EVERYTHING YOU WANTED TO KNOW ABOUT THE GDPR BUT DIDN'T KNOW WHO TO ASK

WHITE PAPER

CHARTERHOUSE
VOICE & DATA

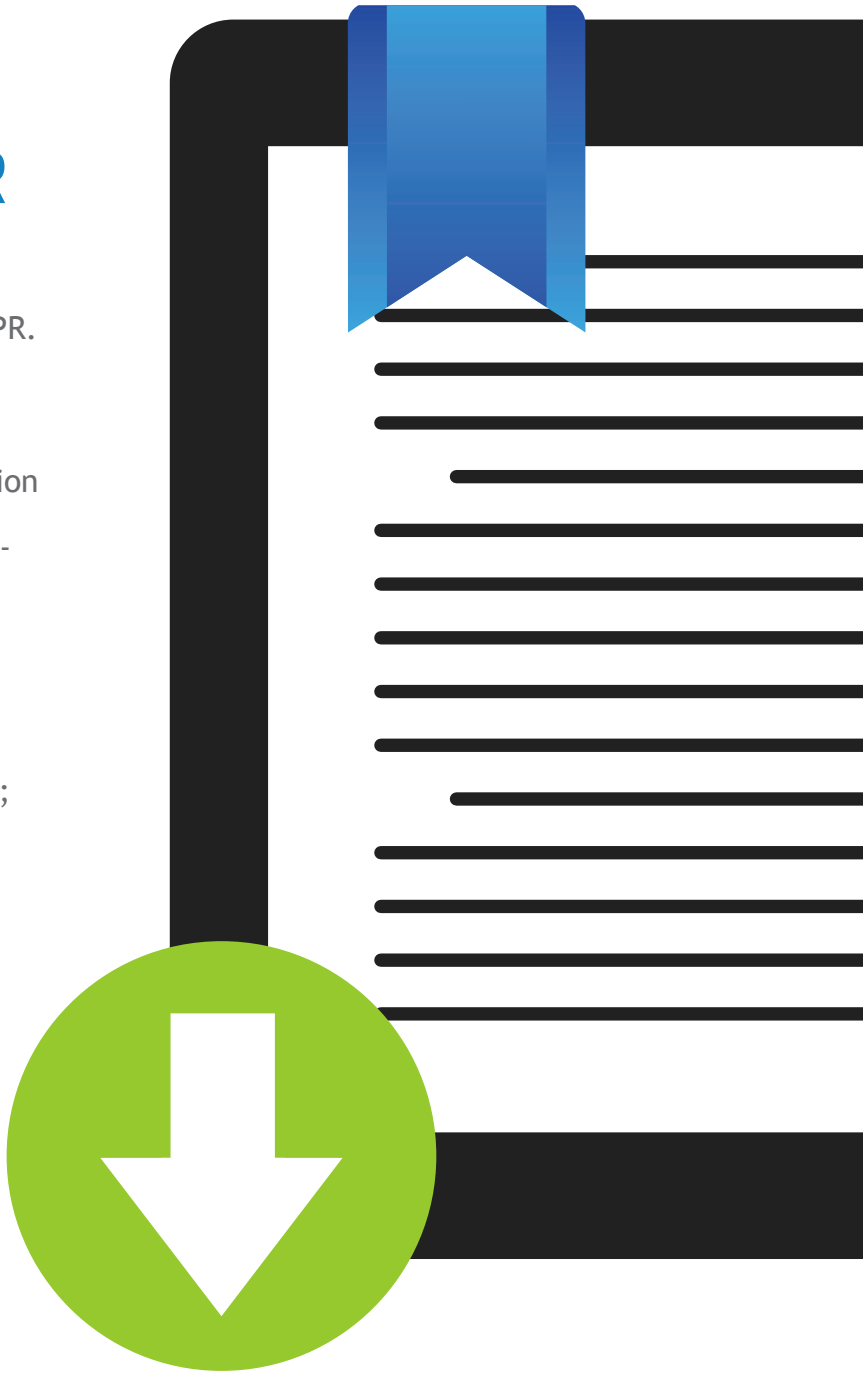
ABOUT THIS PAPER

This paper is targeted at digitally-enabled organisations that need to adapt to the GDPR.

It aims to:

- Brief you on the key points of the legislation
- Highlight the likely impact on your day-to-day working practices
- Establish the potential consequences of non-compliance

Whilst the GDPR is not all about technology; it does have a key role to play in both readiness and compliance. This paper will also explore the concept of “privacy by design” and suggest a roadmap for GDPR-ready organisations ahead of the May 2018



"There are two types of companies: Those that have been hacked, and those that don't know they've been hacked."

John Chambers, Executive Chairman and former CEO of Cisco

THE CHANGING LANDSCAPE OF DATA PRIVACY & SECURITY

While John Chambers' statement may be a slight exaggeration, the sentiment is true. Former FBI Director Robert Mueller is similarly pessimistic. "There are two types of organisation. Those that have been hacked and those that are going to be hacked."

Today's digital enterprises thrive on flexible working; enabling and encouraging employees to work from any device, anywhere. However, the ease with which we access data as part of our everyday working lives comes at a risk. Greater access and availability of potentially sensitive data introduces new cyber-security challenges.

THE NEW NORM?

Data security breaches are becoming commonplace. Since 2013, the Gemalto breach level index has reported more than 7 billion lost or stolen data records - that's over 3,000 records every minute. Identity theft and financial gain continue to be the main motivators, but there is also an increasing trend towards nuisance hacking and state-sponsored cyber-crime.

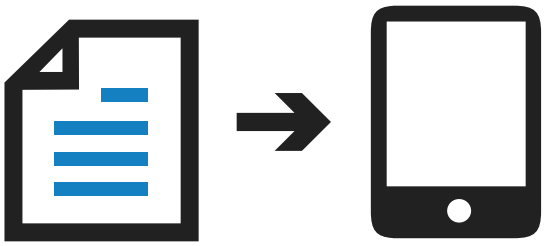
Over the past 10 years, some of the world's largest organisations have suffered data breaches. While the names of these companies will naturally spend more time in the media spotlight, they aren't alone; small and medium sized organisations are equally susceptible to attacks, with the results being just as, if not more devastating.

Why is this the case? Firstly, cyber-attacks have become increasingly sophisticated and well-organised. Secondly, organisations have not been taking sufficient steps to secure their data; both in transit and at rest.

THE NEED FOR CHANGE

In a digital world, the old data protection legislation just doesn't hold water. Many EU states, the UK among them, have been relying on regulations set down in the 1990s. A time when the worldwide web was still in its infancy and we hadn't dreamed of tablets and smartphones.

Big data has become the currency of business and the scope and scale of data captured every day puts consumers at a greater risk of data theft. Something had to change. After a four-year consultation, the European Union finally published its new legislation in 2016; featuring new rules designed to protect the private information of individuals within the EU.



These are not only designed to set a new standard for data security, but to define - and protect - the new and different kinds of data that organisations hold in the digital age. This legislation is known as the General Data Protection Regulation, or 'GDPR' for short.

THE BREACH TIMELINE

2017 Hackers break into the database of telecommunications provider Three and make off with the personal details of over 200,000 customers.

2016 A faulty back-up exposes over 1.3 billion records on spam operator River City Media's database, including email and IP addresses.

2015 157,000 TalkTalk customer records fall into the hands of criminals exploiting a weakness in the firm's website - it's second incident in under a year.

2014 Cyber criminals hack the website of the European Central Bank and steal over 4 million records; including email addresses.

2013 The largest breach in history sees Yahoo lose over 1 billion records, including user names, telephone numbers and dates of birth.

2012 Social networking site LinkedIn suffers a major data breach; resulting in the loss of over 117 million user account records.

2011 Sony suffers an attack by hacking collective Lulzsec, its third breach in a year leads to the loss of over 76 million user accounts.

2010 UK gambling site Betfair is hacked, it waits 18 months before revealing the breach lead to the loss of 2.3 million users' account details.

2009 The largest credit card scam in history sees payment processor Heartland pay over $110 million in compensation to credit card companies.

2008 A hard drive containing the passport, banking and national insurance details of 1.7 million armed forces personnel is lost by the UK MOD.

2007 HMRC lost the records of over 25 million child benefit claimants because the CDs went missing in the post.

2006 A misplaced hard drive sees the details over 3 million applicants for the driving theory test lost by a subcontractor of the Driving Standards Agency.

2005 An unauthorised line of code inserted in Cardsystems network leads to the theft of 40 million credit card holders' data.

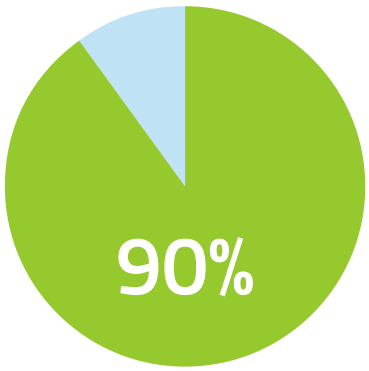
2004 A former AOL software engineer steals 92 million usernames and email addresses. He sells them to spammers who send over 7 billion unsolicited emails

BACKGROUND TO THE GDPR

The General Data Protection Regulation was introduced by the European Union in April 2016, with a deadline for implementation of 25th May 2018. The primary purpose of this legislation is to "strengthen citizens' fundamental rights in the digital age and facilitate business by simplifying rules for companies in the Single Digital Market."[1]

The legislation will protect both citizens and residents of EU countries; ensuring their personal data is safe and only used for activities they are aware of and consent to.

In the UK, this regulation will replace the 1998 Data Protection Act as the single source of data protection regulation that organisations must adhere to.



More than **90%** of Europeans say they want the same data protection rights across the EU – regardless of where their data is processed.

Source: European Commission

WHO DO THESE RULES APPLY TO?

For businesses, these rules apply to both **data controllers** (those who determine the purposes for, and the manner in which, data is processed) and **data processors** (those who process data on behalf of the data controller).

GDPR places more obligations on data processors who, for example, "are required to maintain records of personal data and processing activities"[2]. Processors also have more legal liability if responsible for a breach, especially if they have not complied with the regulation or have acted outside the instructions of the controller.

GDPR also specifies further obligations for data controllers, who must ensure processors - both internal and external - are fully compliant with the legislation.

BREXIT MEANS BREXIT?

The UK's decision to leave the European Union after the 2016 referendum does not mean the UK will be exempt from GDPR – now, or going forward. Not only will GDPR come into force before the UK leaves the EU, the government has also announced that the regulations will apply regardless of the UK's membership status.

Alongside this commitment, the makeup of GDPR itself means that UK businesses would continue to fall under its remit - as GDPR applies to all companies dealing with anyone based in the EU, regardless of where that company is situated.

> "The approach that we've taken in order to maximize the ease with which we can negotiate an uninterrupted and unhindered flow of data is to put GDPR into UK law in full."
>
> Matt Hancock, Minister of State for Digital and Culture

THE INFLUENCE OF IOT

While the GDPR is not designed primarily for Internet of Things (IoT) systems and services, the European Commission is aware of the growing influence of IoT in a world where many suppliers acknowledge that 'data is the new oil'[3].

The result is that much of the data collected through IoT is within the scope of GDPR, placing a strong emphasis on those supplying and utilising IoT to demonstrate compliance.

As international law firm Bird & Bird comment, it is "a law which will significantly overhaul Europe's cornerstone data protection legislation at a time when information systems and digital business underpin human life".

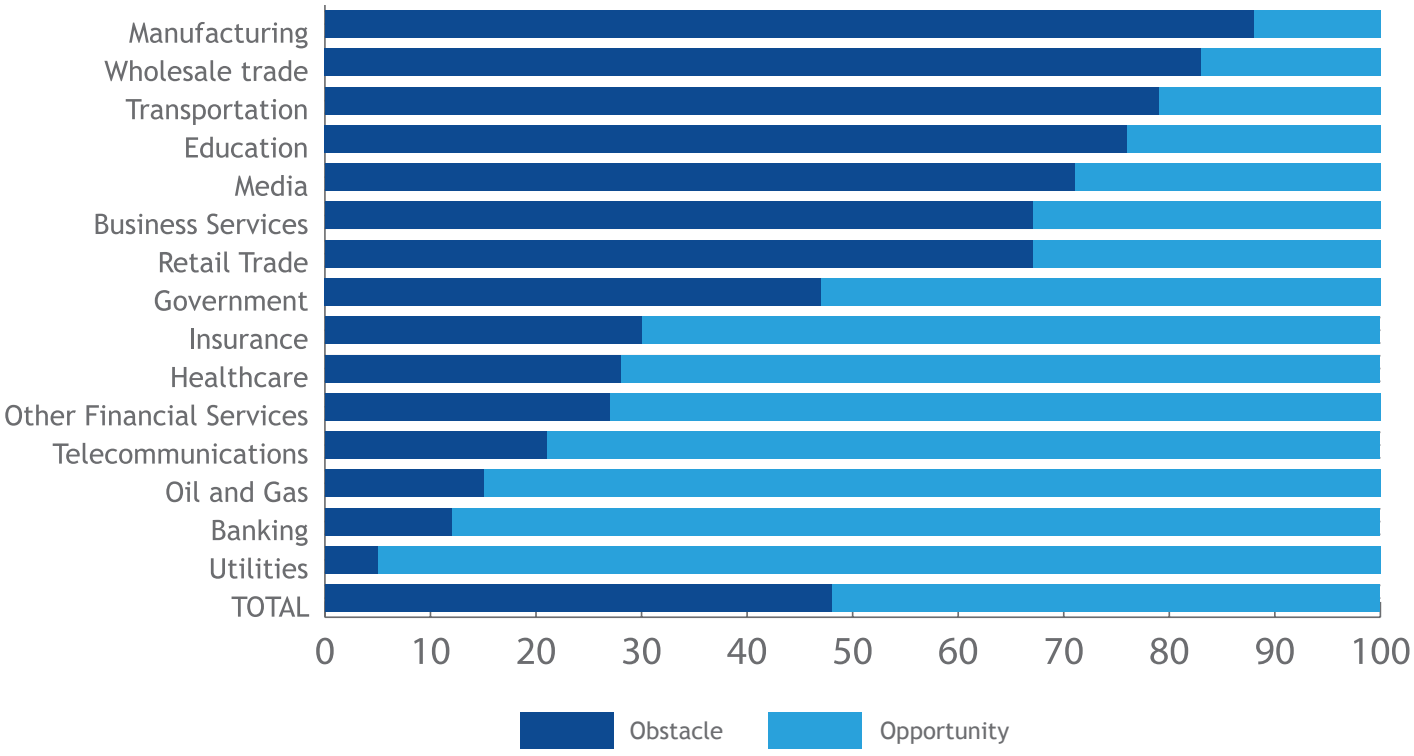
[1]European Commission, [2]Information Commissioner's Office, [3]CCS Insight

HOW GDPR WILL AFFECT YOUR BUSINESS

There are no businesses in Europe, and few across the world, that do not process the data of individuals based in the EU in one way or another. As a result, GDPR applies to businesses virtually everywhere.

OBSTACLE VS OPPORTUNITY

Does GPDR Represent an Opportunity or an Obstacle?



Source: IDC EMEA GDPR Survey 2017.

Research conducted by IDC shows that the reaction to GDPR is mixed among the business community. While some organisations see it as an opportunity to re-architect their information governance, others see it as a chore. The split? About 50:50.

This divide in outlook means that we're likely to see a variation in how organisations will act to meet the regulation. Those with a positive, opportunistic outlook are likely to embrace the spirit of data best practice, while those with a negative outlook are likely to just 'check the boxes'.

THE SCOPE OF PERSONAL DATA

Rules protecting Personally Identifiable Information (PII) are greatly expanded compared to the Data Protection Act (DPA), to address the increasing amount of data that is held about an individual.

The regulation itself is deliberately broad, stating that "the principals of data protection should apply to any information concerning an identified or identifiable natural person".

In a report into the effect of GDPR on the Internet of Things, CCS Insight has suggested that information such as IP addresses, vital sign data and indeed tracking data using mobile network connections will all be covered under GDPR's scope.

Personally Identifiable Information includes, but is not limited to:

- Name
- Address
- Email address
- Telephone number
- Bank account details
- IP addresses
- Video surveillance footage
- Location tracking data & history
- Geo-fencing data
- Wearable technology data

There are also specific rules around the processing of 'sensitive personal data', such as healthcare, financial and children's data.

THE BREAKDOWN OF BOUNDARIES

Once enforced, GDPR will be able to transverse national boundaries - meaning its reach will extend across the world, rather than in Europe alone.

This is because the regulation applies to the personal information of all European citizens and residents, no matter where they - or the organisations controlling and processing their data - are based.

REACTING TO A BREACH

In the event of a data breach, GDPR states that the controller should notify the appropriate supervisory authority 'without undue delay and, where feasible, not later than 72 hours after having become aware of it'. In the UK, this authority is the Information Commissioner's Office (ICO).

If a processor becomes aware of such a breach, GDPR states that they should notify the controller 'without undue delay'. As well as notifying the appropriate authority, GDPR states that data subjects should be contacted by the data controller 'when the personal breach is likely to result in high risk to the rights and freedoms of natural persons'.

EXCEPTIONS TO THE RULE

To avoid notifying the appropriate supervisory authority, your data breach must be 'unlikely to result in a risk to the rights and freedoms of natural persons'.

While this statement is ambiguous, circumstances in which this may apply include where pseudonyms are used to a point that neither hackers, nor the controller themselves, are capable of extrapolating anything meaningful from the data.

Another example may be that the data is securely encrypted. The legislation does provide guidance on the circumstances in which data subjects do not need to be notified; citing three specific criteria:

1. That the controller has implemented 'appropriate technical and organisational protection measures' and applied them to the affected data, such as encryption

2. The controller has taken measures to ensure the risks to the rights and freedoms of those affected are not likely to materialise

3. It would involve 'disproportionate effort' to notify those affected individually, in which case measures such as a public communication should be used

PENALTIES FOR NON-COMPLIANCE

Organisations found to have breached GDPR will be faced with a two-tiered sanction regime. An article by Out-Law, a part of international law firm Pinsent Masons, states that breaches of provisions 'which law makers have deemed to be most important for data protection' could lead to fines of up to €20 million or 4% of global annual turnover.

€20 MILLION

THE FINE SERIAL OFFENDERS COULD FACE UNDER GDPR

Other breaches could see fines up to €10m or 2% of global annual turnover imposed.

While these fines are maximums, to be considered in extreme circumstances, they are greatly increased compared to current UK fines, which do not exceed £500,000 under the DPA.

A DRIVER FOR CHANGE

While many businesses will not have viewed previous regulations and fines as severe enough to provoke change, GDPR's widened scope and heftier penalties will cause them to reconsider their stance.

Gemalto's 2016 Breach Level Index Report revealed that, out of over 1.3 billion breached records in 2016, only 4.2% of data was encrypted. We expect to see this level rise in 2018 and beyond, as GDPR takes effect.

4.2%

Only 4.2% of breached records were encrypted in 2016

Gemalto

THE IMPACT ON YOUR BRAND

In the face of a more structured process for handling a breach, which involves notifying both authorities and those affected, as well as more severe fines, it's imperative that all organisations that may be impacted by GDPR address the legislation fully.

However, there is a third, more unknown quantity that organisations must face in the event of a breach; the impact on their brand reputation. Loss of customer confidence in the face of bad publicity is likely to far outweigh the cost of any fines going forward.

YOUR JUSTIFICATIONS FOR PROCESSING DATA

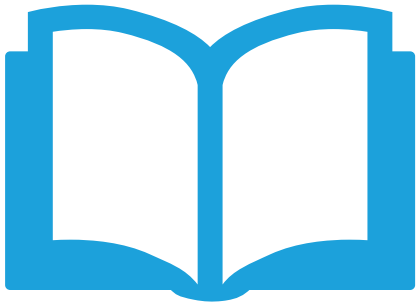
The ambiguous regulation of the DPA gives way to specific, tighter laws about what data is collected, for what reason, and what it will be used for.

Justification for processing must be "specific, informed, explicit, given either by a statement or by affirmative action, and freely given."[4]

This means that a general acceptance of terms and conditions, and a generic privacy policy page on a website, will no longer count as giving consent. ***Organisations need to define what data will be collected, what purpose this is for, and what processing will apply.***

The controller also needs to be able to prove that consent is valid, meaning it cannot be given with a pre-checked box. This consent expires once the purpose of collecting that data has been fulfilled.

[4]CCS Insight



YOUR DATA MANAGEMENT & STORAGE

Under GDPR, an organisation must take steps to ensure their data is adequately catalogued, only used for the purpose for which it was collected, and ideally held securely – be that through pseudonymisation and/or encryption.

The regulation also states that organisations must appoint a Data Protection Officer (DPO) – who may be a member of staff, contractor or trade body – if they:

- **Are a public authority**
- **Carry out large scale systematic monitoring of individuals (e.g. online behaviour tracking)**
- **Carry out large scale processing of special categories of data, or data relating to criminal convictions and offences**

Only companies with fewer than 250 employees, who don't process data on a large scale, are exempt from record keeping under regulation.

In their role, a DPO is responsible for the implementation, testing and ongoing validation of systems and processes implemented, as well as to keep data secure and ensure compliance with GDPR.

They must also work with public bodies, be drafted into any and all strategy involving the collection, processing and storage of data, and act as the first point of call in the event of a breach.

THE RIGHT TO BE FORGOTTEN

Perhaps the biggest challenge of GDPR is addressing people's right to be forgotten. Under the regulation, data subjects have the right to withdraw consent to use their personal information and have an organisation dispose of it.

The most challenging part of the right to be forgotten is that organisations must not only ensure they remove this information from their own databases, but that this request is extended to any and all third parties they have shared this data with.

As and when organisations do receive such a request, they must respond without undue delay (and within one month in any event), although this can be extended in difficult cases.

BYOD: Bring Your Own Device - part of the larger trend of IT consumerization, in which consumer software and hardware are being brought into the enterprise.

Source: TechTarget

COPE: Corporate Owned Personally Enabled - a business model in which an organization provides its employees with mobile computing devices and allows the employees to use them as if they were personally-owned notebook computers, tablets or smartphones.

Source: TechTarget

YOUR DEVICE POLICY: BYOD VS COPE

GDPR may also influence organisations' Mobile Device Management (MDM) policies. In both BYOD and COPE environments, they will need to ensure that business data flowing to and from these devices is classified, secure and in compliance with the regulation.

While COPE allows for tighter control, with organisations able to 'lock down' and control devices, BYOD means hardware is left more open by default. This doesn't, however, mean that BYOD becomes obsolete under GDPR.

Information published by the ICO advises having a clear policy in place, ensuring data is transferred and stored securely, and establishing how to control devices (through MDM software, for example), are all elements to be considered when addressing BYOD.

While this information was originally published with the 1998 Data Protection Act in mind, much of it is still applicable under GDPR.

Rather than this acting as a barrier, it's our opinion that GDPR is an enabler for mobility because it ensures the data flowing between your mobile devices is completely secure.

THE IMPACT OF INACTION

With GDPR influencing so many elements of how data is controlled and processed, organisations will undoubtedly question what would happen if they were to simply do nothing around compliance before GDPR comes into force.

The truth is that these regulations will apply to organisations irrelevant of if they choose to conform or not.

Non-conformance will simply put organisations at a disadvantage to those that do have the correct policies in place.

It's also likely that customers will begin enquiring about the GDPR compliance as part of their due diligence process to ensure that their own compliance is not impacted by a non-compliant supplier.

Choosing not to act on GDPR also places organisations at a much higher risk of breaches occurring, and is likely to face greater fines and penalties if they are found to have purposefully ignored the regulations.

Simply put, GDPR cannot be treated as 'the elephant in the room'.

THE IMPORTANCE OF PRIVACY BY DESIGN

One main school of thought that GDPR will install in digital organisations is that of 'privacy by design'. This means that 'controllers must implement appropriate technical and organizational measures and procedures' to ensure that data is safeguarded by default, and only the minimum and necessary information is collected.

Unfortunately, not all applications to-date have been built with Privacy by Design in mind, meaning organisations will need to consider how legacy applications used to process and store data will be brought in line with the new rules.

> "Privacy by design is an approach to projects that promotes privacy and data protection compliance from the start."
>
> Information Commissioner's Office

THE REGULATION IN PRACTICE

EXAMPLES OF HOW GDPR WILL IMPACT EVERYDAY BUSINESS SCENARIOS

To help you visualise the effects of the regulation, we've put together a number of situations that your business may face and how GDPR will influence these scenarios.

BREACH SUFFERED: ENCRYPTED VS UNENCRYPTED DATA

Setting the scene: You've discovered that your organisation has suffered a data breach and now you must act according to GDPR regulations. In one circumstance, your data is securely encrypted – but in the other, it isn't.

UNENCRYPTED DATA		ENCRYPTED DATA
You discover that your organisation has been breached	1	You discover that your organisation has been breached
You need to work quickly to uncover the extent of the breach	2	You need to work quickly to uncover the extent of the breach
You find that unencrypted personal information has been breached, and must now notify the appropriate regulatory authority (such as the ICO) within 72 hours as instructed under Article 33	3	Check your compliance against Article 33 of the GDPR – is your breach likely to 'risk the rights and freedoms of natural persons'? As your data is encrypted, the answer is 'no' and therefore the regulatory authority need not be informed
You must then, without delay, notify those whose information has been breached as outlined in Article 34 - an exercise involving a large amount of time and resource.	4	Similarly, securely encrypted data means you need not inform the data subjects affected by the breach, as stated in Article 34
You must continue working on the measures you've proposed to take to deal with the breach and mitigate the risk of further breaches. Be prepared to face potential fines.	5	Internally, you should address the security flaws that made the breach possible

THE REGULATION OF SHADOW IT

Setting the scene: Your staff utilise a number of platforms that are not monitored, managed or approved by your IT department. This practice is called 'Shadow IT', and is one that should be strictly controlled by company policies, if not ended, under GDPR.

SHADOW IT PRACTICED		SHADOW IT NOT PRACTICED
Your staff are using a 3rd party video conferencing application to share sensitive customer information with colleagues	1	All your employees are using a video conferencing application that's approved and fully-controlled by your IT department
This platform suffers a security breach and cyber criminals are 'listening in' to your conferences, or manage to steal the stored recording	2	You've implemented Mobile Device Management to ensure no 3rd party apps are used
If this information is likely to breach the rights and freedoms of your customers, you must inform the appropriate regulatory authority	3	Your staff can use conference facilities safe in the knowledge that shared information is secure, managed and encrypted
You may also have to notify your affected customers	4	Should you suffer a breach, it's easier to monitor, manage and rectify
You must deal with the breach and mitigate the risk of any further breaches as per your breach announcement, and be prepared to face potential fines.	5	Because your information is encrypted, it's unlikely that you'll need to write any breach notifications

INTERNATIONAL BUSINESS HOLDING EU CITIZEN OR RESIDENT DATA

Setting the scene: As a consumer, you purchase an item from a US retailer serving the European market. Unfortunately, the retailer suffers a breach and your personal data is stolen. What happens?

1. You purchase your item from the US multinational, submitting personal information including your name, address and bank account details
2. Your personal information is stored on that company's server within the EU
3. The retailer suffers a breach, through which your information is stolen
4. They need to notify the appropriate regulatory authority and persons affected if their rights and freedoms are at risk
5. They then must deal with the breach and mitigate the risk of further hacking as per their announcement, and must prepare to hear from the regulatory authority regarding potential fines.

"Compliance is a top data protection priority for 92% of US organizations in 2016, with 77% planning to spend $1 million or more on GDPR."

Source: PwC

THE ROAD TO 2018: WHAT YOU NEED TO DO

GET A TEAM IN PLACE

Getting ready for GDPR needs to involve people across departments – including IT, Legal, Marketing, Finance and C-Suite. Each will have its own actions, so ensuring your people are informed and working together is key. It's also time to establish if you need a DPO.

SECURITY ASSESSMENTS

Establish **what data you hold, where it's stored and if it's suitably protected**. This should include your Mobile Device Management practices and policies. Produce reports that identify gaps in your security.

ENABLE ADVANCED DETECTION

Consider the impact of 'advanced threat detection' services that give you the ability to detect suspicious behaviour and react to **zero-day** threats that traditional security systems may miss.

ONGONGING REVIEW

Going through this process doesn't mean you're done. You need to subject your policies, security and responses to **continuous review**. You'll also need to consider how future policy changes will impact on your data management and processing.

EVALUATION AND PLANNING

Enter a **discovery process** to understand how your organisation will be affected based on the data you hold. This will help you plan your processes and form the basis of your security assessments. Audit the information you request to ensure no superfluous data is collected.

IMPLEMENTING PROTECTION

Liaise with partners to **implement** and **manage** solutions that will meet your security needs and ensure compliance. Solutions you may need to put in place include next generation firewalls, intrusion detection systems and MDM platforms.

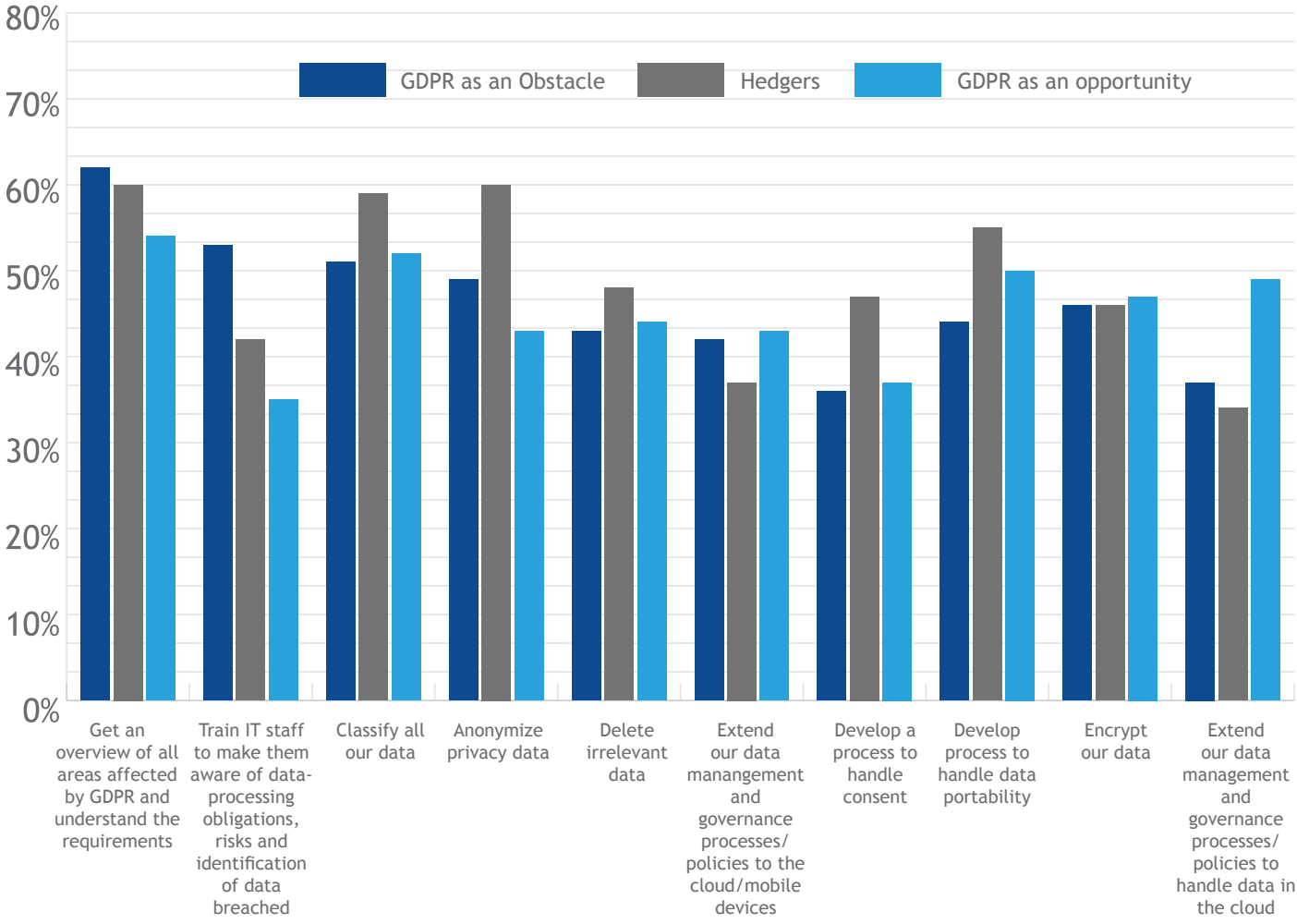
SCENARIO PLANNING

Run through 'what if' situations and develop a mature **incident response** that covers how you'll react to a security breach, how you'll handle your key systems and data, and what you'll do to mitigate the risk of further breaches.

WHAT ARE OTHER COMPANIES FOCUSING ON?

There are no businesses in Europe, and few across the world, that do not process the data of individuals based in the EU in one way or another. As a result, GDPR applies to businesses virtually everywhere.

What are Companies Focusing on?



Source: IDC EMEA GDPR Survey 2017.

Research conducted by IDC, taking into account the viewpoints of those that see GDPR as an opportunity, an obstacle and are hedging their bets, has revealed that the majority of companies are focused on starting with the basics – getting an overview of GDPR, educating staff and classifying their data.

More specifically, those that view it as an obstacle are focusing more on training IT staff around data breaches but are less inclined to educate staff on GDPR's impact.

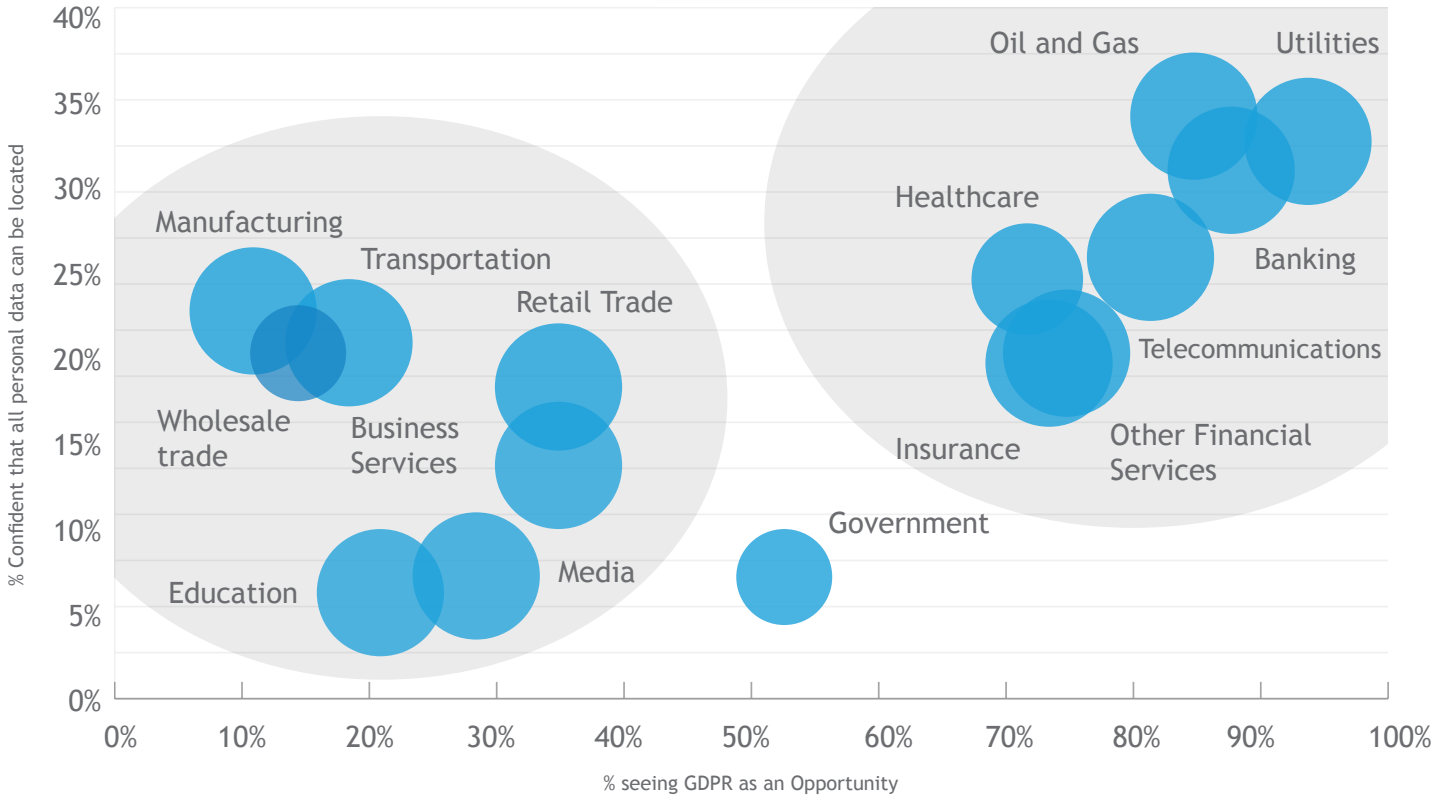
Those hedging their bets are also focused on the IT-elements of the regulation, but are also keen to anonymising data and deleting irrelevant records.

Finally, opportunists are focused on the detail requirements including the development of processes, extending information governance and encrypting data.

HOW READY IS YOUR INDUSTRY?

There are no businesses in Europe, and few across the world, that do not process the data of individuals based in the EU in one way or another. As a result, GDPR applies to businesses virtually everywhere.

GDPR Readiness by Industry



Source: IDC EMEA GDPR Survey 2017.

IDC's research also revealed the readiness for GDPR by industry. Perhaps unsurprisingly, the banking, telecoms, utilities and oil & gas industries are opportunists that are confident in their compliance with GDPR.

Conversely, education and media companies appear to be viewing GDPR as more of a hindrance, and are not confident in their compliance with the regulations.

CONCLUSION

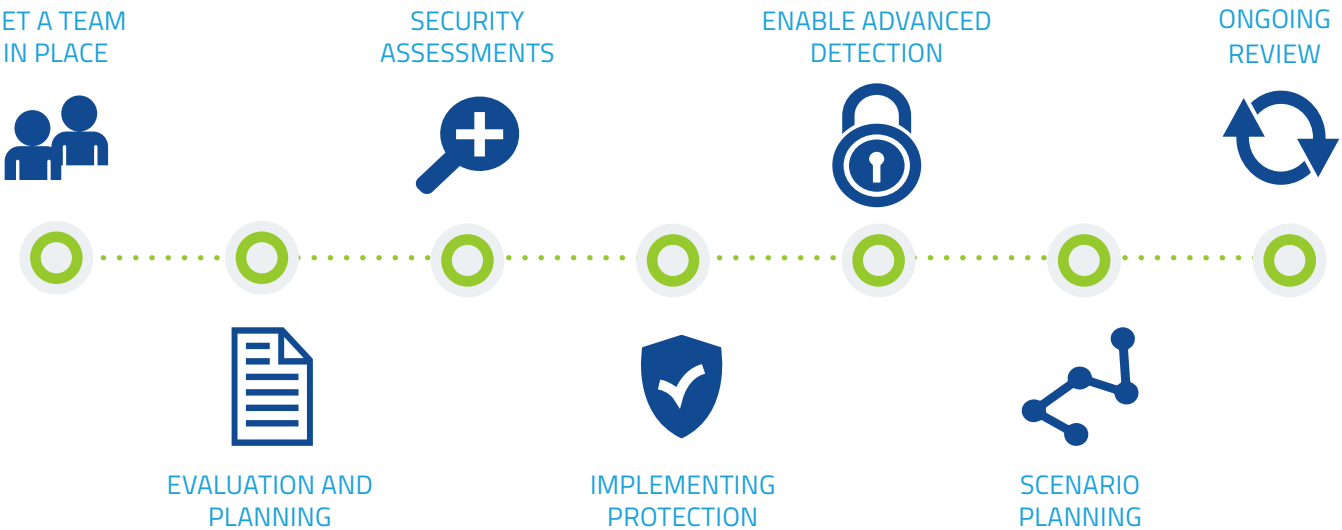
Whether you see GDPR as an opportunity to improve, or a barrier to your everyday activities, the regulation is coming into force and will impact the way you collect, process, use and store data.

When it comes to enterprise mobility, GDPR should not be viewed as a barrier that must be overcome simply to ensure compliance. Instead, it should be considered an investment that delivers tangible, long-term business benefits and ensures that your organisation's sensitive data is fully secure.

Looking to the immediate future, we predict a shift in urgency throughout 2017 and early 2018 as organisations in unprepared industries look to understand these regulations and move toward compliance, while more prepared companies will continue along the path of implementation and testing.

Finally, we do not believe that it's 'too late to start' along the process of compliance if you haven't done so already, and would encourage you to begin the steps outlined in this document so that you can begin to understand how GDPR will impact your organisation.

THE ROAD TO 2018



ABOUT CHARTERHOUSE

Charterhouse Voice & Data is a multi-award-winning solutions integrator of Unified Communications, Document Management Services and Enterprise Security and Mobility. We're passionate about delivering genuine value to our customers and strive to exceed expectations in everything we do.

We work with organisations to help them prepare for the GDPR across a range of industries and help establish what the technological implications of the regulations will be on their business.

If you would like support in preparing for the GDPR, please contact us on 020 7324 7470 or email gdpr@cvd.plc.uk.

Further information on GDPR regulations can be found on the **ICO website**.

CHARTERHOUSE
VOICE & DATA

5 Chapel Place, Rivington Street, London, EC2A 3SB
Tel 020 7613 7400
www.cvd.plc.uk