FIDELIS CYBERSECURITY™

WHITEPAPER

Are You Ready for European Data Protection Reform?

What to expect. How to comply. Top 5 actions to get prepared.

OCTOBER 2015

EXECUTIVE SUMMARY

Data is more valuable and at greater risk than ever. The advent of big data and the increasing use of cloud, mobile and social networks combined with a worsening threat environment make data privacy and data security increasingly important. Data protection has come under scrutiny due to high-profile incidents such as the Sony, Target, Anthem and Ashley Madison data breaches. The way we create, use, share and store data has evolved and most organisations understand the need to secure data. The trouble is that the level of priority given to data protection is not always as high as it needs to be and European laws that govern data privacy and data security have failed to keep pace.

European data protection legislation is changing

In response to the growing threats to data privacy and security, the European Union (EU) is in the process of reforming its data protection legislation with the introduction of the General Data Protection Regulation (GDPR) and the Network and Information Security (NIS) Directive. Intended to replace the existing patchwork of country-specific legislation, the reforms are focused on:

- Modernising and unifying the EU data protection regulations
- Improving consumer protection
- Strengthening critical IT infrastructure against cyber attacks
- Setting a minimum cybersecurity standard across all member states

Organisations are unprepared

The need to address data privacy issues, cybersecurity risks and compliance responsibilities is already a major, far-reaching concern for many organisations. The new legislation will affect firms across all sectors and likely result in extra burdens and restrictions.

The new rules will impact the way in which firms manage cyber defences and will require hardware and software changes along with new reporting requirements. Faced with increased challenges in meeting new levels of data privacy and security, organisations are scrambling to come to grips with the upcoming EU data reforms and make sense of the regulatory and operational consequences.

Businesses operating in Europe or targeting European customers need to start preparing for the new regime and take advantage of new technologies to ensure that they will be able to comply. At stake are the consequences of non-compliance and the financial and reputational impact to the business incurred as a result of losing valuable personal information.

This paper highlights the key points of the proposed regulation and offers guidance on the changes companies must make to their policies, processes and procedures to avoid potential financial penalties and reputational risk.

DATA PROTECTION REFORM – THE TIME HAS COME

Advances in digital technologies are completely transforming the way in which consumers and businesses communicate and conduct business as we have come to rely on the internet for more and more services. With this increased use of online services comes the demand for more personal information, often without consent. The globalisation of data via social networks, cloud computing, search engines and location-based services is fueling growing concerns over the collection, storage, use and loss of control of personal information. And with good reason, as personal data, financial information and health records reside in a myriad of databases, often long after their end-of-use date. When a business fails to permanently erase data and suffers a data breach or cyber attack, consumers are put at risk for identity theft. Failure to respond to such threats results in a loss of consumer confidence, impacts business and can be a threat to national security.

Trail blazer for data protection

The EU has long been a trail blazer when it comes to data protection. The European Parliament and Council Directive 95/46/EC of 1995, which addresses the protection of individuals with regard to the processing and free movement of personal data, has often been described as a gold standard for data protection. Unfortunately, data privacy and security legislation is now lagging behind the advances in technologies used to conduct business. As data breaches and loss of personal data is on the increase, individual consumers and businesses are waiting for the modernisation of data protection to catch up.

New data privacy and security regulations

An increased reliance on the use of the technologies to conduct business, globalisation and growing privacy concerns call for an overhaul of the 1995 legislation and the introduction of network and information security legislation. In response, the EU is in the process of implementing two historic security measures designed to protect data against cyber attacks, put people in control of their personal data and build trust in the Digital Single Market.

General Data Protection Regulation (GDPR)

The European Commission plans to unify data protection within the EU with a single law across all 28 member states . The General Data Protection Regulation (GDPR) significantly overhauls Directive 95/46/EC to align data privacy with the advances of the digital age. Building on the high level of data protection that has been in place since 1995, the Regulation:

- Addresses the handling of personal data within the EU
- Strengthens protections and privacy around personal data
- Extends and expands data subject rights

The European Council, European Commission and European Parliament must all reach an agreement on the draft Regulation before it can become law. It is envisioned that the Regulation will be published in December 2015, subject to agreement between all parties. Once passed, it then becomes immediately effective in EU Member states throughout the European Union. Once formally adopted, organisations will have a two-year transition period before it becomes enforceable in 2017 by Data Protection Authorities (DPAs). The Data Protection Directive (95/46/EC) will be repealed when the final GDPR is officially published.

Network and Information Security (NIS) Directive

The NIS Directive is the first legislation of its kind proposed in the EU. It is an important part of the EU Cybersecurity Strategy initiated in response to growing risk of cybersecurity attacks to public bodies and private organisations across the EU. Proposed in 2013, the NIS Directive focuses implementing the EU Cybersecurity Strategy across Europe and aims to:

- Put measures in place to ensure a high level of network and information security across the EU
- Strengthen IT infrastructure against attacks via the internet
- Ensure a secure and trustworthy digital environment throughout the EU

The Presidency negotiates the terms of the Directive with the European Parliament on behalf of the Council. In order to be adopted, the legal act must be approved by both institutions. Talks will continue under the incoming European Union Luxembourg presidency, with negotiations expected to be concluded in 2015. Member States then have two and a half years to implement the requirements into law.

EU Data Protection Laws are Changing

DATA PROTECTION DIRECTIVE 95/46/EC	GENERAL DATA PROTECTION REGULATION (GDPR)
Local laws across 28 member states	One uniform law
Focus on location of equipment	Focus on the data
Multiple Data Protection Authorities	One-stop-shop
Data controllers only	Controllers and processors
Fines differ between countries	Sanctions and large fines
No obligations to report breaches	Obliged to report breaches without delay
No obligation to have a DPO	DPO required for a larger organisation

THE BUSINESS IMPACT OF GDPR

The GDPR introduces significant data privacy and protection reform and is likely to present increased compliance challenges for many organisations. In addition to substantial changes to business processes, this will result in:

- Increased governance requirements, particularly regarding security measures
- Changes to business culture, such as embedding a culture of privacy by design
- Increased costs to implement new processes and controls in order to respond to newer, stronger rights of individuals (access to data, erasure of data, right to be forgotten, data portability, rectification of inaccurate or incomplete data)
- Increased costs to implement new technologies, policies and processes to comply with security requirements
- Financial risks due to potentially substantial fines for non-compliance

Are You Ready for European Data Protection Reform?

FIDELIS CYBERSECURITY

Focus and scope of the regulation

Whereas Data Protection Directive 95/46/EC focused on the location of the data controller's or data processor's equipment, GDPR addresses the handling of personal data of EU data subjects, regardless of whether the data is stored within the boundaries of the EU or not. The regulation further broadens the definition of personal data to include email addresses, computer IP addresses, posts on social media and personally identifiable data.

The regulation extends to all organisations and people based in the EU. Unlike the existing Data Protection Directive, it will also apply to organisations outside of the EU if they provide goods or services to, monitor the online behaviour of or process the personal data of EU residents.

Increased risks presented by profiling and big data analytics

The explosive growth of internet usage has resulted in numerous data feeds coming from multiple locations, including emails, phones, computers, web logs, social platforms and online transactions. The end result is a big data treasure trove of personal data.

Big data analytics plays a vital role in the digital economy and is now commonly used in the natural course of business. The growth in big data is matched by the growing concerns of EU citizens regarding the collection, sharing and analysis of their personal data; and perceived privacy intrusions.

The regulation introduces a number of restrictions on profiling. In many cases, profiling will only be permitted when:

- Explicit consent of the individual has been obtained
- Expressly authorized by EU Member state law
- Carried out in the course of entering into a contract or executing a contract

Given the complexities of big data analytics, the profiling of personal data will likely become a compliance priority.

New requirements for data processors

The new regulation will impose new compliance obligations and possible sanctions directly on service providers and data processors. This is a dramatic departure from the EU Data Protection Directive as service providers do not have any direct obligations to comply with the current law. Service providers that fail to comply with the new requirements run the risk of direct enforcement by a supervisory agency and significant penalties.

Among the new obligations, service providers must:

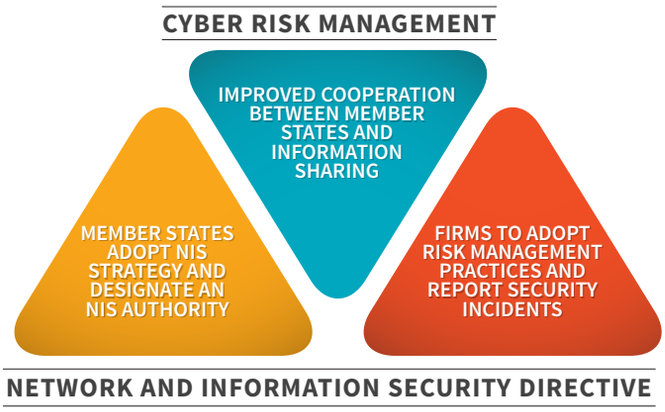
- Implement all security measures as required by the regulation and maintain documentation
- Assist controllers in complying with the obligations for breach notification, data protection impact assessments and prior authorization
- Appoint a Data Protection Officer if data processing thresholds are met
- Comply with international data transfer requirements
- Cooperate with supervisory authority if required

NIS – CLOSING THE GAPS IN CYBERSECURITY

The current approach to network and information security is based on voluntary action. As a result, the national capability and the levels of private-sector involvement and readiness vary considerably between member states. The NIS directive aims to close the gaps in cybersecurity and level the playing field by introducing harmonised rules to apply in all EU countries.

The NIS data security and cyber resilience reform represents the most significant change to data protection in the EU since 1995 and marks the first time the EU will have a consistent framework for information security standards. Aimed at tackling security risks and incidents across the EU, the Directive:

- Attempts to set a minimum level of security across the EU without deterring any member state from setting a higher level
- Allows for flexibility in implementation due to differences in readiness across member states
- Allows member states to develop sector-specific guidelines on what constitutes a reportable incident



Foundation on three key pillars

NIS will require stronger cyber-risk management and incident reporting across the EU. Founded on three key pillars, the Directive calls for:

- EU member states to adopt an NIS strategy and designate a national NIS authority with adequate resources to prevent, handle and respond to NIS risks and incidents
- Improved cooperation between member states and between public and private sectors to share early warnings on risks and incidents, exchange information and counter NIS threats and incidents
- Certain online companies and services to adopt risk-management practices and report major IT security incidents to the competent national authority

Scope of the NIS Directive

For the first time, companies will be under a legal obligation to ensure they have suitable IT security mechanisms in place in order to ensure a secure and trustworthy digital environment throughout the EU. The requirement to report IT security incidents aims to help develop a culture of risk management and make sure that information is shared between private and public sectors. The NIS Directive extends to:

- Critical infrastructure operators in sectors such as financial services, transport, energy and health
- IT service companies, including app stores, e-commerce platforms, internet payment platforms, cloud computing platforms, search engines and social networks
- Public administration and public service companies

ENFORCEMENT AND THE RISK OF NON-COMPLIANCE

The potential for a data breach and its impact on the organisation is no longer just an IT issue. It's a company-wide risk that can have a bottom-line impact. EU countries will be required to put in place dissuasive, effective and proportionate sanctions for non-compliance with either the GDPR privacy requirements or the NIS Directive's cybersecurity requirements. Compulsory reporting requirements will mandate that the breaches must be disclosed.

Non-compliance with the new regulations will have fierce consequences, with penalties far exceeding most local data protection penalties in member countries. Failure to protect customer data may result in legal fines and sanctions, destroy brand reputation, impact customer trust and loyalty and affect profits and stock values.

Independent and better-equipped Data Protection Authorities

Under the proposed GDPR reform, Data Protection Authorities in the EU look likely to be given a broader range of investigative, enforcement and corrective powers, including the power to:

- Investigate non-compliance
- Notify data controllers and/or data processors of an alleged breach
- Order controllers/processors to provide access to information relevant for performance of duties
- Carry out investigations and perform onsite audits
- Order the rectification, destruction or erasure of data
- Impose bans on processing

One-stop-shop

Currently, businesses operating across the EU can be required to deal with DPAs in each EU country, leading to multiple investigations on the same issue and potentially different enforcement actions. The reform proposes that cases be handled by a single regulator based in the country where the business has its main establishment. Intended to reduce administrative burden and ensure fast, consistent application of the law across all member states, the one-stop-shop mechanism has the potential to improve the fragmented regulatory activities occurring under the Data Protection Directive. The one-stop-shop mechanism calls for:

- Every member state to have a competent authority ready to handle any incidents
- All DPAs to cooperate on cross-border cases with a designated leader DPA
- DPAs to achieve a single, supervisory decision in important cross-border cases
- European Data Protection Board to issue binding decisions where necessary

HOW TO COMPLY

The new regulations are expected to be adopted by the end of the year, at which point organisations will have a two-year transitional period to comply with GDPR and two and a half years to comply with NIS. When the regulations become official, penalties for non-compliance will be severe. With no room for complacency, it's imperative that organisations take action now to get the building blocks in place in preparation for compliance. Failure to do so could leave organisations unprepared to defend against cyber attacks and vulnerable to the new, stricter privacy regulations.

With a goal of proactively identifying risk and providing a level of assurance that controls are in place, here are five areas to address to prepare your business for the new regulations.

1. Data subject rights

In addition to retaining existing rights, such as data access, rectification and erasure, the Regulation introduces new and stronger rights for data subjects. These rights include the right of data portability, the right to be forgotten and certain rights in relation to profiling. Actions to take now to ensure that the processing of personal data complies with the new requirements include:

Implement technologies, policies and practices to protect against unlawful or unauthorized processing

- Review existing processing-consent templates and procedures to ensure consents are clearly distinguished
- Put privacy policies, procedures and documentation in order and keep up to date
- Form a governance group that oversees all privacy activities, led by a senior manager or executive
- Implement technologies, policies and practices to protect against unlawful or unauthorized processing
- Identify and assess current profiling activities to determine if they meet the new requirements

2. Data governance and protection

Many companies believe they have a clear understanding of where data resides within their organisation when in fact they often have a one-dimensional view of their data flow. Under the new regulation it will be important for companies to have a holistic view of the data they collect, store and process in their organisation. Actions organisations should take now to establish strong data governance and protection include:

Determine what data is collected from customers, who has access to it, what it is used for and who is responsible for its protection

- Perform a gap analysis of processes for handling existing and new data-protection obligations. Identify controls both in-place and needed to mitigate risk throughout the data life cycle
- Establish a strategy for data classification, retention, collection, destruction, storage and search
- Determine what data is collected from customers, who has access to it, what it is used for and who is responsible for its protection. Destroy unnecessary data; keep only what is needed
- Identify where data is processed within the organisation and through third-party processors from both a functional and geographical perspective
- Appoint a Data Protection Officer, if required by the magnitude of processing

3. Internal audit and risk management

The forthcoming regulations will present a dramatic change for many firms and many will need to make extensive changes to data processing and information security practices. Strong internal audit will be vital in helping organisations to mitigate risk and adhere to increased governance requirements. Actions to take now include:

Adopt internal and external audit processes to identify risk exposures introduced by the new legislation

- Evaluate existing internal audit and risk management functions to determine gaps in staffing and capabilities
- Adopt internal and external audit processes to identify risk exposures introduced by the new legislation
- Establish procedures to provide assurance to Audit Committees that exposures have been mitigated and to demonstrate that processing of personal data complies with the Regulation
- Conduct audits and risk assessments on a periodic basis
- Implement policies that make privacy and security integral to an organisation's processes

4. Data breach readiness and response

Companies must recognise that a data breach can happen and should prepare. Further, it will soon become compulsory to report data breaches to the relevant Data Protection Authority, even if protective measures are in place or the likelihood of harm is low. Actions to take now to be prepared to deal with breaches include:

Develop detection, forensic analysis, eradication and remediation processes to deal with data breaches and stress-test incident response plans

- Be proactive in protecting your systems and employ highly skilled staff
- Implement appropriate technology for active network monitoring and threat detection. Use a layered security defence that includes encryption, anti-malware and endpoint security
- Develop detection, forensic analysis, eradication and remediation processes to deal with data breaches and stress-test incident response plans. Include key stakeholders from across the company and senior management to ensure response activities are consistently applied
- Establish a breach notification plan detailing who is responsible for dealing with Data Protection Authorities, media and other agencies
- Establish relationships with incident response and forensic remediation firms

5. Employee awareness and company culture

There is generally a high level of understanding about the duties related to confidentiality and data protection within a company's risk, security, compliance and legal functions. This level of understanding needs to be extended throughout the organisation. Actions to take now to educate employees on data protection responsibilities and the need for confidentiality include:

Identify parts of the organisation that own, create or are custodians of relevant data types and determine their level of awareness and compliance

- Identify parts of the organisation that own, create or are custodians of relevant data types and determine their level of awareness and compliance
- Provide comprehensive education about data protection compliance. Train employees on how to handle sensitive data and promote internal awareness regularly across the organisation
- Start to integrate data protection considerations across all products and services to drive privacy by design
- Foster a company culture where privacy is considered in every process and at every level

SUMMARY

A rapidly evolving business environment and new technologies combined with eroding customer confidence in online services and increasing privacy concerns is driving demand for data privacy and protection reform. At the same time, high-profile breaches in the media are increasing the pressure and requirements to protect sensitive personal information and critical infrastructure. Against this backdrop, the EU is overhauling its data privacy and security legislation with new requirements that will increase security obligations and impact businesses across all sectors.

The GDPR is intended to unify data protection throughout the EU, strengthen protections around personal data and safeguard and boost the European online economy. The Network and Information Security Directive is focused on promoting cyber security and cyber resilience and protecting critical infrastructure from cyber threats and attacks. Non-compliance sanctions will be significantly increased, with potential fines up to €1M or 2% worldwide annual turnover.

The time to act is now. The new legislation will soon come into play and is likely to require a number of substantial changes to business processes and introduce technical and procedural challenges. Many companies will need to implement processes and technical controls to ensure the protection and confidentiality of customer data. Organisations need to be proactive to get ahead of the changes. Failure to act early could lead to struggling to align policies and procedures with the new requirements. The key is to engage with the right security partners and find the right security tools that build upon your organisation's existing security controls and culture.

How Fidelis Cybersecurity Can Help You

Advanced, targeted attacks are not instantaneous events; they involve a series of actions and multiple phases that occur over a period of time. Professional cybercriminals are so adept at cloaking their activities that they routinely go unnoticed for months, even years, without detection. They conduct detailed reconnaissance activities and, when necessary, develop custom-tailored exploits to penetrate your enterprise network and steal sensitive corporate data, intellectual property, business plans and personal information.

Organisations don't have to live in a state of continuous compromise. Fidelis Cybersecurity offers the complete portfolio of product, consulting services and proprietary threat intelligence that equip you to proactively get one step ahead of any attacker before they achieve their ultimate objective.

Proactive, advanced threat defence

Fidelis Cybersecurity enables organsations to reduce the time to detect, investigate and stop attackers on your network and endpoints at every stage of the attack lifecycle.

- **Detect attacks at every stage of the attack lifecycle.** We don't just look for the tools attackers use. We also look at their behaviour. When we find an attack, we provide visibility that enables you to reconstruct attackers' footprints so you can see where they have been – even when they are accessing devices, such as laptops or mobile devices, that have left your network
- **Investigate and prioritise suspected incidents.** Fidelis helps you focus on the highest priority threats. When an incident arises, we automate the triage and investigation so you can rapidly understand what you're facing
- **Stop attackers and prevent data theft.** When you identify active attacker activity in your environment our products provide multiple approaches to contain it and freeze attackers' ability to move in your network in real-time

Reduce risk, increase efficiency

Our experience in protecting the world's most sensitive networks for over a decade validates that robust network monitoring, not just attempting to find inbound malware, is key to detecting threats before anything is stolen. By focusing on real-time detection, prevention and continuous response, Fidelis empowers organisations to:

- **Reduce theft of assets and data.** Identify and stop targeted attacks at every stage of the attack. We enable security operations teams to analyse and scope potential security incidents within moments after they receive an alert – whether they come from Fidelis, their SIEM or other security systems
- **Improve ROI on security investments.** Get more out of your existing security investments while staying focused on the most important threats. We help you connect the dots between your network- and host-based security solutions so you can follow up on alerts generated by your existing security tools
- **Improve efficiency of security analysts.** Equip front-line security analysts to make better and faster decisions about suspected security incidents and investigate events more quickly
- **Lower incident response costs.** Reduce the number of security incidents and the time to contain incidents with minimum business disruption while accelerating your ability to respond to the alerts that matter
- **Reduce reputation risk.** Protect your credibility by ensuring your customers' data remains private

Fidelis consulting services – the power of experience

Fidelis' security consultants have decades of experience assisting organisations of all sizes to prepare for and respond to security incidents. The Fidelis security team has the scale, experience and credibility you need. In addition to unparalled expertise in defence against cyber warfare, theft of intellectual property, advanced persistent threats and other malicious threat actors, our consultants bring a commitment to confidentiality to protect reputations and valuable brands.

We offer a full portfolio of consulting services designed to enable you to effectively and efficiently respond to and completely recover from a cyber attack:

- **Incident response services.** Fidelis security professionals have extensive experience managing investigations involving nation-state threat actors and financial thieves in both the government and commercial sector. When a breach occurs, our security consultants can determine the scope of the incident, remove attackers from your environment and re-secure your network. Our incident response services include:
  - Rapid threat assessment, containment, remediation and eradication
  - Forensic analysis, from evidence collection to network forensics and data recovery
  - Malware analysis and reverse engineering
- **Proactive security assessments.** Fidelis offers a variety of security assessments that identify current security gaps and provide recommendations on how to mitigate risk and improve an organisation's incident response capability. We can also assess whether attackers are currently present in your environment. Services include:
  - Compromise assessments to detect potential network risk factors
  - Incident response readiness assessments to ensure you have a solid plan
  - Security programme review to guarantee adequate systems security measures and controls are in place
- **PCI services.** Fidelis is a Qualified Security Assessor by the PCI Security Standards Council. Our Security professionals are able to assess and validate your organisation's adherence to the PCI-DSS standard. We provide a comprehensive examination of your organisation's specific business and regulatory requirements
- **Security Operation Centre (SOC) development services.** Fidelis security experts assisted in building one of the longest running security operations centres and have first-hand knowledge of what works and what fails based on our incident response experience. We can assist in taking your organisation's SOC to the next level or help you develop and implement a SOC from the ground up
- **Litigation support services.** Fidelis security professionals possess forensic certifications and are experienced in collecting, analysing and preserving data required for depositions, investigations, discovery and testimony. Our litigation support services include:
  - Examination of computer forensics to prove or disprove an unlawful act
  - Unbiased expert opinions or witness testimony
  - Explanation of complex issues in terms understandable to non-technical audiences