Briefing: new requirements to optimise the use of personal data in new and changing business processes, and technology investments whilst complying with the new EU Data Protection regulation.

September 2016
Introduction

This Governance Guide is intended to provide an overview of the new EU General Data Protection Regulation (GDPR) which DMGT plc and its subsidiary companies will need to comply with from 25 May 2018, regardless of Brexit. This new regulation requires personal data protection to be built in upfront, ‘Privacy by Design’ and maintained throughout the data lifecycle, ‘Privacy by Default’.

This guidance is for Executive decision makers, operating company MDs, product managers, technology leads and project leads. The guidance summarises the key considerations required to help optimise and protect the use of personal data as part of investment sign-off for new or changing business processes, systems and technology investments.
**Summary of GDPR implications**
GDPR will come into force on 25 May 2018. Personal data processing infringements will face fines of the higher of 4% total worldwide turnover of the preceding financial year or €20 million. The appendix provides a high level summary of the key considerations.

**Governance Approach to GDPR compliance**
To coordinate GDPR compliance, a GDPR Working Group has been set up, reporting quarterly progress updates to the DMGT Risk Committee. This working group is chaired by Claire Chapman with each operating business represented by legal and/or Data Protection Officer (DPO) resources.

The focus in calendar 2016 is on assessing the risk across the Group, identifying the gaps, planning and raising awareness. It is proposed that implementation and investment is phased across the Group from April 2017.

Each operating business will develop, implement and monitor their own implementation plan, with support and resources provided from DMGT as required.

Data Privacy Standards and a toolkit will be created to support Group-wide compliance, with updates to Data Protection Governance Guides & updates to DMGT Essentials as required.

For investments in processes, systems, technology and projects involving the use of personal data, it is imperative that business decision makers factor the GDPR requirements into their change plans with immediate effect to minimise further unnecessary additional investment at a later date.

This includes off the shelf solutions and platforms e.g. Software as a Service (SaaS) provided by third parties. We should verify through contracts and practical application that GDPR requirements are adequately addressed.
GDPR and Privacy by Design & Default: Definitions

Privacy by Design
Privacy by design means that each new service or business process that makes use of personal data must take the protection of such data into consideration. An organisation needs to be able to show that they have adequate security in place and that compliance is monitored. In practice this means that an IT department must take privacy into account during the whole life cycle of the system or process development.

Privacy by Default
Privacy by Default means that the strictest privacy settings automatically apply at the point of collecting an individual’s personal data. In other words, no manual change to the privacy settings should be required on the part of the user. There is also a temporal element to this principle, as personal information must by default only be kept for the amount of time necessary to provide the product or service.

Benefits
Good data governance is one of the cornerstones of a successful information business. Designing projects, processes, products or systems with privacy in mind can lead to the following benefits:

- Potential problems are identified at an early stage.
- Addressing problems early will often be simpler and less costly.
- Increased awareness of privacy and data protection across the organisation.
- Organisations will be less likely to breach the regulation and incur fines.
- Actions are less likely to be privacy intrusive and have a negative impact on individuals.
- Can be used as a marketing differentiator and build trust with employees, customers and other key stakeholders.
GDPR and Privacy by Design & Default: Principles

GDPR requirements are not too dissimilar to existing data protection legislation, but do require more evidence of decision making with regards to the protection of personal data, with more significant consequences in the event of a personal data incident/breach.

### GDPR Principles

<table>
<thead>
<tr>
<th>Principle</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Transparency</strong></td>
<td>Tell individuals the specific and lawful purposes for which their data will be processed.</td>
</tr>
<tr>
<td><strong>Data minimisation, Purpose Limitation &amp; Storage Limitation</strong></td>
<td>Only request and retain the data specifically required and do not retain data for longer than necessary.</td>
</tr>
<tr>
<td><strong>Security &amp; Data transfers</strong></td>
<td>Ensuring personal data is held securely. Do not transfer (UK &amp; EU) data to non-EU &amp; non-UK territories unless additional steps are taken to protect data.</td>
</tr>
<tr>
<td><strong>Accuracy</strong></td>
<td>Where necessary, ensuring personal data is accurate and up to date.</td>
</tr>
<tr>
<td><strong>Accountability</strong></td>
<td>The Data Controller must demonstrate steps taken to comply with the regulation through policies and procedures.</td>
</tr>
<tr>
<td><strong>Individual Rights</strong></td>
<td>These include: an individual’s right to access their personal information, the “right to be forgotten” and “data portability”, see overleaf for further information.</td>
</tr>
</tbody>
</table>
The GDPR creates some new rights for individuals and strengthens some of the rights that currently exist. These rights need to be clearly articulated.

The GDPR provides the following rights for individuals:

<table>
<thead>
<tr>
<th>Right</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The right to be informed</td>
<td>which will typically be achieved through privacy notices. This must be at no cost to the individual, in concise, transparent, accessible language; why, how and what personal data is processed and supplementary information on the consent, withdrawal and complaints processes etc.</td>
</tr>
<tr>
<td>The right of access</td>
<td>to provide individuals for free, upon request, within 1 month; their personal data that is being processed and reasons why and supplementary information typically available in a privacy notice.</td>
</tr>
<tr>
<td>The right to rectification</td>
<td>includes entitlement of individuals to have us rectify inaccurate/incomplete data within 1 month (including at third parties where we have disclosed the data), and to explain their right to complain and how.</td>
</tr>
<tr>
<td>The right to erasure</td>
<td>is not an absolute ‘right to be forgotten’, but right to have personal data erased or prevent further processing if; no longer necessary for the original purpose; individual objects or withdraws consent; processing is unlawful; or to comply with law.</td>
</tr>
</tbody>
</table>
The GDPR provides the following rights for individuals (continued):

<table>
<thead>
<tr>
<th>Rights in relation to automated decision making and profiling</th>
<th>allows individuals to obtain and reuse, for free, within 1 month, in a machine readable format, their personal data and move, copy or transfer it from one IT environment to another safely and securely.</th>
</tr>
</thead>
<tbody>
<tr>
<td>The right to object</td>
<td>to direct marketing, processing for scientific/historical research and statistics or legitimate interests or tasks in the public interest/official authority, including profiling; excluding processing affecting legal claims.</td>
</tr>
<tr>
<td>The right to data portability</td>
<td>are to protect individuals from damaging decisions taken without human intervention. Automated processing and profiling must be fair and transparent, with appropriate procedures and security. This does not apply if explicit consent is gained; to perform a contract or is authorised by law.</td>
</tr>
</tbody>
</table>

This is a high level summary and there are many exceptions and specifics to take into account. Your General Counsel and/or Data Protection Officer (DPO) can support you with understanding the appropriate approach to take.
GDPR and Privacy by Design & Default

Does it apply to my business?

Consider the following statements about your organisation:

• Company is registered in an EU Member State
• Company’s subsidiary registered in an EU Member State
• Company maintains a branch in an EU Member State
• Company conducts sustained activity in an EU Member State

If any of the above statements are TRUE GDPR applies to your business.

If none of the opposite statements are applicable, then also consider the following:

• Company offers goods or services to EU data subjects (individuals resident in the EU or EU citizens resident in other territories)
• Company maintains a website with an EU Member State domain name (e.g. “.co.uk”)
• Company offers goods or services in local currency of EU Member State
• Company references EU Member State on website and provides local contact details
• Company uses EU Member state language and customers can place orders in that language
• Company monitors the behaviours of individuals within an EU Member State

If any of the above statements are TRUE GDPR applies to your business.

Note: Although the consequences of Brexit are not yet clear, the UK regulator, Information Commissioner’s Office (ICO), has confirmed that it plans to adopt equivalent to the EU GDPR, for UK and EU data subjects, as the recognised standard of good practice personal data protection.
If GDPR applies to my business, does it apply to my investment?

If personal data is being collected, processed or analysed (profiling), then GDPR applies.

Note: under GDPR, personal data also includes online identifiers such as work email addresses, direct dial work numbers as well as potentially IP addresses and anonymised data that combined could identify an individual.

The next step is to undertake a Privacy Impact Assessment (PIA), which is an integral part of taking a privacy by design approach.

A PIA should be carried out whenever a business plans to:

- Embark on a new project involving the use of personal data;
- Introduce new or upgrade IT systems for storing and accessing personal information;
- Participate in a new data-sharing initiative with other organisations;
- Initiate actions based on a policy of identifying particular demographics;
- Use existing data for a “new and unexpected or more intrusive purpose”.

Note that where a PIA indicates high risk data processing, you will be required to consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.
GDPR and Privacy by Design & Default

What do I need to incorporate when using personal data in new or changing business processes, systems and technology?

**Categorise**
Document and categorise the information you hold and who you share it with.

** Communicate**
Review existing privacy notices and make changes as necessary.

**Privacy by design**
Embed privacy controls into all new projects, processes and systems.

**DPO**
Designate a Data Protection Officer to take responsibility for data protection compliance within your business.

**Consent**
Ensure active positive consent is obtained from the data subject. Explicit consent must be obtained for “special”/“sensitive” categories of data.

**PIA**
Perform a Privacy Impact Assessment (PIA) to identify and minimise privacy risks.

**Procedures**
Ensure you have the right procedures to handle:
- Data Breaches
- Subject access requests
- Children’s data

**Suppliers**
Contact suppliers and verify that any third party processors and controllers are complying with GDPR. Enhanced data security clauses may be required.

**Define**
For each data set held, define whether you are the data controller or data processor.
GDPR and Privacy by Design & Default

What questions should I ask when undertaking a PIA? (1)

- HR Data
- Customer Data
- Supplier Data
- Other

For each suggested category of data above, undertake a risk assessment, by documenting:

**What information is/will be held?**

**Is any of the data held considered “sensitive/“special”?**
(e.g. racial or ethnic origin, political opinion, religious beliefs, trade union membership, physical or mental health, sexual orientation)

**Source of data & demonstration/record of consent?**

**Purpose of holding/processing data?**

**IT Systems or applications used to hold or process data?**
(including form of encryption where applicable)

**Who personal data is shared with?**
(including other DMGT Group companies, third parties, service providers, credit agencies, law enforcement)
GDPR and Privacy by Design & Default

What questions should I ask when undertaking a PIA? (2)

HR Data  Customer Data  Supplier Data  Other

For each suggested category of data above, undertake a risk assessment, by documenting:

- Retention period for data?
- How and what notices about their data was provided to data subject? (e.g. privacy policy, cookie notices, contract clause)
- Any automated profiling used?
- How can a data subject exercise their rights?
- What are the risks to individuals of a data breach associated with this activity?

Complete the privacy impact assessment data questionnaire which covers the key questions above, working with your business’ DPO, General Counsel or equivalent, with support from DMGT GRC (Claire Chapman, Fran Tangye as required) to put in place the appropriate safeguards and mitigations.
Summary of key regulatory requirements

The key agreed outputs of the GDPR are summarised below for context and information:

- This is not guidance, but enforceable EU Regulation i.e. applies to all relevant personal data including online identifiers.
- Applies to all personal data processing activities of DMGT companies where "established" in the EU, offers goods and services in the EU, or monitors behaviour of individuals within the EU (EU includes UK despite Brexit).
- Regulation will come into force 25 May 2018 and was published 5 May 2016, with a 2 year transitional period.
- Failures to comply with the GDPR may lead to fines up to higher of €20m or 4% total worldwide annual turnover of the preceding financial year.
- Requirement to notify regulators within 72 hours of becoming aware of a personal data breach, requires an accelerated internal escalation process.
- At any time, be able to provide an overview of increased accountability requirements e.g. that appropriate technical and organisational measures are in place for personal data processing.
Appendix

Summary of key regulatory requirements
The key priorities for phase 1 (to April 2017) and 2 (to 25 May 2018) implementation activities to meet GDPR compliance are summarised below for context and information:

Priority 1

- **Formal consent must be freely given, specific, informed, unambiguous for each different processing operation (verifiable parental consent required to process personal data of children)**
- **Privacy by design and default: these new privacy requirements to be built into our businesses’ operations upfront**
- **Discussions regarding how/when Privacy Shield may replace Safe Harbour are continuing. Appropriate contractual processes will be used in the meantime**
- **Privacy Impact Assessments are required, where there is a high risk for the rights and freedoms of individuals**

Priority 2

- **Data subjects can request, for free, information on our data processing of them and a machine readable copy of their personal data**
- **A process for removal of consent from individuals must form part of the data processing approach ‘right to be forgotten’**
- **Data Protection Officers (DPOs) will be required at each Operating Company (dmgi, dmge, dmg media, RMS, EII), flexing resources to match risk**
Contact Details
If you would like any further information about any of the above, please contact:

Fran Tangye
Head of Risk, DMGT
fran.tangye@dmgt.com
T: +44 (0)20 3615 0542
M: +44 (0)7775 544695

Claire Chapman
General Counsel & Company Secretary, DMGT
claire.chapman@dmgt.com
T: +44 (0)20 3615 2653
M: +44 (0)7786 474104