GDPR Briefing Note Update & Transition Checklist

January 2016

GDPR had successfully had its second reading in Brussels earlier this month and the legislation was passed. It runs to 209 pages and is roughly three times the length of the UK Data Protection Act 1998. This document provides an update of our latest notes following a long read through over the Christmas break, some additional reading and updates from our advisors.

1. New European data legislation in two parts
    a. The Data Protection Directive for the police and criminal justice sector will ensure that the data of victims, witnesses, and suspects of crimes, are duly protected in the context of a criminal investigation or a law enforcement action. At the same time more harmonised laws will also facilitate cross-border co-operation of police or prosecutors to combat crime and terrorism more effectively across Europe.
    b. The EU General Data Protection Regulation (GDPR) is designed to enable EU citizens and those within the EU to better control their personal data. This principles based EU Regulation is binding on all 28 Member States and creates the legal framework necessary for the Digital Single Market by removing confusing and contradictory laws and regulations and by harmonizing the market by creating a level playing field for the sales of goods and services within the EU.

"EU General Data Protection Regulation is a fundamental agreement with important consequences. This reform not only strengthens the rights of citizens, but also adapts the rules to the digital age for companies, whilst reducing the administrative burden. These are ambitious and forward-looking texts."
Félix Braz, Luxembourg Minister of Justice and President of the Council

    i. It's a massive 'game changer' for companies and the clock is now ticking
    ii. It imposes a raft of NEW duties and responsibilities on companies with punitive penalties of €20m or 4% global turnover
    iii. Companies have to change to resource up and acquire knowledge and skills through training in order to protect business continuity.

2. A recent survey by Computer Weekly (Jan 2016):
    a. More than half of European companies don't know about the legislation planned to unify data protection laws across the EU
    b. Only half of UK IT decision-makers are aware of GDPR, compared with 87% in Germany
    c. The vast majority of cloud providers aren't prepared to meet the requirements of the GDPR.

"It would be a huge mistake to ignore GDPR until it becomes enforceable in 2018."
Eduardo Ustaran, European Head Data Protection Hogan Lovells

"This will impact every entity that holds or uses European personal data both inside and outside of Europe."
Stewart Room, Data Protection Partner, PwC data

"The GDPR looks to adopt prescriptive rules around how organisations will need to demonstrate that they comply with the GDPR. Businesses will have to genuinely adopt governance and accountability standards and not pay lip service to data privacy obligations otherwise they could be in for a surprise as the stiff new fines will apply to that requirement too."
Vinod Bange, Partner, Taylor Wessing

3. Two years of transition
    a. The first line of defence will be adequate training and education for everyone in the organisation – this is a legal requirement under GDPR
    b. Given that many large organisations need to make budgetary commitments to implement the GDPR in the year before commencement in 2018 (i.e. in the FY 2017/2018 at the latest), you should expect pressure on the Information Commissioner's Office to have detailed GDPR guidance completed by the end of this year.
    c. Knowing how much – or how little – effort will need to be devoted to getting this right will be a considerable task in itself, which is why executive education and training is going to be vital.
    d. The new compliance journey will require Data Controllers to:
        i. Map and classify all their personal data
        ii. Perform Data Protection Impact Assessments (DPIA)
        iii. Design privacy protection policies into all new business operations and practices (inc customer contact centre)
        iv. Employ dedicated Data Protection Officers (DPO's) with appropriate resources to carry out the job
        v. Monitor and audit compliance
        vi. Document everything they do with personal data in order to achieve legal compliance
        vii. Ensure that the workforce handling personal data is adequately trained under the requirements of GDPR.
    e. The new transparency framework will require Data Controllers to:
        i. Rewire how they engage with customers and prospects, including their contractual and permissions protocols.
        ii. How clear and full information of what happens to personal data is communicated.
        iii. Report incident of Data breach incident to the Data Protection Authority (Supervisory Authority) within 72 hours of becoming known and in serious cases having to inform the Data Subject too.
    f. New enforcement, sanctions and remedies framework:
        i. Intervention in business operations
        ii. Heavy fines

4. Need for a new mind set – key principles of GDPR
    a. Personal data
        i. Defined in both the Data Protection Directive and the GDPR as any information relating to an person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.
        ii. So in many cases online identifiers including IP address, cookies and so forth will now be regarded as personal data if they can be (or are capable of being) without undue effort linked back to the data subject.
        iii. To be clear there is no distinction between personal data about individuals in their private, public or work roles – the person is the person.
    b. Data Controllers and Data Processors
        i. The GDPR separates responsibilities and duties of Data Controllers and Data Processors, obligating Data Controllers to engage only those Data Processors that provide "sufficient

guarantees to implement appropriate technical and organisational measures" to meet the GDPR requirements and protect data subjects' rights.

ii. Data Controllers and Data Processors are required to "implement appropriate technical and organisational measures" taking into account "the state of the art and the costs of implementation" and "the nature, scope, context, and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals."

c. Security actions that may be considered "appropriate to risk"
   i. The pseudonymisation and/or encryption of personal data
   ii. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data
   iii. The ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident
   iv. A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing

d. Fines & enforcement
   i. There will be a substantial increase in fines for organisations that do not comply with the new EU Regulation.
   ii. The Data Controller and Data Processor - j&s liability to Administration fines
   iii. Regulators will now have authority to issue penalties equal to the greater of €10m or 2% of the entity's global gross revenue for violations of record-keeping, security, breach notification, and privacy impact assessment obligations.
   iv. Violations of obligations related to legal justification for personal data processing (including consent…), Data Subject rights, Personal Data Beaches (PDB) and cross-border data transfers may result in penalties of up to €20m or 4% of the company's annual global turnover in the preceding 12 months.

e. Privacy management – risk based approach
   i. In practice, a company's controls must be developed according to the degree of risk associated with the data processing activities. Under the GDPR, it's essential that all companies conduct an organisation-wide Data Protection Impact Assessment (DPIA) with the focus on protecting the rights of Data Subjects.
   ii. Data protection safeguards must be designed into products and services from the earliest stage of development – Data by Design – and this applies to the Internet of Things (IOT).
   iii. Privacy-friendly techniques such as pseudonymisation will be encouraged, to reap the benefits of big data innovation while protecting privacy.
   iv. There's an increased emphasis on record keeping for Data Controllers – all designed to help demonstrate and meet compliance with the GDPR and improve the capabilities of organisations to manage privacy and data effectively.

f. Transparency principle
   i. Data Controllers and Data Processors must adhere to either an approved Code of Conduct or an approved Certification Symbol to demonstrate compliance with GDPR – which means transparency to Data Subjects on brand compliance to GDPR via a consumer website where compliance and fines will be recorded
   ii. The Processor relationship must be documented and managed with contracts and mandatory privacy obligations that are binding for both parties

g. 'Consent' and 'Legitimate Purposes'
   i. These are two major grounds for legal personal data processing (plus necessary execution of a contract and other grounds).
   ii. For marketers there's been much debate about the type of consent that's required under the GDPR.
   iii. Consent needs to be unambiguous and where processing special categories of personal data (biometric, genetic, etc) it will need to be explicit.

iv. Consent means "any **freely given, specific, informed and unambiguous** indication of his or her wishes by which the data subject, either **by a statement or by a clear affirmative action, signifies agreement** to personal data relating to them being processed"
v. Although the consent itself need not be explicit, the purposes for which the consent is gained **does** need to be "collected for specified, explicit and legitimate purposes". In other words, it needs to be obvious to the Data Subject what their data is going to be used for at the point of data collection.
vi. Consent should be demonstrable – in other words companies need to be able to show clearly how consent was gained and when.
vii. Consent must also be freely given – a Data Controller can't insist on data that's not required for the performance of a contract as a pre-requisite for that contract. And withdrawing consent should always be possible – and should be as easy as giving it.

h. Information provided at Data Collection

The information that must be made available to a Data Subject when data is collected is extremely important and includes:

i. Identity and the contact details of the Data Controller and Data Protection Officer (DPO)
ii. Purposes of the data processing for which the personal data is intended
iii. Legal basis of the personal data processing
iv. Where applicable, the legitimate interests pursued by the Data Controller or by a Third Party and 3rd country transfers informing about security safeguards
v. Where applicable, the recipients or categories of recipients of the personal data
vi. Where applicable, that the Data Controller intends to transfer personal data internationally
vii. Period for which the personal data will be stored, or if this isn't possible, the criteria used to determine this period
viii. Existence of the right to access, rectify or erase the personal data
ix. Right to data portability
x. Right to withdraw consent at any time
xi. Right to lodge a complaint to a Supervisory Authority.

i. Right to Data Portability

i. A clear principle of the GDPR is to allow Data Subjects greater control over their personal data whilst at the same time stimulating growth for new products and services by making it easier for data to be automatically switched to another provider.
ii. This is going to become more relevant in marketing activities within financial services as well as utilities, telecoms and ISPs.

j. Retention of personal data and Right to be Forgotten

i. Data Controllers must inform Data Subjects of the period of time (or reasons why) personal data will be retained on collection.
ii. Should the Data Subject subsequently wish to have their personal data removed and the data is no longer required for the reasons for which it was collected, then it must be erased.
iii. Note that there is a "downstream" responsibility for Data Controllers to take "reasonable steps" to notify Data Processors and other downstream data recipients of such requests.
iv. This area of the GDPR will need further clarification with respect to allowing for the retention of suppression or do-not-contact lists, otherwise that is unworkable.

5. New challenges for Direct Marketing

a. **Where the personal data hasn't been obtained directly from the Data Subject**, eg. using a 3rd party list – the following information is required to be given to the Data Subject:

i. source from which the personal data originates
ii. existence of any profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the Data Subject

b. There are some exceptions
    i. Notably where the effort would be disproportionate, although this isn't likely be a good justification in day-to-day situations
    ii. Where the information has already been provided to the Data Subject.
c. Headaches to marketers using multiple sources of third party data – and to those building such data products.
d. Processing is any automated processing of personal data to determine certain criteria about a person. "In particular to analyse or predict aspects concerning that natural person' s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements".
    i. Certainly impact some marketing processes and services – although the extent of this impact is yet to be understood – where does profiling finish and selection start?
e. Profile or user based advertising
Full personalisation and other ad serving techniques for example rely on a degree of selection normally built on profiles of behaviour or purchase – is explicit consent for this now required? It looks this way.
    i. Individuals have the right not to be subject to the results of automated decision making, including profiling, which produces legal effects on him/her or otherwise significantly affects them. So, individuals can opt out of profiling.
    ii. But, individuals have no right to opt-out of profiling if they have already explicitly consented to it, or if profiling is necessary under a contract between an organisation and an individual, or if profiling is authorised by EU or Member State law.

6. 'Legitimate Interests' and Direct Marketing
    a. GDPR specifically recognises that the processing of personal data for "direct marketing purposes" can be considered as a legitimate interest.
        i. Legitimate interest is one of the grounds, like consent, that a company can use in order to process personal data and satisfy the principle that personal data has been fairly and lawfully processed.
        ii. GDPR says that processing is lawful if "processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a Third Party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of personal data, in particular where the data subject is a child."

7. Breach notification
    a. A "personal data breach" is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"
        i. It's important to note that the wilful destruction or alteration of data is as much a breach as theft. In the event of a personal data breach, the Data Controller must notify the appropriate Supervisory Authority "without undue delay and, where feasible, not later than 72 hours after having become aware of it."
        ii. If notification is not made within 72 hours, the Data Controller must provide a "reasoned justification" for the delay. Notice isn't required if "the personal data breach is unlikely to result in a risk for the rights and freedoms of individuals."
        iii. Data Processor needs to notify the Data Controller in the event of a personal data breach.
    b. Exceptions to notify the Data Subject
        i. The Data Controller has "implemented appropriate technical and organisational protection measures" that "render the data unintelligible to any person who is not authorised to access it, such as encryption"

ii. The Data Controller takes actions subsequent to the personal data breach to "ensure that the high risk for the rights and freedoms of data subjects" is unlikely to materialise.
iii. When notification to each Data Subject would "involve disproportionate effort," in which case alternative communication measures may be used.

8. Data Protection Officer
    a. Requirements of appointment
        i. Under Art.35, GDPR, DPO must be appointed for all public authorities and where core activities of the Data Controller or the Data Processor involve "regular and systematic monitoring of Data Subjects on a large scale"
        ii. Under Art.28, GDPR, no requirement for DPO if Data Controller or Data Processor employing fewer than 250 persons unless the processing carried out is likely to result in a risk for the rights and freedoms of the Data Subject, the processing is not occasional or the processing includes special categories of data..
        iii. Data Controller or Data Processor conducts large-scale data processing of "special categories of personal data" (eg. ethnic origin, religious beliefs, genetic data, etc)
        iv. MUST have expert knowledge of data protection law and practices and MUST keep that knowledge up-to-date
        v. Independent senior manager reporting to the highest level of management (CEO).
    b. Main tasks include:
        i. Informing and advising the Data Controller or Data Processor and its employees of their obligations to comply with the GDPR and other DP laws and regulations
        ii. Monitoring compliance with the GDPR and other DP laws and regulations including managing internal data protection activities, training data processing staff and conducting internal audits
        iii. Conducing a Data Protection Impact Assessment (DPIA) across the whole organisation
        iv. •Maintaining a working relationship with the Data Controller or Data Processor's designated Supervisory Authority and serving as the point of contact on issues relating to processing of personal data
        v. Identified as the main point of contact for inquiries from Data Subjects on issues relating to data protection practices, withdrawal of consent, the right to be forgotten, the right of erasure, etc .

Next steps

Under GDPR a shift change in enforcement will be the principle of "guilty until proven innocent" and the significance of the requirement of the DPO to be independent and reporting any breaches to the Data Protection Authority (Supervisory Authority), which we believe in the UK is a role covered by the ICO and the FCA.

There is also an important next stage in terms of the Guidelines to Supervisory Authorities. We believe that these will be published as early as March. Till then the following check list should form a good starting point for internal discussion.

Check list for transition

1. Record all data processing activity
    a. Produce the record of personal data processing activities for now and the first 12 months under the GDPR transition period.
    b. Highlight all data processing that includes sensitive data, financial data, identity data, location data and photographs.
    c. Ensure that every data processing activity has a deletion schedule.
2. Satisfy condition of lawful processing
    a. There are basically two main ways: (1) Legitimate Purposes or (2) Consent.
    b. You need to plan modifications of existing personal data collection methods and notification of existing Data Subjects.

   c. Think through the implications for direct marketing.
   d. Advise senior management of the business continuity implications.
   e. Record and make sure you can prove when every Data Subject was made aware of this, now or at the point of data collection going forward.
   f. Think about using the transition period to notify existing Data Subjects.
3. Conduct an organisation wide Data Protection Impact Assessment (DPIA) without delay
   a. Define what "high risk processing" means in your company
   b. Start planning to fill any gaps
4. Plan a Data Protection training programme
   a. Make sure everyone in the organisation that handles personal data receives suitable data protection training – both general and specialist training and you have appropriate resources to do this
   b. Have a plan to roll out GDPR-compliant data protection training in the transition period as this will be seen by the Regulator as a mitigating factor in light of any personal data breaches or failures to comply with the GDPR in the future
   c. Don't forget to maintain your own training and development by keeping your knowledge up-to-date as you are directly responsible for making this happen under the GDPR.
5. Keep meticulous records
   a. List all recipients of personal data
   b. Ensure all contacts, training and assurance is carried out as mandated under the GDPR
   c. If personal data is transferred to a third country, ensure the transfer complies with the GDPR, including the required notification to the Data Subject (if required).
6. Protect the rights of the Data Subject
   a. Double-check all Subject Access Requests (SAR)
   b. Double-check all requests to object to processing
   c. Double-check all requests for rectification of personal data
   d. Double-check all requests for personal data erasure
   e. Double-check that data portability processes are in place
   f. Make sure that the company-wide personal data deletion is as per defined schedule.
7. Watch for danger signs
   a. Do a company-wide check to make sure personal data isn't being held that is not in the record of data processing activities and the Data Protection Impact Assessment (DPIA)
   b. Watch out for danger signs such as undocumented personal data, over collection of personal data and the over retention of personal data
   c. All of these will become a fast track to a very large fine in the wake of a Personal Data Breach so best take preventative action now.
8. Plan for Personal Data Breach
   a. Plan for a Personal Data Breach (PDB) – pre-warned is pre-armed
   b. Define or modify PDB reporting processes in order to comply with the GDPR and test it (including resource planning), including the log of PDBs and post-event forensic reports required for each PDB
   c. Make sure you can contact all your Data Subjects in the wake of discovering a PDB where required to do so under the GDPR.
9. Build a 'trip wire map' of GDPR
   a. Understand what in your company will trigger GDPR Administrative Fines
   b. Use your 'trip wire map' to check these contingencies against your current data processing activities in order to reduce the risk to business continuity.
10. Implement formal briefings for your Senior Management Team
   a. Make sure you diarise now formal briefing sessions for the Senior Management Team on the changes you will be recommending that the company makes in this GDPR transition period
   b. Make sure you also diarise now organisation-wide data protection awareness training
   c. Make sure that you have adequate resources and cover in order to carry out these duties and responsibilities