The GDPR: The "whole of business" issue at the top of your board agenda

Data has evolved in our digital economy to become the **lifeblood of global trade**. It affects all businesses and industries and dealing with it is a "**whole of business**" issue, affecting each and every team within an organisation.

With innovation, comes regulation and Europe is on the cusp of overhauling its data protection laws. Despite the outcome of last year's Brexit referendum, at least one constant remains – from 25 May 2018 organisations established in or providing goods or services to data subjects in the EU (including the UK) will need to comply with the enhanced regime under the EU General Data Protection Regulation (the "**GDPR**").

Please click here to subscribe to our'Practical GDPR series'.

Described by the UK Information Commissioner as a "**game changer for everyone**", it follows that GDPR compliance does not have just one natural owner. It is a business-wide effort that requires a cross-functional task force. A successful GDPR implementation programme is therefore not simply a static strategy in the domain of a legal or compliance team - it is an evolving exercise and requires engagement from a range of other business functions across an organisation such as IT, cyber security, HR and procurement, to name but a few.

Oversight and buy-in from senior executives will also be fundamental to cement any such programme in the fabric of an organisation and its overall strategy – and ultimately seek to avoid the potentially far reaching consequences that non-compliance may bring.

Herbert Smith Freehills launches multi-disciplinary practical GDPR series

Following our previous articles on the GDPR, Herbert Smith Freehills' multi-disciplinary Data Protection, Privacy and Cyber Security teams are here to help you successfully navigate the GDPR (and related UK legislation such as the Data Protection Bill) in the run up to 25 May 2018 and beyond, with our series of **cross-practice cross-border briefings and webinars catering for the "whole of business"**. Each briefing and webinar will be written with a particular key business function or functions in mind - placing the spotlight on what we are seeing and hearing in the market alongside our practical experience of dealing with the challenges of compliance from the perspective of assisting clients with implementation.

In this first briefing in the series we take a high level look at the anatomy of a GDPR compliance programme, breaking down the task into more digestible pieces. Subsequent briefings and webinars in the series will take a deeper dive into some of the key considerations in any compliance programme including:

- The rise of the intelligent employer and demystifying consent
- Supply Chain Arrangements: the ABC to GDPR compliance
- The nexus between data protection and cyber security

Please click **here** to subscribe to our forthcoming briefing and webinar series.

Business Impact Summary

The regime of increased sanctions under the GDPR has no doubt been the major catalyst in forcing organisations to focus on data protection risk management and reflects just how important personal data is in our digital economy. It is also a primary reason that data protection and cyber security have been elevated to board level issues in the last twelve to eighteen months. With maximum fines of up to €20 million (£17 million) or 4% of annual worldwide turnover (whichever is greater) for certain breaches, the current monetary penalties of up to £500,000 under the existing regime pale into insignificance. Despite this huge increase in maximum possible fines businesses can take some comfort from the Information Commissioner's Office (the "**ICO**") indicating that issuing fines will continue to be used as a last resort and top level fines will not become the norm, in line with current practice.

Whilst the enhanced compliance requirements under the GDPR are likely to be seen by some as simply codifying existing best practice, for many organisations this is a significant step up in terms of focusing on data privacy. When coupled with the increased sanctions regime, these requirements now give rise to a very different risk assessment for organisations. That is without taking into account the equally significant sting that reputational damage can bring if an organisation gets it wrong.

The GDPR also has a far wider reach when compared to the existing EU Directive. With its "extra-territorial scope", the regulation will extend to organisations located outside the EU that offer goods and services to data subjects residing in the EU or that monitor their behaviour. This could lead to a relatively steep learning curve for non-EU based organisations that are not currently familiar with the standards of a European data protection regime, as well as cries for ways to avoid being caught by the regime accidentally when providing services globally (there is some guidance on this).

All of these factors, coupled with less than nine months remaining for organisations to get their houses in order, mean that organisations should be looking carefully at their existing arrangements and the underlying systems and controls they have in place - as well as considering both their technology selection and process readiness for the GDPR.

The anatomy of a GDPR compliance programme

There is no one-size fits-all GDPR compliance programme. The extent of preparation required will depend on a number of areas, including:

- how established an organisation already is in respect of data protection and its compliance with the current data protection framework;
- whether an organisation is a processor, a controller or both;
- the nature of and extent to which personal data is processed, how and why it is processed and how much of it should be regarded as sensitive;
- how complex its data processing activities are (eg the nature of its supply chain and whether personal data is transferred outside the EEA); and
- the policies, procedures and controls that are currently in place.

Therefore whilst an organisation's data protection practices and GDPR compliance programme will require individual consideration (as will the supporting IT functionality and operational requirements), we set out below some bite-sized next steps for organisations to consider as a starting point to help make the task more manageable. We are able to provide you with more in depth practical guidance on the key considerations and questions set out in this briefing.

1. The starting point

Clearly it is important to lay the ground work for a compliance framework as early as possible – this is even more important given the emphasis on (i) "privacy by design" and "security by design" under the GDPR (ie promoting privacy and data protection compliance from the start of any project, rather than as an after-thought) and (ii) demonstrating compliance, risk assessment and record keeping under the new "accountability principle" (which makes controllers expressly responsible for demonstrating that they comply with the data protection principles).

Identify whether the GDPR applies

- Organisations without a presence in the EU that target or monitor data subjects residing in the EU ought to consider the extent to which the GDPR may apply to them and determine an approach to compliance. An organisation no longer needs to have an establishment in the EU to be caught by the regime.

Executive buy-in/raise awareness

- Earmark key executive stakeholders to support the roll-out of any GDPR compliance programme and raise awareness of the implications for the organisation – the new sanctions regime will also assist in doing this!

Governance, resources and budget allocation

- Consider a governance structure which fosters a culture of privacy and security from the top down and the oversight required to support all stages of any compliance programme.
- Designate appropriate responsibility, resources and related finance for GDPR compliance. This could include investing in any new technologies and team restructuring requirements, as well as making changes to reporting lines as board level reporting is now expected. A cross-functional task force is likely to be useful too. Also consider data protection and security requirements when rolling out any new IT systems.
- Is a Data Protection Officer ("**DPO**") required or desirable? If so, consider whether the role can be fulfilled internally or whether external recruitment or engagement is more appropriate, there may be a number of factors to consider.

Regular guidance updates

- Keep abreast of the latest guidance on the GDPR (including from supervisory authorities (such as the ICO in the UK), the Article 29 Working Party, any industry wide standards, terms or formats) and be prepared to adjust your compliance programme or operational processes accordingly. Further guidance on key topics is still expected in the run up to the May deadline.

Cross border processing

- If an organisation conducts cross-border data processing activities through multiple establishments across the EU then confirm the location of the "main establishment" and who the lead supervisory authority is in respect of cross border processing will need to be confirmed.
- Whilst the GDPR is intended to harmonise the privacy and data protection legislation across the EU, there are a number of "derogations" which allow (and in some instances require) Member States to make local laws. Keep a look out for these local laws which may make harmonisation of your data privacy policies and procedures in all EU Member States challenging. We set out some examples of these variations/derogations in other EU Member States at the end of this briefing.
- Consider also the impact of Brexit (including on the practical geographical aspects of data protection compliance, eg the location of any DPO - What happens if the "main establishment" is in the UK post-Brexit?).

> "A successful GDPR implementation programme is not simply a static strategy in the domain of a legal or compliance team"

2. Fact finding

Identify how your organisation processes data now (what data do you process, where does it go, why do you process it?) to identify what changes you need to make in order to be compliant under GDPR. This may well be time consuming, but is an important step. In particular:

- Understand what personal data (including sensitive personal data) you hold, how data flows around the business (including any international transfers or transfers to third parties), what processing activities are conducted in respect of that data and for how long the data is retained.
- Understand the compliance measures already in place and consider whether these are still appropriate under the new GDPR regime (for example, the basis on which the organisation is currently lawfully processing personal data).
- Conduct an audit of the technology and systems that currently collect, store, process and use personal data (this may, for example, include legacy or cloud related systems) and the extent to which these are currently relied upon to support compliance, including in respect of data security. This should include any customer and employee facing tools or processes to assist with data subject requests.
- Use the results of this fact finding stage to prepare a data flow map for your organisation.

3. Analyse and review

Consider where the organisation currently sits in terms of its compliance, where it needs to get to and then conduct a gap analysis to help determine the most appropriate steps to take. Depending on an organisation's resource and finance constraints, in the lead up to 25 May 2018 it may be necessary to use a "business lens" to prioritise immediate areas to be rectified based on proportionality and risk, documenting all decisions taken. In particular, it may be worth conducting a data privacy impact assessment ("**DPIA**") to identify particular high risk areas and help prioritise actions to take. Some key areas to consider include:

Fair processing notices and consent

- Determine the basis for processing personal data (for example, consent, legitimate interest, compliance with law or to perform a contract) and document that basis (as explained above, record keeping will be key with the new focus on accountability). We will discuss this further in our next briefing, including the new requirements for consent which are likely to make it a less useful basis to rely on for processing employee personal data or personal data relating to pension funds in particular.
- Consider whether consent is the most appropriate option for those processing activities that are currently being conducted on the basis of consent. If so, ensure existing consents meet the new (higher) thresholds ie freely given, specific, informed and unambiguous (bearing in mind consent can be withdrawn and that data subjects need to be explicitly informed of this). If the new thresholds are not met, obtain new consents to ensure they meet the requirements going forward or consider alternatives.
- Ensure simple and efficient processes are in place to enable withdrawals of consent and the reliable recording of consents.
- Update/create appropriate policies and procedures accordingly (eg a privacy policy which contains the information required under the GDPR, updating employment contracts/customer contracts with people (as opposed to corporates) going forward, checking employee monitoring policies are fit for purpose – further guidance on this has recently been issued).
- Determine for how long data should lawfully be retained by the organisation (this will need to be included in the privacy policy).

Supply chain contractual arrangements/intra-group arrangements

- Determine which are your key / high risk contracts (particularly those where there is a large amount of personal data being transferred) and then review:
  - the relevant terms to determine where the organisation's liability currently sits (particularly bearing in mind the greater statutory exposure for both controllers and processors under the GDPR); and
  - what additional provisions may need to be included in the contracts (eg appropriate data security compliance provisions, both before-the-event as well as upon a breach occurring).
- This will help determine whether you need to renegotiate agreements and the scale and scope of any re-papering exercise, such as revisiting liability limits given the increased accountability of data processors under the GDPR.

Security and Data Breaches

- Conduct an assessment of the different types of risk to which your data is subject, and document the risk assessment.
- Analyse existing security measures in light of the increased emphasis on security under the GDPR and the risk assessment conducted.
- Collaborate with IT and security teams to determine the most appropriate technical and organisational measures to protect your data.
- Ensure good practice is followed so that data is unintelligible in the case of unauthorised access or removal (such as "salting and hashing" data).
- Prepare and/or update appropriate IT security, disaster recovery and resilience policies and procedures and ensure that these are reviewed and regularly tested.
- Implement appropriate incident response policies and procedures to enable compliance with the new mandatory breach notification requirements and to effectively manage a major data breach. Consider the extent to which these fit with notification requirements under other overlapping regulatory regimes, and other types of cyber risk.
- Test out your incident response plans to identify any gaps.

- Consider the extent to which a DPIA needs to be conducted for any in-flight projects continuing beyond May 2018 or any new projects, products or services going forward that will begin after that date.
- Check that you have in place an appropriate basis for transferring personal data outside the EEA ie model clauses in place, binding corporate rules (or in the United States that the relevant party has signed up to the US-EU Data Privacy Shield) – whilst this will not change under the GDPR, data subjects will need to be told of the basis for processing, so this should be clear from the outset.
- Consider whether additional investment is required in alternative or enhanced products or tools to comply with the GDPR requirements (particularly in light of the greater need for record keeping and the new or enhanced rights of data subjects that may apply (eg changes to data subject access request requirements (including new time frames), data portability, the right to stop processing data and the right to be forgotten). Data subject access portals may be appropriate to allow individuals to exercise their rights directly in certain circumstances.
- Consider whether you carry out any activities based on automated processing or profiling and if so, consider whether this is lawful as there are new restrictions on profiling.
- Review the organisation's existing insurance policies to assess cover for breach of certain requirements under the GDPR (and cyber security more generally) and consider addressing any gaps in coverage.

> "GDPR compliance does not have just one natural owner"

4. Implementation/ongoing monitoring

Governance and effective internal policies, processes and procedures incorporating the output from stages 1, 2 and 3 above, will be key to successfully implementing any compliance programme.

Governance

- Update and implement appropriate internal data protection policies, codes of practice or incident response plans addressing the key requirements under the regulation. Ensure compliance on a continuing basis in case of future changes, particularly changes in the way in which an organisation uses personal data, or changes to the cyber security risk profile which might require enhancement of the technical and organisational measures in place to protect data.
- In particular, ensure that any policies and procedures for customer facing teams are updated and sufficient in light of the new and enhanced data subject rights that may apply. Consider preparing template request or response letters to deal with these data subject requests.
- Devise and document processes for periodically reviewing and evaluating the effectiveness of data protection policies, codes of practice or incident response plans once implemented (eg through spot checks or audits to monitor compliance).

Training/raise awareness

- Consider training and awareness programmes for all members of the organisation to ensure the compliance regime is adequately implemented into the day-to-day running of the business. For example, ensure employees receive training on new policies, procedures and when to report data breaches.
- It may also be a useful opportunity to remind employees that unlawful processing of personal data can give rise to liability for them (eg if they take personal data with them when they leave employment without their employer's consent this could be a criminal offence).

European Derogations

While the GDPR will go some way to harmonise the inconsistent data protection directive-based legislation that is currently in place across Europe, it has become apparent that Member States are adopting different approaches to one another when implementing the new regulation at a national level. A contributing factor is Article 23 of the GDPR, which enables Member States to introduce derogations to the GDPR in certain situations. As a result, if an organisation needs to implement a GDPR compliance programme across more than one Member State, it will be necessary to consider whether there are any jurisdiction-specific requirements with which it needs to comply.

By way of example, we set out below an overview of how the GDPR will be implemented in France, Germany and Spain:

France

- The **Digital Republic Bill** will be adopted as the national implementing legislation by the end of 2017. Following the implementation of the legislation:
  - Organisations will need to comply with specific doctrines issued by the National Commission on Informatics and Liberties ("**CNIL**") on certain issues such as whistleblowing, employee screening, biometrics, geo-localisation, security standards and cookies
  - Organisations will need to comply with GDPR guidelines issued by the CNIL concerning issues such as prior consent, security breaches and profiling
  - Organisations will be able to use the CNIL online "toolbox" as the basis for their GDPR compliance programme, and access "ready-to-use" template documents prepared by the CNIL (for example Privacy Impact Assessments and model contracts)
  - The CNIL will gain greater investigatory powers and will prioritise investigating data security issues

Spain

- The **Organic Law on Data Protection** will be adopted as the national implementing legislation. The current draft of the legislation suggests:
  - The GDPR sanctions regime will include additional rules in relation to the implementation of sanctions
  - The definition and scope of the "one-stop shop" principle will be amended
  - DPOs will have additional reporting obligations

Germany

- The **German Federal Data Protection Amendment Act** will be adopted as the national implementing legislation (an English version is available here). It is worth noting the rules under this piece of legislation deviate from the position under the GDPR as follows:
  - Data subject rights will be limited to a greater extent than they are under the GDPR (although these provisions may still be revised by the European Court of Justice)
  - The processing of employee personal data will be permitted in a wider number of circumstances than is permitted under the GDPR
  - Organisations will be required to appoint a DPO in a greater number of circumstances than under the GDPR
  - There are special rules concerning video surveillance of publicly accessible areas and more onerous obligations are placed on a data controller acting in this context
  - There will be enhanced rules in relation to electronic marketing

Is your organisation GDPR ready?

The Information Commissioner has issued a timely warning:

"If your organisation can't demonstrate that good data protection is a cornerstone of your business policy and practices, you're leaving your organisation open to enforcement action that can damage both public reputation and bank balance. But there's a carrot here as well as a stick: get data protection right, and you can see a real business benefit."

Whilst the stakes and financial risk exposure are higher under the GDPR when compared to the existing regime, the key to GDPR compliance is not just in satisfying a check list of requirements, but requires a "whole of business" effort to change an organisation's attitude and operational approach to compliance, as well as the way in which compliance filters through an organisation. This is embedded in the "accountability principle" which is one of the golden threads that runs through the various provisions of the GDPR, representing a change in mind-set towards data protection that can help organisations future proof their businesses going forward. Another is "transparency" – ensuring data subjects are aware of how the organisation is processing their personal data and why.

As well as the challenges that the GDPR brings, a well-run GDPR programme also brings with it opportunities beyond simply achieving compliance. It goes without saying that it can build customer confidence and improve customer relationships, data controls and internal data handling. But it is also an opportunity to consider a broader data transformation that will benefit a whole business - streamlining existing data management platforms to add value and lower cost as well as bringing greater flexibility to be able to respond more readily to any future regulatory changes.

With the clock continuing to count down, one thing is for sure: the run up to May 2018 is set to be an incredibly busy period for many organisations, with preparations for the full trio of data protection, cyber security and e-privacy regime compliance.[1]

The remainder of this **"Practical GDPR series"** will help you deep dive into the detail around some of these key requirements. We are also very happy to discuss GPDR implementation, directly with you. We are working with clients on implementation projects right now.

1. The Network and Information Security Directive is due to be implemented and apply to certain "operators of essential services" and "digital service providers" from May 2018. The ePrivacy Regulation (which focuses on the processing of personal data and protection of privacy in electronic communications) is currently scheduled to replace the existing European e-privacy framework from 25 May 2018 as well to align with the GDPR.