The General Data Protection Regulation
Myth, mystique or just misunderstanding?
Planning your approach.

There are few pieces of European Union regulation that have endured the level of intense scrutiny as the forthcoming EU General Data Protection Regulation (GDPR). The proposed wholesale reform of the EU's now decrepit data protection and privacy laws (including the UK's Data Protection Act 1998) date back to the last century and predate Facebook and Twitter. The purpose of this Briefing Note is to bring the main points of GDPR to your attention to ensure that ongoing personal data compliance is escalated as a 'known risk' within your current corporate governance agenda. Using publically available quotations and working directly with our legal advisors, we put forward the key points and responses in the form of a conversation on your behalf to provide definitive answers based on reliable and robust legal opinion.

What is the impact of Brexit?

Brexit does not allow companies to exit responsibility for, or understanding of, what is likely to be a ground-breaking change for many businesses.

Here's what people say.

"It is paramount to understand how GDPR will change not only the European data protection laws but nothing less than the whole world as we know it."[1] Jan Phillip Albrecht LL.M, Member of the European Parliament and Vice Chair of its Civil Liberties, Home Affairs and Justice Committee.

Compliance3 believe that UK business is unprepared in understanding and light on preparation.

"Over two-thirds of European and US CIOs (68%) still don't have a proper plan in place to comply with the coming European General Data Protection Regulation (GDPR), especially when it comes to the mainframe..."[2] Compuware survey.

"97% of respondents have heard of the GDPR but only 7% said they know "a great deal" about it"[3] Lloyd's UK survey.

"94% of Cloud Services Not GDPR Compliant"[4] Security Week.

"GDPR Fines Could Cost Firms Over $320 Billion"[5] Infosecurity Magazine.

Brexit means I don't have to prepare for GDPR, doesn't it?
Highly unlikely. The likely fact is that the UK will have to adopt Data Protection Regulation that is either as rigorous as the GDPR or more so.

Here's why.

There are three paths open to the UK post Brexit:

1. Joining the European Economic Area ("EEA"). This is the route adopted by Norway. Membership of the EEA will require the UK to implement rules and procedures that are equivalent to those of the European Union.

2. UK signs bilateral trade deals with the EU. This is likely to result in the UK having to agree to a duty to apply laws that are at least as demanding as European Union legislation. This is the option that has been adopted by Switzerland.

3. The other possibility is that the UK signs an, or a series of, independent trade deal/deals without taking on the burden of accepting equivalent EU obligations.

Under the first two options, it is clear that the UK would need to adopt Data Protection Regulation that is at least as strict as the GDPR. Under the third option, the UK would still need to adopt "adequate" protections in order for the EU to allow its members to pass information to the UK. In other words, the UK would still need to regulate to at least the standard of the GDPR. Given that such regulation is unlikely to differentiate between individual UK company jurisdictions, it is evident that all companies in the UK should be looking to comply to a standard at least that of the GDPR, and sooner rather than later.

Sooner rather than later?
Yes. GDPR enters into force on the 25th May, 2018. The preparation for compliance is likely to require close attention. The delay by many organisations in addressing adequacy introduces the risk that the correct level of advice and time for implementation may not be available in order to satisfy compliance.

Here is an indication of the questions that should be asked and what can be done now in order to ensure that the transition to compliance with the GDPR or the UK equivalent is as smooth as possible.

1. Carefully review the contents of contracts; do you need a data protection impact assessment?
2. Carefully review your relationships with processors if you are a controller and visa versa.
3. Document all existing customer interaction 'use cases' and review the data that the organisation is processing, including the type of data and any changes to the type of data processed. Ask these questions:
    a. Why do we need to collect that data?
    b. Where is the data going?
    c. For how long is that data stored and why?
    d. Can any data be psuedonymised?
4. Review your processes for data breach notification; security; answering data subject requests; risk assessment.
5. Train your workforce:
    a. Do you need a Data Protection Officer?
    b. Do you have adequate processes in place for employees to handle a serious data breach?
    c. Are you contracts of employment and/or contracts with subcontractors compliant with GDPR?
    d. Are you giving employees the correct information?

This is starting to look onerous. Tell me more.
There is still time to prepare and we can help in all areas of readiness. That means your Board having a clear understanding of the impact of GDPR in terms of corporate governance and risk as well as what that means in terms assessing the operational impact on the customer journey.

We can help you to look in more detail at the disciplines involved, what their functions are, and how they will need to prepare.

I'm starting to understand the scope of what's required. Is there anything else I need to pay attention to?
Yes. Privacy impact statements (PIA's)

Firms may need to undertake a privacy impact assessment.
The GDPR requirement to complete an impact statement in "high risk" circumstances is defined in article 35.

Again, Compliance3, alongside our legal advisors are able to provide the highest level of legal guidance and operational advice in this area.

Let's go back a step. To what, specifically, does GDPR, or a likely UK equivalent, apply?
Good question. Let's take a close look at the application of the regulation. The penalties for infringements are severe, so paying attention to the details is important. Remember, there is still time to get this right, and Compliance3 are able to assist in all areas.

To what does it apply?

The regulation applies to the processing of personal data in the context of the activities of an establishment or controller or processor in the Union, regardless or whether the processing takes place in the Union or not.

Further, the regulation applies to the processing of personal data of data subjects who are in the Union by controllers or processors not established in the Union, where either processing activities are related either to the offering of goods or services to such data subjects in the Union or to the monitoring of their behaviour in as far as their behaviour takes place within the Union.

Here, personal data means any information relating to an identified or identifiable natural person ("data subject"); controller means a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; processor means a natural or legal person, public authority, agency or other body which processes personal data on half of the controller.

Note, a personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

OK. I'm digesting that. Tell me what my obligations are under the new regulation.
Certainly. We'll start by summarising with six principles.

Personal data must be:

1. Processed fairly, lawfully and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency").
2. Collected for specified, explicit and legitimate purposes and not processed in a manner which is incompatible with those purposes ("purpose limitation").

3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimisation").
4. Adequate and where necessary kept up to date ("accuracy").
5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ("storage limitation").
6. Processed in a manner that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage using appropriate technical or organisational measures ("integrity and confidentiality").

That's a clear summary. Can you expand a little?
Yes. Let's focus on a few key Articles.

Article 6 sets the parameters of the lawfulness of processing. It provides processing shall be lawful only if:

a. The data subject has given consent for one or more specific purposes.
b. Processing is necessary for the performance of the contract with the data subject his party knowledge take steps at the request of the data subject prior to entering into a contract.
c. Processing is necessary for compliance the legal obligation to which the controller is subject.
d. Processing is necessary in order to protect the vital interests of the data subject or of another natural person.
e. Processing is necessary for the performance of the task carried out in the public interest when the exercise of official authority vested in the controller.
f. Processing is necessary for the purposes of the legitimate interests pursued by the controller or by 1/3 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.

Article 7 sets out the conditions for consent. It states that, where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data. The data subject shall have the right to withdraw his or her consent at any time.

Articles 15,16 and 17 deal with the right of access by the data subject, the right of rectification and the right to erasure (" the right to be forgotten").

Article 33 sets out what has to be done in the event of a personal data breach. The controller shall, without undue delay and, where feasible, not later than 72 hours after having become aware, notify a personal data breach to the supervisory authority. The processor shall also have a duty to notify the controller without undue delay after becoming aware of a personal data breach.

Article 37 introduces the concept of the data protection officer. It requires the appointment of a data protection officer where the processing is carried out by public authority; where the core activities of the controller or processor require regular and systematic monitoring of data subjects on a large-scale; or where core activities of the controller or processor consist of processing on a large scale of special categories of data.

I better understand. You mentioned that the penalties for getting this wrong are severe, how severe?
Potentially very severe. Certain infringements are subject to fines of 20 million Euros or up to 4% of worldwide annual turnover – whichever is higher. Let's examine some details.

Article 82 gives a right to compensation to any person who has suffered material or nonmaterial damage as a result of an infringement of this regulation. Article 83 restates the proposition that fines should be effective, proportionate and dissuasive. Fines can be imposed in addition to, or instead of, other measures contemplated

by the Regulation and the Article sets out the criteria which should be followed when determining whether and how much to fine.

The Article states that in each individual case, due regard should be taken of

a. The nature, gravity and duration of the infringement taking in to account the nature, scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them.
b. The intentional or negligent character of the infringement.
c. Any action taken by the data controller or processor to mitigate the damage.
d. The degree of responsibility of the controller or processor taking in to account technical and organisational measures implemented by them pursuant to the Regulation.

In assessing, the track record of the controller or processor will be taken into account and any other aggravating or mitigating feature applicable to the circumstances of the case.

Infringements of articles 8, 11, 25-39, 42 and 43 shall be subject to fines of up to 10 million Euros or, in the case of an undertaking, up to 2% of worldwide annual turnover for the preceding year, whichever is higher.

Infringements of articles 5, 6, 7, 10-22, 44-49 and 43 shall be subject to fines of up to 20 million Euros or, in the case of an undertaking, up to 4% of worldwide annual turnover for the preceding year, whichever is higher.

Article 84 provides that member states shall lay down the rules on other penalties applicable to infringements of this regulation which envisages member states take the initiative in introducing domestic legislation, in particular for infringements which are not subject to administrative fines as specified in article 83, and shall take all measures necessary to ensure that they are implemented. It restates the principle that the penalties shall be effective, proportionate and dissuasive.

How is Compliance3 able to help?

Rooted in customer contact processes and contact centre operations, Compliance3 provides an initial opportunity to LOCATE where your organisation is in terms of compliance readiness by benchmarking your organisation against eighteen key assessment criteria

This service clearly identifies the work streams that can be prioritised based on your companies business requirements and appetite for achieving an acceptable risk / cost balance.

This approach also offers optimal cost and time efficiency – you don't pay for, or waste time on, what you don't need. We also have direct licensed access to the Bar negating. You will not need to pay intermediaries to access the reliable and proven legal advice.

Our objective is to get you to a known position where the impact of the General Data Protection Regulation is assessed and managed to a level that can be defended against the Regulator which can be undersigned by the leading QC in this area of law.

References

1. Albrecht, J. 2016. How the GDPR Will Change the World. European Data Protection Law Review 2(3):287.
2. Compuware survey cited by Muncaster, P. 2016. Mainframe Concerns as CIOs Struggle with GDPR Plans. Infosecurity Magazine.
3. Lloyd's. 2016. Facing the Cyber Risk Challenge.
4. Townsend, K. 2016. 94% of Cloud Services Not GDPR Compliant: Report. Security Week.
5. Capgemini survey cited by Muncaster, P. 2016. GDPR Fines Could Cost Firms Over $320 Billion. Infosecurity Magazine.