Complying With GDPR:

What All Organizations Need To Know

WHITE PAPER

ABSOLUTE®

CONTENTS

IS YOUR BUSINESS READY TO MEET NEW DATA PROTECTION REQUIREMENTS?

Data protection laws are more important than ever as individuals become more sensitive about privacy, data protection breaches are daily headline news, and regulatory processes get tougher.

The past few years have seen significant developments in data protection, including an increase in the exercise of rights and more aggressive enforcement by national regulators. The biggest change to the data protection landscape, however, is new regulation standards and rules. If data protection is not already high on your compliance checklist, it should be.

NEW REGULATIONS, NEW STANDARDS

The EU General Data Protection Regulation (GDPR) places major emphasis on enforcement, with potential increased penalties for breaches and with fines of up to €20 million or 4% of an organization's global annual revenue (whichever is greater). In addition, it introduces data-breach-reporting requirements, with a reporting deadline of 72 hours from detection of the breach. The current European Union (EU) data protection rules are a reflection of the technological landscape of their time. They came into force in 1995 when the internet was still in its infancy and only about 1% of people were online. The depth of the newly revised rules, enforced as of May 25, 2018, should compel organizations to begin preparing now.

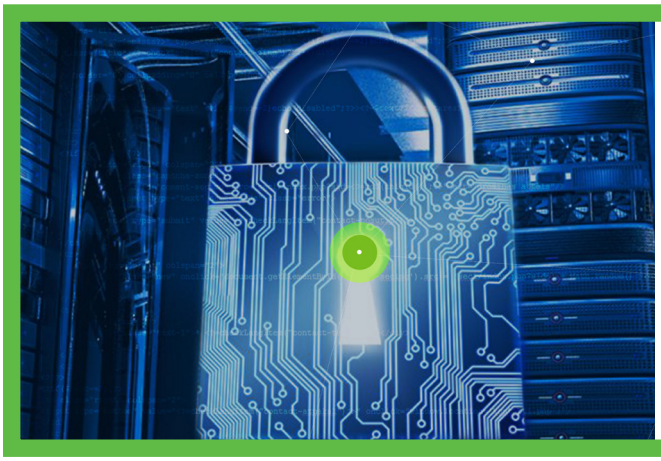
KEY DISTINCTIONS OF THE NEW REGULATIONS

Public sentiment about data protection has changed drastically as data leaks and breaches have become increasingly dramatic and politicized, and the GDPR reflects these changing opinions.

This tide of opinion has influenced the courts—for example, the Google "right to be forgotten" case in 2014 and the Schrems "Safe Harbour" case in 2016—and it will continue to influence the law on a much wider scale with the GDPR.

The Google "right to be forgotten" case is a 2014 judgment by the European Court of Justice concerning a claim brought by a Spanish individual, Mr. Mario Costeja González, who wanted Google Spain or Google Inc. to remove links to announcements concerning him that had appeared in a newspaper in 1998. According to the court, the activities of Google Spain (as an affiliate of Google Inc.) were "inextricably linked" to the data processing conducted by Google Inc.

The Schrems Safe Harbour case is a 2016 judgment, again by the European Court of Justice, concerning a claim brought by an Austrian individual, Mr. Maximillian Schrems. Mr. Schrems claimed that his personal data was transferred from Facebook's Irish subsidiary to the US and was not protected against surveillance by the US intelligence authorities. Between 1998 and 2000, the European Commission (on behalf of the EU) developed the Safe Harbour scheme. It was designed to allow US companies in the EU to transfer personal data from the EU to the US by signing up for a special program that certified them to make such transfers, on the condition that these companies comply with certain requirements and principles.



If data protection is not already high on your compliance checklist, ***it should be.***

A SINGLE SET OF RULES

One of the complaints about current data protection processes is the patchwork nature of enforcement, because each nation has license to implement rules as they see fit. The new rules attempt to remedy this and to streamline enforcement.

The GDPR does not provide room for discretion; any organization doing business in the EU must comply with the same set of rules. However, each EU state will be able to decide which of their unique data protection rules they will keep, meaning organizations that do business in the EU will need to follow:

1. The main data protection rules as set out in the GDPR.
2. Some additional separate national rules.

ONE-STOP SHOP

A very important aspect of the GDPR is that an organization should have to deal with only one data protection regulator, officially referred to under the new rules as a (national) "supervisory authority." But the reality is more complex.

- Where data controllers or processors in organizations carry out data-processing activities that affect data subjects from multiple EU member states, the supervisory authority in the EU member state where the main organization is based will take the role of lead supervisory authority. This means that other member states' regulators may also be involved (as set out under a complex mechanism in the GDPR).
- A national supervisory authority will have apparent sole competence to regulate (although the GDPR doesn't use the word "sole") when either a data protection complaint is made to that supervisory authority or there is a possible infringement of the GDPR, where the issue either relates only to the organization located in the member state of the supervisory authority or substantially affects data subjects located only in that member state.

Under the new rules, there will no longer be a requirement for a data controller to register with a data protection regulator for basic data handling. However, if, prior to data processing, a "data protection impact assessment" (formerly known as a "privacy impact assessment") has been carried out and shows that the planned processing presents high risks for the rights and freedoms of individuals in the absence of measures taken to mitigate those risks, a data protection regulator must be consulted. It may be that local data protection regulators will put some sort of registration process in place where they have concerns.

The new rules will consolidate enforcement and save money on compliance.

UNDERSTANDING THE NEW PENALTIES

Under the new rules, the ceiling for fines has gone up significantly. Three different ranges of fines will be applied in relation to three different categories of infringements. As noted earlier, the proposed highest level of fine is a maximum of €20 million or 4% of the global annual revenue of a business (whichever is greater), which will apply to infringements involving noncompliance with orders imposed by a regulator.

For example, one organization received a fine of £250,000 from a UK regulator in 2013 for failing to prevent a cyberattack. Based on its 2014 revenue, that same company could be fined up to £198 million under the new rules.

It is likely that the powers defined will be well-used. Because the fee for data protection registrations is abolished under the GDPR, fines will be the main source of income for data protection regulators.

WHERE DOES IT APPLY?

This global reach of GDPR may apply where either:

1. A business processes the personal data of EU residents and offers them goods and services, irrespective of whether payment is required; or
2. Where the processing by a business relates to the monitoring of the behavior of EU residents insofar as their behavior takes place within the EU.

For example, a US software company with all its offices in the US that handles the data of EU residents can be investigated, fined and even prosecuted by an EU regulator.

Determining whether an organization situated outside the EU is covered by the EU rules could prove challenging. The fact that a business website or email address is accessible in the EU will not be enough. Other factors, such as the use of a language or a currency generally used in multiple EU member states, may be enough to indicate that an organization is offering goods or services to people in the EU.

NEW RIGHTS

New consumer rights have been introduced, including the right to portability (transmitting personal data from one data controller to another freely) and the right not to be subject to profiling (e.g., analysis or prediction with respect to consumers' economic situations, health, or performance at work). There is also now a statutory right to be forgotten, which is the right to have personal data erased "without undue delay," based on certain grounds, such as when data is no longer being used for the purpose for which it was gathered.

Companies will need much more stringent policies and processes when handling data deletion requests. Ignoring a data deletion request could be a very costly mistake. Part of the solution for large organizations will be the ability to manage data across the device estate to ensure rapid response and, if necessary, deletion.

Ordinary consumers are more aware of their rights now than in the past. In May 2014, Google faced a "right to be forgotten" case involving hundreds of thousands of requests from people who wanted their personal data removed from search results. We can expect these types of requests to continue to increase and for regulators and consumers alike to expect rapid response rates.

THE IMPLICATIONS OF BYOD & REMOTE WORKFORCES

Along with changing laws, modern working practices create unprecedented issues. BYOD (bring your own device) and working from home increase risks for an organization. Even if an employee works from home or from his or her own device, the company will still be responsible for securing personal data.

Most organizations will not want to end working from home, but they may be able to educate their employees and change organizational policies to require employees to work in a more secure way. This could include the provision of better technology (such as secure internet tunnels) and better steps to protect mobile devices.

While new ways of working may lead to greater productivity, we also know that they can lead to serious data breaches. If an employee's tablet containing the details of 100,000 customers goes missing, there could be heavy sanctions if the organization is unable to remotely disable and/or wipe the device. Remote data and device security software can also prevent an errant employee from stealing or losing valuable company data.

Under the new rules, data protection regulators will have the power to impose higher fines.

HOW WILL RESPONSIBILITIES CHANGE FOR COMPANIES UNDER THE NEW LAW?

The new rules say:

> *"With regard to the state of the art and the costs of implementation and taking into account the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals, the controller and the processor shall implement appropriate technical and organizational measures, to ensure a level of security appropriate to the risk."*

So, what does this actually mean? In simple terms, the new rules say that an organization must develop security measures proportional to the risk. It's hard for an organization to stand up to regulatory scrutiny after a breach — if appropriate measures were in place, why did the breach happen? The obligations are twofold:

1. Do a proper risk analysis to try to prevent breaches from happening—this should be done regularly and

COMPANIES NOW FACE THE "**BIG THREE**":
TOUGH REPORTING, MORE RESPONSIBILITY AND HEAVIER FINES.

documented well. Risks change constantly, and the technology available to mitigate those risks also changes, so the risk analysis must be kept up to date; and

2. Do a postmortem of any security incident or near miss and determine how it can be prevented from happening again.

REPORTING DATA BREACHES

The GDPR defines a personal data breach as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed." The new rules also contain two specific data breach regulatory requirements.

First, breaches may have to be reported against set criteria to a data protection regulator without delay and "where feasible" no later than 72 hours after a data controller has become aware of the breach. Reasons must be given when the 72-hour limit is missed. This puts huge pressure on companies. If employees lose their smartphones containing customer details during a week's vacation, then they are unlikely to tell the company until they return to the office (if at all). This means that there will be cases when a data breach occurred but went unreported before the 72-hour period expired, increasing the likelihood the company will face regulatory action. The GDPR increases the chances that consumer victims will win privacy class actions.

Reporting a breach will also most likely mean that the organization will have failed to have "a level of security appropriate to the risk." This obligation puts the onus squarely on organizations; for example, if a device is lost, stolen or hacked, the company, not the end user, will be held accountable for any data that's at risk.

Second, the breach must be communicated without delay to the person whose data has been breached, if the breach is likely to result in a high risk to their rights and freedoms. Some exceptions to this obligation also apply, namely if the data affected by the breach has been encrypted.

If an employee loses a laptop with 100,000 customer records stored on it, the company is obliged to inform every customer that their data has been compromised, if that loss is likely to result in a high risk to the customers' rights and freedoms. The legal consequences, brand damage, litigation and media reporting of an incident would all be significant. Such disasters could be averted if a company has technology in place to prevent this data from being accessed by an unauthorized user.

Companies now face what some might call the "Big Three": tough reporting requirements, greater responsibility to keep data secure and heavier fines.

The logistics involved in reporting a breach are significant under the GDPR — disseminating security information to all individuals and companies with compromised data is not a small task. You might have other reporting requirements as well if you are in telecommunications, financial services or healthcare. You might have to report in multiple languages on different forms prescribed by each regulator. Legal advice will be very important, particularly in the first 24 hours after the breach. You will also need good legal agreements in place to ensure that vendors cooperate and that they have enough financial incentive to help you.

Handling a data breach is complicated, and the more you do now to make sure you have the information you need to report a breach, the better. This includes looking at the

technology options that can help you respond to security incidents, including the ability to determine whether data was accessed illegally. If you can prove no data was accessed, then your regulatory and customer obligations may relax.

NEXT STEPS

The new data protection rules will bring considerable responsibility and sanctions for companies that handle data. It will also bring considerable opportunities for those that help other companies avoid these pitfalls. The responsibilities are so vast that it is important to get the correct advice and to act now.

There will be considerable challenges to comply with the new rules. It will take time to implement the necessary changes, and uncertainties will need to be resolved. Organizations must start now in order to be properly compliant when the new rules come into effect.

Evaluate your GDPR data risk today: **Learn more**.

BEST PRACTICES TO PREPARE NOW INCLUDE:

1	Thoroughly review vendor contracts — vendors' help will be needed, especially in reporting security breaches quickly. Organizations should make sure they have the contractual rights to insist on this and that they can hold their vendors accountable.
2	Prepare to update everything and ensure new detailed documentation and records are ready for regulatory inspection.
3	Review key practical aspects, from data retention, destruction, etc. to all means of collecting data used by the organization.
4	Ensure that new rules such as explicit consent, the right to be forgotten and the right not to be subject to profiling are included in policies and procedures.
5	Put in place a data breach notification procedure, including detection and response capabilities; consider purchasing special insurance.
6	If applicable, appoint a data protection officer.
7	Put in place a data protection impact assessment policy/procedure.
8	Create compliance statements for annual business reports.
9	Train staff on all of the above.
10	Set up and undertake regular compliance audits in order to identify and rectify issues.


SOLUTION SHEET

ABSOLUTE FOR GDPR COMPLIANCE

STAY COMPLIANT WITH PERSISTENT ENDPOINT VISIBILITY AND CONTROL

THE CHALLENGE

absolute.com

ABSOLUTE

ABSOLUTE FOR GDPR COMPLIANCE

GDPR compliance starts with visibility across every endpoint to ensure data protection for any personally identifiable information (PII). Learn how to improve your GDPR compliance with endpoint visibility and control.

DOWNLOAD THE SOLUTION SHEET

/ABSOLUTE®

ABOUT ABSOLUTE

Absolute enables a world where security and IT professionals always retain control over their devices and data. We're the first and only company to offer uncompromised visibility and near real-time remediation of security breaches at the source.

Absolute Persistence® returns devices to their desired state of safety and efficacy after malicious attacks or user error, thanks to our unique location in the firmware of more than 500 million devices built by most of the world's top device manufacturers.

EMAIL:
sales@absolute.com

SALES:
absolute.com/request-a-demo

PHONE:
North America: 1-877-660-2289
EMEA: +44-118-902-2000

WEBSITE:
absolute.com