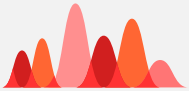
F-Secure

NAVIGATING THE NEW PRIVACY LANDSCAPE

What should organizations do before and after the May 2018 deadline to comply with the GDPR

01 THE GDPR IN A NUTSHELL

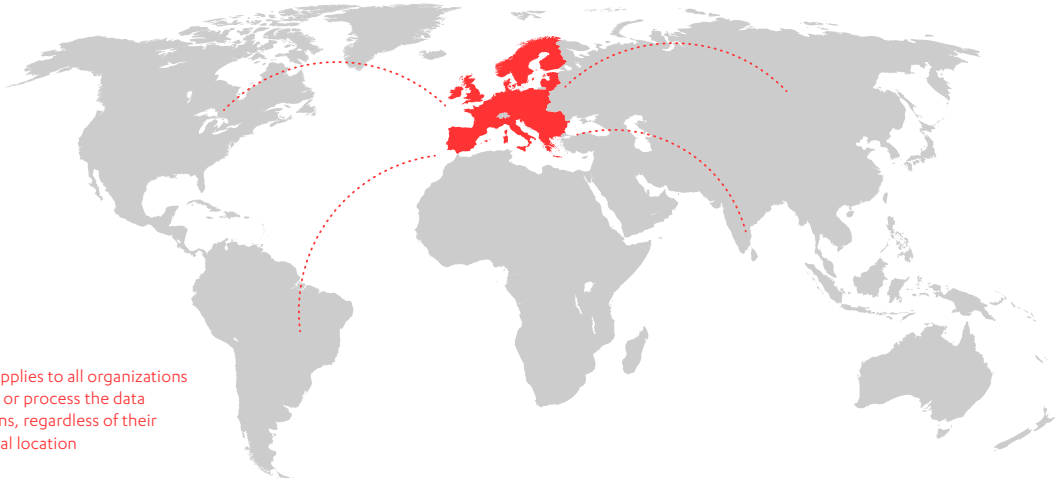


The EU General Data Protection Regulation - in short, the GDPR - will be applied from May 2018. The directive marks the biggest change in EU data privacy laws in more than 20 years, and it will have a transformative effect on the way companies manage and secure personal data.

The GDPR will apply to the processing of personal data by controllers and processors in the EU, regardless of whether the processing takes place in the EU or not. The regulation will also apply to the processing of EU citizens' personal data by a controller or processor not established in the EU, if their activities relate to the offering of goods and services to EU citizens, or to the monitoring of behavior that takes place within the EU.

THE GDPR IS DESIGNED TO:

- Harmonize data privacy laws across Europe
- Empower EU citizens and protect their data privacy
- Reshape the way organizations approach data privacy



The GDPR applies to all organizations that collect or process the data of EU citizens, regardless of their geographical location

With less than a year to go until it comes into effect, organizations are really starting to get to grips with what the GDPR will mean in practice. The regulation will bring with it new obligations, but there's a carrot as well as a stick. Getting data protection right requires an upfront investment, but offers a payoff down the line – not only in better compliance and data breach prevention, but as a competitive advantage. In the long term, the GDPR also has the potential to change the best practices within different industries, in terms of the architecture of personal data processing. After the initial compliance efforts, design changes on both business process and technical implementation levels may be the best way to ensure cost effective data protection in the long term.

Instead of focusing on quick fixes to comply with the GDPR, organizations should look beyond the May 2018 deadline and focus on sustainable improvements to identify business opportunities, while taking a proactive approach towards data privacy and cyber security. To establish this, it's important to prioritize resources, processes and people to ensure you are not only preparing for the GDPR, but also establishing an ongoing program that will eventually evolve into routine business operations.

DATA PROTECTION PRINCIPLES

The GDPR Data Protection Principles provide the conditions on which an organization is permitted to process personal data. Consequently, organizations need to ensure that their data processing activities are carried out in accordance with the Data Protection Principles set out in the GDPR.

Companies today collect vast amounts of data, despite the fact that a growing body of research shows that they do not understand or derive value from more than half of it. The GDPR can be used to evaluate what data can actually be utilized for valuable business insights, to hone processes to collect the right information at the right time, and to develop a stronger bond with the customers from whom data is collected. Simply put, it is an opportunity to make improvements that will improve the management of personal data for the benefit of both the organization and the data subjects.

DATA PROTECTION PRINCIPLES

1. Lawfulness, fairness and transparency

Personal data must be processed lawfully, fairly, and in a transparent manner in relation to the data subject.

2. Purpose limitation

Personal data must be only collected for specified, explicit and legitimate purposes and not processed further in a way incompatible with those purposes. Further processing of personal data for the purposes of archiving in the public interest, scientific and historical research, or statistics shall not be considered incompatible with the initial processing purposes.

3. Data minimization

Personal data must be adequate, relevant and limited only to those use-cases for which it is relevant.

4. Accuracy

Personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, in regards to the purposes for which it is processed, is erased or rectified without delay.

5. Storage limitation

Personal data must be kept in a form which doesn't permit the identification of data subjects for any longer than is necessary for the purposes for which the data is processed. Personal data may be stored for longer periods, as long as the data will be processed solely for the purposes of archiving in the public interest, scientific and historical research, or statistics.

6. Integrity and confidentiality

Personal data must be processed in a manner that ensures its appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organizational measures.

KEY CONCEPTS

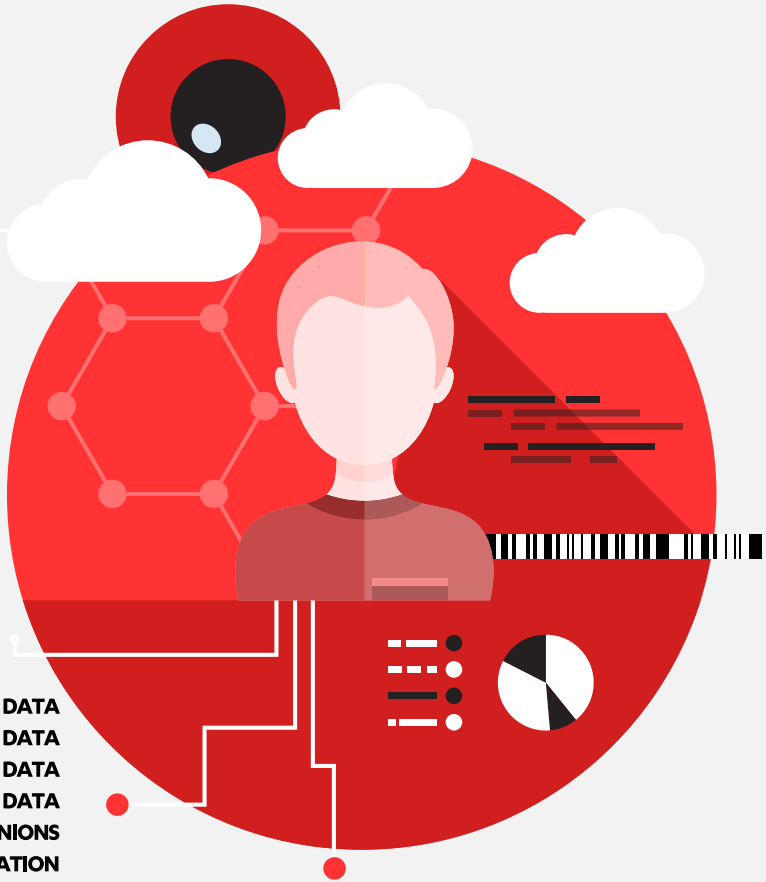
Personal data

The EU GDPR only applies to personal data. Personal data means any information relating to an identified or identifiable person, a data subject. A data subject is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data or any factor specific to the identity of that person. According to the GDPR, certain categories of online data – such as online identifiers, device identifiers, cookie IDs, and IP addresses – may be personal data.

KEY CONCEPTS

Special categories of personal data

The concept of "special categories of personal data" refers to sensitive personal data that are subject to additional protection. In general, organizations require stronger grounds to process sensitive personal data compared to "regular" personal data. Special categories of personal data includes, but is not limited to, data on an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, health, genetic and biometric data.



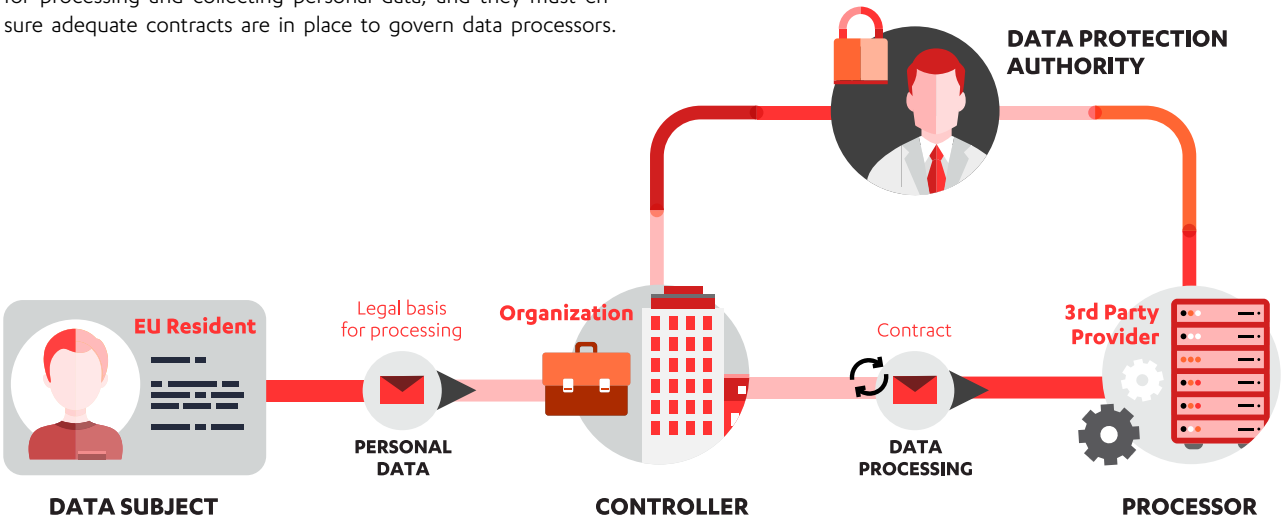
KEY CONCEPTS

Data controller

A data controller is one that, either alone or jointly with others, determines the purposes and means of the processing of personal data. Under the GDPR, controllers still bear the primary responsibility for compliance, although processors also have direct compliance obligations. Controllers must have a legal basis for processing and collecting personal data, and they must ensure adequate contracts are in place to govern data processors.

Data processor

Any entity that processes personal data under the controller's instructions. Many service providers, for example, are processors. Data processors can be held directly liable for the security of personal data.



KEY CONCEPTS

Accountability

At the heart of the GDPR is the concept of accountability for the handling of personal data. The GDPR requires that the controller is responsible for making sure all privacy principles are adhered to. Moreover, the regulation requires that your organization can demonstrate compliance with all its principles.

The new legislation encourages organizations to understand and take ownership of the risks they create for others, and take responsibility in mitigating them. The GDPR is about moving away from seeing the law as a box ticking exercise, and instead working on a framework that can be used to build a culture of privacy throughout the organization. Accountability can't be bolted on, but it needs to be a part of the organization's overall systems approach towards the management and processing of personal data.

KEY CONCEPTS

Consent

The consent of the data subject means any freely given, specific, informed and unambiguous indication of wishes by which the data subject, either by a statement or by a clear affirmative action, proclaims agreement to the processing of their personal data. For organizations that rely on consent for their business activities, the processes through which they obtain consent will need to be reviewed and revised to meet the requirements of the GDPR. Organizations should already focus on ensuring that they present clear and granular consent mechanisms for data subjects. Organizations should keep in mind that consent can be revoked by the data subject, and that may cause challenges as the data processing has to stop throughout the whole pipeline. Therefore, it's often better to seek for another basis for processing instead of using only consent as the sole basis for processing, unless it's strictly necessary.

Transparency

Organizations will need to provide extensive information to individuals about the processing of their personal data. The GDPR combines numerous transparency obligations that already apply across the EU. Data controllers have to provide information about personal data processing in a concise, transparent, intelligible and easily accessible way.

Privacy Impact Assessment (PIA)

A Privacy Impact Assessment (PIA) is the cornerstone of preserving privacy and GDPR compliant business processes and services. A PIA is intended to produce a systematic description of the envisaged processing operations and determine the legal basis for the processing. PIAs should describe the approach that an organization will take to mitigate the risks. Performing PIAs should not be an isolated compliance activity, but embedded in existing processes so that potential privacy risks and associated remediation costs are clearly understood during decision-making and approval.

The GDPR sometimes requires a specific PIA activity called a Data Protection Impact Assessment, or DPIA. The regulation requires that DPIAs are prepared for situations where data processing is likely to pose a high risk to the rights and freedoms of data subjects, particularly when implementing new technologies or during large-scale processing of special categories of personal data. DPIAs should assess the necessity and proportionality of the processing to determine the risks to the rights and freedoms of the data subjects. A more general PIA can be made to fulfill the requirements of a DPIA.

KEY CONCEPTS

Privacy by Design

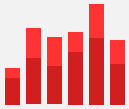
In short, privacy by design means that each new service or business process that makes use of personal data must take the protection of that data into consideration. An organization needs to be able to show that they have adequate security measures in place, and that compliance is monitored. In practice, this means that data privacy must be taken into account during the whole development cycle of a new system.

Privacy by Default

Privacy by Default simply means that the strictest privacy settings automatically apply once a customer acquires a new product or service. In other words, no manual change to the privacy settings should be required on the part of the user. Controllers or processors are only allowed to store data for the shortest possible time it takes to provide a product or a service.

Pseudonymization

Pseudonymization refers to a privacy-enhancing technique where personal data is processed without the ability to link it to a specific person. This is achieved by making the information non-attributable without additional information, which must be kept separately and is subject to various technical and organizational controls. Although pseudonymized information is still a form of personal data, its usage is heavily encouraged by the GDPR – it is even identified as a viable security measure. In addition, it can allow organizations to satisfy their obligations of "Privacy by Design" and "Privacy by Default", and it may be used to justify processing that would otherwise be deemed incompatible with the purposes for which the data was originally collected.



02 KEYS TO SUCCESFUL GDPR PREPARATION

GDPR compliance has widespread implications for various organizational functions, which is why most companies are already working hard to change their operations prior to the May 2018 deadline. Whatever process you decide on, you must start thinking about compliance on the road up to May 2018, as well as the way you'll continue from there. If your first-time compliance efforts won't give you the necessary data and artifacts to work with later, you may end up doing the work twice.

1. First-time compliance

2. Compliance from May 2018 onwards

Organizations should understand that not all GDPR or privacy risks are the same. A data breach is a very different risk compared to a case of non-compliance with subject access requirements, and managing them can be different. Your data privacy procedure should be able to differentiate between different risk scenarios, and prescribe appropriate risk mitigation strategies depending on the circumstances.

In general, companies should move on two fronts:

A. Business process level

Business processes, or value streams or customer journeys, should, should guide GDPR compliance requirements and long-term GDPR compliance work.

B. IT systems level

The systems level work should guide your data breach mitigation work.

The glue between these levels is your service design and enterprise architecture.

COMPANY-WIDE VIEW ON PRIVACY

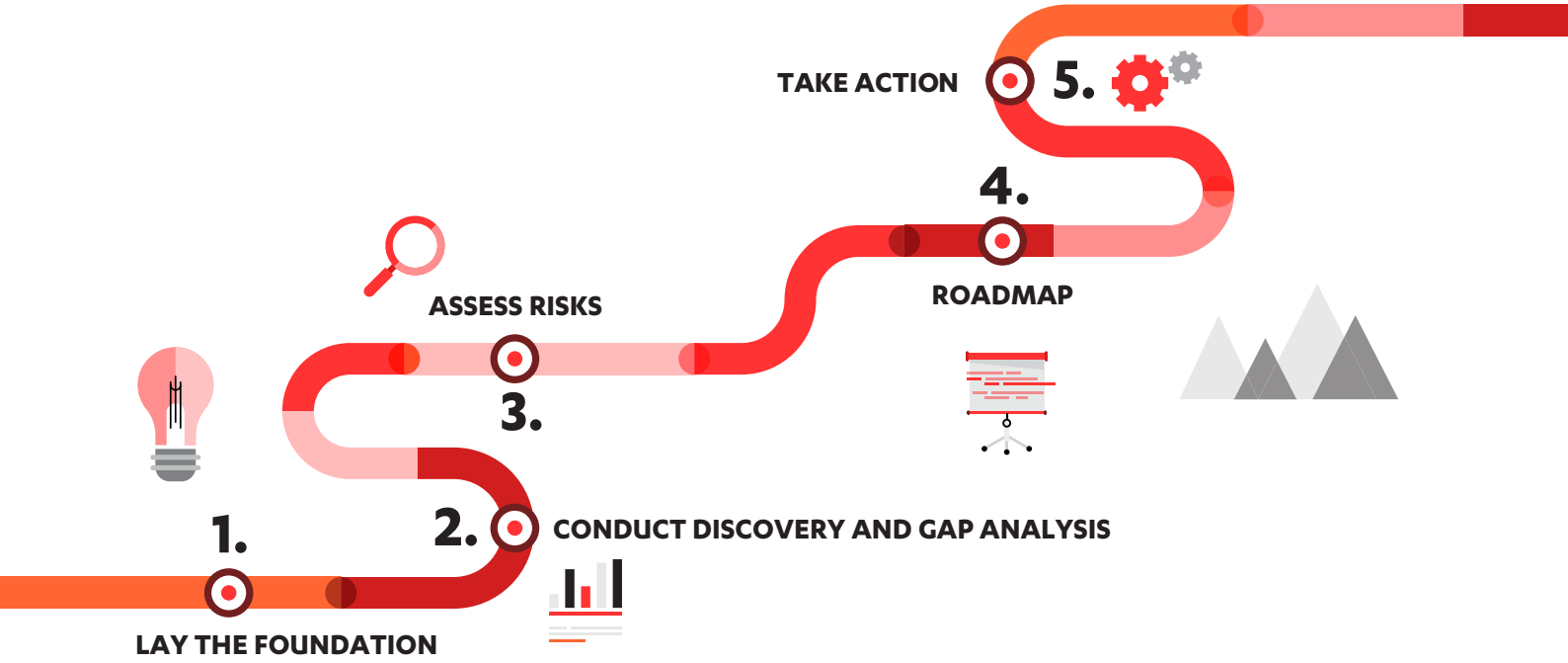
MANAGEMENT VIEW

- Data life cycle, from the viewpoint of a process or customer journey
- Description and lawfulness of data processing
- High level information flow diagrams
- Legal contracts
- Management and mitigation of quantified risks

SYSTEMS VIEW

- Data life cycle, from the viewpoint of technical implementation
- Alignment of technical implementation and description of processing
- Data flow diagrams
- APIs and API contacts
- Security controls

HOW TO STRUCTURE
THE PREPARATION WORK?



HOW TO STRUCTURE
THE PREPARATION WORK

1. Lay the foundation

The first thing that any company needs to do is to review the GDPR thoroughly, and raise awareness of the upcoming changes within the organization. For the success of GDPR compliance, it is essential to get senior level buy-in and properly engage all the key stakeholders. Only after the key stakeholders are committed, can the organization start identifying the most important focus areas for compliance.

Every successful compliance project starts from the organization's core business objectives. The key questions that executive leadership teams should be asking themselves are:

What is it that your business wants to achieve now? What about in 5-10 years?

What (personal) data is needed to achieve these strategic business objectives?

A compliance project will not produce optimal results if it isn't based on a clear business strategy, no matter how well it would be managed.

HOW TO STRUCTURE THE PREPARATION WORK

2. Conduct discovery and gap analysis

Next, you should document what personal data you hold, where it came from, and with whom you share it. It's important to identify and classify all personal data your organization collects, processes and stores. Once you know what personal data is being processed, where, by whom, and how, the next step is to identify where you are with your current compliance measures. Again, this gap analysis should ideally start from the strategic view to personal data.

HOW TO STRUCTURE
THE PREPARATION WORK

3. Assess Risks

Based on the information gathered on your current data processing activities and corresponding compliance measures, you can perform a gap analysis to identify the needed steps for GDPR compliance in May 2018 and years beyond that.

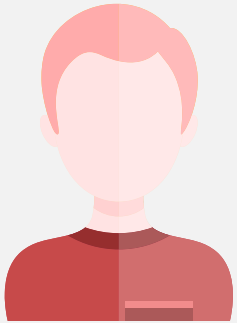
4. Roadmap

Once both your business ambitions and the current state of data privacy is laid out, map your findings against the GDPR requirements to determine high-risk gaps that need to be secured right away, and work to prioritize compliance in general. Your action plan should cover not only all the tasks that need to be completed by May 2018, but any other actions needed to ensure long-term compliance.

5. Take Action

Contribution from various teams is required for any GDPR roadmap to get executed well. In the next chapter, we'll discuss the roles of each organizational function in creating long-term GDPR compliance.

03 WHO SHOULD BE INVOLVED



Most often, the primary responsibility on the GDPR preparation project falls on the shoulders of either the Chief Privacy Officer, Chief Information Officer, Head of Compliance, Chief Information Security Officer, or the like. Choosing the person who should lead a GDPR project also depends on your organization's approach to GDPR, and the specific requirements of your industry.

The GDPR is a business issue that must include all levels of management, from the C-Suite down to various other functions of the organization. The GDPR requires cross-functional collaboration if businesses are to comply with the regulatory changes by 25 May 2018, and drive effective long-term transformations within their organizations.

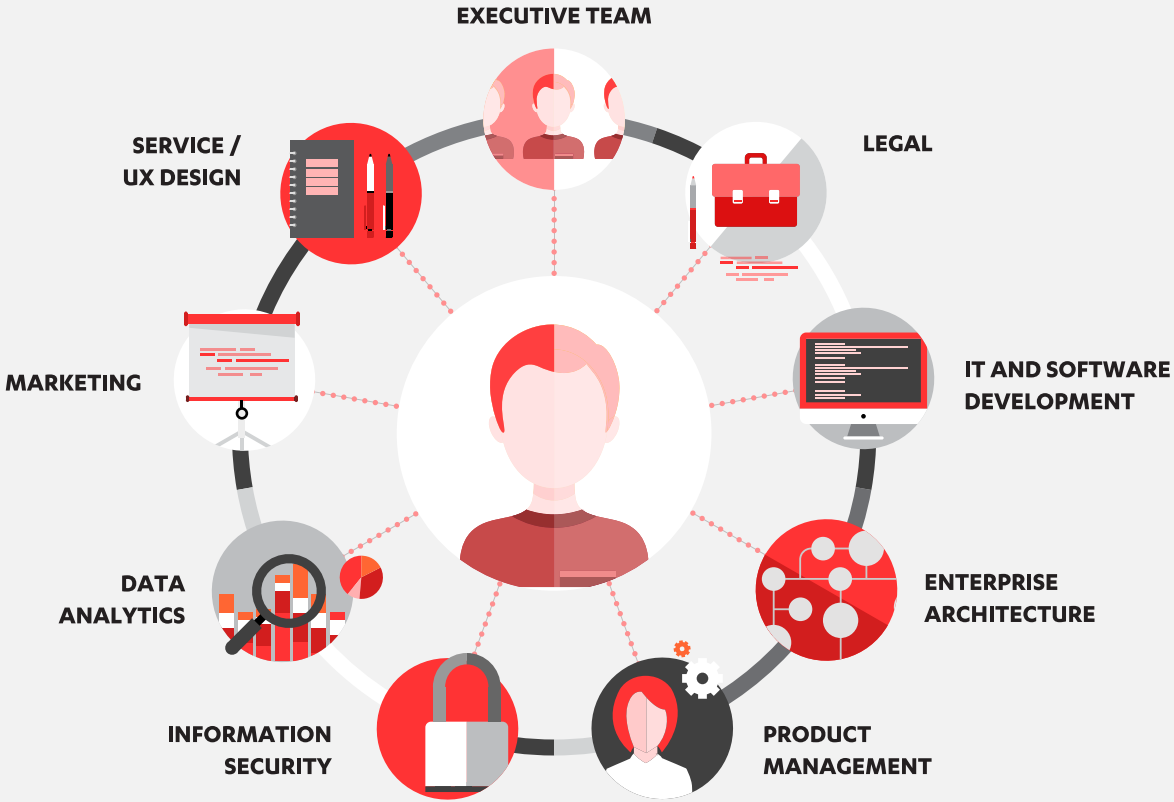
Companies that hold and work closely with EU citizens' personal data should be involving most, if not all, of their departments in the process and ask some basic questions around how and why they collect and use personal data – they should also focus on the value it has to each respective business function. Such an approach will inherently allow the development of a business case for the changes ahead, and create the required motivation within each department to allocate the necessary resources for the project.

GDPR preparation is not just an IT project, and neither is it an initiative solely impacting the work of Privacy or Security Officers – quite on the contrary. Collaboration will be vital in driving compliance. For example, marketers must work closely with the Legal and IT departments in order to be transparent over their handling of customers' personal data, and IT teams should liaise with Legal to review supply chain arrangements, revising contracts where necessary.

The purpose of combining the efforts of various functions in the GDPR preparation work is to:

- Implement GDPR compliant policies, process and procedures across the organization
- Ensure IT solutions will support business objectives
- Ensure that Privacy by Design and Privacy by Default principles are applied across the board
- Raise awareness across the whole business
- Coordinate data privacy activities across all business units

WHO SHOULD BE INVOLVED



WHO SHOULD BE INVOLVED

Executive team

Gaining executive support and cooperation is the first step in complying with the GDPR. Having board level buy-in from the beginning is critical, as is appointing an executive leader for the compliance work. GDPR isn't primarily a security issue nor is it all about IT – it's a business problem that relies on cross-departmental collaboration from all stakeholders to be successful. Appointing a strong centralized GDPR leader with a core GDPR team across different business units is the first step in progressing toward GDPR compliance. However, the core GDPR project team needs to be accountable to the board and executive leadership teams, with direction coming from the top down.

What this boils down to is that executives—the entire C-suite— will need to take responsibility for implementing and delivering GDPR. It is not going to be enough to appoint a Chief Privacy Officer and leave him or her to manage the needed changes without back-up and budget. Instead, there needs to be an organization-wide change in mindset, towards one that supports and promotes data protection – not just because it's required, but because it's the right thing to do for the customers.

WHO SHOULD BE INVOLVED

Legal

An organization's Legal team will need to know the GDPR by heart, and be prepared to advise the rest of the company throughout the preparation process.

It is a common misconception that the GDPR would forbid companies to use personal data for their benefit – this is not the case. In most situations, personal data can still be utilized for the benefit of the business, but organizations will have to rethink why and how it's managed. The collection of data is accompanied by the responsibility for it, for example companies having to inform data subjects on the extent of their collection activities.

In addition to strategic advisory, the Legal team will be involved in the practical compliance work, reviewing any legal agreements with third parties, particularly if the company has controller-processor relationships. All of these need to be revised as part of a GDPR preparation program.

WHO SHOULD BE INVOLVED

IT and software development

Data protection is not the sole responsibility of the IT department, but it's no surprise that IT needs to be a major contributor for the GDPR implementation to have a successful outcome. IT teams are in charge of, for example, the access controls to personal data and ensuring the "ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data".

The GDPR also impacts the software development life cycle (SDLC) for any systems that would process EU residents' personal data. There may be new functional requirements, especially on subject access rights, and of course, software security needs to be ensured. Organizations would also need to gather evidence of privacy and security activities in the SDLC.

The owners of different IT systems need to technically comply with GDPR requirements. Should an IT system have several internal customers, their potential overlapping but divergent systems requirements need to be satisfied.

WHO SHOULD BE INVOLVED

Enterprise Architecture

It is typical that a GDPR program is driven by Legal, Information Security, and IT, but for a GDPR compliance project to succeed, a company's architectural function needs to be also tightly involved. Long-term, and cost effective, GDPR compliance can only be attained if the organization's enterprise architecture supports the GDPR's requirements.

To ensure your organization's compliance, you need a broad overview of the way personal data is used and why it was collected, how it is processed, who has access, where it is stored, which third parties are involved, what internal and external threats there are, and so on. Enterprise architects have a uniquely broad and integrated view of their organization, and have the models and tools at their disposal to assess, improve and assure data protection.

1. Enterprise Architects can provide insights into all processes, applications, and data that are relevant to GDPR compliance. Furthermore, they can offer information on data objects, data flows, and associated responsibilities.
2. Enterprise Architects can draw attention to risks and potential compliance breaches. They can also help technology owners identify technology risks and prepare preventative measures within the scope of their responsibility. The risk identification role of the architects is especially important for the privacy impact assessment (PIA).
3. Moreover, the GDPR not only demands compliance, but also requires you to demonstrate compliance. Architecture and architectural models are the major source of this information, in particular when you need a coherent and connected view of everything related to personal data.
4. Additionally, enterprise architects can be instrumental in defining application development guidelines that conform to the new principles of data protection. Such guidelines will naturally apply to developers, but they also apply to system architects, database architects, security analysts, and other personnel who must be up to speed on the different ways GDPR affects their roles.
5. Finally, enterprise architects are well-situated to ensure continuous compliance with GDPR, and therefore they serve a critical day-to-day role within the processes that the regulation impacts.

Long-term GDPR compliance can only be attained in a cost-effective way if the organization's enterprise architecture supports GDPR's specific requirements. In order for this to happen, the organization's architecture function needs to be heavily involved in a GDPR program – not just as an "informed" party, but as an active participant.

WHO SHOULD BE INVOLVED

Product Management

Product owners are similar to IT system owners, but for software development companies. They must balance feature development with other requirements, like security and privacy, and these are the people who have to implement "Privacy by Design and "Privacy by Default" in practice. Product management personnel become increasingly relevant when trying to maintain GDPR compliance in the long term.

Service / UX Design

There are some specific requirements laid out by the GDPR that need to be taken into account in the customer journey through a service, related to the informing of customers and getting their consent. It is important to think about the ways the new protection measures can be integrated in the service experience without alienating customers.

WHO SHOULD BE INVOLVED

Data Analytics

The GDPR's data lifecycle requirements, particularly those of anonymization and data removal, put up serious challenges for big data and analytics technology on a practical implementation level. Much more will need to be done by way of anonymizing data before it can be analyzed. The GDPR means that any unique identifier, whether a name or a pseudonym, is covered by law, and therefore subject to the same levels of protection.

It's worth reiterating that not all big data is personal data, and it's often possible to take personal data and anonymize it for the purposes of analytics, thus descoping it from data protection regulations. That said, much of big data analytics does involve personal data, and as a consequence data protection is clearly relevant in this space. The UK Information Commissioner's Office (ICO) points to three main areas of consideration:

1. Does the way in which individuals' data is being used have an intrusive effect on them? There's a particular concern here in regards to how data can be used to profile individuals.
2. Is the use of people's data for big data analytics within the scope of what they might reasonably expect?
3. How transparent can the organization be about the ways in which it is processing personal data? Given the complexity of much of big data analytics, this can be a challenge.

WHO SHOULD BE INVOLVED

Marketing

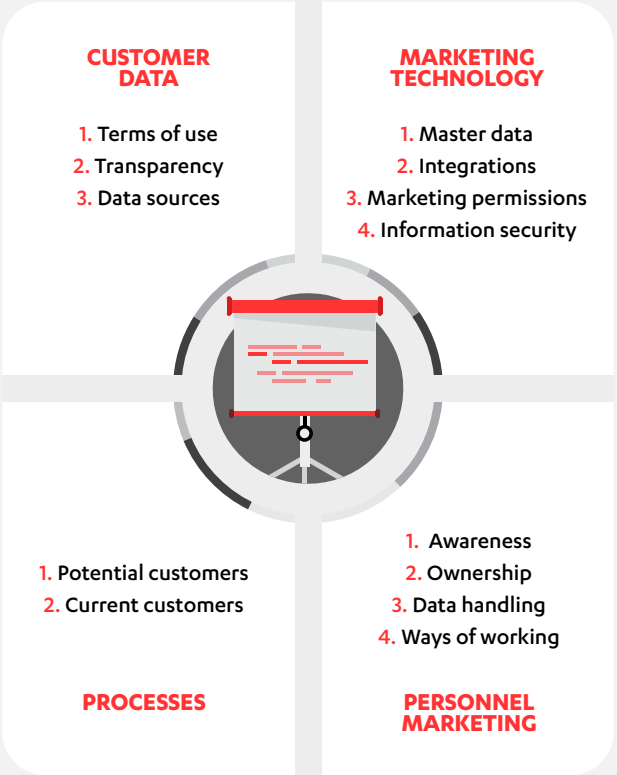
The GDPR will bring with it several changes that affect organizations' marketing operations, especially when it comes to digital marketing.

Website privacy policies need to be reviewed and updated. Also, companies must make sure that their consent management is in shape and functioning properly in all markets. When it comes to marketing automation and CRM, organizations should put pressure on the tool and service providers to make sure that they are compliant with the GDPR and have the rights to use the data. To get all this done, companies need to train their employees and create awareness for the implications that the GDPR will have on their activities – this applies especially to organizations with global marketing teams.

In order for "consent" to serve as lawful basis for processing personal data, it must be: "freely given, specific, informed and an unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her".

The GDPR sets specific requirements for marketing consent. For example, when a marketing consent is revoked, marketing must stop immediately. This may cause challenges, if your marketing data has been shared with agencies in formats such as manual Excel sheets.

In addition to the GDPR, the ePrivacy directive also strongly regulates this area. Thus, the future ePrivacy regulation needs to be watched closely by the marketing function, as it may have an effect on opt-in/opt-out rules and cookie practices.



WHO SHOULD BE INVOLVED

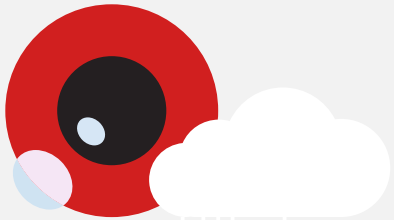
Information Security

IT Security is clearly one of the most important functions when it comes to preparing for the GDPR. The Chief Information Security Officer (CISO) is the most senior decision maker when it comes to cyber security, and is in a pivotal role in protecting the business from damaging attacks resulting in data loss. The CISO and the whole Information Security team should be heavily involved in formulating GDPR plans, as they are central to some of the regulatory changes around data breaches and data privacy.

For anyone working in IT Security, there are a few high level areas to consider when preparing for the GDPR:

1. **Understand the risks** — Information security teams will need to understand exactly what personal data their company is collecting on EU citizens, and if the exposure of that data could fall under the GDPR's definition of a personal data breach.
2. **Breach prevention** — In doing this, companies are able to minimize the risk of a data breach by putting protections in place to make it harder for their data to be hacked.
3. **Breach detection and rapid response** — With the new 72-hour notification mandate, security teams will need to be prepared to react to a breach extremely quickly.
4. **Think beyond the GDPR** — There are numerous other aspects of cyber security risks that information security teams will need to consider, even though they are not laid out in the GDPR. Cyber security is a continuous process, and constant improvement is the only way to stay on top of the game.

In the next section, we'll deep dive into the effects that the GDPR has on cyber security.



127.255.255.255
191.255.255.255
223.255.255.255
127.255.255.255

04 WHY CYBER SECURITY MATTERS

From a GDPR perspective, data controllers are expected to assess whether their processing activities, and the potential risks for data subjects resulting from those activities, are covered by their current security measures. In this regard, the regulation does not state the specific security measures (or the minimum technical standards of such security measures) companies need to undertake to be considered compliant with the legal regime in force. The regulation simply makes it the companies' duty to assess and decide what types of measures shall be implemented in order to comply with the regime stated in the GDPR, and to ensure that all precautions are undertaken to minimize the risk of data breaches and leakages.

Most organizations have deployed comprehensive technical measures around cyber security and data protection. Still, we hear about data breaches that affect millions of users on a monthly basis. Breaches continue to happen because attackers have become adept at targeting attacks and evading defenses. The operating presumption must be that your organization's IT infrastructure is under continuous attack, and potentially already compromised in multiple ways. This effectively shifts the conversation from threat prevention to threat detection and response.

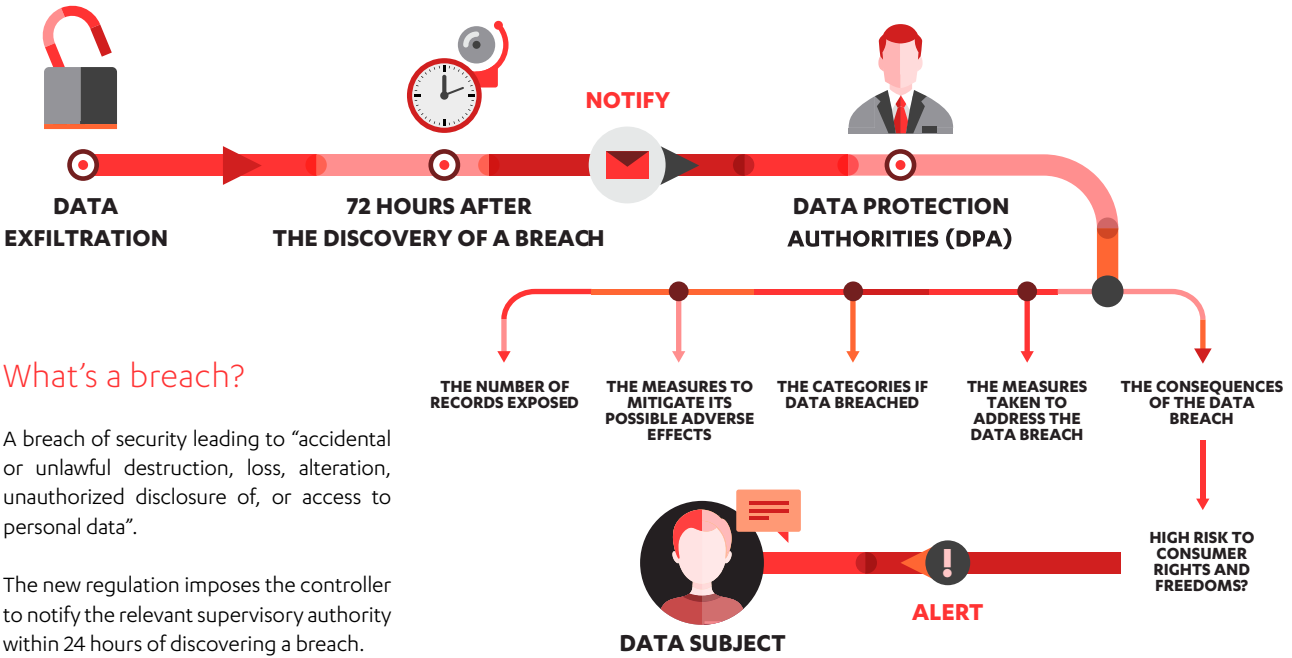
The GDPR will require companies to notify authorities within 72 hours of identifying a breach. This new requirement can be a game-changer. The GDPR requires organizations to provide in-depth details on a breach, including the following information:

1. The nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned
2. The name and contact details of the data protection officer or other contact point where more information can be obtained
3. The likely consequences of the personal data breach
4. The measures taken, or proposed to be taken, by the controller to address the personal data breach, including measures to mitigate its possible adverse effects

All this in just 72 hours. Thus, organizations should consider technology solutions that provide visibility across the network to rapidly detect and understand the full scope of a compromise to aid in fast and effective response. Solutions with behavioral analysis, AI and machine learning will help your organization hunt for the threats that have successfully invaded your organization. Undetected, such exploits can wreak havoc on your infrastructure and intellectual property, and lead to the types of data breaches the GDPR covers.

The bottom line? Companies need to continue investing in threat prediction and prevention, but also focus on building top-notch, 24/7 incident detection and response capabilities.

WHY CYBER SECURITY MATTERS



What's a breach?

A breach of security leading to "accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data".

The new regulation imposes the controller to notify the relevant supervisory authority within 24 hours of discovering a breach.

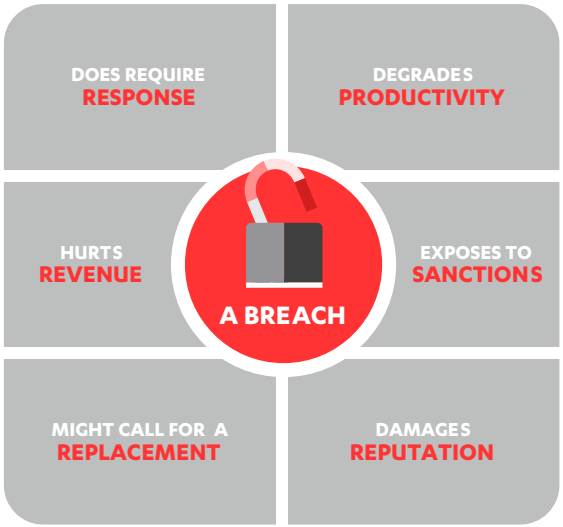
WHY CYBER SECURITY MATTERS

Client data from the F-Secure risk management assessments suggests most large organizations are ill-prepared to handle breaches. While 50% have a crisis management team that's prepared for physical disasters or business disruptions, only 20% are capable of effectively leading during a cyber crisis. 65% of companies have never run a crisis management exercise to rehearse for a cyber incident.

Deploying the appropriate people, processes and technology controls puts you in the best position to protect your organization from accidental or malicious data breaches. By implementing your remediation roadmap and protecting all personal data, your organization reduces both the likelihood and potential impact of a data breach.

And these impacts can, at worst, be substantial, which also signals a high level of risk. Consider the risk of a data breach versus the risk posed by non-compliance with subject access, for example. The notable difference is that in a data breach, you aren't in the driver's seat – you lose control completely.

Many GDPR-related articles put a heavy focus on the fines associated with the GDPR: they can be up to €20 million, or 4% of a company's global annual turnover. But in reality the fines are only a fraction of the total costs of a data breach. More importantly, data breaches usually have far-reaching consequences in the form of degrading revenues, reputational damage, decreases in productivity, and more. For this reason, it's vital to invest in proper breach prevention, detection, and response.

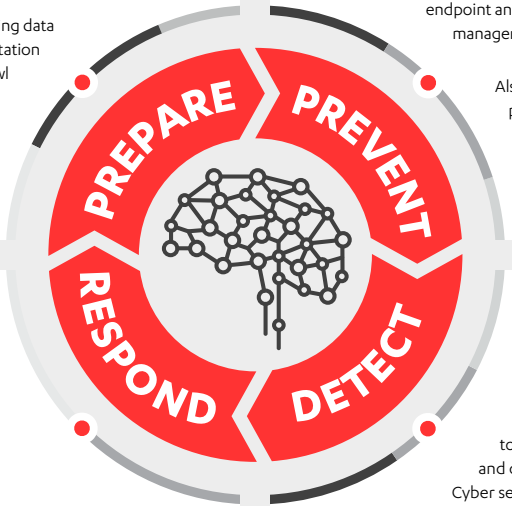


WHY CYBER SECURITY MATTERS

Find out where you process personal data, what is the lifecycle of the data from collection to deletion, and how the data is protected at any stage of the lifecycle.

Reduce your exposure by technically implementing data minimization and anonymization. Apply segmentation to the personal data assets, and reduce the sprawl of personal data through systems.

Create processes and ways of working, for example, internal breach notification and action plan.



Make sure you have the needed preventative measures in place in your systems. This includes, but is not limited to, proper endpoint and service protection, as well as vulnerability management solutions.

Also, cyber security should be weaved into product and service development and purchase processes from the beginning, not as an afterthought.

Make sure that the key people in your organization are ready to respond to breaches and know what to do to mitigate the damage.

After an incident, analyze it thoroughly and learn from it.

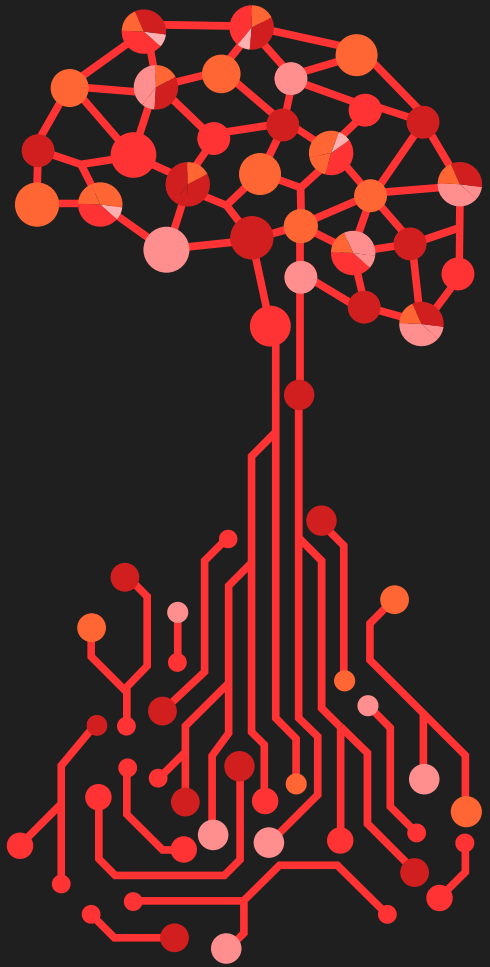
Make sure you have the tools and especially the human expertise you need to recognize incidents and threats, isolate, and contain them right when they happen. 24/7. Cyber security is never "off".

LIVE SECURITY:
A CONTINUOUSLY IMPROVING APPROACH

Cyber security moves too fast for silver bullets. Your attack surface is growing, and attackers are constantly developing new tactics to breach the defenses. In cyber security, there's only one constant. Change.

Ultimately, cyber security comes down to predicting and preventing breaches, detecting the ones that do happen and then responding intelligently to minimize their impact. This takes a combination of human expertise and software scalability. Because you can't improve your cyber security operation without the smartest cyber security talent. And you can't scale what they know without smart technology.

Behind every attack, there's a human attacker. And the attackers are constantly curating more advanced attacks that easily bypass purely automated solutions. That is why also your defense needs to be powered by people. People who can think like the attacker would, react to situations technology is not capable of, and who can train automated technology to become smarter, day by day.



WE'RE F-SECURE

For too many businesses, too many manufacturers, too many people, security is an afterthought. What's the use of being connected to everything, if our data, our identities and our transactions aren't secure?

From almost thirty years of protecting millions of computers around the globe, we know this for sure: you will be the target of an attack. The only question is if you have the needed capabilities to predict and prevent attackers from getting into your systems, detect them in time and respond swiftly and effectively.

To do all that, you need the right team in your corner. For F-Secure, cyber security is more than a product—it's how we see the world. Read our Business Security Insider blog to get the latest insights from the frontlines of the industry. And if you're looking for a cyber security partner that always keeps you one step ahead, we should talk.

www.f-secure.com
business.f-secure.com
www.twitter.com/fsecure
www.facebook.com/f-secure

F-Secure