In 2018, the EU will enact its GDPR data security legislation into law. It includes a number of significant changes, and far stricter rules on how to comply. With the penalties dramatically increased, making sure you’re prepared for the GDPR has become imperative.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Risks to the enterprise – a boardroom topic</td>
<td>4</td>
</tr>
<tr>
<td>What you need to know</td>
<td>5</td>
</tr>
<tr>
<td>Penalty case study: TalkTalk</td>
<td>6</td>
</tr>
<tr>
<td>What should CIOs be focused on?</td>
<td>7</td>
</tr>
<tr>
<td>Common mobility gaps</td>
<td>8</td>
</tr>
<tr>
<td>Breach case study: CardCrypt</td>
<td>9</td>
</tr>
<tr>
<td>Enterprise mobile security</td>
<td>10</td>
</tr>
<tr>
<td>What about Wandera’s own adherence to GDPR?</td>
<td>11</td>
</tr>
</tbody>
</table>
INTRODUCTION

The key aim of the European Union’s General Data Protection Regulation (GDPR), which comes into effect in May 2018, is to give EU citizens greater control and protection of their personal data. It also aims to provide a common regulatory framework for international businesses operating in the EU.

Perhaps most importantly, the provisions extend to non-EU companies processing data of EU citizens, meaning its effects will be felt at most global businesses - including many of those in a post-Brexit United Kingdom.

Whilst the common framework has some benefit to global enterprises, there are new gaps to fill and massively increased financial penalties and risks for non-compliance.

This paper is designed to help businesses manage their mobile data risks in relation to GDPR, which will affect almost every global organisation.

“Firms are in denial about tough new EU privacy law: The world’s toughest privacy law will go into force in Europe 18 months from now, and so far, the strategy of many IT professionals appears to be “pretend it’s not happening.”

DR. RACHEL O’CONNELL
CEO AT TRUSTELEVATE.COM
RISKS TO THE ENTERPRISE – A BOARDROOM TOPIC

The new regulations bring two specific risks to the table which all boards should be considering when planning their approach to the new regulations.

Reputation risk
Companies must disclose data breaches to regulators and in certain circumstances to affected individuals, within 72 hours of their occurrence. This has the potential to be catastrophic in terms of business reputation and shareholder value.

Financial risk
Non-compliance can lead to very significant fines, potentially rising to 4% of worldwide turnover. In the UK for example, this greatly exceeds the current maximum of £500,000. This means that if data breaches remain consistent, the fines paid to the European regulator could see a 90-fold increase, from £1.4bn in 2015 to £122bn after the legislation comes into effect.

- €20m new limit for fines; or
- 4% share of total revenue, whichever is higher
- 90x potential rise in fines for failure to comply

Boards will want to ensure that these risks are appropriately managed and CIOs should be actively preparing now to meet these head on.

“Maximum fines are now up to €20 million or 4% of global annual turnover, whichever is the greater, meaning things could soon get very ugly indeed. Any such penalties will certainly have to be consistently applied by all supervisory authorities for all equivalent breaches or face potential counter challenge themselves, which would all get rather uglier still.”

ANGUS MACRAE, INFORMATION SECURITY MANAGER
WHAT YOU NEED TO KNOW

More kinds of data

Fundamentally, the GDPR applies to ‘personal data’. The working definition for this is that it encompasses anything that includes any kind of online identifier or uniquely singles out a living person on its own or in conjunction with other data. An IP address or geolocation data are both considered personal data in the GDPR rule book.

This even applies to personal data that has been pseudonymised, if the company is not careful about how easy it is to attribute this to particular individuals.

Extended definition of breaches

While previously a breach was focused on events that involved the ‘loss’ of personal data, the new legislation considers a security breach to include the destruction, loss, alteration, unauthorised disclosure of, or even access to, personal data. The range of events that fall under the remit of the GDPR is far greater than ever before.

Lower threshold for severity

Under existing law in the UK, breaches are only penalised if it can be demonstrated that those that have had their personal data exposed have received actual harm or financial loss. The GDPR instead broadens this to any kind of distress, meaning far more security events will soon be under scrutiny.

Being unprepared can result in fines

One of the biggest changes that GDPR will bring is that fines can apply even to situations in which a breach has not occurred. The Supervisory Authority in the UK will be able to penalise any business that fails to observe the principles of the GDPR. That will most likely mean that punishments can be given to non-compliant organisations, even if no security event has taken place.

Less time than before

The GDPR is also stricter on how long companies have to alert the authorities in the case of a breach. There will be a compulsory requirement to inform the Supervisory Authority no longer than 24-72 hours following a breach. Falling foul of this deadline could result in the full administrative penalty of 4% of turnover.

It applies everywhere

The GDPR is applicable to any company that holds personal data on citizens in the EU. Almost every global organisation should be preparing itself for the new legislation, and introduce new measures to ensure compliance.

“UK-based businesses cannot afford to ignore GDPR despite the fact the country has voted to leave the EU.”

DR KUAN HON
CYBERSECURITY EXPERT AT PINSENT MASONS
PENALTY CASE STUDY: TALKTALK

The Information Commissioner’s Office (ICO) is the body responsible for enforcing the Data Protection Act (DPA), the piece of legislation that UK companies must adhere to up until GDPR comes into effect. The new GDPR regulations will supersede national acts such as the DPA, and even for companies operating in the US or elsewhere, if it stores or makes use of personal data on any individual in the EU, it must comply with the GDPR.

This year, the ICO investigated the case of TalkTalk, a UK telecommunications company that had been found liable of failing to sufficiently secure its data. In 2015, a cyber attacker had been able to access customer data ‘with ease’. It determined that the firm could have taken basic steps to prevent the attack from occurring.

Ignorance about the vulnerability was not enough - TalkTalk were unaware of the exploit, which could have been fixed had it been detected. Effectively, it was decided that TalkTalk failed to have appropriate security measures in place, and was thus in violation of the Data Protection Act.

“Cyber security is not an IT issue, it is a boardroom issue. Companies must be diligent and vigilant. They must do this not only because they have a duty under law, but because they have a duty to their customers”, said Elizabeth Denham, Information Commissioner at the ICO.

The breach only affected 4% of the firm’s customers, but the consequences were severe. One year after the breach, TalkTalk were fined £400,000 for the insufficient security practices that led to the success of the attack. Had the new GDPR regulation been in place, this could have been more than €20m.

Moreover, TalkTalk suffered colossal losses in its subsequent fall in share price, as a direct result of the breach. Two weeks before the breach happened on October 21st, the company’s shares were trading at 314p. Two weeks after it, the price had plummeted to just 220p per share, a dip of more than a third and wiping £1bn off the organisation’s market value.

One year after the breach, the stock was still yet to recover, trading at just over 200p a share. Clearly, the impact of a breach can be significant.

“TalkTalk’s failure to implement the most basic cyber security measures allowed hackers to penetrate TalkTalk’s systems with ease. Yes hacking is wrong, but that is not an excuse for companies to abdicate their security obligations. TalkTalk should and could have done more to safeguard its customer information. It did not and we have taken action.”

ELIZABETH DENHAM, INFORMATION COMMISSIONER
WHAT SHOULD CIOS BE FOCUSED ON?

Jim Walker, CIO at Wandera

CIOs need to consider the enterprise risks and must plan to take the following steps ahead of May 2018.

**Step 1: GDPR Assessment**
Familiarize yourself with the regulation and understand your current data protection maturity against the new regulations.

**Step 2: Complete a Privacy Impact Assessment (PIA)**
Assess your current systems and projects to identify key data protection risks.

**Step 3: Establish a Data Inventory**
Know what personal data you collect, process and store, where this happens and who has access. Depending on the complexity of your business, you may need to use a discovery tool to help in this process.

**Step 4: Establish an Improvement Program**
Build a program that addresses your gaps identified in the steps above, but focus on your highest risks and most sensitive data first. Educate your organization on the importance of data privacy. Build new systems and processes with privacy and security incorporated ‘by design’ from the outset.

In summary, start with knowledge gathering, document your current position and your gaps, then address those gaps prioritizing highest risks first.

“It’s a jungle out there when it comes to protecting personal data and privacy”
ARDI KOLAH LL.M, CO-PROGRAMME DIRECTOR, HENLEY BUSINESS SCHOOL
COMMON MOBILITY GAPS

In the world of mobility, innovation happens at a relentless pace. The compromise is that developers have not always embraced the “privacy and security by design” concept.

There are a number of pressing and genuine risks regarding sensitive data, with particular concern to mobility.

- Exposure of customer and employee data. This is due to lack of privacy and security built in to mobile applications and web pages, at both the consumer and corporate level.
- Use of unapproved applications and websites for storing sensitive data.
- Potential for interception of data due to connections to insecure Wi-Fi networks, either by malicious design or by carelessness.

Mobile presents a new frontier for attackers, and is one of the most vulnerable areas for organisations. Many businesses equip their staff with mobile devices, yet will regularly fail to adequately protect the fleet. While some firms are making use of Enterprise Mobility Management (EMM) tools to administer application usage on corporate-owned devices, this level of security leaves dangerous gaps when it comes to preventing data leaks.

“\textit{To avoid disrupting the company too much with major last minute changes, and incurring substantial costs in the process, it is vital that businesses operating in the EU take steps now to move towards compliance with the GDPR. Waiting until early 2018 or even late 2017 will be too late.}”

ANNABELLE RICHARD, DATA PROTECTION EXPERT AT PINSENT MASONS
BREACH CASE STUDY: CARDCRYPT

One data leak incident was uncovered by Wandera researchers in December 2015. The vulnerability was discovered in more than a dozen companies, and included four airlines: Air Canada, easyJet, AirAsia and Aer Lingus.

Each of the companies was found to have been failing one of the most basic of security requirements by not fully encrypting the traffic to the payment portion of their mobile web site or app. This meant that customers who use these services unknowingly may have had their credit card information sent ‘in the clear’, and have been at risk of having that information stolen. Remember, under GDPR a breach does not have to actually happen; a fine can arise even if the company in question merely fails comply with GDPR legislation in general, such as unnecessarily exposing personal data without adequate security measures in place.

All of the identified companies in the CardCrypt vulnerability had exposed the full credit card number unencrypted. Other than Air Canada, all of them also exposed the CVV number. Alarmingly, the amount of additional information that was exposed by some of the companies was significant and included card expiration date, full name, billing address, email addresses and even passport information.

Often in the case of vulnerabilities like those exposed in CardCrypt, communication is not always with the full website, but rather it might be limited to a small number of pages within the site that are unencrypted. These seemingly slip through the development process, and leave isolated pages at risk, such as the upgrade payment pages in this instance.

CardCrypt underlines the relative weaknesses, even within large companies, in securing the whole end-to-end service, and not just the front door, or the main site where users buy tickets.

What CardCrypt demonstrates is that data leakage is real, dangerous and even commonplace in the mobile environment. That global, recognisable enterprises that employ hundreds of IT personnel were at risk of such a major data breach reveals just how exposed many businesses are to data leak events. Under the new GDPR, with its wide-reaching scope and severe punishments, it’s absolutely imperative that organisations invest in data-level mobile security solutions before the legislation comes into effect.
ENTERPRISE MOBILE SECURITY

Whilst the highest risk areas will likely need specific dedicated processes and tools to eliminate risk, the long tail will require tools that take a broad approach to appropriately manage data risk.

Due to our gateway approach, Wandera is uniquely positioned to give you the data and tools required to identify and manage risks from mobile device usage.

Wandera can assist in the discovery phase by providing the data needed to understand mobile use, such as the applications and web sites accessed, as well as who accesses them and from where.

Wandera specifically addresses the key risks associated with mobile device use, all of which could lead to potential data breach.

**Threats**

Know when your organization is under attack, ensuring rapid compliance with GDPR notification deadlines.

**Vulnerability assessments**

Know when your organization has holes that need to be patched before they are exploited, avoiding extremely expensive incidents, such as was the case with CardCrypt or with TalkTalk.

**Data leaks**

Know which applications and sites are not protecting your employees’ private data.

Wandera has also built options that provide you with best in class security as well as options to protect or anonymize data in line with your preferences.

“We believe the only way to ensure compliance with the incoming GDPR legislation is to embrace a mobile security solution that affords total data visibility. Whichever technology you choose to adopt, our guidance is to select a platform that operates at the cloud level as well as the device level, eliminating blind spots and giving you absolute confidence that your organisation is as best equipped as it possibly can be when it comes to reducing risk.”

DR. MICHAEL COVINGTON, VP PRODUCT AT WANDERA
WHAT ABOUT WANDERA'S OWN ADHERENCE TO GDPR?

Ben Oxnam, COO at Wandera

At Wandera we take data privacy very seriously. Our business reputation is dependent on our continuous ability to manage and secure our customers' and our own data.

We've been building our processes and products with security and privacy in mind since day one. We only use globally resilient and ISO9001 compliant data centers in the provision of our services. Our data is logically segregated meaning logs of data related to our customers’ mobile usage can only be matched to user data by Wandera's systems. We've built monitoring tools that give an immediate notification of any potential breach to our own services. Another new feature is Usage Anonymization, which gives pseudonyms in the place of the names of employees, helping our customers stay compliant with regulation if they would prefer to be more respectful of the privacy of their staff.

Like many companies there will be gaps that we will need to address over time. For example, we are awaiting further guidance on the need, or otherwise, to appoint a Data Protection Officer.

In the meantime we continue to put security and privacy at the forefront of everything we do and we are here to assist our customers to do the same.

To find out how Wandera will reduce your organisation's exposure to security risks, request a free demo of the platform.

wandera.com/demo