Preparing for GDPR Compliance: A Technology Brief for Security & Privacy Practitioners

WHITE PAPER

Contents

Please note: the purpose of this brief is not to provide legal advice for specific organizations, and all organizations affected by the GDPR are encouraged to seek competent legal advice from either Corporate Counsel or an external law firm.

1.0 Why read this brief?

The General Data Protection Regulation will change the way you do business

The EU General Data Protection Regulation (GDPR) comes into force on May 25, 2018. Every organization — regardless of its location — doing business with EU customers will need to make changes to its technology, processes, and people to comply with the new rules.

This guide helps security and privacy professionals understand the GDPR requirements they need to start tackling with immediate effect, and provides an independent perspective on the solutions available to help bridge the technology gap.

The threat landscape cannot be ignored

Personally Identifying Information (PII) has become an increasingly important topic in cyber security as the focus of cybercriminals has moved from the theft of financial data to personal data. According to the Breach Level Index,[1] over 9 billion data records have been stolen since 2013 – an astonishing 5.2 million per day on average. Your organization will almost certainly be the victim of a targeted cyber-attack at some point and there is a greater than 1 in 10 chance that this will lead to serious data loss and/or reputational damage.[2]

Why you can't afford to ignore GDPR

- Fines of £17.5m or 4% of global turnover, whichever is higher
- Key principles such as the right to be forgotten and information requests
- The requirement to notify a data breach within 72 hours
- The need to establish a clear legal basis for holding and processing personal data

2.0 What are the legal consequences of technology failure for organizations?

Organizations that fail to translate the requirements of the GDPR into their technology run the risk of failure and non-compliance, leading to financial, reputational and legal damage.

The key legal consequences are:

1. Regulatory investigations and inquiries, during which the organization can be required to disclose its records, risk assessments, technology designs, audit reports and other assessments and incident logs.
2. Regulatory enforcement orders, which can extend to stopping the use of personal data by an organization, and the redesign of business processes and the technology environment
3. Regulatory fines, subject to a cap of 4% of annual turnover*
4. Exercise and enforcement of individuals' rights

5. Compensation claims by individuals who feel their rights have been impacted

** Illustrative example: A UK bank suffered a significant data breach of personal data during 2016, and if this had been subject to the financial penalties of the GDPR, could have seen a fine approaching £2 billion, in addition to other indirect impacts including reputational damage.*

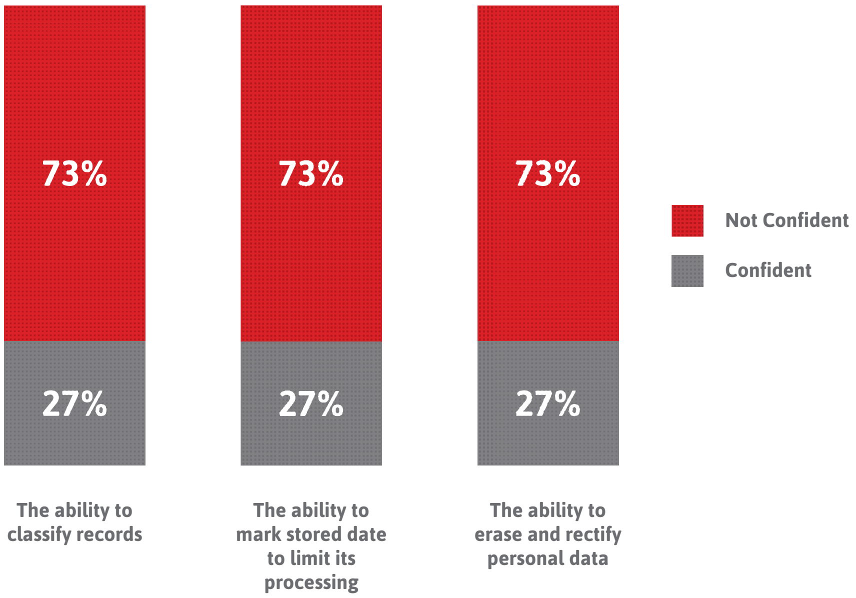
Did you know?

According to research conducted by Osterman Research, Inc. almost 3 out of 4 enterprise IT decision makers don't feel they meet the compliance requirements of GDPR. Three quarters of Information Security Officers believe that the expectations of GDPR will greatly impact IT purchases and security provisioning

In the UK, the current information commissioner at the Information Commissioner's Office (ICO), Elizabeth Denham, has stressed that fines are the last resort; focusing on the £17m headline maximum fine is failing to take the opportunity to step up the quality of data protection. The ICO only levelled fines in 16 of the most serious of over 17,000 cases reviewed in 2016-17. That being said, government funding for the ICO has been slashed and the service will need to self-fund from this year.

From a security design point of view, the rule of thumb is that a breach is inevitable. It's simply a matter of time. That would make EU GDPR a "tax" of up to 4% of a company's revenue valid, by default, on all business that handles the personal data of EU citizens. The task then becomes one of exempting yourself from this tax through demonstrable investment on sensible and proportionate information security.

Figure 1
Organisational Confidence in the Ability to Meet Key Requirements of the GDPR



Source: Osterman Research Inc.

3.0 Taking a risk based approach to technological measures

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. However, the GDPR does not offer a precise prescription for all technologies required 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.

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.**

There is nothing particularly innovative or new about the technology solution areas involved with meeting compliance requirements, but all companies handling EU citizen's personal data may now have to revisit risk calculations because the new penalties for failing to comply with EU GDPR will be much higher than those currently levied.

Providing evidence of risk mitigation counts as much as securing data

According to GDPR requirements, organizations must demonstrate that they have implemented appropriate measures to mitigate privacy risks. Even in the absence of a breach or customer complaint, regulators may request firms to exhibit evidence of their compliance and risk management strategies, including a privacy impact assessment (PIA). Security teams play a crucial role in building this documentation. For example, they must demonstrate that they have deployed access controls and rights management, paying special attention to processes for access recertification. Tokenization, encryption, and key management controls will require documentation, as well.

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.

With due regard to the state of the art

One of the challenges facing lawmakers is how to account for future technological innovations without having to re-issue a legal framework every time something new comes to market.

Within the GDPR, the phrase "with due regard to the state of the art" is such a future-oriented attempt. While a few specific technological approaches are mentioned in the text of the GDPR – such as encryption and pseudonymization – organizations are given a much broader mandate to ensure the state of the art for data protection is considered when selecting or designing applications, services, and products used for processing personal data (Articles 25 and 32).

For example, new state of the art approaches currently coming to market include behaviour analytics, privileged access management and format-preserving encryption (FPE).

4.0 Selected technological provisions of the GDPR - Articles & Recitals

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

The following highlights major provisions in the GDPR for technological measures to protect data.

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)

Privacy-by-design will be the biggest challenge to address. The GDPR states that firms must consider privacy at the start of any new project and ensure that the right security controls are in place throughout all development phases. Sustained collaboration between teams will be critical, so firms will have to establish new processes to encourage, enforce, and oversee it.

This article also 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

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. 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.

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 (C), Integrity (I), Availability (A) 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 organizational measures for ensuring the security of the processing.

The CIA triad is an established model in information security. Whilst a lot of the GDPR is concerned with privacy (an aspect of confidentiality), risks from unlawful destruction, loss and alteration of data are also highlighted which broadens the range of threats to data and technology solutions that need to be considered.

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.

The Data Breach Notification requirement will be a game-changer.

The GDPR gives companies 72 hours from the moment they become aware of them to report any data breaches to authorities and affected customers. Compliance with this requirement will be tougher than many companies expect.[4] They will first have to understand and share complicated details with regulators about any exfiltration of personal data, including how many records were lost or stolen, over what period. However, the bigger challenge is that they'll also have to share those details with customers. That means you and your incident response team will have to craft clear, compelling messages that reflect adequate levels of competency, sensitivity, and customer care.[5]

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.

Recital 39

Any processing of personal data should be lawful and fair. Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing.

Recital 49

The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned.

This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems.

These principles cover a very wide scope and are challenging, but according to the European Commission[6] "will incentivise businesses to innovate and develop new ideas, methods, and technologies for security and protection of personal data."

GDPR compliance: where technology is impacted

✔ Article 15 – Right of access by the data subject

✔ Article 16 – Right to rectification

✔ Article 17 – Right to erasure (right to be forgotten)

✔ Article 18 – Right to restriction of processing

✔ Article 19 – Notification obligation regarding rectification or erasure of personal data or restriction of processing

✔ Article 20 – Right to data portability

✔ Article 21 – Right to object

✔ Article 22 – Automated individual decision-making, including profiling

✔ Article 25 – Data protection by design and default

✔ Article 32 – Security of processing

✔ Article 35 – Data protection impact assessments

5.0 Transition to the GDPR – technology goals aid business transformation

The GDPR's focus on technology is much more explicit than its predecessor, the Data Protection Directive. If it is to be properly effective, however, the GDPR must assist in the delivery of business transformation and legal compliance.

In the PwC report April 2017, "Technology's role in data protection – the missing link in GDPR transformation"[7], this is distilled down to three specific technology goals. It is helpful to refer to these as "guiding principles" when considering the GDPR technological impact within your organization.

Technology goal #1

Driving data protection principles into technology, through appropriate technical and organizational measures

The data protection principles set out the core compliance goals of the law. They have been at the heart of European data protection regulation from its very beginning in the 1960s. The principles must be delivered through technology and organizations must take 'appropriate technical and organizational measures' to do so. When developing those technical and organizational measures, organizations must have full regard to the 'nature, scope, context and purposes of processing' and 'the risks of varying likelihood and severity for the rights and freedoms of natural persons'.

The obvious implication of this requirement is that risk assessments must be performed in all cases. These risk assessments require a deep understanding of the effect that technology can have on individual rights and freedoms.

Technology goal #2

Ensuring the technology environment can protect individuals' rights

If people are to have control over their personal data, they need rights over that data and transparency about what is happening to it. But the exercise of these individual rights is only truly effective if an organization's IT systems are fully responsive to them, and have the right functionality embedded in them.

The core individual rights are the 'right of access', 'right to rectification', 'right to erasure' (or the 'right to be forgotten'), 'right to restriction of processing', 'right to data portability' and 'right to object'. In a functional sense, these rights require the technology to:

- Connect individuals to their personal data;
- Categorise personal data by type and processing purpose;
- Map or trace the full information lifecycle;
- Perform search and retrieval;
- Enable rectification, redaction, erasure and anonymisation;

- Enable freeze and suppression;
- Enable the transmission of personal data from one technology stack to another.

All of this must be protected by appropriate security.

Technology goal #3

Adopting a proper approach to technology design and deployment

One of the GDPR's innovations is the inclusion of requirements that provide organizations with practical assistance in how to flow data protection into technology. These are:

- **Accountability** – proving that technology works properly
- **Records of processing activities** – understanding the data lifecycle and what technology does
- **Data protection by design and default** – getting technology right from the start
- **Data protection impact assessments** – understanding technology risk
- **Breach notification** – delivering transparency in technology failure

Collectively, these new requirements provide a 'user manual' for delivering operational success.

6.0 Case studies in reducing data security risk

Two examples provided by the SANS Institute[8] 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 organizational measures for ensuring the security of the processing" of personal data.

Case Study 1: Tightening Access and Automating Security Procedures

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

Analysis of the company's 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.

Case Study 2: Continuous Firewall and Device Monitoring

Company: A large-scale business services provider delivering business process outsourcing to more than 20 top-tier companies and government agencies in the UK.

The company 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.

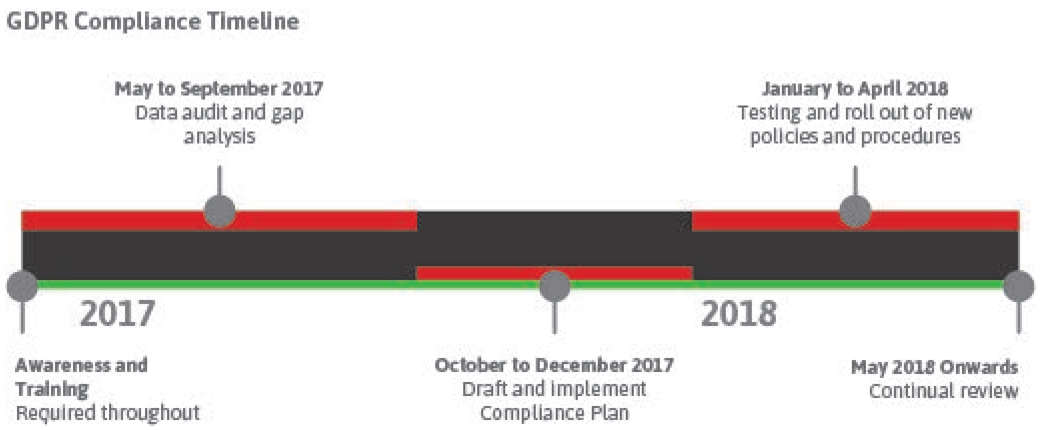
In response, the company automated its firewall audits and management to detect security and compliance problems. It tracks the identity of these problems and the responses to them so that the company's staff can confirm they have been resolved.

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.

7.0 Practical steps: What should organizations do now?

Technology needs to be brought into planning and decision-making processes at an early stage within change programmes. It should be one of the key considerations for an organization in making decisions about meeting its requirements and mitigating the risks.

Technology projects are lengthy exercises, and even a straightforward data management initiative with a singular objective can take 3 to 6 months to complete.



Source: Boyes Turner, July 2017, "GDPR: Getting ready for data's new dawn"[9]

Setting the vision and strategy for the GDPR based on an assessment of an organization's economic goals for personal data, its risk positions and its full range of obligations, is the first task.

From that foundation, there are four key activities that organizations should initiate:

Step 1: Call to action to engage a diverse and executive stakeholder group to drive GDPR change

Organizations seeking to achieve GDPR compliance will need to engage multiple stakeholders across a range of functions (IT, Compliance, Legal, HR, Customer Service, Marketing, etc.) to gather the organizational backing for the changes required. In building this coalition, it is important to note that, as well as achieving GDPR compliance, the consequent improvements of adopting good data management and security principles can deliver tangible benefits back to the enterprise. These include:

- Driving commercial performance through higher quality and more accurate data.
- Greater insight into customer needs leading to improved customer satisfaction.
- Considerable cost reduction opportunities by reducing IT infrastructure footprint.
- Opportunity to simplify the applications landscape.

The stakeholder group will be instrumental in securing budgets, resources, generating urgency and clearing the path for a consolidated programme with the backing of the board and executive.

Step 2: Assess the gap between functional GDPR requirements and technical capabilities

Enterprises should undertake a technology functionality gap analysis, whereby the technology-driven requirements of the GDPR are assessed against the technology capabilities of the organization, covering the entire data lifecycle management process and its associated policies, infrastructure, security and controls. The requirements will be driven by the Principles, Rights and Build requirements of the GDPR and the gap analysis will expose deficiencies, vulnerabilities, potential threats, and areas of non-compliance.

Step 3: Prioritise and sequence the change required by executing a risk and cost/benefit analysis

In the world of technology just about anything and everything is possible. In the real world however, time and money are limited resources, and is why the only realistic way to address the GDPR's requirements is through a risk-based approach, where the highest risk areas are addressed first and most comprehensively. Accordingly, enterprises should use the findings of their gap analysis, a cost/benefit analysis and scenario testing to identify and plan their priorities.

Step 4: Design and mobilise the GDPR transformation programme for change

A GDPR programme will be complex and transformational in nature, as it will change the way the organization's people, processes and technology interact around the handling of personal data. An integrated transformation programme structure should be adopted. This will comprise:

- Operating model for GDPR with associated organization change

- Compliance implementation of policy, procedure and control design and implementation
- Operational change and process redesign
- Technology programme consisting of detailed design, build, test and deployment
- Management of change activities including communications, training and behaviour change
- Programme and project management to govern the programme

8.0 The role of external advisors and technology vendors

While the GDPR technology framework is intended to provide a comprehensive view, organizations will have to make difficult choices about when, where and what to invest in to provide maximum protection. While some will have the scale and resources to deploy technology covering the entire GDPR technology framework, most will assess risks differently and deploy resources in a more focused manner.

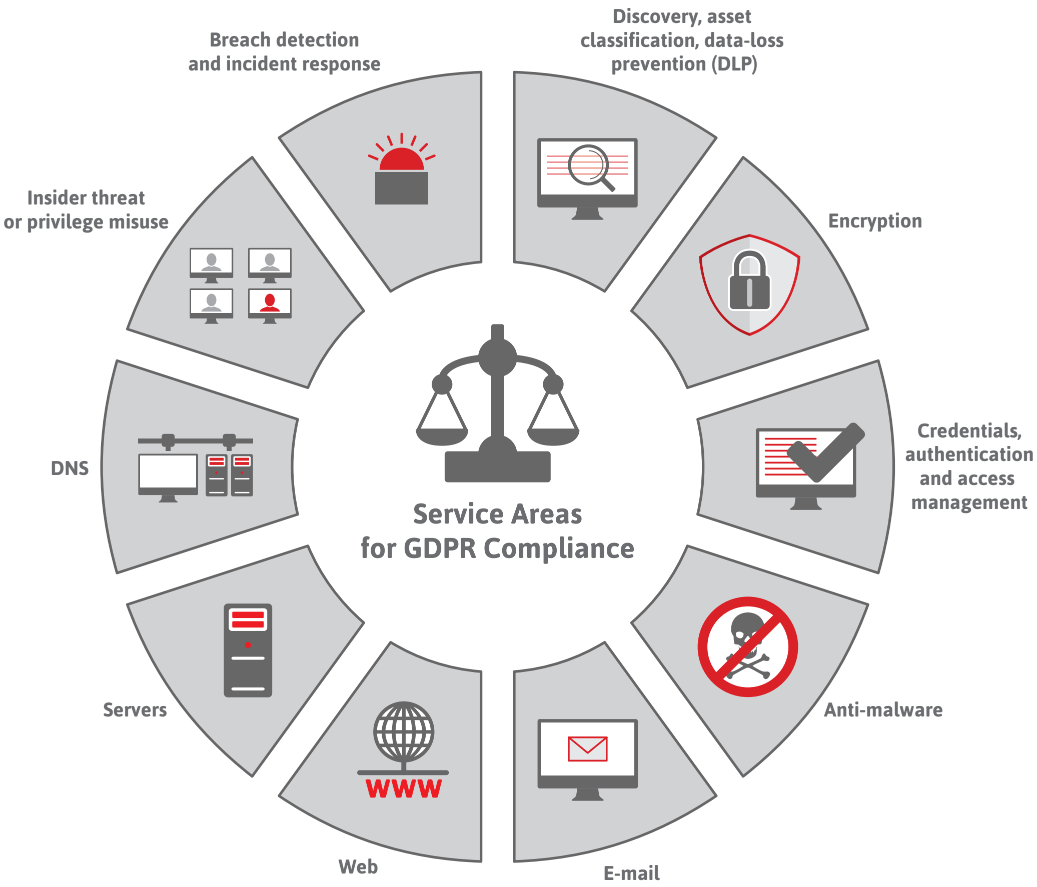
The expertise to advise on and deploy technologies will often not exist within an organization. Professional advisors, software vendors, system integrators, and IT service companies and the contractor market are resources which can plug capability and capacity gaps, especially where they bring proven expertise and understanding about the specific challenges of the GDPR.

Additional factors for vendor selection of GDPR solutions may include:

- Breadth of an integrated portfolio and interoperability with other vendors' solutions.
- Depth of analytics embedded into the solution to drive effectiveness and efficiency.
- Proven data privacy, data security and sector domain experience.
- Simplicity in packaging, such as a modular approach to procuring and deploying solutions.
- Market reputation, longevity and roadmap for product development around the GDPR solution set.

> *"The complexity of a GDPR programme is significant and the time to act is now. That means building the right team to deliver GDPR compliance is critical. Careful consideration should be given to selecting the right partners to assist an organization in achieving the strategic imperative of GDPR compliance."*
>
> Stewart Room, PwC Partner, Global Cyber Security & Data Protection Legal Services Lead & Co-Global Data Protection Lead

9.0 Technology service areas for GDPR compliance



It is impossible to create a single digestible document that might comprehensively cover a general plan to meet EU GDPR compliance for any possible organization. The following is a digest of likely "hot topics", arranged in a narrative structure, with an effort to be informed about recent evidence from real breaches in data security.

Applications used to collect, store and process personal data

GDPR mandates the provision of modern applications to govern the business processes of handling personal data about EU residents. These applications need to be demonstrably designed with security by design and by default - but also meet the various rights of the EU resident; the right of access, the right to rectify, the right to erase, the right to restrict processing, and the right to transfer, among others.

Mapping an organization's need for personal data, establishing and tracking consent, or other legal basis for holding and processing that data and keeping appropriate records of consent, activity logs and access is likely to be, of itself, a major task, particularly if handled in-house. Organizations should be challenging their IT applications provider for details of how these requirements are met in current applications - or consider moving to a provider which can meet these requirements.

As a consequence of GDPR, there are a new breed of cloud-based services available that are specifically designed to provide companies that lack the in-house capability, to meet GDPR requirements for consent capture and tracking, for example.

Dodging the bullet - PCI DSS, scoping and GDPR

One thing that working with PCI DSS in the retail and e-commerce industries teaches you very quickly is that an opening step to minimise the cost of compliance is to render as much of the corporate network out of scope to minimise the footprint for audit and certification. The same approach might be adopted in GDPR compliance.

First is the ruthless extermination of extraneous data relating to EU residents. If it is not absolutely required - don't collect it in the first place. The second technique might be the pseudonymization of personal data. This means separating data that can uniquely identify an individual from other operational data about them or the transaction they are engaged with.

Pseudonymisation tools can reduce the risks associated with breaches somewhat, but GDPR takes the view that if the data can conceivably be combined with other data to uniquely identify an EU resident, then it is still in-scope. Only fully anonymisation, that is complete separation of personal data from other associated data, would constitute sufficient technological process to render a data set out of scope. There can be no way of recombining the data with other data to identify a specific natural person.

A third technique is a general approach to limiting the number of people, applications, third parties and trust relationships that are involved or trusted by the operational personal data management system. Also to reduce the complexity of code associated with data management. In short - simplify.

Regardless of attempts to minimise the attack surface area and extent of data collection and processing, inevitably most businesses will find themselves with an amount of data regarding EU residents that needs securing and so the challenge remains. How do you go about securing personal data?

Securing personal data

Outside of the operational everyday use of applications that process or store personal data, one needs to ensure their confidentiality, integrity, and availability (CIA). The EU GDPR is notable in not being prescriptive in the technology, techniques or tools to be employed by business in this task. Given the rather fragmented nature of the network security industry - it's also difficult to find good information about a systematic approach to achieving compliance.

There are a variety of cybersecurity frameworks available that can help guide an organization's approach to reviewing their protection of data covered by the GDPR. For example; US National Institute for Standards and Technology (NIST), RFC2196 the IETF site security handbook, and ISO27001.

The NIST cybersecurity framework, for example, establishes five core functions in managing cybersecurity risk; Identify, Secure, Detect, Respond and Recover. Breaking the problem down into smaller areas to focus on is a reasonable idea.

Solution area #1 - Discovery, asset classification, data-loss prevention (DLP)

The first step in most information security frameworks is developing an understanding of what you are protecting. In a limited sense, identifying what personal data is held by an organization, where it is, what applications can access it. More modern and larger organizations have increasingly complicated digital estates. Virtualisation, cloud services, SaaS, peer-to-peer applications and many other innovations has made identifying where data is held, which device holds it, what network it traverses and even, in some cases, which CPU is processing it, an ongoing process of discovery, rather than a one-off audit.

Copies of personal data are not only found in operational systems, but also in test or development environments, analytics and log servers, exported onto company laptops or mobile devices, replicated into cloud storage or collaboration tools and even backed up remotely. Modern serverless cloud services are even challenging the assumed integrity of the bus that connects the CPU to the RAM and storage within a hardware device - now individual computing functions can be outsourced to a third party and processed on a generic processor in a cloud facility.

In light of the massive volumes of data that exist in unstructured forms across an organization, and the ever increasing diffusion of the infrastructure that is employed to process and store it, a technological response to locate, identify, catalogue and classify all of the pertinent data sources is an essential step and lays the foundation for taking action of protecting the data.

Data Loss Prevention (DLP) Applications that sit on endpoints and servers promise the capability to track down, classify and block sensitive data at a device level. Effective tools, by nature, can be monstrously complicated and aimed more at enterprises. Enterprises may also make use of “outside-in” scanning, which looks for devices visible to the Internet or containing data pertaining to company trademarks, addresses or sites. There are also software visibility tools that can track cloud server deployment on AWS and Azure, for example, and spot when servers are outside the corporate perimeter.

Discovery services build asset databases that can then be used to inform risk analysis and testing programmes.

Solution area #2 - Encryption

Assuming that breaches are inevitable, one of the first questions that will be asked of any organization after loss of data is “Was the data encrypted?” The GDPR specifically mentions encryption and it is one of the few specific technologies called out in the text of the GDPR.

If an organization has lost data in a breach and has not encrypted it, then that would be a clear indication that they have failed to meet the standards of protection required by the GDPR - because not only did the security fail, allowing the breach, but they had not understood that 100% information security is not possible to achieve. Organizations will find it difficult to refute an argument that they have not taken proportional steps to secure personal data.

All personal data, at rest or in motion, should be encrypted to minimise the damage caused by a breach.

The main task in implementing encryption systems is identifying and classifying the data to be encrypted and then the right application or device to do the encryption. It is easy to forget personal data potentially held in unstructured form - e-mail servers and recordings of telephone calls - or support process information such as back-ups and any copies used for development or testing.

There has recently been a spate of databases containing personal data appearing on insecure cloud servers when a third party or developer has quickly spun up a storage instance to stash a database for some work project, and then forgotten about it.

Encryption can be bypassed and the two most common methods are by malware intercepting the data outside of its encrypted state or the prior theft or use of compromised credentials used to access the data. So these areas should be considered next.

Solution area #3 - Credentials, authentication and access management

In the 2016 Verizon Data Breach Report, 80% of actual data breaches analysed came from outside of the company from which the data was stolen. The number one tool employed was the use of stolen, weak or default credentials to gain access (involved in 63% of confirmed breaches). For systems that are used to process or access stored personal data, passwords are no longer sufficient (if they ever have been).

Multi-factor authentication (MFA), particularly for key applications and privilege levels (administrators, for example) might have prevented some extraordinary breaches such as security consulting and audit firm Deloitte Touche Tohmatsu suffering from a breach involving an unauthorised actor having administrative access to their entire email system for an indeterminate period of time - certainly months.

However evidence from the market suggests that MFA is not employed as widely as it should be. Dropbox revealed in 2015 that only 1% of Dropbox accounts were protected by multi-factor authentication. For many users, MFA is simply annoying and restrictive - but failing to employ it in systems handling personal data, or supporting functions such as IT, is a big miss.

In addition to MFA, to reduce the impact of the loss of credentials, companies will want to educate users about good password practices, employing password management tools, registering company domains with databases of breached username/passwords in historical breaches and testing user passwords against brute force tools or assessing whether they are re-using passwords between home and work accounts.

IT and security teams also need strong procedures and tools around installing new IP devices on networks, or creating new instances of storage or processing capability using cloud services. IoT devices such as CCTV cameras, screens and environmental telemetry controls have been known to come with static default passwords or firmware flaws and in tests, such devices can be compromised within 90 seconds of being becoming visible on a network.

The use of bogus credentials has also been apparent in social engineering attacks such as Business E-mail Compromise (BEC) where company administrators have been fooled into releasing sensitive data simply by someone requesting it under the guise of a board member or trusted colleague.

Controls: At best, passwords offer only weak protection regardless of apparent length and strength. Multi-factor authentication should be mandated on all administrative business functions of any importance as well as business communication hubs (social media, for example). Education and password management tools should be augmented. Register company domain on haveibeenpwned.com or similar.

Solution area #4 - Anti-malware

Malware was the second most common tool involved in data breaches in 2015 (according the the Verizon data breach survey). Here 'malware' includes viruses, worms, trojans, backdoors, keyloggers, RAM scrapers and other software designed with malicious intent. In any form, malware is a great risk to the security of business networks in general and personal data specifically.

There are a number of mechanisms commonly involved in malware outbreaks. Phishing e-mails with infected attachments, or containing links to websites with malware laced in the content downloaded, malware woven into web-based adverts or hidden in innocuous applications available for users of mobile devices and exploits of software vulnerabilities, even USBs left near corporate offices labelled "private photos" or similar.

Tools employed to try and control malware outbreaks include, but are not limited to, e-mail filtering, anti-malware gateways, endpoint protection, application patching, restricting introduction of unauthorised hardware/storage and LAN segmentation to limit the spread of an infection or worm.

Encryption may not protect a company from malware since Ransomware threatens the availability of data, RAM scrapers and keyloggers operate outside of the traditional encryption envelope and credentials pinched by malware might be used to access data in its unencrypted format.

Increasingly even regularly updated hash or signature-based malware detection is ineffective. Network and endpoint behavioural analysis (H-IPS, N-IPS) and machine learning are driving the solution and attack complexity upwards.

Radical solutions in high-security environments have to consider physical segmentation of networks from those used for outside communications - but there are families of malware designed to exfiltrate data from air-gapped networks. Demonstrated techniques have included several categories of out-of-channel communications including data transmission through acoustic, light, EM, magnetic and other more exotic methods.

Typically more of interest to academics and military organizations, it is nevertheless a useful exercise in “blue team” security design to imagine systems robust against sophisticated actors - also a cautionary note for other organizations of the challenges in preventing breaches.

Solution area #5 - E-mail

E-mail was the killer application that motivated organizations to embrace Internetworking in the 1980 and 90s. Its use in business is now near-ubiquitous and when an organization bans use of e-mail by staff it makes the news. Where e-mail has been cut, typically because of concerns about employee productivity and work-life balance rather than security, e-mail is often replaced with a slew of new applications - chat and collaboration tools.

As a ubiquitous business tool with the capability to transfer data in, out and within the business, it has to be well-policed. Threats to information security by e-mail are many, varied and now so common they border on the mundane. Organizations should be on the look-out for malware in attachments, links to malware-infested web-sites, BEC phishing and whaling as well as sensitive data being sent out of the company as attachments or embedded within the body of an e-mail.

Over-exposure to lists of cyber security dos and don’ts and repeated training on threats via email has had an impact in the efficacy of “the human firewall”. In tests of business workers, nearly 30% of phishing emails are opened and over 1 in 10 people (12%) click on attachments they were not expecting. Only 3% of phishing emails were reported to management. Users clearly need help rather than further punitive awareness training videos.

E-mail databases are often replete with personal data, and are critical enough for the company to have invested time and effort on backing up the data. GDPR compliance will probably mean a lot of attention being given to the cultural use of e-mail within the organization, the policies around data encryption, attachment handling, inbound and outbound filtering and long-term archiving and retrieval.

Controls: E-mail filtering - block undesirable attachment types. Anti-malware and endpoint protection. Employee education. LAN segmentation. Multi-factor authentication. Data loss prevention and outbound monitoring.

Solution area #6 - Web

Web browsing is nearly 28 years old and it has come along way since NCSA Mosaic and Netscape in the nineties. For many today the world wide web and the application ecosystems that it supports ARE the Internet. It is nearly as ubiquitous as e-mail as a communication tool.

Employees browsing the web is an inbound vector for malware and outbound vector for, possibly sensitive information, sent to remote and unknowable web servers and uncountable third-party plug-ins. Companies also have estates of devices and third party services that use web control panels for administration. Company web servers offer businesses a way of automating contact with consumers and may form part of a technology solution for managing personal data.

So whether it is protecting web users within the workforce, preventing abuse of browsing facilities, defending company web applications inside and outside of the company network, the web is deserving of special attention. Speaking of web servers takes us onto the next solution area.

Solution area #7 - Servers

In actual data breaches, 35% of the assets targeted were company servers. Some were hacked using stolen credentials, others succumbed to zero-day or other vulnerabilities and still more were exploited by common web hacks such as SQL-injections and cross-site scripting (XSS).

The number one cause of actual data breaches in 2015 in financial services, entertainment, education, and information markets was web application attacks and it was a significant factor in breaches for manufacturing, professional services and retail sectors as well. If companies begin to use web tools to automate EU GDPR compliance activities such as data export, amendment and portability, web application attacks and abuse of web facilities by bots will increase.

Web servers are commonly connected to databases containing vast repositories of personal data. Alongside critical network protections, company web assets need specific web-application firewalls (WAF) to make sure that organizations don't fall foul of abuse by bots, or simple web hacks.

Server software is vulnerable to being exploited through flaws in the software itself. Software flaws are published regularly and software vendors develop security patches that are designed to cover the vulnerability and prevent an attacker compromising the server. In the worst-case compromise, an attacker can obtain administrative access and complete control through arbitrary code execution and then escalation of privileges. Lesser attacks may involve the ability to eavesdrop, or simple denial of service.

In many data breaches, attention is drawn to the patching process and policies in place in an organization. Companies often do not run the latest operating software or application versions as updating systems is complex, expensive and prone to errors making it expedient (or even necessary) to stick with legacy environments.

The recent worm outbreaks across the globe have made it clear that this vector is a concern for hundreds of thousands of businesses. The recent attacks have been for direct material gain (ransomware), but there would be nothing to stop a worm from exfiltrating data from infected systems rather than encrypting it and trying to extort money for its return.

A methodical approach to patches emphasising consistency and coverage beats expedient patching. Published vulnerabilities are exploited quickly - particularly vulnerabilities in Adobe and Microsoft software. One recent report put the median at 30 days. Old vulnerabilities are still heavily targeted and a patch may not be available - as such older systems may need to be isolated from other devices on the network and access restricted to prevent worms or other automated infection.

Routine and frequent vulnerability scanning might show a company what the attacker can already know about their estate and prompt useful remediation activities. Where patches are not available - or have to be subject to scrutiny because they might themselves impact the availability of a web application, companies might need to the tools to rapidly move servers to different security zones on the network with more aggressive filtering and monitoring until patches are available.

Controls: Server discovery. Remove unused services. Firewalling (including WAF). Consistent and comprehensive patching. Isolation of vulnerable servers. Regular vulnerability scans. Management of administrative access. Constant monitoring.

Solution area #8 - DNS

Another critical Internet service that is often considered a weak spot for attack is the Domain Name System - the mechanism by which machine-readable addresses are converted to human-readable words.

Admin account for company domains must be secured to ensure they are not hijacked and people redirected to false websites. DDoS is a constant threat to DNS servers and can result in an effective lack of availability of all online systems that rely on it. There are man-in-the-middle attacks that can see user sessions hijacked and redirected by employing domain names that are similar to, or common mis-spellings of corporate domains. Discovering these kinds of fake or pharming sites and then working to inform and educate customers and shut down offending sites might require technology solutions, particularly for organizations with large estates of domains.

Solution area #9 - Insider threat or privilege misuse

If outsiders are implicated in 80% of actual data breaches, that still leaves a sizable threat from insiders. Breaches may be proportionately rarer from someone inside the business, but they have the potential to be much more damaging. Insiders have knowledge, contacts, trust, and frequently, fewer defences to work around to achieve their objectives.

Financial gain and espionage are the main drivers of insider misuse of data access privileges, but grudges are a factor too. Fewer breaches were found to be because of management and senior staff (14%), and those with privileged access such as IT or security (14%) compared to other levels of seniority and access (35%). Most insider misuse was abuse of existing privileges for unsanctioned use, but there is also a strong threat from data mishandling (copying data to shared external drives), introduction of unsanctioned hardware or software and moving data off company premises using portable media.

Denial of service attacks from insiders has faded in recent years, but staff with administrative access to databases, portals or network devices are frequently trusted with the keys to the kingdom and have the capacity, if not generally the inclination, to fundamentally undermine availability of IT services.

Controls - Make sure privileges stop as soon as an employee stops working for a company. Monitor worker access to sensitive data particularly. Data Loss Prevention tools on common outbound data applications (cloud storage such as Dropbox, The Box and others and e-mail) can help identify data exfiltration attempts. A CASB solution might allow more granular control of user access to public cloud applications. Focus on USB drives and other portable media. Network monitoring for unsanctioned devices and applications to control 'shadow IT'. Quis Custodiet Ipsos Custodes?

Solution area #10 - Breach detection and incident response

The tail-end of the GDPR requirements is for companies to be in a state of constant readiness to respond with speed and transparency upon detection of a breach in security that has placed personal data at risk. Companies must notify the authorities (the Information Commissioner's Office - ICO in the UK) when a serious breach is detected and also the impacted users if their personal data is at risk as a consequence of the breach.

Cyber attacks vary wildly in their level of sophistication and subtlety. Technical solutions that could help in detecting subtle breaches include IPS, honeypots, log analysis, and strong security incident event management (SIEM). Regular penetration tests, DDoS tests and vulnerability scans can help identify holes in defence in advance of actual data loss.

For some breaches, however, is is most likely that the first sign of a breach will come from outside the business from law enforcement finding data after a raid or botnet shutdown - or a security researcher identifying a weakness in defences. In any event, a response plan needs to be in place with access to the tools and processes to quickly gather reliable evidence and to ensure required standards of communication to the authorities and the end users occurs in a timely manner.

In publications, the ICO is keen to point out that notification is not required for every breach and it is OK to provide notification of a possible breach in advance of having the full information as long as that information is forthcoming in a timely manner. The more severe the risk, the greater the need and expectation of rapid, accurate and transparent notification.

Other controls to consider

There are many potential other areas of control to potentially consider such as equipment and media disposal, physical security, USB or portable media management, mobile device management, but comprehensive analysis is outside the scope of this document. GDPR is not specific and any technical response is likely to be an evolution of security practises - tightening up controls where personal data is involved - much as in the same way PCI DSS focused SecOps on parts of networks and businesses that handled payment card data.

In networking circles, the Open-standards Interconnect (OSI) 7-layer model is well known and routinely referred to when discussing matters of interoperability and security across network devices. Each layer of the model has a specific function and is reliant or related to layers below.

Information security within an organization can also be visualised in layers and alongside the NIST cybersecurity framework, could lead to a method of systematically mapping and analysing an organization's information environment.

10.0 Further reading

- **NIST Cybersecurity Framework** (**NIST** CSF) https://www.nist.gov/cyberframework
- **"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 "What Works" case studies:** www.sans.org/critical-security-controls
- IETF Site Security Handbook (RFC 2196) including list from C. Pfleeger, "Security in Computing", Prentice-Hall, 1989

11.0 References

1. http://breachlevelindex.com/
2. http://quocirca.com/content/trouble-your-door-targeted-cyber-attacks-uk-and-europe
3. Osterman Research, Inc., 2017, White Paper: *GDPR Compliance and Its Impact on Security and Data Protection Programs*
4. European companies today still lag behind those in other regions in the prioritization of IR and forensics capabilities. For more details on the effects of data breaches on business reputation and how companies are preparing to meet GDPR's notification requirement, see the *"Vendor Landscape: Global Legal Privacy And Cybersecurity Services"* Forrester report.
5. For more information, see the *"The Forrester Wave™: Customer Data Breach Notification And Response Services, Q3 2015"* Forrester report.
6. http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm
7. 2017 PricewaterhouseCoopers, *"Technology's role in data protection – the missing link in GDPR transformation"*
8. A SANS Whitepaper, Benjamin Wright, Attorney, February 2017, *"Preparing for Compliance with the General Data Protection Regulation (GDPR) A Technology Guide for Security Practitioners"*
9. Boyes Turner, July 2017, White Paper: *"GDPR: Getting ready for data's new dawn"*
10. https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

About activereach

activereach is a UK-based Technology Integrator providing bespoke IT solutions to customers in the areas of Security, Collaboration and Connectivity. With a proven track record of delivering defined cyber security projects & professional services, activereach consults on the widest range of market-leading cloud & on-premise security solutions.

activereach has helped hundreds of businesses across the UK, Europe & Middle East – ranging from FTSE 500 enterprises and financial institutions to retailers and SMEs – manage and secure their network infrastructures, voice & data communications and critical information assets. Operating across activeNETWORKS, activeCONNECT and activeDEFENCE technology divisions, activereach is headquartered near London, UK.

For further information please visit www.activereach.net.

About the Author

Max Pritchard is the Senior Pre-Sales Consultant at activereach. He has over twenty years' experience in networking and security including working for Internet service providers, hosting virtualisation and automation companies and systems integrators. He consults with companies across the UK and Europe on IT risk management and cybersecurity solutions.

activereach Ltd.

4 Cliveden Office Village, Lancaster Road, High Wycombe, Bucks. HP12 3YZ
Tel: 0845 625 9025 / Fax 01494 980 255 / Email: contactus@activereach.net

Ref: WP.GDPR.2017.1