BOOST PERFORMANCE
Improving Customer, Partner & Shareholder Value

BOOST REDPAPER - *Winter 2018*

GDPR – *What you need to know...*

Get ahead: Ask Boost to create you your own library of client-facing assets.

GDPR – *What you need to know…*

GDPR builds on the 1998 Data Protection Act (DPA), founded on taking care of, and lawfully processing, personal data. It's a new regulation, but data protection is not new. The requirement to protect data has always been in place, but GDPR will poses more serious consequences for those organisations that cannot demonstrate they are taking data protection seriously.

Getting to grips with GDPR is key!

Why bother about EU General Data Protection Regulation (GDPR)?

Despite Brexit these new EU data protection rules will apply and be relevant to UK organisations. Failure to comply will result in a fine being applied for which there are three levels, the highest level being 4% of annual global turnover or €20 Million (whichever figure is the greater). Another example of the tiered approach being applied could be a company being fined 2% for not having their records in order, not notifying the supervising authority (SA) and individual/data subject about a breach, or not conducting a Data Protection Impact Assessment (DPIA). It is important to note that these rules apply to both controllers and processors, meaning 'clouds' will not be exempt from GDPR enforcement.

There may also be special rules for public bodies. Plus, organisations that breach GDPR may also be subject to additional private claims for compensation by individuals.

Simply, if you don't follow the basic principles for processing data, such as consent; ignore individuals' rights over their data; or transfer data to another country; you could incur significant financial penalties.

Although GDPR doesn't come into force until May 2018, organisations of all sizes need to act now to understand these changes, what they mean and how they can best prepare for these new rules to make sure they are compliant.

Who does GDPR affect?

It affects every business within all 28 EU Member States as well as those outside of the EU that process the personal data of EU residents. In the UK we also have our national data protection rules through the Information Commissioners Office (ICO) which will continue to apply until a decision is made on how these are to be treated as a result of GDPR. So, for now UK Data Protection laws and GDPR will both apply to UK organisations.

What does GDPR apply to?

Personal data, similar to that provided for under the Data Protection Act 1998 (the DPA), so it's nothing that we don't already have an awareness of.

Personal data is information relating to an identified or identifiable natural person. Under GDPR this will now be extended to online identifiers, such as an IP address. Special categories of personal data/sensitive data, such as sexual orientation and religious beliefs, continue to be covered, and will also be extended to include genetic and biometric data.

How does GDPR benefit individuals and businesses?

Personal data breach reporting has a strong public policy purpose. The law is designed to push companies and public bodies to step up their ability to detect and deter breaches. What is foremost in regulators' minds is not to punish organisations, but to make them better equipped to deal with security vulnerabilities.

The public need to have trust and confidence that a regulator is collecting and analysing information about breaches, looking for trends, patterns and wider issues with organisations, sectors or types of technologies. It will help organisations get data protection right now and in the future.

The new legislation is focused on giving consumers more control over their data and increasing the accountability of organisations. The Information Commissioners Office (ICO) are currently working alongside other EU data protection authorities to produce guidance that will set out when organisations should be reporting, and the steps they can take to help meet their obligations under the new data breach reporting requirement. You can find some examples and explanations provided by the ICO here.

There are so many questions around GDPR, with lots of people feeling in the dark…

The official Regulation document from the European Council is 88 pages long and most of us wouldn't be able to fully understand this document, so to help you we've covered off the main questions and issues that are front of mind for businesses of all sizes to highlight some of the key points you should be aware of when working towards your organisation being GDPR compliant.

Frequently Asked Questions (FAQs)

This Whitepaper is aimed at businesses of all sizes to help them understand and prepare for GDPR we therefore thought it most useful to understand the concerns of such organisations and gather the opinions of experts in answering those questions that are increasingly being asked.

1. What's the exact date the new GDPR will come into force? The rules will fully apply from 25th May 2018.

2. What will change with the introduction of these new regulations? Organisations will answer to one data protection regulator called a 'supervisory authority' (SA).

3. Who does the GDPR apply to? 'Controllers' and 'processors' of data need to abide by the GDPR. Even if controllers and processors are based outside the EU, the GDPR will still apply to them so long as they are dealing with data belonging to EU citizens.

It is the controller's responsibility to ensure their processor abides by data protection law and processors must themselves abide by the rules to maintain records of their processing activities. If processors are involved in a data breach, they are far more liable under GDPR than they were under the UK Data Protection Act.

4. What about Brexit? The UK is due to leave the EU in March 2019, almost a year after GDPR comes into force so GDPR applies to UK businesses from the outset and will continue to apply if you sell goods or services to people in other EU countries.

Also, the UK Government has indicated that it will implement an equivalent legal mechanism to GDPR.

5. Who does GDPR affect? GDPR applies to businesses and organisations located within the EU as well as organisations located outside of the EU, if they offer goods or services to, or monitor the behaviour of, EU individuals/data subjects. It applies to all companies processing and holding the personal data of individuals/data subjects residing in the EU, regardless of the company's location.

6. What is the difference between a regulation and a directive? GDPR is a regulation - 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 for achievement.

7. Will the fines really be enforced? Yes. Each Member State will have individual discretion on criminal sanctions for GDPR infringements. At this time it is too early to predict how different supervisory authorities (SAs) will enforce their powers but it's inevitable there will be variable approaches as some SAs will be more proactive than others. Overall, the majority of SAs will simply tighten their current enforcement practices to align with GDPR.

8. What constitutes personal data? Any information related to a natural person or 'data subject', which can be used to directly or indirectly identify that person. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address.

9. What consent must be given to process personal data? Consent must be provided by an individual/data subject for the processing of their personal data. The request for consent must be given "in an intelligible and easily accessible form", with the purpose for data processing attached to that consent to make it unambiguous. As such, inactivity or pre-ticked boxes will no longer constitute consent for the processing of data. Organisations will be required to demonstrate that individuals/data subjects have actively consented to the processing of their data. They will also be required to keep a record of how and when consent was provided and, generally, stop processing data if consent is removed.

An additional layer of protection has been provided for children (generally those under the age of 16, although this age can be reduced to not less than 13 should a Member State determine that this is acceptable). In these circumstances, consent is required from the person who has parental responsibility for the child whose data is to be processed.

The conditions for consent will strengthen with GDPR, as organisations will no longer be able to utilise long illegible terms and conditions full of legalese. The company must also provide and use terms and conditions that relate to the data, its use and how this will be managed.

Companies must ensure data consent is clear and distinguishable. It must be as easy to withdraw consent as it is to give it. Companies must be able to demonstrate that the individual has given consent for their data to be processed.

Explicit consent is required only for processing sensitive personal data (such as data revealing racial or ethnic origin, health data or genetic data).

10. Can I still market to my existing customers? Yes, providing you meet the new rules around consent. Where personal data is processed for direct marketing, the individual's right to object/unsubscribe/opt-out should be apparent and brought to their attention.

11. Does the GDPR apply to cold calling? Yes! If customers haven't opted-in to your communication this would be classed a s a breach of GDPR.

12. What is the "right to be forgotten"? This is the right of the individual to have their personal data deleted "without undue delay", for example where data is no longer necessary for the purposes it was initially collected or processed, or perhaps where the annual permission has not been updated/provided.

13. What rights does an individual/data subject have? As under the Data Protection Act (DPA), there is a right of access to the data stored and confirmation of the processing of it. GDPR removes the requirement for the payment of a fee (currently £10) except in circumstances where a request is manifestly unfounded or excessive, or where information has previously been disclosed. Most requests should be completed within 30 days of the initial request.

If any information held is incorrect, the data subject is entitled to request it be rectified. Where information has been disclosed to third parties, the disclosing party is obliged to ensure that this information is also rectified.

Where there is no compelling reason for personal data to be held, a subject has the right to request that any data be deleted. Further, the data subject may request that any processing of data ceases. This request must be complied with unless there are compelling and legitimate grounds for processing of that personal data.

14. Will I need to register with the Information Commissioner? The regulation removes the obligation for data controllers to register (notify) with a regulator (in the UK this is the Information Commissioners Office(ICO)). Controllers are, however, obliged to undertake periodic assessments of the data that they process and the impact upon the protection of the data that they are processing (these assessments are called Data Protection Impact Assessments). This obligation will be pertinent to those industries where big data (i.e. large amounts of data) is prevalent, such as social media providers, or those who use data to determine trends or behaviours. In these circumstances, there will be an obligation to notify a regulator where an assessment indicates that the processing would result in a high risk in the absence of measures taken by a Data Controller to mitigate the risk.

15. Dœs my business need to appoint a Data Protection Officer (DPO)? A small business would not be expected to appoint a DPO as the scale wouldn't warrant this. A DPO should only be appointed if the core activities of the Data Controller consist of:

- Processing operations which require large-scale, regular and systematic monitoring of data subjects, i.e. Banks, Insurance Companies, Law Firms;

- If you are a public authority or carry out large-scale processing of special categories of personal data: those revealing racial/ethnic origin; political opinions; religious or philosophical beliefs; trade-union membership, and the processing of genetic and biometric data to uniquely identify an individual; data concerning health or sex life and sexual orientation (this can only be processed under strict conditions such as where consent has been given), or data relating to criminal convictions or offences.

If your organisation dœs not fall into one of the above categories you do not need to appoint a DPO. For more detail see **Article 37 of the GDPR**

16. What is the difference between a data processor and a data controller? A controller is the entity that determines the purposes, conditions and means of the processing of personal data, while the processor is an entity which processes personal data on behalf of the controller.

17. Accountability. Many organisations will already have adequate measures in place due to the Data Protection Act (DPA), however, it is likely that others will be required to examine and address their current practices to ensure compliance with GDPR. Organisations will be required to show how they adhere to the regulation's principles by, for example, demonstrating the procedures they have in place to protect the data they hold.

18. What is a data protection impact assessment (DPIA)? Under GDPR Data Controllers must carry out DPIAs to "evaluate, in particular, the origin, nature, particularity and severity" of the "risk to the rights and freedoms of natural persons" before processing personally identifiable information. The DPIA "should include the measures, safeguards and mechanisms envisaged for mitigating" the identified risks.

Why is a DPIA needed?

To reduce a project's privacy risks. An impact assessment helps to identify and address risks at an early stage by analysing how the proposed uses of personal information and technology will work in practice, and proposing methods to mitigate identified risks.

When should DPIAs be conducted?

DPIAs should be carried out when new projects are planned, or when planning revisions to existing practices. According to the ICO, businesses conducting DPIAs should ensure that their project plans are flexible enough to allow for changes if the DPIA identifies any privacy issues that need to be addressed.

According to the GDPR, a DPIA should focus "on those types of processing operations which are likely to result in a high risk to the rights and freedoms of natural persons by virtue of their nature, scope, context and purposes".

The GDPR specifies four examples of when processing is likely to result in a high risk to the rights and freedoms of an individual and when a DPIA must therefore be carried out:

- a systematic monitoring of a publicly accessible area on a large scale (e.g. CCTV, drones and body-worn devices)
- a systematic and extensive evaluation of personal aspects relating to individuals which is based on automated processing and on which decisions are based that produce legal effects concerning individuals or similarly significantly affect them (e.g. such as automatic refusal of an online credit application or e-recruiting practices without any human intervention)
- processing on a large scale of special categories of data (e.g. health, religion or ethnic origin) and
- processing on a large scale of personal data relating to criminal convictions and offences.

Guidance from the Article 29 Working Party (A29WP) makes it clear that if there is any doubt as to whether a DPIA is required, one should be carried out.

To help data controllers determine whether a DPIA is required the A29WP's guidance sets out criteria which might trigger a DPIA including:

- where an individual is being evaluated or scored (in particular, where it relates to health, work, behaviour, location or movements) or subjected to automated decision making (see Automated decision making under the GDPR)
- where processing is carried out on vulnerable individuals (e.g. employees, children and the elderly) because their relationship with the data controller is imbalanced, meaning they can't consent or oppose to their personal data being processed
- where the processing might prevent individuals from exercising a right, using a service or entering into a contract and using a new technology where it involves novel forms of data collection and usage.

The A29WP makes it clear that carrying out a DPIA is 'a continual process, not a one-time exercise'.

It also strongly recommends that data controllers carry out DPIAs for processing operations which are already underway and will continue on/from 25 May 2018. Furthermore, DPIAs should 'as a matter of good practice … be continuously carried out on existing processing activities, and re-assessed after 3 years, perhaps sooner, depending on the nature of the processing and the rate of change in the processing operation and general circumstances'.

What do DPIAs require an organisation to do?

An organisation is required to document:

- what kind of personal information will be collected in the project;
- how it is collected, used, transmitted and stored;
- how and why it can be shared; and
- how it is protected from inappropriate disclosure at each step.

What should a DPIA look like?

The GDPR doesn't mandate what form or structure a DPIA should take. Although this is left to data controllers to determine, the A29WP guidance:

- includes examples of EU-generic and EU sector-specific frameworks (annex 1) and common criteria to clarify the basic scope of the GDPR and provide enough scope for different forms of implementation (annex 2) and
- encourages the development of sectorspecific DPIA frameworks.

The GDPR doesn't require a data controller to publish its DPIAs but the A29WP encourages sharing non-commercial/ sensitive parts of a DPIA, or just a summary, 'to help foster trust in the controller's processing operations, and demonstrate accountability and transparency' and 'where members of the public are affected by the processing operation'.

19. How does GDPR affect policy surrounding data breaches? Proposed regulations surrounding data breaches primarily relate to the notification policies of companies that have been breached. Data breaches which may pose a high risk to the rights and freedoms of individuals must be notified to the relevant DPA within 72 hours and to affected individuals "without undue delay".

Organisations will have to provide certain details when reporting, but where the organisation doesn't have all the details available, more can be provided later. The ICO will not expect to receive comprehensive reports at the outset of the discovery or detection of an incident – but they will want to know the potential scope and cause of the breach, mitigation actions you plan to take, and how you plan to address the problem.

Organisations should be aware that the ICO will have the ability to issue fines for failing to notify and failing to notify in time. Fines can be avoided if organisations are open and honest and report without undue delay, which works alongside the basic transparency principles of the GDPR.

In the event of a breach, the ICO ask that you:
Tell it all, tell it fast, tell the truth

20. Do I have to report all personal data breaches?
Under the current UK data protection law, most personal data breach reporting is best practice but not compulsory. And, although certain organisations are required to report under other laws, mandatory reporting of a personal data breach that results in a risk to people's rights and freedoms under the GDPR will be a new requirement. The threshold to determine whether an incident needs to be reported to the ICO depends on the risk it poses to the people involved.

These new reporting requirements will mean some changes to the way businesses, organisations and even the ICO identify, handle and respond to personal data breaches.

Any breach of security which leads to *the destruction, loss, alteration or unauthorised disclosure of, or access to, personal data* is likely to be a breach of the regulation. Organisations need to remember that if there's the likelihood of a high risk to people's rights and freedoms, they will also need to report the breach to the individuals concerned.

High risk situations are likely to include the potential of people suffering significant detrimental effect – for example, discrimination, damage to reputation, financial loss, or any other significant economic or social disadvantage.

Not all breaches are reportable, if organisations aren't sure about who is affected, the ICO will be able to advise immediately and, in certain cases, order them to contact the people affected if the incident is judged to be high risk.

Just to be clear – up until 25 May 2018 all personal data breaches will be assessed under the current Data Protection Act.

What can you and your organisation do now to prepare for GDPR?

You should be preparing now by ensuring you have the roles, responsibilities and processes in place for reporting; this is particularly important for medium to large organisations that have multiple sites or business lines.

Next, consider what policies and procedures are currently in place, and whether these meet the obligations imposed under GDPR. Then start examining the types of incidents your organisation faces and develop a sense of what constitutes a serious incident in the context of your data and your own customers.

Being compliant with GDPR is a good thing, but it won't protect you from a breach of your data or the impact this could have on your organisation. You are not going to prevent every attack or mishap imaginable, but what you can do is take and demonstrate reasonable measures in the safeguarding of your data. Your corporate objective around data is therefore to tick the boxes for GDPR but to also protect your data.

The key to GDPR and other regulations is a sound approach to data protection across the organisation. Focusing purely on compliance is the wrong approach as many compliant organisations have still encountered serious issues with data protection and suffered significant impact as a result.

A true approach to data protection should be embedded into your business, strategies, transformation and commercial arrangements. This will lead to a far more mature stance, and with that comes compliance.

A rather large number of organisations are not complaint with DPA today, so won't be compliant with GDPR. And, as with DPA we will only begin to understand GDPR more through the arising court cases and legal challenges.

Data protection requires practical knowledge, experience and business empathy to determine what's possible, what's a priority, what's a risk. Many organisations won't have this available to them but can access it through purpose-built tools that will search their data, analyse it and then organise this in a way that enables them to achieve regulatory compliance and tackle data protection holistically to achieve zero breaches – **Osprey from Gravicus** is a smart and simple solution for business wide data protection that limits the complexities around information, data management, analytics and defensibility. It also allows for the movement of data without compromising usability, flexibility and scalability.

Osprey was developed by leading experts over several years and based upon 'what the customer wants/needs' to create a next generation information governance system that analyses, organises and acts on information within unstructured data through a multitude of AI capabilities to provide users with the ability to make sense of their data, reduce risks, reduce costs and achieve regulatory compliance.

To help further the ICO has produced **Preparing for the GDPR: 12 steps to take now** to give organisations a list of the key issues they need to address in their preparations.

References for rurther reading

1. ICO Breach notification. https://iconewsblog. org.uk/2017/09/05/gdpr-setting-the-recordstraight- on-data-breach-reporting/

2. Preparing for the GDPR: 12 steps to take now. https://ico.org.uk/media/for-organisations/documents/1624219/preparing-for-the-gdpr-12-steps.pdf

3. Guidance from the Article 29 Working Party. http://www.rawlisonbutler.com/blog/data-protectionneed- carry-data-protection-impact-assessment/

4. Article 37 of the GDPR. https://gdpr-info.eu/art-37-gdpr/

About Boost Performance

Boost is improving the business performance of technology companies by revolutionising the "assisted sales & marketing" experience.

Our services include:

Value Proposition Design

Multi-Media Content
& Asset Creation

Demand Generation
Design & Implementation

Sales & Marketing Consultancy (commission/
rebate plans, sales processes etc)

Sales Enablement

Telemarketing

Salespeople- as-a-Service (in partnership
with Sales Gym 360, Westcoast, and the Raw Talent Academy)

Join the revolution.

To learn how Boost can help you improve your business performance, contact us today.

0203 740 4074
contactme@boost-performance.co.uk
www.boost-performance.co.uk

BOOST PERFORMANCE
Improving Customer, Partner & Shareholder Value