IMPERVA®

GDPR: New Data Protection Rules in the EU

WHITEPAPER

Authors: Jonathan Armstrong and André Bywater

Cordery®
Legal.Compliance

What's Required and How to Comply

Improving Security to Protect Consumers' Personal Data

The European Union is changing the way it regulates data protection in the wake of large-scale cyber attacks and data loss incidents. Targeted attacks like those that hit TalkTalk in the UK and Anthem Healthcare, Target, and Yahoo in the U.S. have shown that security breaches are a real public concern—impacting millions of customers and damaging corporate reputations in an instant.

At the same time, privacy activists have campaigned for greater protection of personal data. In 2015, the Schrems case successfully opposed the transfer of data on EU citizens to the US. This case invalidated the EU-US Safe Harbor Privacy Principles, creating a major shift in data protection requirements.

The pace of change is set to increase even further with the coming General Data Protection Regulation (GDPR). Enforcement of the GDPR will begin on 25 May 2018, and the new rules apply to all organisations that do any business in the EU or process personal data originating in the EU.

For the reasons explained in this white paper, businesses need to start working towards compliance now. This paper looks at the new data security requirements under the GDPR and provides practical tips on how to prevent a data breach disaster from happening to you and your customers.

Some technical terms are used in this paper. If you are not familiar with these terms, please refer to our glossary.

Data Protection in the EU: a Look Back and a Look Ahead

Data protection, until now, has mainly been regulated in the EU under the 1995 Data Protection Directive (Directive 95/46/EC), designed to control the processing of personal data. EU Member States had to adopt their own national law to implement this Directive. For example, the UK enacted the Data Protection Act in 1998 (known as DPA 1998). These rules have been effective in changing the data security culture in Europe, but the rules also had their critics. Many in Europe looked at US data breach laws as a model for European legislation, a way to expand or augment the existing EU data protection rules.

The new GDPR rules are in the form of a Regulation—imposing data protection standards that should, in theory, be the same in all 28 EU Member States. No further legislation will be required by EU Member States to turn this into law. Enforcement will be the responsibility of each Member State, and unlike past Directives, the GDPR encourages centralised co-ordination of enforcement across the EU. There will be no centralised EU data police.

What are the New Rules Related to Data Security?

Most of the new rules on data security are contained in four articles of the GDPR:

- Article 32: Security of processing
- Articles 33 and 34: Breach notification
- Article 35: Data protection impact assessment

Benefit of Data Minimization, Breach Example: Kiddicare, May 2016

A massive data breach at UK retailer Kiddicare exposes personal data of 794,000 people. The private data was stolen from an unmonitored test server. After several months and multiple customer complaints, an internal incident response effort was unable to detect the source of the breach. A third- party security company confirmed the identity of the breached server. Kiddicare reported the confirmed incident to the Information Commissioner's Office (ICO) and made a statement to the BBC to minimize brand damage. The ICO is investigating the breach.

The new General Data Protection Regulation (GDPR) includes requirements that should improve how companies internally monitor data activity enabling them to both detect and investigate a breach event. Also the use of actual customer data in a test environment illustrates the need for data masking—a data minimization technique that is specifically referenced in the new GDPR guidelines that went into effect in May 2016.

Read the complete report. (Financial Times subscription is required)

Example narrative provided by Imperva, Inc.

We will look at each of these articles in detail. It is important to say that the GDPR is a lengthy 88-page document, and it is not written in the most clear, helpful language. We have simplified much of the terminology in this paper to provide a user-friendly reference. We do, however, recommend that IT and compliance professionals read the full GDPR text, which is more detailed. You will find a link to it at the end of this paper.

Making sure that personal data is secure is the cornerstone of the new regulations. The GDPR also introduces two new security breach reporting requirements—including reports to the regulators and reports to any individual whose data has been compromised.

There is wide definition of "*data breach*" under the GDPR. It includes destroying, losing, altering, or improperly disclosing personal or sensitive personal data. A data breach can include data in transit or data at rest.

Article 32: Security of Processing

Article 32 is the main provision which sets out what companies must do to secure personal data.

In many respects the data security provisions in Article 32 are similar to those in the 1995 Data Protection Directive as well as local data security laws in each EU Member State. In Article 32, there is a complicated definition of the data security responsibilities, but in simplified terms, it says that those handling data, for example, data controllers and data processors, need to introduce appropriate technical and organisational measures to secure the data. This assessment will need to consider the technology that is available, implementation costs, the type of data, and how it is being processed.

Article 32 then says that some of these technical and organisational measures should include:

- Systems and processes to ensure data remains confidential
- Systems and processes to ensure data can be restored if there is an incident
- A process for regularly testing and assessing your data security measures

In addition, organisations, should consider their other obligations under the GDPR. For example:

- Is it necessary to store the data in the first place?
- Does the business know that real data should not be used to test new systems?
- Is the data out of date?

As with similar provisions in existing law, for example principle 7 of the DPA 1998, the test under Article 32 is likely to be retrospective and objective. This means that if there is a breach, the regulators are likely to ask themselves if there was any data security technology that could have prevented the breach. If so, the company will have to come up with very strong reasons why this technology was not implemented. Saying you did not know about it, or your company did not budget for it, is unlikely to be a suitable defence.

Article 32 also emphasises the need for a process of regularly testing, assessing, and evaluating security measures. Again this is similar to existing legislation and codes of conduct issued by data protection regulators. For example, the Dutch data protection regulator has said for any data breach plan to be effective, it must be tested at regular intervals and improved as necessary.

Article 32 requirements include both technical and organisational measures. We already know that good information security depends on good people and good technology. The GDPR emphasises this as a legal requirement.

How Might the GDPR Work in Practice?

Cases under the existing data security laws show how the GDPR might work in practice. For example, in September 2015 the UK Data Protection Regulator, the Information Commissioner's Office (ICO) took action after an airline had a data security breach—even though it was a relatively small incident.[1] It happened when a temporary employee emailed a scanned picture of an individual's passport to his personal email account. The temporary employee had not been trained, and yet he had the same access privileges as permanent employees who had undergone background checks before they were given access to the database. The ICO determined that the airline should have put basic controls in place, and as part of the regulatory settlement the airline agreed to introduce a new policy of categorising data and establishing different levels of security protection that would apply to each category.

In a second example, the ICO took action against the UK government-owned non-profit Student Loans Company (SLC) after a series of data breaches that exposed customers' records.[2] The ICO determined that proper data breach detection measures were not in place and that SLC's processes left private documents even more vulnerable than less sensitive data. The organisation was ordered to improve its processes, install new software, and implement a new employee training program.

Article 33: Breach Notification to the Regulator

Article 33 says that data breaches have to be reported to the relevant regulator, "*without undue delay*" and in most cases not later than 72 hours after becoming aware of the security breach. There are some exemptions, but these are likely to be limited in practice.

There is a separate definition of supervisory authority in the GDPR. We can expect some guidance on how reports will have to be made, but it could be the case that a company will have to submit reports to each of the data protection authorities in every member state where individuals, who are likely to be "*substantially affected*" by the breach, reside. Organizations will also have to report to their home data protection regulator. Data processors also have to notify data controllers, "*without undue delay*" after becoming aware of a data breach.

Article 33 also specifies what type of information the notification must include. Again, we could see differences across Europe as some data protection authorities already have their own procedures for notifying a data breach. At minimum, the type of information that a data protection authority will expect will include:

- Nature of the breach
- Type of breach
- Type of data affected

[1] https://ico.org.uk/action-weve-taken/enforcement/flybe/

[2] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2014/05/student-loan-company-rapped-after-data-breaches/

Benefit of breach detection and investigation capabilities

Breach Example: Sage Group Ltd., August 2016

A concerned privacy consult outs a Sage Group PLC (SGE:LSE) data breach on August 13, 2016, after Sage refuses his calls. The reluctance to acknowledge the breach was well founded. The London Stock Exchange responded to the breach news with a four percent drop in the Sage stock price while no less than six global news and security organizations including the Financial Times published articles highlighting the Sage breach.

The personal details and bank account information for employees of as many as 300 large UK companies may have been part of the breach. Sage is unable to confirm the extent of the breach or pinpoint what was stolen. A malicious insider is presumed to be the person responsible for the breach.

This breach is a clear example of miss-placed trust. The absence of sensitive data and privileged user monitoring created an environment where a malicious employee was able to scan and amass private data under Sage's protection. Under the current UK privacy laws, the UK Information Commissioners Office will have limited ability to penalize Sage for failing to protect the data. Under GDPR the official investigation and penalty phase would prove significantly more daunting with penalties as high as €10m or 2% of worldwide annual turnover of proceeding year, whichever is higher.

Read the complete report. (Financial Times subscription is required)

Example narrative provided by Imperva, Inc.

- Approximate number of people affected
- Approximate number of records affected
- Name and contact details of the data protection officer or another contact point for information
- Consequences or projected consequences of the data breach
- Measures taken or proposed to address the breach

Article 33 also reminds companies that they will need to keep proper records available for inspection.

It will be difficult to make a report within the 72-hour deadline, especially if the report has to be made in different formats to different regulators in different languages. To have a chance of complying, businesses will need to be able to detect, report and analyse breaches quickly—ideally in a format that regulators can easily understand. A good firewall and good compliance monitoring tools will be essential. At minimum, businesses will need systems that:

- Monitor activity and detect threats
- Issue threat alerts, quarantine and block attacks, and stop unauthorized activities immediately
- Identify unusual uses of data
- Make it easy to flag issues quickly
- Identify, tag or rank data based on its sensitivity level
- Produce reports—perhaps in different formats for different recipients
- Make these reports easy to use and understand
- Maintain and store records in the event of a GDPR audit or review

It is important to remember that this obligation to report to a data protection regulator can work in parallel to other data breach reporting obligations—for example financial services and the health sector may already have an obligation to report a breach. Telecoms and similar companies already have a general data breach reporting requirement under another EU Directive. In addition, some EU countries, including Germany, Austria and The Netherlands have introduced their own data breach reporting requirements.

We are likely to see a significant number of data breach reports under Article 33 when the GDPR is first enforced. We saw this when The Netherlands introduced a similar requirement to Article 33 in their legislation in January 2016. They received more than 1,500 notifications in the first four months with around 70 regulatory actions ensuing.

How Might This Work in Practice?

A case in April 2016 shows the need to act quickly. In this case EE Limited, a telecom company, received a call from a customer who said that he thought he had been the victim of identity fraud. EE received the call on 14 January 2016. The customer service representative reported the incident to their line manager by email the same day but they didn't report the matter to EE's internal security team. The line manager came back to the office on 18 January 2016 when he told the

security team, and they told the ICO. The ICO found that EE had violated a data breach reporting law that already exists for telecoms companies which in some respects is similar to Article 33. The ICO imposed a monetary penalty for failure to make the notification quickly enough.[3]

While only one customer may have been impacted in this data breach, it suggests that regulatory bodies are taking even small incidents seriously. We can only imagine the implications for a larger data breach.

Article 34: Breach Notification to the Affected Individual

Article 34 contains a second data breach reporting provision, requiring organizations to notify the victims whose data was stolen, lost or compromised.

This obligation applies in cases where the breach is likely to result in, "*a high risk to the rights and freedoms of individuals*". Again, the individuals impacted must be told about the data breach without "*undue delay*", but the 72-hour time limit does not appear here.

The communication must be in clear, plain language, and the same sort of details will have to be in the communication to victims as those provided to regulators under Article 33. However, the Article 34 communication is not necessary if:

- The data remains secure due to protective measures like encryption
- Subsequent measures successfully protected the data from being stolen or exposed
- Identifying and notifying all victims would involve "*disproportionate effort*"

If you're relying on the "*disproportionate effort*" exemption, then there will need to be public communication such as a newspaper advertisement instead. When a company is considering making a report through public communication, data protection authorities may assess the circumstances and add their own additional requirements. In some cases, for example, the authorities may require notifications to be sent directly to individuals impacted by the data breach.

Article 35: Data Protection Impact Assessments

In addition to reporting data breaches, the GDPR requires organizations to do more to stop breaches from happening in the first place. Article 32, which we've looked at already, is part of that. But Article 35 takes it further by introducing a new requirement to do a Data Protection Impact Assessment (DPIA) when adding "*new data processes or new technologies*". DPIAs have been around for a time—they were also called Privacy Impact Assessments or PIAs—but the GDPR makes them mandatory in some circumstances. A DPIA is a type of risk assessment of the impact of the new processing activities or technologies on the protection of personal data. A data protection regulator will also have to be consulted prior to personal data being processed where an assessment, "*shows that the processing would result in a high risk if measures are not taken to reduce that risk*".

Most organisations will need to set up policies and procedures for undertaking DPIAs, and while this may seem to be a compliance burden, it's best to consider DPIAs as enabling you to get a better grasp on your data processing and to reduce risk. The assessment will likely require you to identify the databases used to store personal data or sensitive personal data. Once identified and categorized, you must make sure these databases are secure.

[3] https://ico.org.uk/action-weve-taken/enforcement/ee-limited/

Consequences

Under the GDPR, data protection regulators will have the power to impose high fines for failure to comply with the new rules. Three different levels of fines will be applied in relation to three different categories of infringements. The highest level is either a maximum of €20 million ($xxx U.S.) or 4% of the global annual turnover or revenue of the offending organisation, whichever is greater. When setting the fines, the model being adopted is similar to the existing EU competition/anti-trust enforcement regulations. In some respects, much of the GDPR has been inspired by the EU's success in competition and anti-trust law enforcement. Since 2012 alone, the EU has levied fines of almost €6 billion for unfair or monopolistic practices. This is an enforcement model that the creators of the GDPR want to emulate.

Given the potentially higher fines for infringements, the data protection compliance drive for businesses will now be more important than ever. GDPR fines may be levied anytime after the May 2018 enforcement date. In the meantime, other countries with their own existing privacy laws will continue to issue fines for privacy and security violations.

What About Other Liability and Compensation?

In the US, one of the emerging trends we have seen is the rise in class action law suits following a security breach. It is important to remember that the GDPR strengthens the opportunity for people affected by a data breach to initiate their own court proceedings.

Under the new rules, any person who has suffered "*material or non-material damage*" due to a privacy infringement has a right to compensation from the organisation that caused or failed to prevent the damage. Important legal issues in this area have been before the courts in the UK case of Vidal-Hall. This case sets a precedent allowing people affected by breaches to get together to claim compensation. In addition, Austrian proceedings against Facebook have been brought by Max Schrems. View the summary of progress in that case.

Because of the added costs a data breach may now bring under these new rules, businesses will need to do everything within their power to minimise the potential for damage claims.

New Cyber Security Directive

In addition to the GDPR, the EU has passed a new Cyber Security Directive, known as the NIS Directive, in July 2016, which will mean additional cyber security laws across the EU by May 2018.

The new EU Cyber Security Directive is more focused on EU Member States, requiring them to improve their national cyber security capabilities and improve co-operation between Member States to fortify cyber security across the EU. This Directive will also affect EU-based businesses as appropriate security measures will need to be put into place, and incidents will have to be reported to national authorities by operators of essential services and providers of key digital services.

Unlike the GDPR, the NIS Directive does not impose breach notification obligations on everyone. It is focused primarily on operators of critical infrastructure in certain sectors, including financial services, transport, energy, water, and health—so-called "*essential services*"—along with enablers of Internet services such as online payment, cloud computing and search engines. Since this is a Directive, not a Regulation, there will be local differences in how this law is applied across Europe, and UK implementation could be affected by Brexit.

Action Plan

The new rules will bring a high level of compliance obligations–with significant financial, administrative, and resource costs, including IT. Although enforcement of these new laws doesn't begin until 2018, organisations will need the time to ramp up data security. The following are ten compliance practices to start implementing now:

1. Put a data breach notification plan in place, including intrusion detection and threat response capabilities.
2. Review your insurance coverage–breaches are costly and the GDPR will increase that cost.
3. Research and deploy data security solutions. You will need to have the right technology in place to keep data secure, facilitate compliance audits, and create reports when a breach happens.
4. Thoroughly review vendor contracts. You will need your vendors' help, especially since you need to report security breaches very quickly. Make sure that you have the contractual rights to insist on this and make sure that you can hold your vendors and their sub-contracted data processors accountable. It would also be wise to insist your vendors use dedicated software and hardware to prevent and report breaches and certify their compliance to a recognised international standard.
5. Prepare to update all data collection, processing, security and data destruction processes. Be sure to keep detailed documentation and records ready for regulatory inspection or compliance audits–and factor this into your business overhead and annual operational costs.
6. Review the data you store and analyse your policies on data handling, including test data usage, data retention and destruction. Minimising data storage–will be key under the GDPR.
7. Consider appointing a data protection officer. It could even be mandatory under the GDPR, depending on what your business does. Regardless, you'll definitely need someone to manage security audits and be on hand to deal quickly with regulators after a breach.
8. Develop a Data Protection Impact Assessment policy and process.
9. Communicate with your board and senior leadership. They too need to know how to react to a security breach–and quickly.
10. Train your staff on all of the above. This includes practicing your data breach response plan, just as you would a fire drill.

Conclusions

We are already seeing a number of businesses change their practices and behaviours as a result of the GDPR. It is certain that data security will have a much greater prominence and is a now top priority on the agenda of most boards. Given the constant barrage of threats and the greater consequences created by the GDPR, businesses must be able to prevent, detect, and respond to security breach incidents immediately. For most, a data security incident is a question of when, not if. Businesses must do all they can to protect personal data. They must be able to prove that they did all they could, and they must be able to respond quickly when incidents occur. These issues are business critical and the time to prepare for change is now.

About the Authors

Jonathan Armstrong

Jonathan is an experienced lawyer at Cordery with a concentration on technology and compliance. His practice includes advising multinational companies across Europe on matters of risk, compliance and technology, including breach prevention, mitigation and response.

He has handled legal matters in more than 60 countries and is a frequent broadcaster for the BBC and other channels.

Jonathan is also one of three co-authors of the LexisNexis definitive work on technology law, "*Managing Risk: Technology & Communications*".

In addition to being a lawyer, Jonathan is a Fellow of The Chartered Institute of Marketing. He has spoken at conferences in the U.S., Canada, China, Brazil, Singapore, Vietnam and across Europe.

Jonathan qualified as a lawyer in the UK in 1991 and has focused on technology, risk and governance matters for more than 20 years.

Jonathan was recently ranked as the 14th most influential figure in information security by the Onalytica Data Security Top 100 Influences and Brands Survey.

André Bywater

André Bywater is a commercial lawyer with a focus on regulatory compliance, processes and investigations. His practice has engaged both the private and public sectors.

André was based in Brussels for many years, focusing on a multitude of EU legal issues across Europe and beyond. He has assisted and advised mainly European and U.S. in-house counsel and other company personnel.

In addition, André has addressed a variety of legal matters in the context of EU-funded projects, building the expertise and capacity of government ministries and agencies in Central and Eastern Europe and further afield. He therefore brings a wide range of experience and skills to his practice.

He qualified as a lawyer in the UK in 1993. He is a fluent French speaker with a reasonable command of Russian.

Reference Materials

Glossary

Full GDPR Text

Directive on Security of Networks and Information Systems (NIS Directive)

Imperva GDPR Resources

Disclaimer

This white paper is for informational purposes only and the information in this white paper does not constitute legal advice and should not be relied upon as such. The law changes regularly and this paper sets out the position in August 2016. If you need legal advice on a specific matter, you should consult with a qualified lawyer. To the fullest extent permitted by law, neither Imperva nor Cordery make any representations, warranties, guarantees or undertakings related to the information provided in this report.