THE HIDDEN DANGERS OF THE GDPR

ultima
URM | ULTIMA RISK MANAGEMENT

The General Data Protection Regulation (GDPR) is designed to bring about a greater consistency of data protection legislation and approach across the EU and beyond. It addresses the changing nature in which personal data is being used, or in some cases abused, and will have a wide-ranging impact on all organisations processing personal data.

With the additional obligations that the GDPR introduces, along with enhanced powers of enforcement and the potential for severe financial penalties (e.g. up to 4% of global turnover), this is quite simply a piece of legislation that organisations cannot afford to ignore.

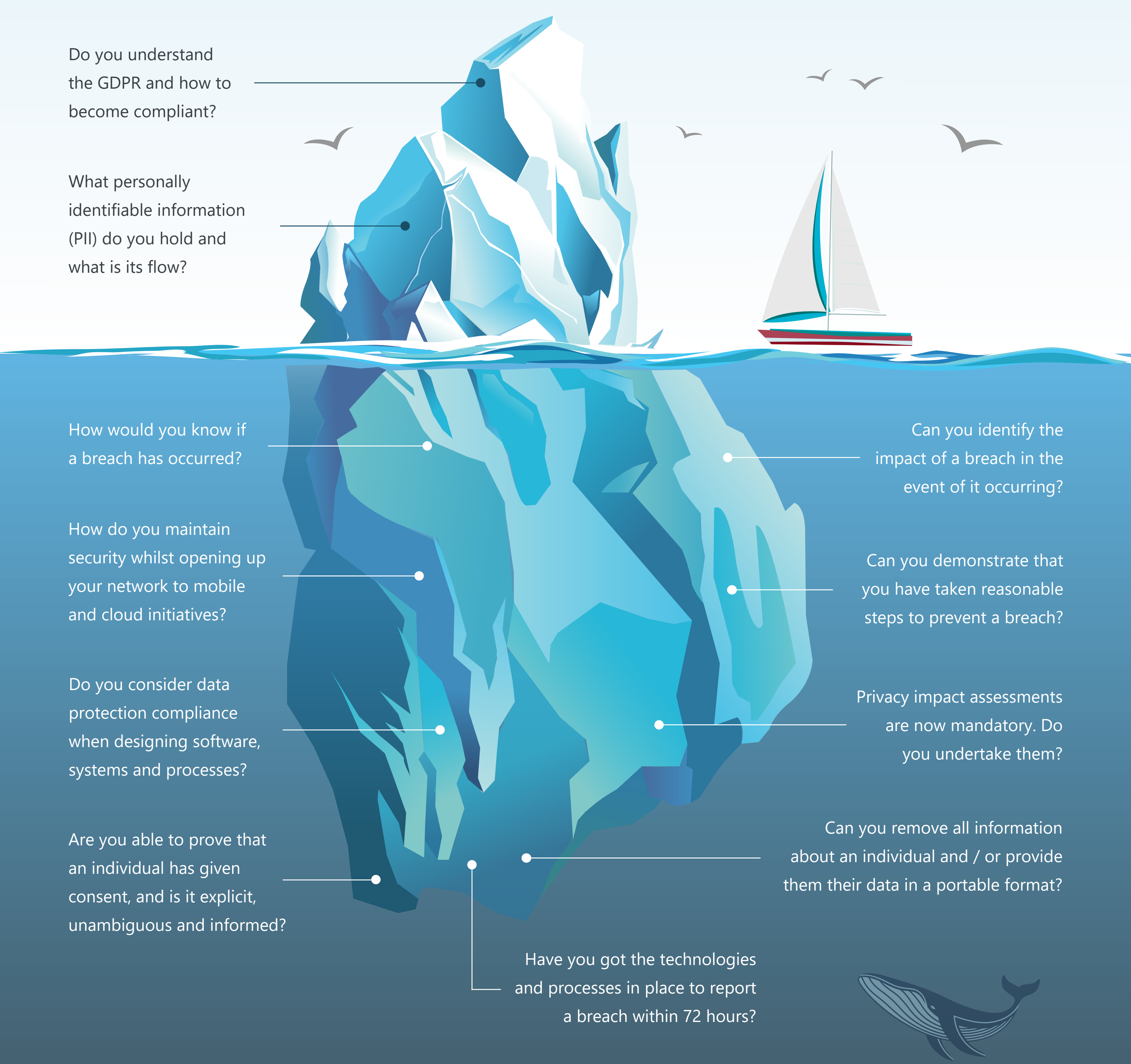
The GDPR forms part of the data protection regime in the UK, together with the new Data Protection Act (DPA) 2018. As and when the UK leaves the EU, the new DPA will replace the GDPR. The GDPR applies to EU-based companies, and those that collect data of EU citizens, regardless of their physical presence.

The drivers for GDPR are two-fold. The EU wants to grant people more control over how their personal data is used. It also wants to give organisations a simpler, clearer legal environment in which to operate, making data protection law identical throughout the single market.

While the GDPR applies to personal data, the definition of that data has been significantly broadened and is more detailed compared to former legislation such as the Data Protection Act.

With the GDPR, information such as an online identifier (e.g. an IP address) can be classed as personal data. The more expansive definition contains a wide range of personal identifiers, reflecting changes in technology and the way organisations collect information.

Achieving compliance presents considerable challenges and therefore demands a business-wide approach.



Awareness

The principles of the GDPR are similar to the DPA, with several key enhancements and additional obligations which will impact every organisation. Understanding what PII exists as well as how it is stored, processed and protected is essential to remaining compliant and to ensure that the rights of the individual are protected.

Security Controls

Protecting PII is essential in order to comply with the GDPR. Organisations will be required to implement both technical and governance measures in order to address the risks posed. This will mean ensuring the ongoing confidentiality, integrity and availability for your data processing systems.

Accessibility

Businesses will be required to make it easy for individuals to exercise the right of access to their information, the right to object to direct marketing and profiling, and to move their data between suppliers. The GDPR recommends that individuals are provided with remote access to a secure self-service system, granting access to their information.

Breach Notification

A personal data breach refers to a breakdown in security, leading to the destruction, loss, alteration, unauthorised disclosure or access. The consequence of a breach is more than just the loss of personal data. Once discovered, it must be reported within 72 hours and if considered high risk, the individuals must be notified.

1

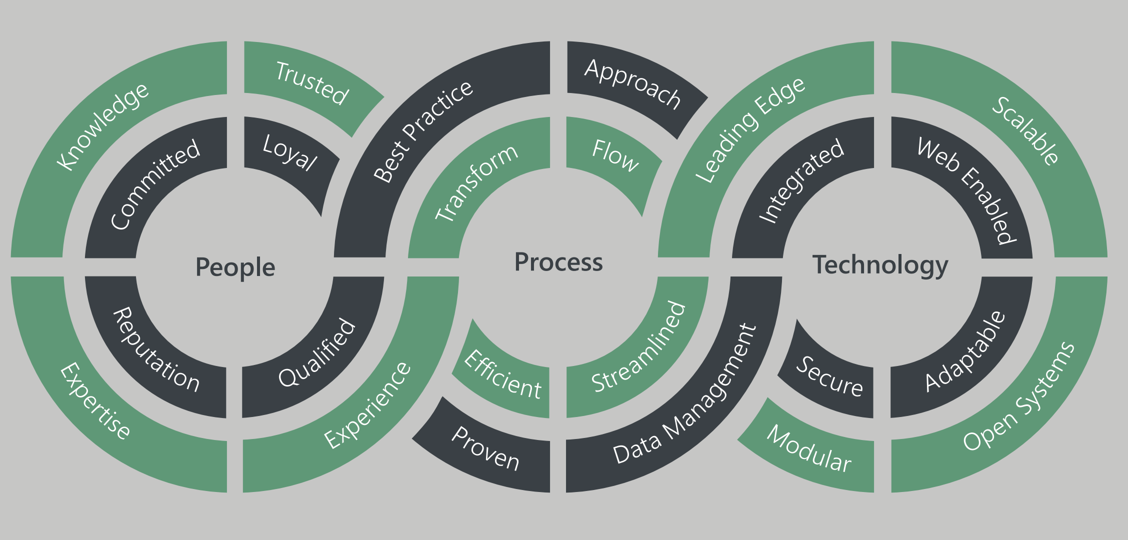
Ultima's Solution to the GDPR Challenge

Whilst technology will ultimately play a vital role in achieving and maintaining compliance with the GDPR, people and processes are often the weakest link.

We understand this consideration and, drawing on our group capabilities, adopt a holistic approach to achieving compliance through an integrated framework of readiness services.

These services are designed to help establish a baseline now the GDPR is in full force. They are based on our proven information security model, delivered to help organisations achieve assurance and compliance to Standards and legislation such as ISO 27001, DPA and PCI DSS. These engagements are designed to help you address key aspects of the GDPR including:

- Explicit Consent
- Right to be Forgotten
- Data Portability
- Breach Notification
- Privacy Impact Assessments
- Privacy Notices
- Record Retention
- Access Control
- Accuracy - Integrity
- Subject Access Request



Our services will assist you in identifying, assessing and managing key PII considerations such as:

Data Identification

Understanding where PII data is received, handled, processed, shared and stored is crucial, both in terms of protecting and managing it correctly, as well as following through on requests to provide or erase it.

Metadata

With requirements to limit data retention, basic information on when and why data was collected, together with its purpose is required to demonstrate compliance with the GDPR's core principles.

Monitoring

With the breach notification requirement in place, your organisation needs to be able to identify unauthorised data disclosure and unusual access patterns to files containing PII and escalate accordingly.

Privacy

GDPR requires you consider data protection compliance when designing software, systems and processes. You must demonstrate that you have implemented measures that meet the principles of data protection by design.

2

Getting Started

Ultima offers a wide range of services to support compliance with the GDPR, covering everything from awareness through to discovery, planning and ongoing auditing. Complementary services to get you started include:

Awareness, Training and Planning

The key to complying with the GDPR is to understand what it means to your organisation, what your risks and issues are, and to create a proactive plan to address any deficiencies found. Ultima provide a number of services to help you identify the key changes and challenges associated with the GDPR and to provide clear and practical guidance on how to prepare for compliance.

Discovery

A real challenge with the GDPR is identifying what data exists and, in particular what is classed as PII, as well as how it is being processed, shared and secured. Ultima's discovery services are designed to help address this by identifying what PII you currently maintain, how it flows throughout your organisation, and how robust your existing security infrastructure is in protecting that data from external cyber threats.

Awareness Workshop / Public Training Course

The objective of this interactive one day course is to provide a comprehensive understanding of the proposed changes to data protection legislation and what the implications are for your organisation.

Key sessions include:

- Understand the background and objectives of GDPR
- Understand the key differences from DPA 1998
- Detailed review of the new GDPR principles

+

PII Data Flow Workshop

Understand where data comes into your organisation, how it is processed, where it resides and who you share it with by conducting a personal data flow analysis. A high level report will be produced enabling you to identify the findings along with a list of actions.

- The volume and nature of existing PII data and how it flows through your organisation
- Weaknesses relating to systems, processes, data life-cycle management and third party sharing
- Controls that will protect your PII data
- Compliance levels with the DPA / GDPR

+

Gap Analysis - Compliance Roadmap

This service is designed to provide your organisation with an assessment of how closely you comply with the GDPR, along with an indication of those areas / activities you will need to focus on in order to achieve compliance. The output is a compliance roadmap which identifies those gaps which need to be addressed ahead of the GDPR coming into effect. This gap analysis will:

- Identify your current compliance position
- Deliver a compliance roadmap with key activities and milestones

+

Cyber Security Assessment

A modular service that offers:

Threat Analysis Assessment - Provides a threat assessment report comparing your security estate to recognised best practice along with recommended remediation actions.
CREST Accredited Vulnerability Assessment - Performed externally, providing contextualised insight into the risks and gaps across your security layer.
Infrastructure Review - Baseline your infrastructure and document findings against industry best practice such as Government 10 Steps to Security and Cyber Essentials.

+

Compliance Roadmap Review

This service offers an independent review by a recognised expert of your organisation's compliance plan / roadmap, providing guidance around priority areas and topics which are missing or would benefit from further attention. The benefits of this service are:

- Gain confidence that you have considered all areas of the GDPR as part of your compliance road map
- Ensure you are correctly prioritising which areas to tackle and when
- Understand where you can integrate compliance into other business processes

+

Data Discovery Assessment

Once PII dataflows have been established, the next step is to identify where PII data is stored. Using appropriate tools, this service is designed to help with the discovery of:

Structured Data - Data with a high level or organisation, such as information in a relational database.

Unstructured Data - Data that either does not have a predefined data model or is not organised in a pre-defined manner. Typically text-heavy but may contain data such as dates and numbers. Media files (such as video and images) are also considered unstructured.

+

Implementation Planning

This planning service is designed to assist you in defining and formalising a response plan for the GDPR in order to drive the adoption of change to achieve compliance. It covers the following key areas:

- Policy
- Process
- Training
- Risk / Privacy Impact Assessment
- Technology
- Data Protection Officer (Training)

+

Technology Solutions

The GDPR requires you to keep personal data secure, which can involve technical measures such as minimising processing of PII and applying suitable security measures. Whereas technology alone cannot solve the GDPR problem, there are a number of technology solutions that can facilitate the protection of PII data and enable you to meet the GDPR requirements such as breach notification and response. Such technologies include:

- Threat Prevention, DLP and Advanced Data Governance
- Threat Detection and Response
- Analytics, Reporting and Forensics

3

Who Are We?

Ultima is not just a technology partner. Within the group, we have been delivering technology solutions since 1991 and governance, risk and compliance services, notably around information security and data protection since 2005. We are in a unique position to offer you a holistic approach to achieving GDPR compliance leveraging people, process and technology solutions.

Compliance with the GDPR requires support from a different kind of partner, who will take time to understand what the GDPR means to your organisation and offer clear and practical guidance on what steps you need to take in order to achieve compliance. Ultima is that partner. Contact us today to learn more about the GDPR and the range of services we offer.

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

ultima
URM | ULTIMA RISK MANAGEMENT

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