplier, although a contract change note achieved the transfer legitimisation and the supplier removed all legacy test data sets. As a corrective action, procedures and tools to provide pseudonymisation of test data were implemented. As a result of retrospective agreement of improved security measures, including the right to audit the supplier, the organisation was forced to accept the security risk for the remaining duration of the supplier agreement.

Lessons learned confirmed requirements for third party supplier evaluation and privacy impact assessment processes, which were subsequently documented and adopted as part of the organisation's ISO 27001 information security management system.

Head Office
Gainsborough House
Manor Park, Basingstoke Road
Reading, Berkshire, RG2 0NA

0333 015 8000
enquiries@ultima.com
www.ultima.com