KASPERSKY lab

GDPR – more than checkboxes

Cybersecurity solutions on their own cannot ensure compliance but do provide effective protection against data breaches and sensitive data leakage.

www.kaspersky.com

#truecybersecurity

GDPR – more than checkboxes

"No privacy without security" is a long-standing tenet of data protection. As the EU General Data Protection Regulation becomes reality, it's time to take a look at how cybersecurity technologies can support the broader data protection and privacy aims of the Regulation.

Personal data: a cash cow for cybercriminals

Personal data is literally everywhere.

People routinely submit personal information to organizations of all kinds, often without questioning or understanding why or how it will be used – or the unknown third parties it will be shared with.

In 2017, 23% of organizations subject to GDPR said they'd experienced a cyberattack in the previous 12 months.[1]

We've all scrolled to the end of a vague End User License Agreement (EULA) and clicked 'Agree', without really knowing what will happen to our data. By making service conditional on doing this, many organizations effectively force users to take the risk that their data could end up in the wrong hands. Unfortunately, it often does.

While the majority of organizations do their best to protect the data they gather, it's often done without any real sense of purpose beyond vacuuming up information that 'might come in handy.'

With the best will in the world, a lack of established processes, combined with limited awareness of the accompanying risks and responsibilities, often means data is collected and stored without any security precautions. Worse still, it's often shared with (or sold) to third parties without implementing any data protection agreement – or the data subject's knowledge or explicit consent.

Unfortunately, the type of personal data that's useful to your business is also lucrative to cybercriminals: from loyalty programs to payment data, date of birth and medical records, anything that helps your business personalize customer experience or take care of employees is highly attractive to cybercriminals. Ultimately, it becomes a kind of criminal currency, exchanged and traded on the black markets of the Darknet.

From May 25th 2018, when something like this happens, it won't just be your unfortunate data subjects' problem – it will be yours too.

1 Marsh: GDPR Preparedness: An Indicator of Cyber Risk Management (October 2017)

59% of businesses assume that their IT security will be compromised – and recognise the need to be prepared for these events.[2]

Data breach? Fine

Following a massive customer data breach in 2015, UK telecoms company TalkTalk was fined a record-breaking £400,000 by the Information Commissioner's Office.

The fine was so high because it was found that the breach could have been prevented if the company had taken basic steps to protect customer data.

Under the GDPR's maximum penalty of 4% of global turnover, that £400,000 fine could be as much as £60 million – if the full extent of the law was exercised. At the very least, audits, monitor and an overhaul of processes would be involved – all of which cost money.[3]

Four little letters, one big data protection initiative

The headline issues of a 4% of global turnover fine and 72 hour breach notification requirement are attracting a lot of attention. But it's worth stating that GDPR is your chance to take stock of what you do with the personal data you collect – and ask yourself why you're doing it.

It's also a perfect time to re-consider your organization's approach to cybersecurity – because while security technologies on their own cannot ensure compliance, they play a key supporting role in helping companies achieve their data protection goals.

What it is, what it isn't...

Despite the large number of documents, how-tos and other publications that followed its announcement, basic understanding of many aspects of the GDPR remains vague. Some C-level managers continue to believe the legislation doesn't apply to them because "We don't have that kind of data." Others believe it's a once-off checkbox exercise before carrying on business as usual.

Unfortunately, they're both wrong:

- You have employees, right? The information you typically gather and process about them is personal data and falls under GDPR. Every company that collects, processes and/or stores personal data, including employee information relating to a transaction or activity in the EU– or outsources it to a third party – is obliged to protect it.
- GDPR is not prescriptive, it's a framework. There's no list of tasks to tick off before arriving in data protection Nirvana.

While GDPR provides rules to follow for compliance, there's little detail on the specifics of how to get there – the techniques are largely left to each organization to decide for itself. The key point is that, because data protection is a process, this is something that companies should continually work on.

There's no standard approach to gauging compliance. Box-ticking can only get you so far. Circumstances (and associated risks) change and lists are seldom exhaustive, meaning weak spots can be overlooked in any 'one size fits all' approach.

Ultimately, it's what your business does to help avoid an incident – along with your strategy for early detection and tracing – that will go a long way towards helping you with GDPR.

Kaspersky Lab's next-generation technologies and solutions can help your organization achieve its cybersecurity goals as part of its overall GDPR compliance strategy.

Let's take a look at wat that means from a practical perspective.

2 Kaspersky Lab: Global IT Security Risks Report 2017

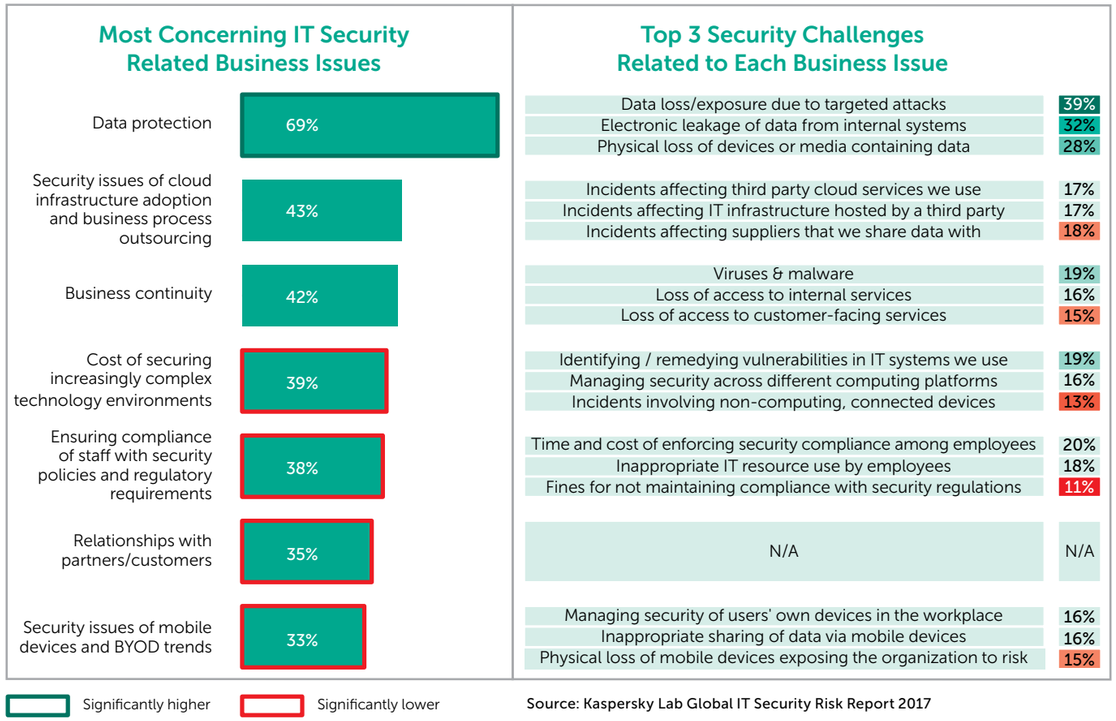
3 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/10/talktalk-gets-record-400-000-fine-for-failing-to-prevent-october-2015-attack/

Prevention is better than cure

Human actions – both unintentional and deliberate – play a significant role in personal data breaches. But the leading cause of PII-related security incidents continues to be cyberattacks, which are not only growing in volume, but changing all the time. That's why cybersecurity plays such a fundamental role in data protection and breach prevention strategy.

Sixty-nine percent of IT professionals say data protection is their number one concern, with 38% saying that ensuring staff compliance with security policies and regulatory requirements is a concern.

Top IT concerns



Source: Kaspersky Lab Global IT Security Risk Report 2017

Security of processing – Article 32 of GDPR

Article 32 of GDPR calls for appropriate technical and organizational measures to ensure a level of security appropriate to the risk when controlling or processing personal data. These include:

- Pseudonymization and encryption of personal data
- Measures to support ongoing confidentiality, integrity, availability and resilience of processing systems and services
- Capacity to restore data availability and accessibility following an incident
- Ability to conduct periodic testing and evaluation of technical and organizational capacity to secure data and handling.

Cybersecurity plays a role in both data protection and ensuring system resilience.

When you consider that, in 2017, 24% of businesses reported the loss, leakage or exposure of data as a result of a malware attack[4], it's easy to see why an effective cybersecurity strategy plays such an important supporting role in GDPR compliance and overall risk reduction.

And one of the best places to start hardening corporate IT defenses is the Endpoint. Here's why...

4 Kaspersky Lab Global IT Security Risk Report 2017

Beginning at the end (point)

When it comes to improving overall IT security hardening and data protection strategy, endpoint protection is a great place to start. It's an area of corporate defense that can be improved today – without impacting or depending on progress with other, new processes.

- Endpoints remain the number one target for the majority of today's cyberattacks – and email is the number one malware vector for business[5].
- They can become a 'window' to the sensitive data your company processes, even if the data itself is located on a remote server.
- As the main building block of your IT network, endpoints in the same location must be monitored to ensure timely alerts for suspicious activity; even those not directly involved in processing personal data can pose a significant threat when connected to the same network, as malware attacks can spread, compromising the entire data processing infrastructure.

49% of businesses experienced a malware attack in 2017, an increase of 11% on the previous year[6].

In this environment, detection rates really matter. With more than 300,000 new malware variants detected every day, even a 0.9 percent difference in threat detection capability can translate into hundreds of thousands of pieces of malware over the course of a year. And because the most advanced malware typically falls into the last 1-2% of attacks, that extra sliver of detection could can make the difference between coping with a cyberattack and it taking your business down – particularly for smaller businesses.

The most effective endpoint detection solutions don't stop at a single layer of prevention and detection; they use multiple layers of next-generation technologies capable of detecting, blocking and mitigating even the most sophisticated, unknown threats.

65% of businesses hit by ransomware in 2017 lost access to a significant amount of their data. A third never saw it again[8].

Kaspersky Endpoint Security for Business combines the world's most tested, most awarded security[7] with multiple layers of next-generation security technologies to protect business endpoints from every type of threat. Our behaviour engine is powered by unique, dynamic machine learning technology and cloud-assisted threat detection to mitigate known, unknown and advanced threats, as well as evolving attacks such as ransomware, which present a direct threat to personal data integrity and availability.

Block before they load

52% of businesses say end-user carelessness is the biggest weakness in their IT security strategy[9].

Preventing an attack before it can do damage is a key aspect of system hardening and resilience. To this end, finding – and plugging – vulnerabilities and gaps in key software applications can help prevent cybercriminals from exploiting widely used business software to access and steal personal data.

Why does this matter? Think about it: phishing attacks, ransomware, malicious attachments, spyware are just some examples of data-stealing cyberattacks that operate on the premise that end users will click without thinking. Just one well-disguised email with a convincing attachment is all it takes to cause a serious data breach.

The **Host-based Intrusion Prevention System** (HIPS) in Kaspersky Endpoint Security for Business provides a further layer of resilience. It detects and blocks unwanted or malicious program activity in real time, without impacting on the performance of legitimate applications. Based on the latest, cloud-based threat information, applications are assigned one of four Trust Categories that govern the kind of access they have to sensitive system elements. From a GDPR perspective, this can provide additional security by restricting access to selected files/directories by applications with low trust levels.

5 Verizon Data Breach Investigation Report 2017
6 Kaspersky Lab Global IT Security Risk Report 2017
7 https://www.kaspersky.com/top3
8 Kaspersky Security Bulletin: Story of the Year 2017
9 Kaspersky Lab Global IT Security Risks Report 2017

Kaspersky Lab's **Vulnerability and Patch Management** (included in Kaspersky Endpoint Security for Business Advanced) add an extra layer of security to your defenses. It finds and patches vulnerable applications before their vulnerabilities can be exploited. Because it enables automation, IT teams can be relieved of the operational burden of implementing patches on time; scheduling allows you to push non-urgent patching to out of hours, taking the pressure off infrastructure.

For true multi-layered protection, Kaspersky Lab's endpoint-based **Exploit Prevention** technology can mitigate even previously unknown, zero-day exploits, building on the Behavior Engine's capabilities to cover the broadest range of exploit types.

Don't collect if you can't protect: Storage

Endpoints are where personal data and people meet - and the associated risks have to be mitigated. But even after the number of employees trusted with handling PII is narrowed (in keeping with GDPR-aligned processes), there are still risks associated with where and how data is stored. For both stronger security and better visibility, regulated storage facilities (such as file servers or connected storage) are assigned, subject to strict access policies and continuous monitoring. Unfortunately, this highly sensitive role makes them lucrative targets for data thieves – underlining the need for strong security.

Kaspersky Security for File Servers (available as part of Kaspersky Endpoint Security and Kaspersky Total Security for Business), and **Kaspersky Security for Storage** can provide comprehensive protection of regulated data storage. In addition to powerful multi-layered protection, these solutions are designed specifically with server and data storage needs in mind, ensuring the lowest possible impact on performance or stability, regardless of workload. They also include a unique anti-cryptor[10] mechanism that blocks effects of remotely launched ransomware – which can cause significant, lasting damage if launched on a machine with network access to PII data-processing servers or storage.

Guarding the bottlenecks

Email and Proxy servers are the two gateways through which cyberattacks can reach inside the corporate IT network – or personal data can leave; even data sent accidentally, due to human error still constitutes a breach. Guarding these two bottlenecks at the corporate defensive perimeter is crucial.

Kaspersky Security for Mail Servers and Kaspersky Security for Internet Gateways[11] can help reduce these risks considerably, stopping up to 95% of incoming threats before they reach the endpoint, eliminating the human factor and attacks specifically targeting endpoints. In addition, the risk posed by personal data entering or leaving systems can be managed by denying certain file types from entering or leaving.

10 Kaspersky Security for Storage supports anti-cryptor functionality only for NetApp connected storages
11 Are also available as a part of Kaspersky Total Security for Business

- 18% of businesses have experienced data loss through the physical loss of devices or removable media.
- 16% have experienced data exposure through the physical loss of mobile devices.
- 15% of businesses have experienced the inappropriate sharing of data via mobile devices.[12]

Mobile devices – moving targets

Thanks to their suitability for data storage, transfer and sharing, mobile devices have long played an important role in personal data processing – and just like other technologies, specific attention should be paid to securing them.

Kaspersky Security for Mobile is an integral part of Kaspersky Endpoint Security for Business, combining effective threat protection with data safekeeping measures such as encryption and business data separation – along with tools for remote management. All this creates a solid basis for secure mobile device use, including any that are part of the PII processing chain.

Silver linings for every cloud

Forty-three percent of businesses say security issues related to cloud infrastructure are a top IT security concern.[13] Kaspersky Hybrid Cloud Security makes it easy to secure data-processing workloads – including PII – regardless of physical/virtual state or location (on-premises/cloud). It provides the same comprehensive security for virtualization-enabled infrastructure, servers and virtual desktops alike. The majority of security layers featured in applications for physical workloads are also available in formats specifically designed for virtual systems.

Training – forewarned is forearmed

GDPR mandates the promotion of data privacy and security awareness among employees – including, where appropriate, training. While process-related aspects of data handling, such as proportionality, purpose, privacy by design will form the cornerstone of GDPR-alignment for most businesses, broader awareness of cybersecurity, email threats and other online threats to data safety have an important role to play.

Kaspersky Security Awareness Training supports the promotion and awareness of data protection best practices in the workplace using gamified scenarios to facilitate understanding of cyberthreat awareness and prevention. By helping reduce data risks associated with human error, companies can enhance their compliance beyond check-boxes and promote overall awareness and safer practices.[14]

Understanding the risks

Article 35 of the Regulation includes measures that can be taken to mitigate risks, including 'safeguards, security measures and mechanisms to ensure the protection of personal data.'

From a cybersecurity perspective, this can include assessing any data processing software for vulnerabilities or risks associated with the way it's been implemented. Where personal data processing is a mission-critical element of business processes, viewing the whole IT infrastructure as a unified 'personal data processing facility' is a helpful approach to successful risk assessment. The cybersecurity expertise required to perform this task is seldom available in-house, meaning many organizations work with dedicated third party cybersecurity experts to achieve this.

12 Kaspersky Lab Global IT Security Risks Report 2017
13 Kaspersky Lab Global IT Security Risks Report 2017
14 Kaspersky Lab's offering complements the process-related training rather than replace it

Too much at this stage?! The case for security education

More than half of businesses agreed that the actions of careless staff was their biggest IT security weakness; Educating staff about the threats which exist and how to protect against them is therefore obviously essential!

	% of Respondents Agreeing with Each Statement	Change from Last Year	Change Particularly Significant for
We need to employ more specialists with specific experience in IT security, rather than general IT professionals	53%	+79%	VSB ↑ SMB
The biggest weakness in our IT security strategy are the careless actions of our employees/users	52%	New	
We now assume that our employees have insufficient awareness of the cybersecurity issues that can lead to incidents	49%	New	
Our knowledge of IT security threats specifically targeting our business is far from ideal	46%	+5%	VSB ↑ SMB
Many of our employees do not follow IT security policies properly	44%	New	
Our employees are not honest when IT security incidents occur they tend to hide problems to avoid punishment	40%	New	

This is particularly true for larger businesses who were significantly more likely to agree with these statements.

Kaspersky Security Assessment Services can help with Application Security Assessment – checking if the software used in data processing is vulnerable to abuse and exploitation. Kaspersky Lab experts can also conduct **Penetration Testing**, to reveal your IT network's weak points and provide the advice needed to mitigate them. This helps ensure that systems and processes are refined for better security, facilitating a healthy Data Protection Impact Assessment.

Cybersecurity can support GDPR

At its core, GDPR is designed to protect and empower data privacy in a world where technology has transformed the way personal information is collected, shared and stored.

While the regulation itself applies from May 25th 2018, the long lead-in time has given organizations time to take stock of their data processing approach – and implement changes in keeping with the technologies they use and the types of data they collect and manage.

For most organizations, GDPR has presented an opportunity to review and improve their data processing – and, by extension, their cybersecurity. That in itself is good news for cybersecurity experts who have long complained about businesses being careless about the protections and processes they use to secure their data and systems. GDPR gives businesses a great opportunity to review their cybersecurity posture from a data security perspective – after all, what's good for personal data safety can be good for the safety of many other aspects of your company's business. Kaspersky Lab's portfolio of solutions, while not ensuring GDPR compliance by itself, is ready to reduce your company's PII processing risks – and all the other cyber threats you face today.

Kaspersky Lab
Enterprise Cybersecurity: **www.kaspersky.com/enterprise**
Cyber Threats News: **www.securelist.com**
IT Security News: **business.kaspersky.com/**

#truecybersecurity
#HuMachine

www.kaspersky.com