TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an “as is” condition.
<table>
<thead>
<tr>
<th>Page</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Executive Summary</td>
</tr>
<tr>
<td>5</td>
<td>What is the GDPR?</td>
</tr>
<tr>
<td>6</td>
<td>Puzzling Out the Implications of the GDPR</td>
</tr>
<tr>
<td>10</td>
<td>Does the GDPR Unveil New Risks?</td>
</tr>
<tr>
<td>13</td>
<td>The Path to Compliance</td>
</tr>
<tr>
<td>16</td>
<td>Data Protection by Design</td>
</tr>
<tr>
<td>18</td>
<td>Cybersecurity in the Context of the GDPR</td>
</tr>
<tr>
<td>21</td>
<td>GDPR Compliance Through a Smart, Optimized and Connected Threat Defense</td>
</tr>
<tr>
<td>22</td>
<td>How Trend Micro Can Help</td>
</tr>
<tr>
<td>26</td>
<td>Putting the Right Pieces in Place: An Evolving Puzzle to Solve</td>
</tr>
</tbody>
</table>
Executive Summary

The EU General Data Protection Regulation (GDPR) obligates global organizations to protect the personal data for any and every citizen of the European Economic Area that they are connected to. With non-specific guidance on how “all data must be protected”, the GDPR is not a technology standard and does not promote specific technological approaches. However, with the regulation in effect since May 25, 2018, over 59,000 data breaches reported, and with definitive fines applied for both breaches and non-compliance, it’s clear that organizations need to look at how they are protecting personal information closely.

In order to help organizations better understand the role of cybersecurity in the context of GDPR, this white paper provides a high-level overview of the regulation, along with a framework to help keep you on the path to ongoing compliance. As a part of this, the paper focuses on the guidance to use state of the art cybersecurity and what that means to organizations as they put all the pieces together for ultimate compliance. To help IT and compliance professionals, who are critical part of the ‘GDPR team’ in any organization, the additional benefits of a sound cybersecurity strategy are discussed, and the significant role that Trend Micro can play in compliance— and beyond— are outlined.

Key findings

- **New duties, new rights.** Organizations anywhere in the world that collect or process personal data on EU residents must comply with the provisions of the GDPR, which impose new duties for organizations and the obligation to support the new set of rights given to individuals.
- **Privacy by design.** Data privacy must be embedded right from the outset of any action or project involving personal data. As a result, privacy must be prioritized during the design phase of information technologies, processes, and systems.
- **Dissuasive fines.** Failure to comply with the regulation can drive significant fines, reputational damages, discontinuation of data processing operations, and submission of complaints by individuals, with many significant fines already being levied due to non-compliance.
- **Multiple stakeholders.** The journey to compliance should focus on three key areas: 1) Legal and compliance. 2) Data. 3) Technology – and bring together stakeholders from across the organization.
- **No silver bullet.** Any plan of action requires that a variety of tasks are performed, including data mapping, readiness assessment, governance and accountability issues, review of data management practices, and more.
- **State of the art cybersecurity.** Cybersecurity should be smart, optimized, and connected. It must be multilayered and enable widespread integration, meaningful security analysis, sharing of threat data and collaboration between security solutions, real-time incident response capabilities, and centralized visibility. Most importantly, the definition of state of the art will change over time, a concept that is critical to creating an effective security strategy for the GDPR.
What is the GDPR?

Over the past several decades, the issue of data privacy has proved to be quite challenging across the Europe. The German State of Hessen enacted the world’s first data protection law in 1970 and many other German states and then European countries followed suit. In 1995, the European Community – the predecessor of the European Union - enacted the EU Data Protection Directive in an attempt to harmonize national laws and eliminate trade barriers in Europe. However, the member states of the European Community implemented the directive with nuanced differences resulting in independent national frameworks that drove inconsistencies between states. A result of four years of work, the EU’s General Data Protection Regulation (GDPR), which was adopted in April 2016, has standardized data protection legislation across the European Union (EU)¹, updating existing data protection laws to cover previously unforeseen data usage patterns.

“In order to ensure a consistent level of protection for natural persons throughout the Union and to prevent divergences hampering the free movement of personal data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators, [...], and to provide natural persons in all Member States with the same level of legally enforceable rights and obligations and responsibilities.”

Puzzling Out the Implications of the GDPR

The GDPR, with its set of new rules and duties, is a game changer for any organization processing personal data. The legislation applies to all companies, within or outside the EU, dealing with the personal data of individuals residing in the Union. Both controllers – that set out the reasons and means for processing personal data – and processors – that store, digitize, and handle the information on behalf of the controller – are responsible for managing the mountains of personal data subject to compliance with the GDPR. The regulation has been applied consistently in each member state resulting in significant new business obligations for both businesses and citizens.
Duties for organizations

- **Expanded scope**: The GDPR is applicable to any organization dealing with the data of individuals of the EU and refines the definition of personal data. This includes organizations inside AND outside of the EU.

- **Breach notification**: Personal data breaches must be reported to the GDPR supervisory authority within 72 hours. Impacted individuals may also need to be notified if their rights and freedoms are in jeopardy.

- **Privacy Impact Assessments (PIAs)**: PIAs are required to identify privacy risks to individuals when collecting, using, processing and disclosing their personal data.

- **Data Protection Officer (DPO)**: Organizations must appoint a DPO to be in charge of managing GDPR compliance across internal or outsourced data processing.

- **Codes of conduct**: General or industry-specific codes of conduct and certifications provide organizations with useful guidance on approaches to data privacy issues.

Rights of individuals

- **Right to information and explicit consent**: Individuals must be informed of the retention period of their personal data, of their rights to withdraw their consent anytime, and/or file a complaint.

- **Right to be forgotten**: Individuals can rightfully erase their personal data on several grounds and across multiple controllers.

- **Right to data portability**: Individuals may request a copy of their data in a digital and commonly used format from the controller for transfer to another party if desired.

- **Profiling acceptance**: Individuals have the right not to be subject to a decision based solely on profiling.

Privacy by design

- **State of the art cybersecurity**: Best-of-breed methods, processes and technologies to ensure best-in-class cybersecurity.
International Scope of the GDPR and Proof of Compliance

Lothar Determann, a lawyer and expert in privacy law compliance, gives a broader view of the GDPR scope, sharing an excerpt of the third edition of his *Field Guide to International Data Privacy Law Compliance*:

"In May 2018, the new EU General Data Protection Regulation (GDPR) will enter into effect in all Member States of the European Economic Area ("EEA") with immediate effect on companies. Many companies outside the EEA will also be subject to the GDPR, if, for example, they collect personal data from EEA consumers.

The GDPR, the first significant update of EU data protection laws since 1995, provides for draconian fines, and brings many major changes for companies, including:

- Companies must conduct impact assessments for sensitive data processing and document all data processing activities and compliance efforts in prescribed record formats. This includes categories of data and data subjects, purposes of processing, recipients, international transfers and suitable safeguards, time limits for erasure, technical and organizational security measures (Art. 5, 30, 35). Organizations are forced to prepare proof of compliance documentation, and identify and close gaps.

- Companies outside the EEA must designate a representative within the EEA, which will expose them to local jurisdiction and availability to a much greater degree.

- Companies must implement robust data retention and deletion programs to comply with more stringent rules regarding data access, rectification, and erasure.

- Companies must provide more detailed privacy notices to data subjects, disclosing identity and contact details of the data controller (and representative in the EEA for foreign companies); contact details of the data protection officer; purposes of data processing and legal basis; legitimate interests pursued by the controller or a third party, if that is the basis for justifying the processing; recipients or categories of recipients; for international data transfers, the existence or absence of an adequacy decision by the Commission and information on safeguards; and many other details.

Besides the GDPR, companies will have to continue complying with national data protection laws. Unlike the Data Protection Directive of 1995, the GDPR applies directly to companies, with no implementation into national law. But, national laws can provide for additional or stricter rules and will remain effective until revoked. 50+ sections in the GDPR allow countries to enact more detailed or stricter rules on various subjects. The GDPR is intended to create greater harmonization in European data protection laws and it has the potential to achieve this if EEA Member States withdraw their existing national laws in favor of the new GDPR. However, some EEA Member States will keep existing laws around and thus create uncertainties regarding the degree of preemption and harmonization. Another uncertainty factor adding in Europe is the UK’s exit from the EU, which could result in the introduction of different privacy laws in one of the most important jurisdictions in Europe by the size of its population and economy."
The phrase “data is the new oil” is one that is increasingly apt in the world of electronic business and online commerce, but the ability to ‘strike it rich’ is difficult, as data is often too raw, partial, siloed, and difficult to locate within an organization. Data-centricity is about having the right consolidated set of data, in the right format, to be mined through analytics in order to derive decision-making insights, and ultimately competitive advantage. Within the framework of the GDPR, EU citizens own their personal data and only give it to companies on “loan”. They are concerned about the use of their data and willing to engage with organizations they trust and perceive to offer the greatest privacy protections. To ensure that data processing does not adversely impact the rights of individuals and guarantee that personal data is kept private at any time, the GDPR often refers to the concept of state of the art security, based on constantly evolving best practices and technology, that apply multiple layers of protection for data to address a wide range of risks, including:

- access or manipulation by unauthorized third parties
- unauthorized or unlawful data processing
- theft, accidental loss, damage or destruction
- unauthorized disclosure

For global organizations, the GDPR harmonizes the currently fragmented legal framework for privacy across the EU, providing one data protection regulation with both data security and business outcomes for large organizations.

Importantly, the regulation similarly requires small to medium-sized businesses (SMBs) to manage their data flows, transfers, and processes to fully comply with the regulation. Like their larger counterparts, SMBs are expected to measure the risks of their business practices over the privacy of individuals, align their interests with the rights of individuals, and provide proper documentation that guarantees that these considerations are within their business decision-making process. Organizations with less than 250 employees are allowed specific exemptions under the GDPR owing to the smaller risks that they might pose compared to bigger organizations. To this effect, supervisory authorities in each country are encouraged to take account of the specific needs of SMBs in the application of the GDPR. For instance, organizations with less than 250 employees are relieved of maintaining a record of processed activities, and EU member states can decide whether they are required to designate a Data Protection Officer (DPO).
Does the GDPR Unveil New Risks?

Activities around compliance with the GDPR must take into account technology trends and patterns of usage emerging in the market. In the traditional IT environment, personal data remained within known boundaries. Yet, as the Internet of Things (IoT), Industrial Internet of Things (IIoT), mobility, and the cloud are now commonplace, data is getting spread across multiple environments, with complex data flows a pervasive part of IT. Assessing data that requires tamper-proof security can, therefore, be challenging, and protecting it even more complex due to poor visibility.

In their annual study, the Ponemon Institute reported an ever-rising cost of a data breach, which now amounts to USD 3.86 million per incident, a 6.4 percent increase over one year\(^2\). Associated costs include multiple elements such as investigation, remediation, forensics, notification of the impacted parties, support, etc. The GDPR introduces an additional layer of cost, as the regulation sets significant administrative fines that may be imposed for non-compliance. With two tiers of financial penalties described in the regulation, the size of the fines can be substantial and impactful to the business.

While the size of the fines under GDPR have the potential to significantly impact the financial viability of a company, they are likely to be discretionary rather than mandatory in many EU states. The imposition of fines by national supervisory authorities will be combined with an assessment of an organization’s ability to prove its intention to comply with the GDPR.

With over 59,000 data breaches reported to GDPR authorities since the regulation took effect\(^3\), it’s clear that the challenge of protecting private data and complying with hard-hitting regulations like the GDPR will not be easy.
While most fines levied to date have been small, Google was recently fined €50 million by French authorities—not for a breach, but for non-compliance with the regulation\(^1\). While Facebook was fortunate to have missed the GDPR enforcement deadline with its Cambridge Analytica breach, it was fined £500,000 last year by the ICO in the UK\(^2\). It now faces a significant potential fine in the US, with the Federal Trade Commission (FTC) pushing for a multi-billion dollar fine relating to the same incident.\(^6\) With the GDPR as a reference, many countries, including the new California Consumer Privacy Act (CCPA) coming online in 2020, will be introducing new privacy regulations in the coming years, making it more complicated to comply and increases the importance of a security approach that helps to address privacy requirements more consistently. According to the Trend Micro Cyber Risk Index over 80 percent of businesses, from small to large, expect that a cyberattack will infiltrate their organization within the next 12 months, highlighting that most organizations see significant risk in the way they currently deal with cybersecurity.

Importantly, non-compliance impacts can go beyond monetary fines, including an order to discontinue data processing operations, which would be catastrophic for data processing-intensive operations. Organizations should not overlook the fact that the GDPR empowers individuals to a level unseen before, enabling the submission of complaints that could drive additional financial and brand damage. Finally, the reputational risks must be considered, as customers demand the ability to deal with organizations that will process their data in a lawful way and support their requests for data erasure or transfer.
WannaCry ransomware: an early wake-up call for the GDPR

In May 2017, the WannaCry ransomware surprised many organizations around the world, with some experiencing a complete stoppage of business as a result. This malware encrypted corporate data - including personal data - on vulnerable systems, and asked for a ransom. This event grabbed the headlines of the international media as a testimony that many organizations remained vulnerable to sophisticated attacks. The attacks continued through 2018, remaining one of the top detections for ransomware in 2018.7

Can rogue data encryption be somehow related to personal data breach as defined by the GDPR? The answer is a YES, as Art. 4.12 of the regulation defines such an incident as “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed”. This leads to another question: would the targeted organizations be fined if a WannaCry-like compromise happens again now that the GDPR is in effect? The probability is high, knowing that the victims did not patch the known Windows SMB vulnerability used by the ransomware. Of course, the GDPR does not specifically require every company to upgrade their systems, but this is considered as an industry best practice to prevent exploits. When the patching procedure fails, or if no virtual patching technology is available, it will be quite difficult to convince the authorities that best efforts were made to protect personal data, which will likely result in some sort of negative result for the organization.
The Path to Compliance

While many organizations were not compliant by the May 2018 deadline, many are still on the path to compliance today. A recent report from Cisco highlighted that while most organizations believe that they are compliant today, many still have work to do.

Importantly, while many organizations believed that they were compliant, there has been an evolution of understanding what businesses are doing and subsequent decisions rendered by the authorities. One of the most high-profile cases to date was Google. In January 2019, the search engine giant was fined €50 million by France’s data protection authority (DPA) for non-compliance with GDPR, accusing Google of a lack of transparency and the personalization of its ads without valid consent.

Source: Cisco 2019 Data Privacy Benchmark Study,
GDPR compliance involves many stakeholders with proven expertise in operational, legal, and technical areas, but the leader of this project is now the Data Protection Officer (DPO), a new role imposed by the GDPR. In this transversal function, the DPO, whether employed or under a service contract, is required to work in close collaboration with all stakeholders, with full support from the top management to engage the necessary resources and ensure that compliance with the GDPR is prioritized. Organizations, according to their size, industry, and other specificities, will have to conduct their own customized compliance program. For most companies, complying with the GDPR requirements involves considerable organizational resources, a change in data processes, and investment in security processes and technologies—there is no single technology or process that will deliver compliance across three key areas to be considered:

**LEGAL AND COMPLIANCE**

The GDPR introduced new requirements for legal compliance functions. Many organizations require a Data Protection Officer (DPO), as a key role to ensure compliance. An estimate of 28,000 new DPOs will be required in Europe alone. If the GDPR is not complied with, organizations will face the heaviest fines yet—up to 4% of global turnover.

A renewed emphasis on organization accountability requires proactive, robust privacy governance: organizations should review how they write privacy policies, to make these easier to understand.

- General Counsel/Legal
- Privacy Officer
- Chief Risk Officer
- Chief Compliance Officer

**TECHNOLOGY**

New GDPR requirements mean changes to the ways in which technologies are designed and managed. Documented privacy risk assessments will be required to deploy new systems and technologies. Security breaches will have to be notified to regulators within 72 hours, which means implementing new or enhanced incident response procedures. The concept of ‘Privacy by Design’ has become enshrined in law, with the Privacy Impact Assessment expected to become commonplace across organizations in the next few years. In addition, organizations will be expected to consider data masking, pseudo-anonymisation and encryption.

- Chief Information Officer
- Chief Information Security Officer
- Chief Technology Officer

**DATA**

Individuals and teams tasked with information management will be challenged to provide clearer oversight on data storage, journeys, and lineage. Having a better grasp of what data is collected and where it is stored will make it easier to comply with new data subject rights—rights to have data deleted and to have it ported to other organizations.

- Chief Data Officer
- Chief Operating Officer
- Chief Marketing Officer
- Data Stewards
- Digital Leads
As a result, leading consulting firms like Deloitte recommend looking at GDPR compliance as a framework of tasks, rather than thinking of a technology as a silver bullet to the problem. With that recommendation in mind, organizations should look at initiating action now. While the list below is not meant to be exhaustive, it does provide a high level framework for actions that organizations should be taking in order to achieve compliance:

**Organizations must break down the vast number of requirements of the GDPR into a set of manageable components, and define a target state for each of these with tangible outcomes to be achieved for compliance. This should also be complemented by a view on what the longer term target state might be as privacy frameworks evolve. Bringing together different stakeholders and being clear on accountabilities for implementation, defining what the organization’s risk-appetite is and agreeing scope is not always straight forward given the different background and viewpoints that each will bring.**

Too often there is a vacuum between stakeholders, with legal teams expecting the business to be able to take their regulatory interpretation and implement change, and business owners expecting a lot more detail on exactly what needs to be done at a granular level. The alignment of legal, risk and compliance individuals with process and system owners is key, so that both sides have a clearly agreed and actionable set of requirements and outcomes.
Data Protection by Design

Data protection by design – also referred to as privacy by design – must be one of the primary guiding principles of the action plan, which will result in data privacy being an embedded element right from the outset. As a result, privacy processes and technologies must be prioritized during the design phase of information technologies and systems.

According to Art. 25 of the GDPR, the technical and organizational measures for protecting personal data should be consistent with the risk presented: the higher the risk, the more rigorous the measures that the controller or the processor must take. The GDPR assesses the notion of risk through specific data protection parameters that need to be considered, in particular the nature, scope, context and purposes of a data process. Moreover, the regulation clearly relates the risk to the measures taken in order to preserve the rights and freedom of individuals. This approach, in fact, considers the impact of a potential breach of personal data on individuals as a key facet of risk assessment. While data protection by design can be one of the biggest challenges to address for organizations where teams with different backgrounds are not used to continuously collaboration, it definitely needs to be a priority for cybersecurity and marketing teams as they design and support new business applications. As a global leader in cybersecurity, Trend Micro’s approach to data privacy is comprehensive and holistic, including how we are leveraging the GDPR to be our new baseline level of data protection across the globe. Across the entire company, including our product & service development, we have security foundations built-in that all help to deliver on data protection by design and privacy by default.

Too often, when S&R professionals face a daunting challenge, they search for a single technology to solve it. In the case of data security, such a technology does not exist. Instead, you need a framework that outlines how you discover, classify, analyze, and ultimately defend data with a mix of security processes, technical controls, and a willingness to instill a culture that respects and appreciates privacy.

Source: Forrester, "Protect Your Intellectual Property And Customer Data From Theft And Abuse", Stephanie Balaouras, July 12, 2017
Drawing the right data map

While working on their GDPR-compliance project, organizations need to dig deep down into their corporate resources to identify personal data stores, processes and exchanges, and define the scope of data that needs privacy. To say the least, this task is daunting, and sometimes discouraging: data, which was once kept within the boundaries of traditional networks, has today gone viral, migrating to mobile endpoints, smart devices, the public cloud, partners/processors sites, and more. In fact, a recent Cisco survey highlighted that while 42% organizations cited that meeting data security requirements was the most significant challenge of getting ready for GDPR, 31% said cataloging and inventorying data was the most significant.

The good news is that technology can really help as part of the overall compliance project. Data Loss Prevention (DLP) is a security technique that screens applications, systems, devices and any other assets, such as email systems, Microsoft SharePoint servers, file servers or even SaaS applications like Microsoft Office 365, to spot personal data. This is done with the help of templates that contain specific formats, keywords or expressions to be searched for, to track credit card details, personal addresses or social security numbers, for example. With this automation, personal data discovery is carried out faster and with few false positives.

A consistent data map should not be based solely on personal data at rest. Data in transit, including the data that flows between systems, within an organization or with a third party, also needs to be mapped to provide comprehensive visibility. At this stage, the GDPR-compliance team can define the actions needed to ensure data privacy. Here again, DLP proves its worth as a tool that is on a perpetual mission, permanently monitoring any suspect data disclosure, poised to stop any and all actions that could result in a potential disclosure. So, is DLP the silver bullet? The short answer is no. As referenced in the Forrester quote, organizations need to look at compliance in the context of a framework of actions and technologies. However, DLP can be a valuable technology technique under the following considerations:

- First, DLP is often viewed as intrusive for employees, and even probably not tolerated in some EU Member States because it can violate employee privacy. The issue here is to precisely define what can be monitored and what cannot.
- Second, to maximize privacy, DLP must be backed by best practices. These include the need to centralize personal data to the best possible extent in order to shrink the scope of data to be safeguarded, and implement efficient access control and back-up strategies.
- Third, DLP must be combined with other technologies to deliver the appropriate level of security. These include encryption, data breach detection, file integrity monitoring, application monitoring and intrusion/vulnerability management features, to name a few.

In summary, while DLP can play a key role in GDPR compliance, it is clear that no single technology can solve all challenges, and that multiple layers of security must be used.
Cybersecurity in the Context of the GDPR

Network and information security is covered by the GDPR. Recital 49 of the regulation focuses on the capacity of a network or an information system to resist accidental events as well as malicious actions that compromise the availability, authenticity, integrity and confidentiality of personal data, whether stored or in transit. Unauthorized access to personal data, and any unauthorized disclosure of such data, is considered as a major issue, requiring controllers and processors to evaluate any related risks, maintain security at an appropriate level, and restrict personal data processing to a limited scope.

Data protection by design and by default is prioritized by the GDPR, and organizations are expected to implement appropriate technical and organizational measures. Any system related to personal data processing must integrate security right from the design stage. As an example, Art. 32 sets forth pseudonymization and encryption as proven features to protect personal data, as the release of unintelligible scripted material does not adversely impact individuals. Data protection impact assessments are required when a type of processing, in particular using new technologies, may result in a high risk to the rights and freedoms of individuals. This assessment has to include the measures envisaged to address risks, protect personal data and demonstrate compliance (Art.35).

The GDPR recognizes that data security technologies may be legitimate to protect data, which implies preventing rogue access to networks and data, malware, and cyberattacks. Translated into practical language, this means the deployment of cybersecurity technologies.

State of the Art is a Must

Throughout the language in the regulation, there is one concept that is frequently mentioned: state of the art (Art. 25 and 32). But, what is state of the art? The Cambridge dictionary defines it as “Very modern and using the most recent ideas and methods”, while Wikipedia sees it as the “Highest level of general development, as of a device, technique, or scientific field achieved at a particular time”. Although subtly different, both definitions introduce the notion of time, and the underlying idea that state of the art varies over time. What is considered state of the art today will likely be different at a future date. When applying it to cybersecurity, this means that innovation is the spearhead of the continuous development of efficient security methodologies and technologies. For methodologies, organizations are encouraged to leverage recommendations from existing authorities: the CNIL\(^9\) in France, the ICO\(^10\) in the UK, or the ENISA\(^11\) at European level, just to name a few of them. In parallel, leading industry analysts and large consulting firms have defined a set of best practices that will help organizations achieve the appropriate level of cybersecurity as a part of the overall compliance process.
Best-of-Breed and Best-in-Suite: How They Contribute to the State of the Art

Over the past couple of decades, selecting appropriate security technologies has swung between two different approaches: Best-in-Suite and Best-of-Breed, or, to put it in simple words, adopt an integrated application suite from a single vendor, or packages from different vendors who are considered to be the best in their category. Both approaches have their pros and cons in terms of management complexity, integration cost and, most important, efficiency. Yet the issue is: can state of the art security be achieved through just one of these approaches?

This heated debate, which is one of the oldest in corporate IT is, behind the curtains, somehow ironic: almost all organizations have a hybrid approach, a mix of suite-based and point solutions selected with the goal of delivering state of the art cybersecurity. At Trend Micro, this observation shaped our beliefs on what it takes to reach the state of the art, and helped us identify four key drivers: features, collaboration, completeness, and ecosystem fit.

In the late 2000s, security features like reputation services, anti-malware, encryption, and firewalls were considered premium capabilities. However, with the passing of time and the increasing sophistication of threats, additional techniques, such as behavior analysis, machine learning, and host-based IPS (deep packet inspection) were developed and deployed, redefining the state of the art. Each feature should not be considered individually, but as part of a collaborative process where security and intelligence data are shared amongst all. Completeness is about implementing security in three areas that really matter to corporate security: the network, the user and the data center/cloud. Threat intelligence must be shared among these segments to understand an attack from end to end. Last but not least, is the capacity to mix and match both the best-of-breed and best-in-suite approaches? This is done by opening up to an ecosystem of partners, where third party products, new or existing, can be seamlessly integrated with this collaborative and advanced security fabric that organizations call for. Completely aligned to the concept of state of the art, the Trend Micro XGen security strategy delivers a cross-generational blend of threat defense techniques, applied individually at the right time and powered by global threat intelligence data.

XGen security delivers a cross-generational blend of threat defense techniques
Personal data breach reporting obligation and the need for a response plan

The GDPR introduced for the first time an EU-wide personal data breach reporting requirement. So far, at the EU level, there have been sector-specific notification obligations applicable to providers of publicly-available electronic communications services under the ePrivacy Directive and to operators of essential services under the Directive on Security of Network and Information Systems (NIS Directive). Data breach notification regimes in EU member states such as Germany and the UK were also in place.

The GDPR defines personal data breaches more broadly than existing breach notification laws in the U.S. and obliges data controllers to notify personal data breaches to the supervisory authorities, as well as to affected individuals, except when the breach is unlikely to result in a high risk to those individuals’ rights or freedoms. Data processors have no reporting obligation vis-à-vis the supervisory authorities or individuals, but must inform data controllers without undue delay of a personal data breach. One of the controversial aspects of the new requirement is that the supervisory authority must be notified where feasible, within 72 hours of when the controller identifies a breach. Controllers must document personal data breaches to allow supervisory authorities to verify compliance with the notification requirement. Non-compliance with the new requirement is a serious violation of the GDPR, subject to an administrative fine of up to €10 million or, in case of an undertaking, up to 2% of total global turnover, whichever is higher.

Implementing a data breach management program is therefore a good business practice and a bulwark against these sanctions. In addition to these fines, there are other serious consequences, such as individuals’ complaints, claims for damages, suspension of data processing and significant reputational damage. Proper policies, procedures, checklists, templates and documentation will be key to meet the data breach reporting requirements under the GDPR - as well as those in different jurisdictions around the world - and tight reporting deadlines. Awareness campaigns and training for staff members is important. The program should also be tested and regularly reviewed and updated, when necessary.

To prepare for any potential breach, controllers and processors need to assess and amend existing technical and organizational security measures. Measures like encryption may even exempt the controller from communicating a personal data breach to the affected individuals. Moreover, companies should review the selection of their vendors, ensure that due diligence procedures cover data protection and security, negotiate appropriate contractual terms and monitor compliance. Responsibilities should be assigned in advance across a multi-departmental team comprised of legal, compliance, IT security, HR and communications. Companies could look into public relations firms, credit monitoring services, forensics firms, public communications firms and external counsel (legal privilege) in advance. Finally, insurance policies should be reviewed to ensure they sufficiently cover the costs of a data breach.
GDPR Compliance Through a Smart, Optimized and Connected Threat Defense

Thwarting modern advanced malware and targeted attacks requires rethinking your current IT solution strategy and adopting an approach that includes broad environment integration, meaningful security analysis, threat data sharing, collaboration between solutions, proven incident response capabilities and centralized visibility across the entire security arsenal.

A smart defense leverages a cross-generational blend of threat defense techniques that are layered to protect personal data against known and unknown threats, whether data is at rest, in transit, or at any stage of processing. While new security techniques will be introduced over time to address new threats, current techniques are still relevant and necessary for data protection. This cross-generational blend of techniques enables the most appropriate and efficient technique to be used to address each threat—there is no such thing as a security silver bullet.

Optimization is critical during the deployment on your defense mechanism: your security must be woven into the personal data processing fabric, with techniques that efficiently secure both legacy and new enterprise environments, including cloud and containers. This optimization provides visibility across users, servers and networks, enabling organizations to analyze and assess the impact of threats, evaluate the technical security infrastructure posture, and quickly get a birds-eye view of incidents that have occurred across the enterprise.

A connected defense helps to both prevent and remediate personal data breaches by sharing real-time threat intelligence and automated security updates across all security layers. This proactive process stops malware—like ransomware—before it can impact personal data. Infected systems hosting personal data are isolated while malicious traffic that may retrieve, edit or delete personal data is blocked.

A smart, optimized and connected defense strategy protects the enterprise across the entire threat lifecycle. This leads to fewer compromises, substantially shorter dwell times for threats that do manage to slip through, and far less effort and expense required for incident response. This is a strategy that shows clear evidence that an organization has invested in state of the art security as a part of GDPR compliance.
How Trend Micro Can Help

By deploying the appropriate technologies, organizations can implement a multilayered, state of the art cybersecurity strategy that helps to ensure data privacy and GDPR compliance. GDPR-compliance projects are an ideal opportunity to review and improve the overall cybersecurity posture of any organization, as there are multiple use cases that must be addressed to comply with the regulation. Each case requires a close look to assess the related risks and consider the best approach to keeping personal data private. The following use cases are specific examples that Trend Micro’s broad portfolio of security solutions can be used to help you on your compliance journey.

We are now PCI compliant and we are closing in on GDPR compliance. We couldn’t have achieved that without Trend Micro.

Tim Masey, Director of Cybersecurity, Carhartt

Users are a major source of risk for personal data loss and several scenarios should be considered, including the accidental loss or theft of an unencrypted laptop, mobile device or backup on a flash drive. Data can also be unintentionally disclosed when users email personal data outside the organization (especially if the email is sent to a wrong recipient), or when they use non-corporate systems like personal webmail services or public sharing web sites. Data disclosure can also be the result of deliberate theft by a user, including printing sensitive documents or copying in-scope information from network servers or a database to an USB flash drive.

Trend Micro’s solutions for personal data protection:

- **Integrated Data Loss Protection (DLP)** helps to identify & protect personal data
- **Endpoint Encryption** secures personal data from device loss

Employees can be exposed to identity theft through phishing and social engineering attacks, falling victim to an email containing a malicious URL or attachment. They are also vulnerable to web exploits, device and OS vulnerabilities, application vulnerabilities and infected flash drives. And when surfing on a malicious web page, they face the risk of a drive-by-download or a browser/plug-in exploit.

And with the emergence of Business Email Compromise (BEC)—a sophisticated type of scam where email accounts of executives are spoofed to convince employees to conduct fraudulent transfers—even the most security-minded employees are at risk.
Trend Micro's solutions for employee protection:
- **Email Security** blocks malicious emails
- **Endpoint Security** protects user devices from known & unknown threats (ransomware)
- **Web Security** shields web browsing activities
- **Network Security** blocks network exploits & detects potential breaches
- **Writing Style DNA** uses AI to "blueprint" a user's style of writing to decipher to block BEC attacks

Your corporate IT infrastructure hosts a diverse range of devices, servers, applications, shared file servers, databases, and more, each a potential target for a breach. Internet-facing servers & applications can be infected through exploits and configuration weaknesses, becoming the launch point for internal propagation. Protecting personal data across the IT infrastructure requires the layering of multiple security techniques, including blocking unauthorized access to servers and applications that process or store personal data. Organizations should also implement security best practices such as OS hardening, changing default credentials and leveraging secured access to any IT resource.

Trend Micro's solutions for corporate infrastructure protection:
- **Hybrid Cloud Security** secures server workloads & applications across the data center & cloud
- **Network Security (via IPS)** shields on-premises infrastructure from known & undisclosed vulnerabilities

While cloud and on-premises IT share similar risks (exploits, weak security practices, etc.), the responsibility for security in the cloud is shared between the IaaS provider and the organization. IaaS solutions provide a secure infrastructure for workloads to run on, but the security of hosted applications and any personal data processed or stored in the cloud is the responsibility of the customer. Organizations should leverage the built-in cloud and SaaS configuration capabilities in combination with additional security controls to protect workloads and data in the cloud.

Trend Micro's solutions for data in the cloud protection:
- **Hybrid Cloud Security** automates server & container workload protection across multi-cloud deployments
- **Cloud App Security** protects SaaS environments like Office 365 from ransomware & phishing

A smart, optimized and connected defense strategy protects the enterprise across the entire threat lifecycle. This leads to fewer compromises, substantially shorter dwell times for threats that do manage to slip through, and far less effort and expense required for incident response. This is a strategy that shows clear evidence that an organization has invested in state of the art security as a part of GDPR compliance.
Security is a critical factor in healthcare and is integrated into any upgrade to our systems. This data is coveted by cyber criminals. We cannot afford an attack of ransomware or any other malware. Added to this are strict regulations, including the new General Data Protection Regulation, or GDPR, in the European Union.

Miquel Mauri, Systems Administrator, Mutua General de Catalunya

The GDPR requires data breaches be reported to an appropriate supervisory authority once discovered. Since today’s sophisticated malware uses multiple evasion techniques once they have penetrated an enterprise, their dwell time inside an IT infrastructure may be weeks, if not months, before they are discovered. To close this breach detection gap, organizations should closely monitor their environment, using state of the art tools to identify Indicators of compromise (IOCs) and correlate seemingly disparate actions to uncover any potential breach.

Trend Micro’s solutions to detect and respond to security breaches:

- **Breach Detection System** identifies suspicious activities that may lead to data loss risk
- **Connected Trend Micro** solutions across user, data center and cloud environments enables rapid response and remediation of breaches
Putting the Right Pieces in Place: An Evolving Puzzle to Solve

The EU General Data Protection Regulation is designed to protect the rights of individual data, regardless of where the originating company resides. In many ways, the enactment of the GDPR can help organizations deal with a single regulation across countries instead of attempting to comply with multiple, contradictory laws that exist today. In fact, the European Commission said that the regulation would yield 2.3 billion Euros in savings each year to organizations through the simplification of compliance while transacting business across multiple countries.

The path to compliance holds many financial, cultural, and organizational challenges, with the overarching challenge of ensuring that compliance fits in with the goals of the business. The opportunity is to leverage the mandated changes to increase overall corporate and brand value, making the best use of data while respecting the law. However, in order to do this, the approach to compliance needs to be able to transcend moment-in-time compliance and evolve with the business. The mandate to apply state of the art security in the GDPR is an opportunity to align compliance today with changes that are inevitable in the ever-changing world of threats.

To help you on your journey to compliance and beyond, Trend Micro delivers state of the art security through our XGen™ security strategy, enabling organizations to leverage cybersecurity solutions that address threats today and tomorrow, while fitting in with the needs of your business.

The GDPR is undeniably a major change and challenge, but change invariably brings opportunities with it. This is an opportunity to more completely understand the individuals who you do business with, whose data is managed by an organization that is eager and willing to find new, innovative ways to engage with them. The regulation also presents an opportunity to leverage cybersecurity to strengthen and expand your business.

You can find out more about how Trend Micro can help you with the GDPR at www.trendmicro.com/gdpr.
Contributors

This document is the collaborative outcome of Trend Micro experts from around the world. We have also received third party support and would like to convey our special thanks to Monika Kuschewsky, Peter Gooch and Lothar Determann for their expert contribution to this publication.

Monika Kuschewsky is a Partner at Squire Patton Boggs. A Lawyer, a Certified Information Privacy Professional/Europe and Company Data Protection Officer, she is also the general editor of Data Protection & Privacy – International Series, a multijurisdictional reference guide published by Thomson Reuters for companies, legal professionals and data protection officers, covering 46 major jurisdictions worldwide.

Peter Gooch is a Partner within Deloitte’s Cyber Risk Services and specializes in Privacy, Data Protection and Cyber security. As the leader of Deloitte UK’s Privacy practice, Peter has extensive experience in privacy assignments having developed and implemented global privacy frameworks at variety of multi-national organizations and supported many organisations with their GDPR readiness.

Lothar Determann practices U.S. and German law and advises global companies on privacy law compliance for 20+ years. He teaches computer and data privacy law at the Freie Universität Berlin in Germany, at the University of California, Berkeley School of Law and Stanford Law School. This year, he will publish a third edition of his renowned Determann’s Field Guide to International Data Privacy Law Compliance, which will cover the GDPR for the first time.

Footnotes and references

1. The GDPR will actually apply to the European Economic Area (European Union states, as well as Iceland, Liechtenstein and Norway).
2. Ponemon Institute, “2018 Cost of Data Breach Study”
3. Data Breach Today, “Data Breach Reports in Europe Under GDPR Exceed 59,000”, February 6, 2019
5. ICO issues maximum £500,000 fine to Facebook for failing to protect users’ personal information
7. 2018 Trend Micro Security Roundup, March 5, 2019
Trend Micro, a global leader in cybersecurity, is passionate about making the world safe for exchanging digital information, today and in the future. Artfully applying our XGen™ security strategy, our innovative solutions for consumers, businesses, and governments deliver connected security for data centers, cloud workloads, networks, and endpoints.

With over 6,500 employees in 50 countries and the world’s most advanced global threat research and intelligence, Trend Micro enables organizations to secure their connected world. www.trendmicro.com. [WP04_Solving_the_GDPR_Puzzle_190523US]

www.trendmicro.com/gdpr