WHITE PAPER

proofpoint

THE GDPR PLAYBOOK

DISCOVER, PLAN, AND ACT ON THE UPCOMING EU DATA PROTECTION REGULATION

TABLE OF CONTENTS

INTRODUCTION

After years of negotiations, the European Union General Data Protection Regulation (EU GDPR) will come into effect on 25 May 2018, replacing the 22-year-old EU Data Protection Directive.

At its core, the GDPR aims to put EU residents in control of their personal data. It regulates how their data is collected, processed, stored, deleted, transferred, and used. Any company (local and international) that does business in Europe or handles the personal data of EU residents must comply with the new rules.

Developing a plan to comply with the new rules it is critical for all organisations. Failure to do so could lead to unprecedented fines of up to 4% of annual global revenue or €20,000,000, whichever is higher. This amount is significantly higher than any penalties data protection authorities (DPAs), within individual EU countries, have the power to issue today.

But what does successful compliance look like? What changes will organisations have to make to internal processes and what technologies should your company leverage to ensure that the personal data of EU residents are protected? How can IT and security professionals embed ‘privacy by design’ to their development lifecycles?

This GDPR playbook will guide you through how to:

1. **Discover** the current state of personal data processing within your organisation
2. **Plan** to drive the business towards full GDPR compliance
3. **Protect** all identified personal data
4. **Enhance** your compliance program through ongoing privacy assessments

Term	Defination
Data Subject	A natural individual who can be reasonably identified, directly or indirectly, by processing their personal data.
Personal Data	Any information relating to an identified or identifiable individual; an identifiable person is one who can be identified directly or indirectly, by use of personal data that could be combined with other data that would make an individual reasonably identifiable. This includes anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or online identifiers (including IP addresses and device IDs).
Controller	The person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Controllers state how and why personal data is processed. They are responsible for determining the purposes and means of the processing of personal data. But they may not be the organisation that processes the data itself. Think of a controller as the company with the direct connection with the individual/data subject and determines the means and purpose of data collection.
Processor	The person, public authority, agency or other body which processes personal data on behalf of the controller. In other words, processors act on the controller’s behalf. While the controller is the entity that makes decisions about processing activities, the processor is the vendor contracted by the controller for collecting and carrying out the processing of personal data.
Data Breach	To demonstrate the GDPR’s broad definition of ‘data breach,’ here’s the full legal definition. *‘Personal data breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed’.* While broad, the regulation does call out special categories of personal data that are subject to additional controls and should not be collected unless absolutely necessary. These include genetic or biometric data (think Fitbit data), data on political opinions, religious beliefs, or sexual orientation (think Tinder).

UNDERSTANDING THE GDPR: SEVEN PRINCIPLES TO KNOWS

Digital transformation is changing the way we work. In the modern business, employees and the devices they use to access personal data, can be anywhere. And increasingly, our marketing and customer experience teams are driving customers to engage with the business digitally through social media, mobile applications, and traditional online and email channels.

As business applications that process personal data move to the cloud, and as customers share more information through new digital channels, the risk of exposure of personal data increases. The EU GDPR is fundamentally concerned with reducing that risk. The 99 articles in the regulation sets rules on what private data can be collected, when it can be collected, and how that data should be processed and secured.

Before any action can be taken to move towards full compliance with the EU GDPR when it takes effect in May 2018, organisations must first fully understand the requirements. Built on the foundation set by the Generally Accepted Privacy Principles (GAPP) framework, the GDPR comprises seven key principles under which all regulatory rules and requirements fall.

PRINCIPLE 1: LAWFULNESS, FAIRNESS, AND TRANSPARENCY

Consumer consent is critical: Core to the GDPR is the idea of consent—the explicit consent that any EU resident must first give before their personal data can be captured, processed, and stored. To support this requirement, the GDPR narrows the scope of the EU Data Protection Directive's 'opt-in' system. It states that personal data must be collected for a very specific, pre-defined purpose. This purpose must be clearly communicated to each individual.

Shifting data control back to the individual: The 'fairness' element of the principle mandates that all EU individuals have the 'right to be forgotten' or request that their personal data be deleted from all data stores within the organisation (and from those of its third-party suppliers). What's more, 'transparency' gives individuals the 'right to access' all personal data currently being held by the organisation. Individuals can request a copy of all data held in a structured, digital, and commonly used format—a request that must be fulfilled within a month of receipt. In essence, the 'lawfulness, fairness, and transparency principle' shifts the control of personal data back into the hands of the individual.

PRINCIPLES 2 & 3: ACCURACY AND PURPOSE LIMITATION

Data authenticity is a must: Closely linked to the principle of transparency is that of accuracy. The 'accuracy principle' mandates that all personal data must be accurate and kept up to date. It gives individuals the right to request that inaccurate information be corrected. The 'purpose limitation principle' instructs that personal data can only be processed for its initial intended purpose; further processing of the collected data is prohibited without renewed consent from the individual.

PRINCIPLES 4 & 5: DATA MINIMISATION AND STORAGE LIMITATION

Limiting the scope of data collection and storage: The GDPR introduces the concept of 'Privacy by Design and by Default'—integrating data protection and privacy controls into the development lifecycle of new business processes, applications, and services that touch personal data. The 'data minimisation principle' states that only the personal data that is absolutely necessary should be collected. Further, the 'storage limitation principle' mandates that personal data must be stored for no longer than is required and that individuals must be informed about the planned retention period for their personal data.

PRINCIPLE 6: INTEGRITY AND CONFIDENTIALITY

Encryption is the cornerstones of protection: Personal data should be protected appropriately according to the 'integrity & confidentiality principle'. Building on 'privacy by design', the GDPR states that personal data should be rendered anonymous where possible. This anonymization ensures that EU residents can no longer be identified by the data. As such, restrictions on processing the data are circumvented. In addition, Article 25 of the GDPR mandates that controllers implement appropriate technical and organisational controls to safeguard the processing of any personal data that cannot be made anonymous. The effectiveness of implemented controls must be measured and documented on a regular basis.

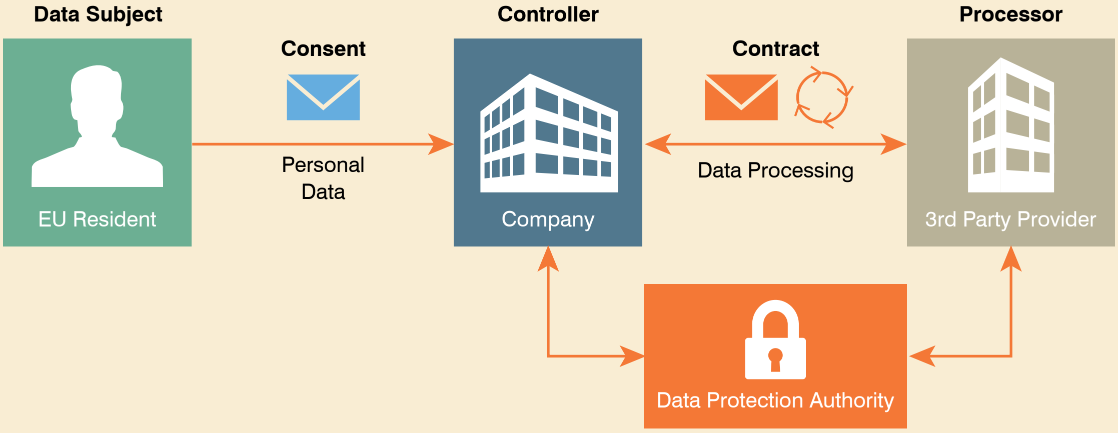
PRINCIPLE 7: ACCOUNTABILITY

Data Protection Officers govern adherence to regulation: The final principle, the 'accountability principle', instructs that all organisations processing personal data of EU residents must be able to give evidence to demonstrate compliance with all other principles. As such, organisations that systematically collect and process personal data must appoint a data protection officer (DPO). This role will be pivotal in governing the implementation of controls necessary to comply with the GPPR rules.

Data breach notification becomes mandatory: All controllers and processors of personal data must designate a supervisory authority—a country DPA who, in addition to the DPO, maintains primary oversight of all data-processing activities. Each organisation must implement a data-breach notification scheme that ensures all known breaches are reported to the appropriate DPA within 72 hours and records of these data breaches are stored.

Heightened requirements for processors. The onus is on organisations to continuously monitor, review, and enhance controls to limit and secure the processing of personal data. And for the first time, the responsibility doesn't fall fully on controllers. Under the regulation, data processors are also responsible for the maintaining the privacy and confidentiality of personal data. They must ensure adequate technical and administrative controls to protect personal data. Data must also be processed solely according to any contracts laid out between the controller and the processor. Notably, the gap between controllers and processors in terms of risk and liability has shrunk.

THE GDPR PUTS EU CITIZENS IN CONTROL OF THEIR DATA.



WHY THE GDPR MATTERS: ACCOUNTABILITY WILL DRIVE INVESTMENT

Is your business, brand reputation, and bottom line worth preserving?

The GDPR completely changes the risk profile almost all organisations will face in 2018; it sets very high sanctions for non-compliance to the stated principles. The highest fines of up to €20,000,000 or 4% of total worldwide revenue of the preceding year (whichever is higher), apply to any breaches of the first five principles (lawfulness, fairness, and transparency; accuracy and purpose limitation; and data minimisation and storage limitation). Lower fines of up to €10,000,000 or 2% of total worldwide revenue, apply to breaches of the sixth and seventh principles (integrity, confidentiality, and accountability). This penalty applies to any breach in which a company failed to either implement appropriate security controls or disclose the breach within the prescribed 72 hours.

Under the GDPR, organisations that are found to have deliberately not implemented controls to comply with the seven principles can expect the highest fines—and lasting damage to their corporate reputations. In addition to direct fines for noncompliance, the GDPR allows individuals to sue any organisation that has caused 'material or non-material' damage due to a breach of their personal information.

What's more, suppliers and third party partners that process personal data on behalf of other companies will for the first time face these fines. Processors will be directly liable to the same sanctions if they too fail to meet the GDPR's compliance criteria. Any processing of personal data done outside of contractual agreements is subject to non-compliance fines.

IMPLICATIONS ON UK DATA PROTECTION LAWS:

Brexit will have limited impact on the adoption of the GDPR in the UK. According to the UK's DPA, the Information Commissioner's Office, *'the GDPR will apply in the UK from 25 May 2018. The government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR'.*

So it's clear that the potential impact to businesses could be substantial. But just how big a problem are data breaches? The future does not always resemble the past, but we can look to data breaches disclosed in past years as a guide. According to the PwC 2015 Information Security Breaches Survey, 90% of the 664 large UK organisations surveyed suffered a security breach—this was up from 81% in 2014.[1] In the U.S., the Identity Theft Resource Center reported a record 1093 breaches in 2016 (up 40% from the previous year), these breaches led to the exposure of 36,601,939 records.[2]

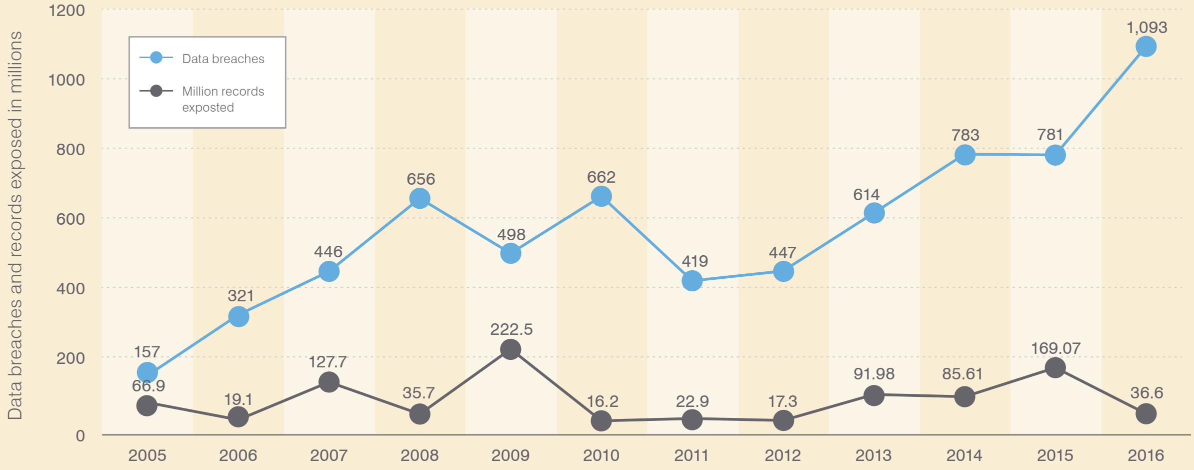
This all boils down to business impact. GDPR is not just a legal, compliance, privacy or even data security challenge. It is a business issue that requires board-level engagement. It will transform the ways in which organisations collect, process, store, share, and destroy personal data. The potential of huge fines, penalties, and risk of follow-on individual claims—let alone the potential reputational damage—are all reasons to invest in the right people, process and technology controls.

ROADMAP TO COMPLIANCE: DATA GOVERNANCE IS A LIVING, BREATHING PROCESS

So how can you comply with GDPR principles? The regulation gives guidance and in some cases specific recommendations on the people, process and technology controls your organisation must implement to comply with the seven principles. These include controls such as:

- Encrypting personal data
- Preventing unauthorised access to or use of personal data and the equipment used for its processing
- Ensuring the ongoing confidentiality and integrity of processing systems and services
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- Regular data protection impact assessments to evaluate the origin, nature, particularity and severity of data privacy risks

DATA BREACHES ARE THE NEW NORMAL



Source: Identity Theft Resource Center

- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring that data processing is secure

With over 50 mentions of the word ‘security’ in the full regulation document, security and protection are clearly at the core to the GDPR. But before you can begin implementing these controls, your organisation must first understand its current state. How is personal data currently being processed within the business? What controls are in place today? What are the gaps between the current state and full compliance with the GDPR?

STEP 1: DISCOVER—CONDUCT A DATA AUDIT

You can’t protect what you can’t see. The first step to comply is to identify and classify all personal data your organisation collects, processes and stores.

This is easier said than done. Today’s business transcends the bounds of traditional perimeters. It takes place over email. It flows through social networks. And it plays out on mobile devices and in the cloud. As the modern workforce has moved beyond the network, so does the personal data it accesses and stores. That’s why 46% of privacy professionals are most concerned that they do not have a full picture of where personal information is stored and processed outside of their main systems and servers.[3]

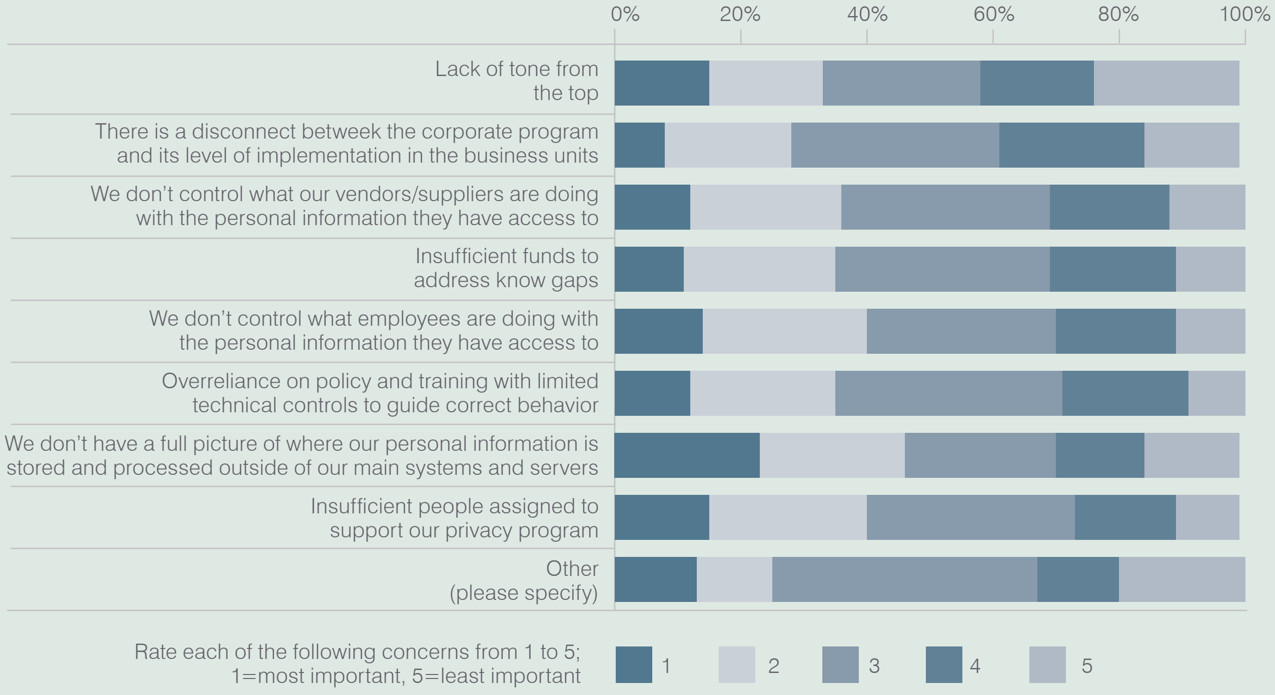
Start with an assessment of current state by conducting a data audit. A data discovery effort requires looking within and beyond your network—into every channel, every device, and every location—to identify and classify all structured and unstructured EU personal and sensitive data being captured, processed and stored. The classification of discovered data will determine the needed levels of security controls. Of course, all personal data that can identify EU residents must have the highest level of controls implemented.

Following identification and classification, map out your data-collection and -use processes. Your team will need to determine how personal data flows through the business and its supply chain. And you must and identify which third parties are processing personal EU data from on behalf of your organisation.

DATA VISIBILITY AND CONTROL A KEY CONCERN FOR PRIVACY PROFESSIONALS

EY chart—giss: what concerns most when it comes to how privacy is managed?

EY’s Global Information Security Survey 2015 privacy questionnaire asked 630 privacy professionals what concerned them most when it comes to how privacy is managed in their organization.



Source: EY Global Information Security Survey 2015

Your IT and security teams must work with legal, compliance, audit, and privacy teams to determine what controls already exist to protect personal data. Some appropriate controls may already be implemented by disparate parts of the business. Suppose the security team has done the work to become ISO 27001- or FedRAMP-compliant; it may already have a data classification scheme and an identity and access management program in place. Compliance to security frameworks is evidence you may be able to use to demonstrate to GDPR regulators that you take data protection responsibilities seriously. It should put your business in a better position to clearly define investments made in protection. But note that adherence to security frameworks alone does not cover all GDPR requirements.

STEP 2: PLAN—DEVELOP A REMEDIATION ROADMAP

Once the current state of data privacy at your organization is determined, map your findings against GDPR requirements to determine high-risk gaps that need to be secured right away. During this phase, your organization will need to translate all GDPR requirements into a controls roadmap.

This step has several facets.

Policy creation drives changes in behaviour
As part of the remediation plan, your business will need to create a set of data protection and management policies that align with the GDPR requirements. The policies must clearly define how personal data should be accessed, handled, processed, secured and stored within the organisation. These policies should be reviewed and approved by business units that will be affected by them.

Incident response plans aid response efforts: The GDPR gives clear guidelines on what must take place in the event of a data breach. Once your business is aware of a breach of personal data, you must notify affected individuals and your supervisory authority about the breach. As such, your organisation will need to develop and document an incident response process that can identify and respond to any breaches of personal data.

The focus, however, should be on recovery before notification. After detecting a breach, the business must work to restore data protection to normal levels and update controls. The incident-response plan must then also include a data deletion and breach notification process to ensure that breaches can be reported to the relevant supervisory authority within the required 72 hours.

To be successful, you will need to ensure that remediation plans are closely aligned to business processes. In other words, your deployment should enable business in a secure and compliant way. Well-aligned plans also ensure continuous visibility into new business processes that capture personal data and thus need appropriate controls.

STEP 3: PROTECT—IMPLEMENT PROCESS AND TECHNOLOGY CONTROLS

Deploying the appropriate people, process and technology controls puts you in the best position to protect your organisation from accidental or malicious data breaches of personal EU resident data.

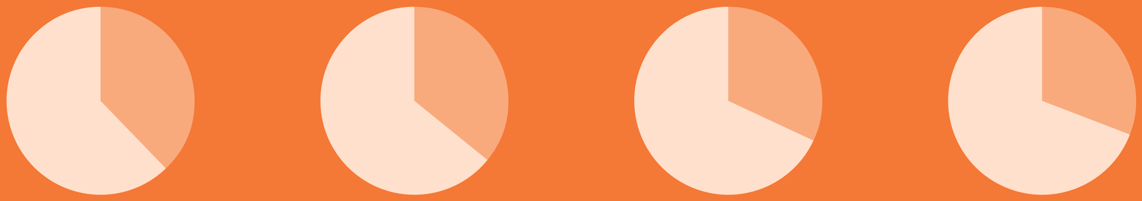
By implementing your remediation roadmap and by encrypting and protecting all personal data, your organisation reduces both the likelihood and impact of a data breach. It also reduces the risk of high fines in the event of a breach. Start by prioritising high risk parts of the business—processes that fundamentally could affect the privacy rights of EU residents. Below are some recommendations for controls that can be implemented internally to manage the protection of personal data processed by your organisation.

People—DPOs maintain oversight: If you process significant amounts of personal data on a regular basis, your business will be required to elect a DPO (be that an internal individual or an external service). This role will be critical in advising your business in all matters relating to complying with the regulation. Make sure that your DPO reports to the CEO and is involved in all issues relating to protecting and monitoring personal data.

People—business engagement will drive success: Nothing can really happen without business or executive engagement. That's why engaging senior management and forming the right team are key to successful GDPR readiness. The GDPR presents a unique opportunity to make the need for security controls to a board-level decision. A central compliance team should review the GDPR programme on an ongoing basis to measure progress to full compliance. This team (made up of legal, HR, PR, business unit leads, the DPO, IT and security) should also run periodic table-top exercises. There exercises should include mock cyber-incidents, customer requests, or data breaches to ensure that the controls put in place actually work.

CISOS WORK TO CLOSE PRIVACY GAPS

Privacy priorities for the net 12 months



38% Privacy training and awareness

36% Privacy policies and procedures

32% Privacy assessments

31% Privacy incident response

Source: PwC Global State of Information Security® Survey 2017

People—employee training programs must change behaviour: Security training programs will need an overhaul—the focus must be on changing the behaviour of your users. Internal users need to be educated on the data security risks associated with specific actions. But this must be coupled with programmes to monitor and change the behaviours of high risk users.

Process—privacy by design and by default: GDPR rules mandate safeguarding the processing of personal data. To comply, your organisation will need to ensure that controls are implemented throughout the development lifecycle of new applications and services that touch personal data. Business units, security, IT, marketing, legal, privacy and DevOps teams must collaborate to ensure that data protection is at the forefront of any major business project.

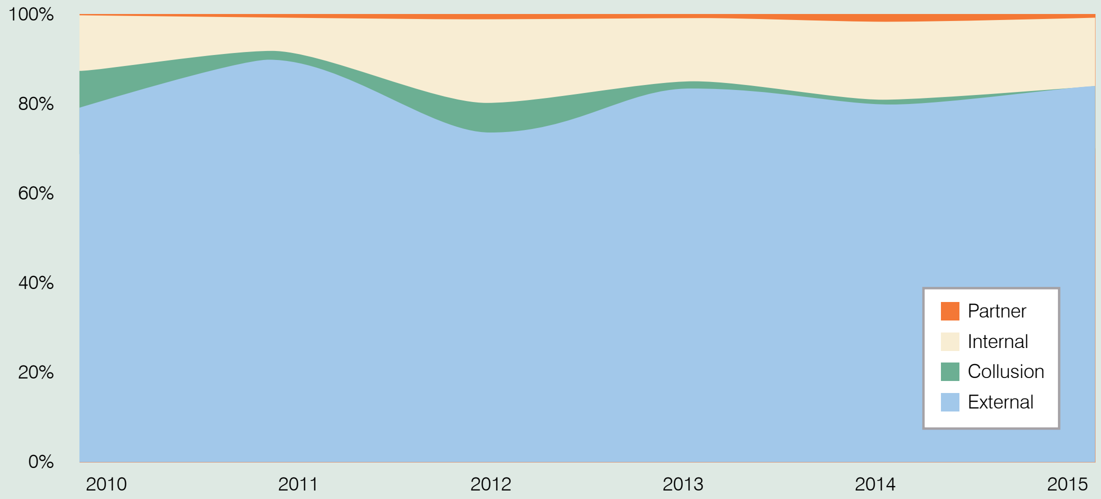
Process—identity and access management maintains control: You must implement a process that sets user access levels to critical systems (including cloud services) that store and process EU data. You must be able to track and monitor access to data and if needed, restrict that access to reduce the risk of a data breach.

Process—evidence based documentation: Keeping extensive internal records of data protection activities and incidents is required under the new regulation. The DPO will ultimately be responsible for demonstrating that your company adheres to the GDPR requirements and data protection policies created. In addition, strict rules have been set that mandate documenting all data breaches that involve personal information of EU data residents. You will need to develop a process to log, store, analyse and report any breaches (and corresponding controls that were implemented) to the supervisory authority.

Technology—data encryption: The GDPR's guidance on encryption is clear—encrypt personal data so that in the event of a data breach, the exposed information is rendered unreadable and thus reduces the risk of 'material or non-material' damage to the individuals affected. In addition, the GDPR states that EU residents do not have to be notified of data breaches of encrypted data rendered unintelligible. By encrypting personal data at rest (in storage, cloud servers, databases, or end-point devices using full-disk encryption) and data in motion (messaging encryption including emails, data files, and instant messaging; internally and between the organisation and partners), your organisation can also reduce the risk of sanctions or individual claims. Key management will be a challenge for many organisations as the scale of encryption grows. Finding encryption solutions and services that are automatic, policy-driven, and that offer access-controlled key management capabilities is crucial.

Technology—data loss prevention: Implementing encryption is vital to ensure that personal data is rendered unintelligible. But that's only the start. The ultimate aim should be to ensure the availability and confidentiality of data. More specifically, you should invest in solutions that monitor data at rest, data in use, and data in motion. These capabilities help detect and prevent any unauthorised processing of personal data that goes against your data protection policies. Deploying data loss protection solutions prevents deliberate, accidental, or inadvertent exposure of personal data.

OVER 80% OF REPORTED DATA BREACHES DUE TO EXTERNAL THREAT ACTORS



Percent of breaches per threat actor category over time (N=8,158)

Source: 2016 Verizon Data Breach Investigations report

Technology—network compromise prevention and detection: Monitor and protect personal data and devices stored within and connected to your corporate network. Segment and restrict access to parts of your network that store and process highly sensitive personal data. Access and analyse network vulnerabilities and external threats that aim to exploit them. Only by continuously monitoring and protecting your corporate network can your business better defend against threats that aim to steal personal data.

Technology—messaging and content protection: More than 90% of all data breaches start with email. Your business must deploy solutions that protect against phishing and highly targeted business email compromise (BEC) attacks. These controls should have the capability to filter malicious content and prevent internal users from interacting with threat actors seeking to gain access to the personal information of EU residents.

Technology—archive management: Set automated retention periods within databases and archives. Automated discovery and deletion capabilities are also necessary—you must be able to identify and delete all personal data on individuals should you receive a 'right to be forgotten' request.

STEP 4: ENHANCE—MONITOR CONTROL EFFECTIVENESS WITH REGULAR ASSESSMENTS

Once you have deployed controls to fill all identified gaps, you need to assess how effective they are on a regular basis.

Ongoing controls testing embeds best practice: Regularly evaluate your data protection risks. Test your incident response plans. Assess the resilience of your information systems to defend against identified risks and gauge the effectiveness of deployed security controls in preventing data breaches.

Vendor risk assessment is a must: Your organisation has a responsibility to vet the security controls of all third-party vendors that process personal data on your behalf. Assess the security levels within suppliers (processors) and contracts with those suppliers to determine whether they comply with the GDPR processing requirements. If not, you must negotiate a new data processing agreement to meet the requirements.

Your business can use security framework compliance as a means to demonstrate investments in protection. Controllers, in turn, should look for vendors compliant with similar frameworks. Assess compliance levels of all current and new vendors on an ongoing basis.

THE GDPR COMPLIANCE CHECKLIST

Here's a quick checklist to assess if you're ready for GDPR compliance.

Discover—Conduct a Data Audit

- □ our business knows (and has documented) what personal EU data it currently holds and processes
- □ our business knows how all personal EU data was captured
- □ our business knows where all personal EU data is held
- □ our business knows all third parties that process personal EU data on its behalf

Plan—Develop a Remediation Roadmap

- □ our business has created and communicated a data privacy and processing policy
- □ our business has a plan in place to detect, respond to, and report on breaches of personal EU data

Protect—Implement process and technology controls

- □ our business has designated a data protection officer
- □ our board and business management are aware of, and involved in the GDPR program
- □ our business has implemented a user awareness program on data protection
- □ our business captures EU personal data based on individual consents
- □ our business has implemented data protection controls for all major business projects
- □ our business has set user access levels for systems that process personal EU data
- □ our business encrypts all personal EU data
- □ our business has implemented advanced security solutions to prevent data breaches

Enhance—Monitor Control Effectiveness with Regular Assessments

- □ our business has a process to test the effectiveness of data protection controls (within your business and within all third parties that process data on your behalf)
- □ our business conducts a data protection impact assessment for all new processes and systems that touch personal EU data

CONCLUSIONS AND RECOMMENDATIONS

With data breaches at an all-time high, the time is now for organisations to identify and protect all personal EU data, and drive towards compliance to the GDPR–failure to do so will lead to significant disruption of business. What's more, adhering to a compliance and standards based framework can ultimately help the business attract and retain more customers. In the case of the GDPR, compliance demonstrates the organisation's investments in security, privacy, and customer care.

By building trust with consumers, businesses can differentiate and grow in an ever more competitive and global market. Your organisation must look within and beyond its network to identify and protect all personal EU data. We recommend a four-pronged approach to bridging the GDPR compliance gap:

1. 'Discover' and classify all personal data.
2. Create a 'Plan' to close all identified protection control gaps.
3. 'Protect' all personal data by developing and implementing appropriate security controls.
4. 'Enhance' security controls by monitoring, detecting, responding, and reporting on all policy violations and external threats.

[1] PwC 2015 Information Security Breaches Survey.
[2] Identity Theft Resource Center Data Breach Report 2016.
[3] EY 2015 Global Information Security Survey.

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organizations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.

proofpoint™ www.proofpoint.com