SECURE COMMUNICATIONS AND INFORMATION SYSTEMS

**GDPR**

The General Data Protection Regulation (GDPR) is the new EU Regulation relating to the processing of personal data belonging to people living in any of the EU member states (Data Subjects). GDPR replaces the 1995 Data Protection Directive 95/46/EC from which the UK Data Protection Act (DPA) heralds.

## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is the General Data Protection Regulation (GDPR)?</td>
<td>5</td>
</tr>
<tr>
<td>GDPR Is A Unifying Regulation</td>
<td>5</td>
</tr>
<tr>
<td>Why Do We Need The GDPR?</td>
<td>5</td>
</tr>
<tr>
<td>What Does GDPR Give Us?</td>
<td>6</td>
</tr>
<tr>
<td>The Principle Of Accountability</td>
<td>7</td>
</tr>
<tr>
<td>The Principle Of Transparency</td>
<td>7</td>
</tr>
<tr>
<td>Strengthened Data Subject Rights</td>
<td>8</td>
</tr>
<tr>
<td>The Rules For Gaining Consent Have Been Tightened</td>
<td>8</td>
</tr>
<tr>
<td>GDPR Extends Its Geographical Jurisdiction</td>
<td>9</td>
</tr>
<tr>
<td>GDPR Tightens The Definition Of Personal Data</td>
<td>10</td>
</tr>
<tr>
<td>Breach Reporting Rules Have Been Tightened</td>
<td>10</td>
</tr>
<tr>
<td>Data Processors Are Now Liable Under Certain Section Of The GDPR</td>
<td>11</td>
</tr>
<tr>
<td>Data Protection Officers Are Now Mandatory For Some Organisations</td>
<td>11</td>
</tr>
<tr>
<td>Data Protection By Design And By Default</td>
<td>11</td>
</tr>
<tr>
<td>GDPR And Risk</td>
<td>12</td>
</tr>
<tr>
<td>Data Protection Impact Assessments (DPIA)</td>
<td>13</td>
</tr>
<tr>
<td>In Summary</td>
<td>15</td>
</tr>
</tbody>
</table>
What is the General Data Protection Regulation (GDPR)?

The General Data Protection Regulation (GDPR) is the new EU Regulation relating to the processing of personal data belonging to people living in any of the EU member states (Data Subjects). GDPR replaces the 1995 Data Protection Directive 95/46/EC from which the UK Data Protection Act (DPA) heralds.

The government has confirmed that the UK’s decision to leave the European Union will not affect the commencement of GDPR.


The new GDPR thus comes into force in its entirety on the UK on 25th May 2018.

GDPR IS A UNIFYING REGULATION

The General Data Protection Regulation (EU) 2016/679 GDPR is a regulation – rather than a directive, as was its predecessor the 1995 Data Protection Directive 95/46/EC.

A “regulation” is a binding legislative act. It must be applied in its entirety across the EU.

A “directive” is a legislative act that sets out a goal that all EU countries must achieve. However, it is up to the individual countries to devise their own laws on how to reach these goals. https://europa.eu

The 1995 Data Protection Directive 95/46/EC resulted in each EU member state developing their own individual data protection laws based upon this directive. As a result organisations operating across multiple member states found themselves navigating through a complex legal labyrinth of multiple laws.

Thankfully GDPR replaces this legal complexity with a single unified law1 significantly simplifying the regulatory environment for organisations operating across the European Union.

WHY DO WE NEED THE GDPR?

The 95/46/EC Directive was issued over twenty years ago – technologically, economically and socially an ocean away from the situation we find ourselves living in today.

We have moved from the days where static desktop computers were the norm, mobile phones were mobile phones, and internet connectivity was for the few, requiring the use of dial up connections. The growth of the internet, superfast broadband connections, sophisticated mobile processing devices and social media, to name but a few, has created an explosion in the way we share, store and process personal data.

1GDPR does allow member states to introduce National Derogations in a few areas as defined in GDPR Article 23. Further details can also be found on derogations on the Information Commissioners website: https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/national-derogations/

[RECITAL 6]

“Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities”. [Recital 6]

We take our data with us on our devices, share it over multiple platforms and with multiple entities, and store it in unfamiliar and unseen “cloud” locations.

More and more organisations are collecting and processing our personal data, and the volume that exists within the ether has exploded over recent years, and is continuing to grow at an incredible rate. Much of this data is processed electronically, although manual processing of data is still very much an issue. Our expectation upon providing this information to such organisations is that they treat our personal data with respect and do not share or process our data in ways we do not expect. From experience however, not all organisations manage our personal data in line with these expectations.
The survey additionally found that around one in five of the companies surveyed had experienced a data breach during 2016. This is in spite of a year on year increase in the amount of money being spent on mechanisms to ensure the security of data. This is where GDPR comes in. GDPR brings with it strengthened legislation with tougher enforcement measures to govern the way we protect personal data and implement data security for that data in the context of today’s challenges.

WHAT DOES GDPR GIVE US?
Akin to the DPA, GDPR looks to put a data protection framework in place to govern all aspects of the processing of an individuals’ personal data. GDPR brings with it a host of updated measures aimed at clarifying and improving the rules relating to the processing and protection of personal data. It looks to strengthen the rights of those who have their data processed by others, whilst enabling and supporting the necessary exchange and use of that data to support business and commerce. Of significance relating to the changes that GDPR brings, the fines that are imposable for non-compliance have been increased greatly. Organisations breaching the requirements of GDPR could potentially face fines in the region of 20 Million Euros or 4% of their annual turnover (whichever is the greatest). This is a significant increase.

THE PRINCIPLE OF ACCOUNTABILITY
A new accountability principle places an on-going responsibility on Data Controllers to demonstrate that they comply with the requirements of the GDPR. This places an increased burden on the Data Controller to develop and maintain appropriate and sufficient internal records. Accountability will be essential when justifying actions to regulators. Whilst not explicit on the exact concessions that will be applied to fines imposed for a breach of personal data, the regulation does say that “when deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them.”

Additionally, when we provide our data to these organisations we assume that our data is going to be secure. This sadly is not always the case. With this growth in the volume of personal data being processed, the number of people and organisations looking to exploit it for nefarious purposes has also seen a large increase. The Thales 2017 Threat Report (which is reissued yearly) assessed data breach statistics and on-going security spend across over 450 companies internationally. The report states “our 2017 report finds a global situation where spending on security is up – sharply in some sectors – yet successful data breaches are also up significantly.” The survey additionally found that around one in five of the companies surveyed had
Organisations will need to provide transparent information to their data subjects about what data they hold on them, what they do with that data, and what their rights are in respect of that data.

**STRENGTHENED DATA SUBJECT RIGHTS**

Existing data subject rights currently defined under the DPA will still be enjoyed by data subjects within the EU. These however have been strengthened and extended to include three new rights:

- **The right to be forgotten** – the right to have your data erased.
- **The right to object to processing** – only processes consented by the data subject may be undertaken (where consent is the legal basis for processing).
- **The right to data portability** – the right to take your data with you, even if this is to a competitor.

Organisations must have in place the necessary mechanisms to enable data subjects to exercise these new rights when GDPR comes into force in 2018. Some organisations will already adhere to one or more of these rights and have the infrastructure in place to do so. For others this may represent quite a change from the way in which they currently operate, and necessitate the introduction or modification of both technical and organisational measures to meet these new requirements.

**THE RULES FOR GAINING CONSENT HAVE BEEN TIGHTENED**

Consent is an emotive subject. All of us have received unwanted marketing communications from organisations and many privacy policies will currently assume consent by virtue of us using a product or visiting a web site. Under GDPR this will no longer be acceptable.

Organisations will now have to make consent a clear and positive action. Pre-ticked boxes are no longer acceptable, and consent must not be hidden in reams of terms and conditions. Additionally an organisation must ask us to provide separate consent for each processing activity it undertakes.

[RECITAL 32]

“Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject’s agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement.” [Recital 32]

The means by which consent is obtained will need to adhere to the principle of transparency, meaning that organisations must make the process of gaining our consent clear and simple.

Organisation must also ensure that they provide a means of redacting that consent, and ensure that the mechanisms provided to achieve this is are as simple and easy to use and access as the mechanisms used to obtain their consent in the first place.

Under the principle of accountability all consent gained by an organisation must be verifiable, and as such a record of consent and how it has been obtained will need to be kept as part of the corporate record keeping process.

Under the principle of accountability all consent gained by an organisation must be verifiable, and as such a record of consent and how it has been obtained will need to be kept as part of the corporate record keeping process.

GDPR EXTENDS ITS GEOGRAPHICAL JURISDICTION

GDPR has extended its reach and now covers any organisation processing the data of EU data subjects, regardless of where that organisation resides.

[ARTICLE 3]

“This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.” [Article 3]
The regulation is applicable to any organisations who:
- Offer goods and services to individuals in the EU (including free of charge),
- Monitor the behaviour of data subjects within the EU.
This increase in the territorial scope of GDPR, brings a number of overseas organisations within the reach of the new regulation. This may come as something of a surprise to many of these organisations, who will now have to ensure that a complete data protection framework and supporting security measures are put in place within the timeframe for compliance.

**GDPR tightens the definition of personal data**
The definition of what constitutes an individual’s personal data has been extended to include a range of different identifiers as given in Recital 30 below:

**[RECITAL 30]**
“Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags.” [Recital 30]

As a result, a variety of information not previously considered to be personal data, and hence not managed as such, now needs to be protected. This will affect most organisations, and will require some form of change to ensure that all data falling within this definition is now processed legally in accordance with GDPR.

**Breach reporting rules have been updated**
GDPR requires that an organisation inform the relevant Supervisory Authority (the Information Commissioner’s Office (ICO) in the UK) of certain types of data breach (defined within the regulation) within 72 hours. This is a relatively short timescale in which to respond and organisations may need to update their breach reporting and management mechanisms to meet this requirement.

Reporting of breaches to the individuals involved is only required if the risk to those individuals is deemed to be “high”, but the strict 72 hour reporting deadline is not imposed here. Instead the breach needs to be reported to the data subject "without undue delay". GDPR doesn’t however specify what it means by “undue delay”, and this is somewhat open to interpretation.

**Data processors are now liable under certain section of the GDPR**
Whereas previously the legal responsibility for data protection fell firmly in the lap of the data controller, the GDPR now defines a number of legal obligations for which the data processors themselves are responsible. GDPR requires that data processors maintain records of data processing activities undertaken on behalf of a controller, and mandates that they have data security measures in place to enable that data to be adequately protected. Data processors must also comply with breach notification requirements, and data subjects will be able to claim compensation from data processors if they unlawfully process their personal data.

Significantly data processors may also be subject to the increased fines for non-compliance of 20 million Euros or 4 % of their annual global turnover.

**Data protection officers are now mandatory for some organisations**
Whilst many organisations already have a nominated Data Protection Officer (DPO), GDPR now legally requires certain organisations to formally appoint an appropriately trained and resourced DPO. Section 4 of the GDPR defines the responsibilities of the DPO, and gives the conditions under which an organisation is legally obliged to appoint a DPO.

Article 37 states: “The controller and the processor shall designate a data protection officer in any case where:
(a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
(b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
(c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.”

**Data protection by design and by default**
Privacy by design is a concept which requires that data protection be considered at the start of the lifecycle of any project, and that it be a consideration throughout the lifecycle (in the same way that safety or security are currently considered in a through-life manner for many projects). Privacy by default requires that systems are designed and configured to be inherently secure, by applying the strictest privacy settings at all times and allowing the least necessary access and functionality for each process and user. These principles are not new. They were previously however a legal requirement under DPA. Under GDPR they must be explicitly considered for all projects. Again this may require organisations to update processes...
and procedures, and make changes to the supporting measures they already have in place.

**GDPR and Risk**

GDPR talks extensively of risk in the context of the “risk to the rights and freedoms of natural persons” and the “risks inherent in that processing”. It broadly advocates a risk driven approach to the data protection processes adopted by an organisation, and clearly states that the technical and organisational measures put in place by an organisation to implement data protection policies be selected on the basis of risk.

From this it is clear is that an appropriate and proportionate process for assessing risk in terms of the risk to the data subjects, and a process to govern how technical and organisational measures are selected, needs to be adopted.

GDPR stops short however of defining a suitable risk based approach, or recommending a risk assessment technique to use in support of this.

It is expected that guidance will be developed in support of this requirement, but currently organisations must choose their own approach to assessing and managing the risks posed by the processing of personal data.

Most organisations will have corporate risk based processes in place and will maintain a corporate risk register. Similarly most organisations will have some form of information security infrastructure in place, and some will have a risk driven management process underlying this security infrastructure.

These existing processes will need to be extended or supplemented accordingly to bring data protection into the risk management activities of the organisation. In the absence of current guidance each organisation will have to decide for themselves how they will achieve this, which standards they may or may not decide to adopt and adhere to in support of this, and the scale of any process that they put in place.

As a further burden to organisations already being required to update their internal data processing framework, the requirement to comply with the principle of accountability will require an organisation to be able to demonstrate how they comply with these requirements. This process will require them to document the process that they are using, and ensure that all relevant risk assessments and organisational and technical measures put in place in accordance with that assessment be documented and stored in a clear and accessible manner.

**DATA PROTECTION IMPACT ASSESSMENTS (DPIA)**

GDPR requires that a Data Protection Impact Assessment (DPIA) be undertaken for any process that will result in a high risk to the data subjects.

Article 35 discusses more details concerning the required Data Protection Impact Assessment.
In Summary

The above discussions look at some of the key areas within the pages of GDPR, but are in no way an exhaustive critique of the Regulation. What is clear from this initial look at the Regulation is that many organisations will have quite a lot to do to get ready for GDPR (some more than others). There are a number of major areas of change which will potentially impact organisations processing personal data belonging to EU data subjects. How it will impact these organisations will vary depending on many factors such as the level of maturity of that organisation, where they operate, how much data they process, what data processes they carry out, and what the risks to the data subjects whose data they process are.

The GDPR itself is an extensive regulation with over 250 pages to be digested by organisations, and this in itself will take time and resource. Understanding what compliance means for a specific organisation will further add to this burden.

Each organisation will need to undertake a GDPR impact assessment in order to determine what they need to do in order to comply7 with the new GDPR. They will need to identify where new or updated measures (both technical and organisational) need to be put in place, and address the issue of risk and how they will identify and adequately mitigate any identified risks to their data subjects.

All this needs to be done to enable the organisation to then plan and implement changes in time to meet the 25th May 2018 deadline. For many organisations this may prove to be both time consuming and costly. The cost of not complying however may be far greater.

Detailed guidance and advice to support organisations in their understanding and application of GDPR is sparse but under development. There are a number of areas where clarification on the intent of the law contained within GDPR is needed. Advice is gradually being developed, but some interpretations of GDPR may well only be proven through case law.

With less than a year to go until GDPR is enforced organisations do not have the luxury of waiting until this detailed guidance and understanding is available. Organisations must act now.

Current advice and information (including a copy of the GDPR) can be found at the below two websites. Both are excellent starting points for anyone embarking upon their GDPR journey.

- The EUGDPR website: www.eugdpr.org
- The Information Commissioners Office (ICO) Website: https://ico.org.uk/for-organisations/data-protection-reform/

Further advice and support can be obtained from: www.thalesgroup.com/en/tcc-uk

Assessment, but again the details are currently lacking. The Article 29 Data Protection Working Party has recently issued some draft guidance and advice concerning DPIAs. This is not binding nor endorsed by the EU, but will provide some additional information to organisations looking to implement a DPIA in the short term.

As a word of caution, since the regulation itself is legally binding organisations will additionally need to seek independent legal advice in support of their compliance activities.

7As a word of caution, since the regulation itself is legally binding organisations will additionally need to seek independent legal advice in support of their compliance activities.