COMPLIANCE, THE ‘PRIVACY BY DESIGN’ APPROACH TO PROTECT PERSONAL DATA
CONTENTS

Executive summary 3

The GDPR and its impact 4

New challenges with protecting personal data 5

The ‘Privacy by Design’ approach 6

How Symantec Unified Security Strategy supports ‘Privacy by Design’ 8

Working with Symantec Strategic Partners 11

Further reading 13
EXECUTIVE SUMMARY

The European Union's General Data Protection Regulation (GDPR)\(^1\) is coming. It will create additional security and privacy obligations organisations need to comply with. Executives should not wait for the legislation to come to force. Instead they should look at how to prepare their employees, processes and technologies to comply. For each organisation the solution to securing personal data will differ, but there are common themes to comply with the GDPR. Implementing security best practices with 'Privacy by Design' built-in will make businesses more prepared, reduce risks and costs.

Recommendations for organisations that have to comply with the regulation

1. Implementing the GDPR is a board-level issue for organisations and compliance must be agreed at this level. Form a governance group under the direction of the CIO, CISO and Data Protection Officer.

2. Understand what data you need and what data you collect. How much you process and whether you do not need to collect or retain data. Have mechanisms in place that would allow you to be able to delete data with confidence.

3. Identify the flow of personal data into the organisation and how it is processed, secured, stored and deleted.

4. Assess whether the level of security offered by current policies and procedures is adequate to offer protection against unauthorised processing and data loss.

5. Assume a 'Privacy by Design' stance when re-engineering processes, policies and where relevant, products and services involve the processing of personal data to ensure compliance happens by default.

6. Review any breach notification processes to assess whether your company has tools on hand to investigate the extent of any compromise within a 72-hour notification deadline.
THE GDPR AND ITS IMPACT

Today, personal data protection laws across the EU are not fully harmonised. Whilst they mostly share the same origins, they are a result of each EU member state’s interpretation of the EU Data Protection Directive 95/46/EC of 1995. The GDPR creates a new legal instrument across all 28 member states with one binding regulation replacing all the different interpretations of the previous directive. Additionally, it takes into account new technologies and trends such as cloud computing, social, and others which were not used in 1995.

Now, every organisation managing the personal data of EU residents, including non-EU firms that operate inside EU borders, has to comply with a single set of rules on how personal data is acquired, stored, and secured, taking into account the rights of individuals to access, challenge, and amend their records.

Organisations might be required to appoint a so-called Data Protection Officer (DPO), but they also have to implement a data privacy framework, understand the location of personal data it holds and where it flows, as well as carry out mandatory impact assessments. Another important element of the GDPR is the Mandatory Breach Notification. This means loss of personal data may need to be reported ‘without undue delay’, most likely as quickly as 72 hours.

Non-compliance with the GDPR could be very expensive. Fines for non-compliance could reach €20 million or in case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding year, whichever is the higher. Therefore, implementing the GDPR is a board-level issue and compliance processes should be agreed at this level. For organisations that don’t have legacy systems in place, this might be the opportunity to redefine existing security programs and implement a ‘Privacy-by-Design’ framework.
NEW CHALLENGES WITH PROTECTING PERSONAL DATA

The fast-evolving data privacy threat landscape has forced organisations to confront the hard reality of carrying substantial risk, strong enforcement and the need to face many challenges in managing and protecting personal data. These issues are exacerbated by the increased frequency with which data breaches are made public every month. Recent news reports are a testament to the struggles companies now face.

A major problem organisations have is the data protection policies and processes required to contend with this overlapping set of organisational, business and technology challenges. Isolated development of IT technologies, policies or workflows will not provide the answer for GDPR compliance.

The challenges of protecting personal data include:

- Lack of appreciation for security - perhaps due to the lack of awareness of the legal and financial consequences.
- Poor security hygiene within the organisation, which breeds non-enforcement of compliance security policies.
- Lack of organisational ownership, or accountability, from business owners.
- The sheer amount of data collected and the inability to track down and suppress useless data.

Inadequate visibility of data locations and flows is a major concern for those needing to comply. According to the analysts at the Ponemon Institute, 36% of business critical applications are already in the cloud. The concerning statistic is IT departments are not aware of half of them. With the rise of ‘Shadow IT’ in organisations, those responsible for compliance risk losing control altogether.

The growth in data is at an all-time high and shows no signs of abating, compounding this lack of visibility. The analysts who researched IDC’s Digital Universe study predict data will grow by 44 zettabytes over the next five years thanks to Big Data, the Internet of Things (IoT), social media and metadata. IT trends like cloud, mobility and virtualisation increase the complexity of business critical systems and drives up the costs to locate, classify and protect information.

Most pressing, the evolving threat landscape makes it harder for organisations to keep data secure. As Symantec’s latest ISTR report revealed, one million new malware threats are released every day. Consequently, a growth in targeted attacks and advanced persistent threats has caused companies to be more reactive in their approach to cyber security. An issue intensified daily by large, well-skilled hacker groups targeting both organisations and individuals.

Without executive sponsorship, changing the IT and security culture is almost impossible. For business leadership to support the requirements for the GDPR and comply with it, IT teams need to communicate in the risk-based language their business colleagues understand. This requires the collection of information and report back on issues using dashboards to explain the impact of emerging cyber risks to the business. The ‘Privacy by Design’ approach, mandated by the GDPR, gives guidelines to organisations on how to approach personal data protection.
THE ‘PRIVACY BY DESIGN’ APPROACH

Ann Cavoukian, Former Canadian Information and Privacy Officer, developed the approach ‘Privacy by Design’ 5. Its seven Foundational Principles are based on the view that privacy cannot be assured solely by compliance to regulatory frameworks. Privacy assurance has to be an organisation’s default mode of operation.

The EU legislator has endorsed these concepts and the Privacy by Design approach is going to be mandated by GDPR as one of the requirements for data controllers. However it does not explicitly define all the concepts in detail, leaving some room for interpretation.

One of the most prominent and mainstream concepts is ‘End-to-End Security’, guaranteeing Full Lifecycle Protection of Personal Data, from the creation and storage of the data to the point when it becomes obsolete. In the era of data breaches this principle is very critical. It shifts the focus to Detection and Response of risk rather than solely the protection of data. Risk Management, prior to a personal data incident, and Response Planning, after the incident, are equally vital parts of the End-to-End Security Management to prevent or mitigate the impact of data breaches.

Fig 2. Privacy by Design - Data Breach End-to-End Security diagram
To properly manage risk, it is vital to PREPARE thoroughly. To achieve this, personal data, particularly its location, access policies and risk posture as well as infrastructure vulnerabilities all need to be assessed. Security intelligence gives organisations a greater understanding of the external threat landscape, including its perpetrators and the likely threat vectors, allowing security managers to predict possible threats.

Once the infrastructure and personal data vulnerabilities have been assessed, it is time to PROTECT. Developing and implementing safeguards onto vital infrastructure will contain the impact of a possible attack and allow organisations to mitigate the unintentional disclosure of information by well-meaning insiders.

However, it is unfortunately impossible for organisations to be 100% secure from data breaches. It is not a question if, but when data breaches become evident. This is where having a Response Plan including how to DETECT an incident or a breach in place, comes into play.

Statistics show it takes 229 days on average for an organisation to detect an attack, by which time the data leakage has, most likely, already occurred. This delay is a result of security teams working in silos and becoming overwhelmed by point solutions which frequently generate too many alarms.

Security Monitoring services and especially modern Advanced Threat Protection (ATP) solutions can significantly reduce the time to detect an attack or breach and additionally provide a clear understanding of the impact of these incidents. But there’s more.

If a breach occurs, organisations need to implement the RESPONSE phase of ‘End-to-End Security’. This includes the technical remediation of the incident and covers the guiding principle of the framework for all stakeholders involved: Visibility and Transparency. This is in line with the GDPR mandatory breach notification which states organisations need to report a breach involving the loss of personal data as quickly as 72 hours. It will be costly if organisations do not have the correct incident response process to be compliant making it harder to mitigate reputational and financial risks.
HOW SYMANTEC UNIFIED SECURITY STRATEGY SUPPORTS ‘PRIVACY BY DESIGN’

Symantec’s Unified Security Strategy helps to comply with the security requirements of the GDPR as it supports the ‘Privacy by Design’ principles. It contains the building blocks of **Information Protection** and **Threat Protection** to protect personal data, mitigate data losses and stop unauthorized access to both data and applications.

Symantec security software and services are available either on-premise or in the cloud with data centers which span the whole world and many of them are located in Europe. They are scalable and secured to the highest standards such as ISO 2700x or SAS 70 type I and II. Symantec guarantees industry-leading SLAs for availability and malware detection rates. To further increase privacy, encryption and an anonymisation layer within the underlying **Unified Security Analytics Platform** secure personal identifiable information.

**Cyber Security Services** support organisations by monitoring and detecting data breaches faster than enterprises and SMBs can do themselves. Incident Response provides preparation, pre-built processes and technology to react effectively and mitigate the impact of risk. All these security solutions and services are backed by the Unified Security Analytics Platform, the largest civilian threat intelligence network for advanced security decisions of known and unknown threats.

---

**Fig 3. Symantec Unified Security Strategy diagram**

**Cyber Security Services**
- Managed Security Services
- DeepSight intelligence
- Incident Response
- Security Simulation

**Threat Protection**
- ENDPOINTS
- SERVERS
- GATEWAYS

**Information Protection**
- DATA
- IDENTITIES

**Unified Security Analytics Platform**
Log and Telemetry Collection, Integrated Threat and Behavioral Analysis, Unified Incident Management and Customer Hub, Inline Integrations for Closed-loop Actionable Intelligence, Regional and Industry Benchmarking.
1. PREPARE

As stated earlier, organisations face major challenges protecting the data they hold. To adequately prepare, the IT GRC (Governance, Risk and Compliance) framework helps assess potential risks, reports back to the board and remediates gaps with advanced security measures. Here is how.

Symantec’s IT GRC solution, Control Compliance Suite (CCS), delivers core assessment technologies to enable security and compliance programs, and support IT operations in the data center. CCS provides asset auto-discovery, automates security assessments across technical, procedural, and third-party control, then calculates and aggregates risk scores according to business-defined thresholds. Organisations can use this information for operational and mandate-based reporting so they can prioritise remediation and risk reduction for GDPR related data.

Similarly, Symantec’s Data Loss Prevention (DLP) discovers all types of personal data with content-aware detection technologies. It is effective whether personal data is at rest, in motion or in use. DLP detects data stored across endpoints, mobiles, storage systems, networks and even in the cloud. IDC estimates that by the end of 2016, 50% of customer data will be in the public cloud, compared to less than 5% in 2013, meaning DLP strategies have to support emerging technologies such as cloud and mobile.

2. PROTECT

Threat protection solutions stop incoming attacks against personal and other confidential data. Symantec’s full portfolio of threat protection technologies is designed to provide protection against all key threat vectors—endpoint, gateway, and server. Symantec Advanced Threat Protection (ATP) is a new single solution that uncovers, prioritises and remediates advanced attacks across the organisation and is the first product available in the market that does this across the endpoint, network and email control points from a single console, without having to deploy any new agents.

Again Symantec Data Loss Prevention is key in protecting personal data. It not just discovers where personal data is located, it also allows organisations to block or encrypt transactions which endanger identified personal data without unnecessary impact to business processes.

DLP scans personal data, flags confidential content and monitors activity on the network. If a user attempts to unintentionally move personal data over unsecure networks, instead of simply blocking the transfer, and potentially frustrating the user, DLP provides the option to encrypt the personal data before authorising the transfer, allowing organisations to proactively prevent user error and ensure business continuity, all while helping educate employees on security best practices.

Regulatory requirements such as GDPR make encryption a necessity for many. Companies must have an auditable encryption solution in place to protect the privacy of customer data. In many cases with encryption in place, organisations can remove the need to disclose if a data breach occurred.
Authorized access to applications and data – whether on-premise or in the cloud – is another cornerstone of Symantec’s Information Protection strategy. The Validation and ID Protection Service (VIP) provides strong authentication that enables organisations to secure access to networks. The Identity Access Manager (SAM) solves cloud security challenges using identity and context-based access control across multiple cloud applications.

3. DETECT

Almost all organisations are experiencing a critical shortage of security staff. It is expensive to hire, train, and retain skilled in-house security analysts, researchers, and responders. So it is unsurprising the average time to detect a breach is 229 days. According to Ponemon Institute, this gives enough time for cyber criminals to steal sensitive data, costing organisations an average $3.5M per breach.7

Symantec Cyber Security Services (CSS) address this critical shortage of security expertise and minimise detection and response times. Each CSS offering extends the current capabilities of companies and is tightly integrated to provide additional insight and context across Managed Security Services (MSS), DeepSight™ Intelligence, Incident Response, and Security Simulation.

Symantec ATP offers fast detection of Advanced Persistent Threats leveraging correlation of inbound traffic events over multiple control points such as endpoints, networks and email. The correlation engine (Synapse) and the cloud-based sandbox technology (Cynic) process and analyse information such as portable executables, Java, containers, Office docs, PDF and other suspicious file types. Symantec ATP guarantees highest detection rates and uncovers advanced attacks in under one hour.

4. RESPOND -

An end-to-end response plan can be very complex. It integrates steps from Incident Response (IR) plan assessment, incident triage, and containment all the way through to various post-incident activities such as PR/Crisis management and litigation support. Perhaps as a result, according to the joint Symantec & Deloitte report ‘Winning the Cyber War’,8 two third of companies don’t actually have complete confidence in their response plan.

To complement existing onsite capabilities of customers, Symantec offers Incident Response Services as part of its Cyber Security Services portfolio. Those services will help to comply with the Mandatory Breach Notification and support to meet the deadline of 72 hours.

Recognising that some risks cannot be eliminated completely, organisations have increasingly turned to Cyber Insurance as a method of mitigating and transferring the risk of exposure to cyber events and data breaches.
WORKING WITH SYMANTEC STRATEGIC PARTNERS

Complying with the General Data Protection Regulation requirements can take a long time to get ready. Implementing a practical end-to-end plan and deploying the right security mechanisms, data governance regimes and replicating all the mitigations across the supply chain and partner ecosystem is challenging for CIOs to manage.

To help organisations comply with the regulation, Symantec provides the security strategy and solutions to protect personal data and business processes around the data lifecycle. The focus is on Threat Protection, Information Protection, Cyber Security Services and IT Governance, Risk and Compliance. Security is one important pillar, but the spectrum of regulatory requirements GDPR presents is wide and covers consumer profiling restrictions, personal data workflows - including user rights to have their data deleted - and structured documentation of data processing operations. To address these tasks for our customers, Symantec leverages its strong relationships with leading global consulting firms and system integrators.

Symantec’s Strategic Alliance Partners offer risk and compliance assessments, penetration testing and additional advisory services to develop a practical plan in identifying, managing and protecting personal data throughout its lifecycle. Another area of joint cooperation is Incident and Breach Response with the fast detection and effective reaction needed to comply with the mandatory breach notification. While Symantec strengths lie in incident triage and onsite analysis benefiting from its huge Unified Security Analytics Platform and threat telemetry, partners provide additional skills and practical experiences around IR plan development, remediation services, public relations and crisis management, expert witness and litigation support as part of an overall end-to-end incident response plan.

Some of the Symantec Business Consulting Partners will use the threat and risk telemetry to provide more accurate tools for the cyber insurance industry in order to recommend best insurance products and policies to their clients.

Not all companies will be ready to deploy and run new security and compliance processes for the GDPR on their own, especially those lacking IT personnel and skills. So Symantec’s partners address the growing demands of privacy regulations and offer organisations services such as Managed DLP, Managed Compliance or Compliance Reporting to embrace the law.
With Symantec's technical security expertise coupled with its partners' business consulting and managed/hosted services is the perfect way to implement ‘Privacy by Design’.

**Symantec Global Strategic Partner Ecosystem**

**Cyber Security Services**
- Managed Security Services
- DeepSight Intelligence
- Incident Response
- Security Simulation

**Threat Protection**
- ENDPOINTS
- SERVERS
- GATEWAYS

**Information Protection**
- DATA
- IDENTITIES

**Unified Security Analytics Platform**
Log and Telemetry Collection, Integrated Threat and Behavioral Analysis, Unified Incident Management and Customer Hub, Inline Integrations for Closed-loop Actionable Intelligence, Regional and Industry Benchmarking.

**Compliance as a Service**
- Compliance Reporting Service
- DLP Assessment
- Malicious Activity Assessment

**Managed DLP**
- Outsourcing/Hosting
- Personal Data Workflows
- PR/Crisis Management

**Privacy Impact Analysis**
- Risk Assessment
- Cyber Insurance
- System Integration

Fig 4. Symantec Global Strategic Partner Ecosystem diagram
ABOUT SYMANTEC

Founded in 1982, Symantec has evolved to become the global leader in cyber security, with more than 11,000 employees in more than 35 countries. Operating one of the world’s largest cyber intelligence networks, we see more threats, and protect more customers from the next generation of attacks. We help companies, governments and individuals secure their most important data wherever it lives.

FURTHER READING:

• A new dawn for Data Privacy -  
  A Symantec Perspective on EU Privacy Regulations >

• A new dawn for Data Privacy -  
  Infographic >

• Wall Street Journal: Keeping your data safe >

SOURCES:

1. EU General Data Protection Regulation; CIO Magazine & Symantec
2. Data Breach the Cloud Multiplier Effect, Ponemon, June 2014
3. IDC’s Digital Universe Study
5. Privacy by Design – The 7 Foundational Principles Information and Privacy Commissioner of Ontario, revised version from January 2011
7. 2014 Cost of Data Breach Study: Global Analysis, Ponemon Institute, May 2014
8. Symantec and Deloitte Research: Winning the CyberWar, April 2015