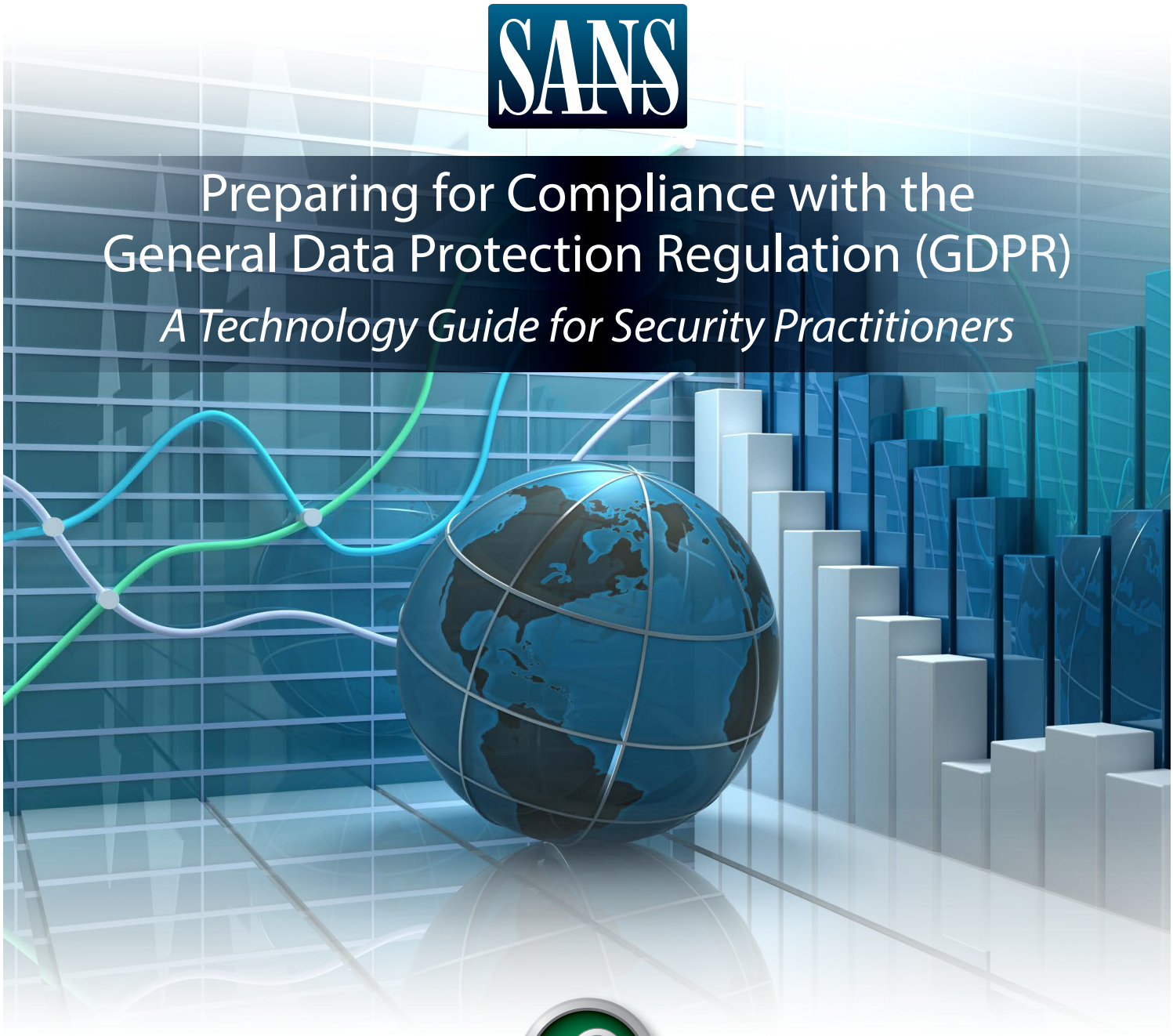


Preparing for Compliance with the General Data Protection Regulation (GDPR)

A Technology Guide for Security Practitioners

A SANS Whitepaper

Written by Benjamin Wright, Attorney

February 2017

Sponsored by
Skybox Security

Executive Summary

Adoption of the new General Data Protection Regulation (GDPR) is motivating organizations worldwide to improve existing technical controls for securing personal information. Organizations should be especially aware that the GDPR and other recent legal developments amplify the negative repercussions of a data security breach—meaning organizations have increased incentives to avoid a breach.

Data security law in Europe continues to evolve. Enactment of the GDPR, which takes effect May 25, 2018, will impose formal, new data security requirements on organizations within the European Union, affecting many companies.

In parallel, in October 2016, France adopted the Digital Republic Bill. It dramatically increases fines on those organizations that fall short on security. For larger, multinational organizations, these types of new security regulations reflect three major trends:

- Greater potential monetary penalties imposed by regulators
- More rules for disclosure of data breaches
- Increased exposure to diverse proceedings and investigations into whether data security is adequate

As a consequence, larger organizations should begin immediately to redouble the implementation of information security controls and technologies, which includes automated IT security monitoring, testing and measuring.

This paper provides recommendations and a checklist for technical compliance with the GDPR. These recommendations are equally imperative for avoiding a painful data security breach. Included are several case studies showing how companies can effectively use advanced technology for regulatory compliance and reduced breach risk.

Breaches Cost Money

The following are examples of substantial fines imposed by non-U.S. government authorities for inadequate data security:

- The Spanish Data Protection Agency imposed a fine of €1.08 million on a television production company that, among other infractions, failed to secure personal information belonging to 7,000 television show contestants. The failure allowed hackers to access the contestants' personal information.
- In the wake of a 2015 data breach affecting 150,000 customers, the UK's Information Commissioner's Office fined communications service provider TalkTalk £400,000.
- Grupo Financiero Banorte, the third largest bank in Mexico, suffered a data breach in late 2014/early 2015. Upon investigation in 2015, Mexican authorities fined the bank 32 million pesos (USD 2 million).

What Is the GDPR?

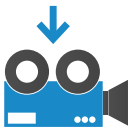
Chain Reaction

Organization gives notice of data breach

Supervisory authority makes public announcement and opens investigation

Other authorities across the EU open investigations

Collective actions are filed in German and French courts



News media investigate

The General Data Protection Regulation [Regulation (EU) 2016/679 of the European Parliament and of the Council 27 April 2016][1] applies to all European Union member states. It replaces the Data Protection Directive 95/46/EC (the 1995 Data Directive).[2] The GDPR extends the historical EU expectation that personal data be kept secure and holds an organization accountable for data security. It also does the following:

- Defines measures data holders must take to protect data
- Emphasizes enforcement expectations
- Enables large fines to be levied
- Imposes broad disclosure requirements for data security breaches

When it comes into effect May 25, 2018, the GDPR can apply to a remarkably wide range of organizations that control or process data about EU residents. This includes many organizations without a physical presence in the EU.

Under Article 3(2)(a), for example, the GDPR applies to each and every non-EU retailer in the world selling goods to data subjects in the EU and processing customers' personal information.

Moreover, the GDPR will likely have ramifications beyond Europe, given the EU's role as a thought leader on data protection. The privacy principles articulated in the 1995 Data Directive have shaped law adopted in Asia-Pacific nations (e.g., the APEC Privacy Framework), Latin America and elsewhere. And the state of California recently adopted privacy rules for "smart" power grid security that reflect the influence and principles of the 1995 Data Directive.[3]

This paper focuses on selected provisions of the GDPR as they pertain to technical measures an organization must institute to protect data and some recommendations on how practitioners can comply with those provisions.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation): http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

[3] Public Utilities Commission of the State of California, Decision 11-07-056 July 28, 2011. See especially Attachment D: "Rules Regarding Privacy and Security Protections for Energy Usage Data." http://docs.cpuc.ca.gov/WORD_PDF/FINAL_DECISION/140369.pdf

Sections of the GDPR Applicable to Information Security Technology

The GDPR sets forth a complex regime of measures an organization must take to protect personal data, including the appointment of a data protection officer and the maintenance of detailed documentation to prove compliance. But the GDPR does not articulate a precise prescription for the technology that must be used to secure data.

At this time, data security implementation details are left to interpretation in the GDPR. While it is binding, enforceable law, we see the regulation as a work in progress.

EU regulators informally acknowledge the GDPR sets broad, ambitious goals, while leaving the details to be articulated in the future. As a result, some regulators are openly concerned that inconsistent and/or incomplete interpretations will emerge.[4]

The overriding issue is whether data is at risk and which practices and technologies will effectively reduce the risk.

What we do know is the GDPR takes a risk-based approach to requiring particular technical measures. Higher risk mandates more expense and effort to secure data. The overriding issue is whether data is at risk and which practices and technologies will effectively reduce those risks.

Article 32 is the primary provision requiring technical measures to protect data. Article 32 emphasizes that the degree of effort invested in a particular measure must be informed by the risk present in a particular setting or application.[5] Thus, for example, a non-EU retailer processing the data of many thousands of EU data subjects is expected to implement stronger measures to protect its data than would a retailer processing data for only a handful of data subjects.

In practice, risk is to be evaluated by a particular organization, its data protection officer and any relevant legal authority authorized to investigate a situation or an implementation.

The GDPR might be enforced in numerous different ways. A common scenario for enforcement against a multinational organization would be by way of a proceeding under a "supervisory authority." A supervisory authority would be a competent government agency in a member state akin to what is known as a data protection authority today. A single supervisory authority will normally have lead responsibility for investigations and enforcement against the organization in regards to its operations throughout the EU. The supervisory authority is expected to cooperate with other relevant EU authorities.[6]

Although a multinational organization could face differing interpretations of the GDPR's technical requirements, the important point is that the GDPR is supported with enforcement mechanisms, and those mechanisms far exceed what has been in place until now.

[4] Bojana Bellamy and Markus Heyder, "How to build a cathedral in two years: EU Regulators Urge Industry to Help Flesh Out the GDPR," Privacy Perspectives, April 1, 2016, https://iapp.org/news/a/how-to-build-a-cathedral-in-two-years/

[5] Eduardo Ustaran, "Why the GDPR is Good News for Business," Hogan Lovells, Chronicle of Data Protection, September 28, 2016, www.hldataprotection.com/2016/09/articles/international-eu-privacy/why-the-gdpr-is-good-news-for-business

[6] Eduardo Ustaran, "Why the GDPR is Good News for Business," Hogan Lovells, Chronicle of Data Protection, September 28, 2016, www.hldataprotection.com/2016/09/articles/international-eu-privacy/why-the-gdpr-is-good-news-for-business

Reducing Vulnerability: Case Studies

Two examples demonstrate how implementing automated network controls, testing and monitoring can reduce an organization's data security risks.

Each of these also demonstrates how organizations can implement the requirements in GDPR Article 32: "a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing" of personal data.

Tightening Access and Automating Security Procedures

A large UK-based outsourced customer management service provider controls and processes great quantities of personal information throughout Europe and elsewhere.

Analysis of its data security revealed a lack of visibility into its complex network environment, including more than 80 firewalls. It lacked confidence some new firewalls had been implemented with the organization's own policies. Its manual change management processes were slow and costly, which resulted in an inability to track changes and verify the firewalls were properly implemented. The company determined its risk profile was unacceptable and sought to become compliant with the Payment Card Industry (PCI) Data Security Standard and ISO 27001.

The company deployed an automated, integrated solution to reduce its systemic risk. The solution allowed staff to visualize and document all firewall rulesets to optimize its firewalls. This approach further allowed the company to tighten the access paths to its network and to change management. The new approach provided an automated process to scan for, assess and resolve network vulnerabilities.

As a result, the company materially reduced its overall network risk profile and improved its continuous, documented, provable compliance with standards and decreased its chances of a data security breach.

Continuous Firewall and Device Monitoring

A large-scale business services provider delivers business process outsourcing to more than 20 top-tier companies and government agencies in the UK. It was using resource-consuming manual management processes to achieve PCI compliance, including network security, data security, vulnerability management, access control, security monitoring and information security best practices.

The company's increasing network complexity was making the cost of compliance unsustainable, and the company was not able to prove its firewalls were PCI compliant.

In response, the company automated its firewall audits and management to detect security and compliance problems. It tracks the identity of those problems and the responses to them so that the company's staff can confirm they have been resolved. Furthermore, analytics can find and remedy hidden risk factors by assessing interactions between network devices and zones. The company achieved reliable and continuous confirmation of its PCI compliance and, therefore, reduced its chances of a data security breach.

The GDPR in the United Kingdom

The United Kingdom played a major role in drafting and negotiating the GDPR. The UK government has signaled its intent to enact the GDPR into UK law, regardless of the UK's referendum to leave the European Union, which is commonly referred to as *Brexit*.[7]

Accordingly, British guidance on information security technology is directly relevant to interpreting the GDPR. British guidance and experience are discussed on Page 10.

Collective Proceedings to Enforce Data Security

A new and important legal action for data security enforcement, known as a collective proceeding, is emerging in Europe. It is akin to a class action lawsuit, a common and potent means of information security enforcement in the United States.

In Europe, this action will vary from country to country, but, generally, a collective legal proceeding (lawsuit) can be enacted on behalf of data subjects to ensure this data is protected. A proceeding seeks to force a data-holding organization to secure the data of a large number of data subjects, and prove that it has secured the data to the satisfaction of a third party such as a court.

In Germany, a collective legal proceeding can, for example, be brought by a consumer protection association against an organization that is allegedly failing to protect personal data. It can result in the award of attorneys' fees for the party initiating the proceeding.[8]

As a practical matter, attorneys' fees are important. In the U.S., the possibility of winning a plaintiff's attorneys' fees often drive a class action lawsuit. And those fees are often the largest cost imposed on an organization named as a defendant in a data security class action lawsuit.

Elsewhere in the EU, France adopted its law for collective proceedings, which is similar to German law, in November 2016.[9]

The adoption of collective legal proceedings in Europe compounds the legal risk of any organization suffering a data security breach.

[7] "UK Government Confirms Implementation of GDPR in UK," Hunton & Williams, Privacy and Information Security Law Blog, November 3, 2016, www.huntonprivacyblog.com/2016/11/03/uk-government-confirms-implementation-gdpr-uk

[8] Daniel Felz, "Germany's Christmas Present: Data-Protection Class Actions," Alston & Bird Privacy and Data Security Blog, January 6, 2016, www.alstonprivacy.com/germanys-christmas-present-data-protection-class-actions

[9] "France Adopts Class Action Regime for Data Protection," November 30, 2016, Privacy & Information Security Law Blog, http://huntonprivacyblog.com/2016/11/30/france-adopts-class-action-regime-for-data-protection-violations

Compiling a Track Record of Compliance

Although the GDPR formally goes into effect in May 2018, an organization would be wise to begin compliance measures now. Undertaking meaningful steps toward comprehensive security compliance demonstrates to courts and regulators that an organization is a responsible steward of data and potentially worthy of lenient treatment if security shortcomings were to come to light, whether before May 2018 or afterward.

Steps for Implementing Security Technology for Compliance with the GDPR by a Larger Multinational Organization

1. Don't wait. Start now.
2. Establish a track record of compliance before the formal effective date: May 25, 2018.
3. Document your review of technology for GDPR compliance and your steps toward achieving compliance.
4. Institute a constant and ever-improving process of analyzing the risks that apply to the data for which you are responsible.
5. Adopt a routine for maintaining the considerable documentation expected under the GDPR.
6. Evaluate and implement technologies identified in this paper not only to achieve compliance with the GDPR's security expectations, but also to prevent a breach from ever happening.
7. Stay abreast of and implement authoritative global guidelines on information security, such as NCSC's 10 Steps to Cyber Security. [See "Further Reading" – Page 12]
8. Recruit, train and appoint a qualified data protection officer.
9. Monitor efforts at an EU level and in member states to prepare for enforcement of the GDPR.
10. Establish familiarity with the supervising authority or authorities most relevant to your operations. Become familiar with its staff and procedures.
11. Monitor technical guidance and, possibly, codes of conduct from relevant EU authorities, such as regulators in member states and EU-wide authorities, such as the Article 29 Working Party, which will become known as the European Data Protection Board.

Further, by starting to build a track record of compliance today, an organization begins to build data protection processes so that it can be more effective and efficient when the formal requirements come into force.

France has forthrightly signaled it essentially expects compliance with the GDPR immediately. France adopted a law known as the Digital Republic Bill, October 7, 2016. This aligns current French law with many (not all) of the requirements of the GDPR and dramatically increases the fines for noncompliance. The French data protection authority (*Commission Nationale de l'Informatique et des Libertés*, or CNIL) now has the authority to impose fines of up to €3 million. Fines were previously limited to a maximum of €150,000.[10]

Officials from other EU data protection authorities have said they are looking to the GDPR as expected best practice even before it takes effect.[11]

[10] "Entry into Force of the French Digital Republic Bill," Hunton & Williams LLP, October 31, 2016, www.lexology.com/library/detail.aspx?g=1d008c03-4ab3-4f0d-ae1d-9d7d5438eda4

[11] Tim Van Canneyt, "Belgian Privacy Commission changes enforcement attitude as fining powers are announced," Privacy, Security and Information Law, May 6, 2015, http://privacylawblog.fieldfisher.com/2015/belgian-privacy-commission-changes-enforcement-attitude-as-fining-powers-are-announced

The Chain Reaction to a Data Breach Notification

The GDPR will require organizations in all EU member states to disclose data security breaches. This disclosure requirement may be the single most compelling provision for data security in the GDPR.

Although similar requirements have been in effect in Germany for several years, they have not been widely applicable across Europe until now.[12]

As has been true in the U.S., when an organization notifies the public and/or the government of a data breach, the notification can trigger a chain reaction of invasive and expensive legal, political and news media investigations into the organization's data security practices.

The U.S. has long been the world leader on data breach notification laws. As has been true in the U.S., when an organization notifies the public and/or the government of a data breach, the notification can trigger a chain reaction of invasive and expensive legal, political and news media investigations into the organization's data security practices.

The state of California adopted the first major data breach notification law, which became effective in 2003. Although California is just one of the 50 U.S. states, its notification law had a nationwide effect. Many businesses that operate in the state, but that have headquarters elsewhere, were forced to notify the public after a data breach. If you must tell your California customers about a breach, then inevitably any people outside California expect to be told about it, too.

As a consequence of the California law, companies across the U.S. have been hit with multiple lawsuits and investigations on the heels of data security breaches. When an organization tells the public about a breach, class action plaintiff lawyers learn what they need to initiate lawsuits. In addition, many regulators—including those outside the jurisdiction that requires the notice—see a need to investigate. Those regulators can include attorneys general in states outside of California, as well as U.S. federal regulators, such as the Federal Trade Commission, and even privacy commissioners in Canada. Legislative bodies and news media also instigate these types of investigations.

A similar chain reaction can be expected to unfold in Europe. A multinational company may, for instance, give public notice of a breach under Belgian law (or Belgium's current understanding of best practice). But data supervisory authorities in France and other countries may deduce that an investigation is warranted under national law, too. In addition, an EU-wide authority such as the Article 29 Working Party (to become known as the European Data Protection Board) may open its own investigation. Plus, a collective proceeding (class action lawsuit) can emerge in a country like Germany. And the news media will investigate as well.

[12] Bridget Treacy, "Local solutions to data breach notification laws," Data Protection Law and Policy, September 2009, www.hunton.com/files/Publication/3cc163bc-2dc5-468a-8fc9-630449e85f8d/Presentation/PublicationAttachment/f8d2e83d-6c2e-48b6-b710-472861045be5/Local_Solutions_Treacy_9.09.pdf

When the GDPR goes into effect, the requirements for public notice of a breach will expand across Europe for the first time. And the potential for fines imposed by regulators will expand tremendously.

Public disclosure of a breach can cause negative publicity and damage an organization's reputation. This has played out many times in the U.S. The most alarming example was the 2013 data breach at retail giant Target, which negatively affected sales and eventually contributed to the resignation of Target's top executives.

With the GDPR on the horizon, companies must be acutely aware of the breach notification requirements.

The paramount question the GDPR poses to security practitioners is not "What checklist of measures must I follow to pass an audit?" Instead, the paramount question is "How do we avoid a breach?"

A Breach Investigation Always Finds Fault

Another aspect of an investigation triggered by a breach notice merits attention. When an investigation ensues after a breach, it is relatively easy for the investigator to conclude that security was faulty and penalties should be imposed. A breach happened, so obviously the security was inadequate, argues the investigator.

Contrast this with an investigation (or audit) of security when no breach has happened.[13] If there has been no breach, then the investigator must evaluate many debatable factors. The investigator—such as a national data protection authority or an on-site data protection officer—must consider the abstract risks to data and must compare the data holder's actual security practices against best practices, recommended guidance and so on. Often the investigator must work harder and muster greater resolve to conclude that security falls short to the point that security is inadequate and substantial penalties or corrections are warranted.

Avoid the Data Breach

The paramount question the GDPR poses to security practitioners is not "What checklist of measures must I follow to pass an audit?" Instead, the paramount question is "How do we avoid a breach?"

[13] Many kinds of investigations can be undertaken in the absence of a breach. Regulators, courts and data protection officers can and will launch investigations (sometimes called lawsuits or audits) to inquire whether an organization is in compliance with data protection requirements. These investigations can happen under many different circumstances.

Selected Provisions of the GDPR

The GDPR regulates organizations that control or process personal data, recognizing that such entities vary by size, sophistication, amount of data processed and so on. As such, no single program of technical measures will fit all organizations. While some will implement technical measures directly, others will turn to third parties to protect their data from unauthorized use, access, loss and corruption.

The following highlights major provisions in the GDPR for technical measures to protect data. Later in this paper, we will recommend how to comply by pointing to recognized guidance and instructive case studies and scenarios.

Article 5(2) and Article 30

These articles place obligations on an organization to demonstrate that it is in compliance. Compliance might be demonstrated, for example, through the creation and maintenance of documentation that proves the organization is using technology for continuous monitoring of data and continuous evaluation of vulnerabilities.

Article 25(1)

Requires an organization to implement data protection principles, such as data minimization, to safeguard data and protect the rights of individuals, technically known as "data subjects." The exact words of the regulation do not limit the rights that must be protected to only privacy rights. Therefore, the rights referred to in the words of the regulation might be privacy rights, civil rights, rights to freedom, rights to be forgotten or other rights. The requirement calls for the use of both technical and organizational measures.

Article 28

An outsourcer (data processor) must have technical and organizational controls in place to ensure data is protected and documentation to prove compliance.

Article 32

Requires an organization to implement technical measures to ensure data security. Although Article 32 gives examples of security measures, it does not provide a comprehensive list of security measures. It motivates an organization to find, implement and revise effective security measures in light of the dangerous and rapidly changing information security threat landscape.

Article 32 mentions in particular:

> (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Article 32 further calls attention to risks "from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data."

Articles 33 and 34

In the event of a data security breach, these articles call for the evaluation, documentation and notification of the breach. Notification under Article 33 is provided to a relevant supervisory authority. Notification under Article 34 is provided to individual data subjects.

Automated IT testing, monitoring and analysis would enable the discovery of a breach. Automation also can evaluate breaches and provide information required to determine whether notification is necessary and, if so, the content of notification.

Examples of Best Practices

Currently, the GDPR, including Article 32, compels companies to look at existing best practices and recommendations. Examples of some authoritative guidelines for information security follow.

Authoritative UK Guidance

The UK's National Cyber Security Centre has published authoritative, actionable guidance for organizations to achieve cyber security and compliance with security obligations in its "10 Steps to Cyber Security."[14]

One of these 10 steps calls for monitoring to detect attacks, respond to attacks and account for activity. It states the following:

> System monitoring provides a capability that aims to detect actual or attempted attacks on systems and business services. Good monitoring is essential in order to effectively respond to attacks. In addition, monitoring allows you to ensure that systems are being used appropriately in accordance with organisational policies. Monitoring is often a key capability needed to comply with legal or regulatory requirements.[15]

[14] "10 Steps to Cyber Security," National Cyber Security Centre (United Kingdom), www.ncsc.gov.uk/guidance/10-steps-cyber-security

[15] "10 Steps to Cyber Security," National Cyber Security Centre (United Kingdom), www.ncsc.gov.uk/guidance/10-steps-cyber-security

Authoritative Guidance from CIS Critical Security Controls

Another source of authoritative, actionable guidance is the CIS Critical Security Controls for Effective Cyber Defense.[16] These have been developed by the Center for Internet Security with international support and input, including that of the UK's Centre for the Protection of National Infrastructure. The Critical Security Controls are consistent with the "10 Steps to Cyber Security" and match many of the controls delineated in another widely recognized standard, ISO 27001.[17]

An example of the technical guidance in the Critical Security Controls is CSC 4 "Continuous Vulnerability Assessment and Remediation." It recommends that organizations "continuously acquire, assess, and take action on new information in order to identify vulnerabilities, and to remediate and minimize the window of opportunity for attackers."[18]

CSC 4.1 specifically advises:

> *Run automated vulnerability scanning tools against all systems on the network on a weekly or more frequent basis and deliver prioritized lists of the most critical vulnerabilities to each responsible system administrator along with risk scores that compare the effectiveness of system administrators and departments in reducing risk.*

[16] Center for Internet Security, Critical Security Controls, www.cisecurity.org/critical-controls.cfm

[17] ISO/IEC 27001 - Information security management, www.iso.org/iso/iso27001

[18] SANS Institute, "Monitoring and Measuring the CIS Critical Security Controls Poster: Products and Strategies for Continuously Monitoring and Improving Your Implementation of the CIS Critical Security Controls," www.sans.org/media/critical-security-controls/SANS_CSC_Poster.pdf

Conclusion

Eventually, the GDPR can be expected to affect a very large number of organizations worldwide, either because they process data from the EU or because local jurisdictions adopt similar rules.

The GDPR institutes general, broadly worded standards for information security in the EU. These can be enforced through routine administrative audits and procedures. The greatest initial enforcement of the GDPR will likely result from investigations launched in response to breaches reported under GDPR Articles 33 and 34. As organizations consider the impact of regulation, the incentive increases for ever-improving security to prevent breaches. A reported breach has the potential to trigger the most invasive investigations, resulting in the greatest legal punishment, and to inflict the greatest damage to reputation.

Further Reading

"10 Steps to Cyber Security," National Cyber Security Centre (United Kingdom)
www.ncsc.gov.uk/guidance/10-steps-cyber-security

Center for Internet Security, Critical Security Controls
www.cisecurity.org/critical-controls.cfm

The GDPR Portal
www.eugdpr.org

SANS Institute's many "What Works" case studies, which demonstrate how real-world security practitioners protect data, avoid breaches and reduce risk.
www.sans.org/critical-security-controls

About the Author

Benjamin Wright, a SANS senior instructor, practicing attorney and author of several technology law books, including *Business Law and Computer Security*, teaches the Law of Data Security and Investigations course for the SANS Institute. This unique five-day course trains security, forensic and legal professionals to cope with the risks surrounding data breaches, digital investigations, electronic discovery and technology contracts. With 26 years in private law practice, he has advised many organizations, large and small, on privacy, e-commerce, computer security and email discovery. He has been quoted in publications around the globe, from The Wall Street Journal to the Sydney (Australia) Morning Herald. Benjamin maintains a popular blog at http://hack-igations.blogspot.com.

This paper provides general, summary education to the public. It does not provide legal advice for any particular situation. The reader should not rely on this paper as a complete or accurate statement of law. If the reader needs a complete and accurate statement of law, or legal advice for a particular situation, then the reader should consult a competent lawyer.

Sponsor

SANS would like to thank the sponsor of this whitepaper:

SKYBOX™ SECURITY