SOLUTION BRIEF

Data Center Group
IT Cybersecurity

GDPR: Tough Data Protection Measures for Meeting Today's Threats

Table of Contents

Introduction

Today, many organizations are focusing on a new regulatory framework, the General Data Protection Regulation (GDPR) adopted in the European Union, that mandates stricter data protection practices. Set to take effect on May 25, 2018, these changes affect not only enterprises established in countries that are members of the EU, but anyone selling or offering goods or services or monitoring the behavior of individuals in the EU. With these regulations about to take effect, now is the time to ensure that compliance plans are being enacted and that enterprise security provisions are sufficient to satisfy the new, strict requirements of this law.

The passage of GDPR has spurred multinational corporations to reassess their approach to data privacy and security in advance of the enforcement deadline. In a survey conducted by PwC (PricewaterhouseCoopers), over half of US multinationals say GDPR is their top data-protection priority. For enhancing information security, 77 percent plan to spend USD 1 million or more on initiatives to comply with GDPR.[1]

State-of-the-art technology for implementing cybersecurity measures has rapidly become essential for enterprises, particularly as countries outside of the EU are also updating and strengthening the way they approach data privacy of citizens. Rather than viewing the GDPR requirements as an oppressive burden, forward-looking companies are taking the opportunity to rethink protective measures in relation to overall security and privacy, maintaining the integrity of their brand, and ensuring long-term relationships with customers.

Intel offers security capabilities that start at boot protections embedded in silicon and extend all the way through the software stack (in some cases, co-engineered collaboratively with ISV partners). These technologies (discussed in more detail in the second half of this solution brief) help protect data in each state: data in use, in transit, and at rest.

Rethinking Data Protection and Risk as GDPR Takes Effect

Larger companies with compliance operations in keeping with Directive 95/46/EC (which the GDPR supersedes) Europe's Data Protection Act of 1998 should have fewer problems responding to the latest regulation, although they still need to be aware of some important changes. Many startups, however, and smaller companies may not be fully versed in the data protection issues that are at play and need to become familiar with the regulations and respond accordingly.

Managing risk is never about eliminating risk. Risk is inherent in all activities, and it is often illustrated as a triangle, as shown in Figure 1. The three edges of the triangle represent your assets, their vulnerabilities, and the threats to those assets. Your assets include your employees, your supply chain and customers, your processes, applications and data, equipment, structures, financial holdings, and so on. Every asset could eventually have vulnerabilities. Employees may quit, equipment may break down, unexpected occurrences can expose new vulnerabilities. In the cybersecurity realm, there are many different vulnerabilities to monitor as data is being processed, including applications, operating systems, network connections, storage resources, and more.

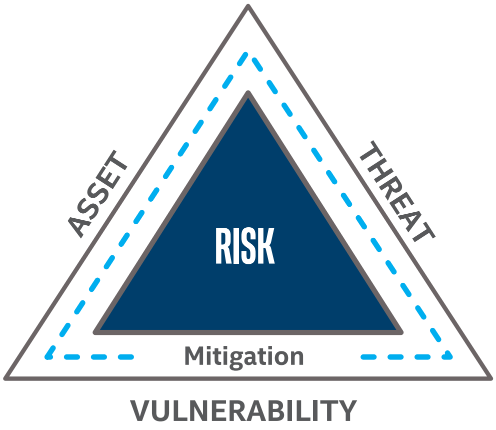

Figure 1. Factors affecting risk management.

Shifting Responsibilities

One significant aspect of GDPR is that the burden of responsibility for protecting data is shared jointly between the data controller and data processor(s). Ultimately, the data controller bears primary responsibility for the security and privacy of the data and is tasked with the handling and safekeeping of all personal information that applies to an individual in the EU. Responsibilities extend across the full arc of the data's life cycle (in use, at rest, and in transit). The data processor, acting on behalf of the data controller, stores and processes the data, and under the GDPR is responsible for violations of provisions that apply to it. A data controller typically uses the services of several data processors. These data processors may include:

- Cloud service providers (CSPs) generally
- Software-as-a-service (SaaS) vendors
- Third parties that provide analytics, billing, payroll, loyalty programs, and other value-added services

If a breach occurs at any of these data processors, both the data controller and the data processor can be held accountable. Both can be fined and penalized. Taking a broad view of the security measures throughout the enterprise infrastructure—including the various functions performed by the data controllers—is the best way to ensure compliance with GDPR.

Stricter Measures of Accountability

Given the increasing instances of serious data breaches, the rigorous safeguards outlined by GDPR are timely. Millions of personal records were compromised in 2017 because of breaches at Equifax, LinkedIn, Yahoo, MySpace, Dun & Bradstreet, and other large enterprises.[2]

Every company that falls within the province of GDPR is accountable for meeting a number of personal data protection requirements. These requirements include:

- Having set data protection policies in force
- Evaluating periodically how effectively current safeguards are working
- Performing regular audits of data processing operations
- Ensuring that partners and suppliers are also keeping on top of these requirements

Depending on the nature of the breach, the controller may need to notify both the relevant supervisory authority and all individuals whose data was exposed. The controller will have 72 hours, from the time it learns of the breach, to notify the supervisory authority.

An industry study conducted jointly by Experian Data Breach Resolution and the Ponemon Institute determined that despite awareness of regulations and risks, many companies are falling short of responding to the challenge. Michael Bruemmer, vice president, Experian Data Breach Resolution, noted, "Despite increasing reports of the damage caused by global data breaches, the study emphasizes that *the increasing risk of a global data breach, as well as the experience of going through one, isn't enough to lead CIOs and CSOs to prioritize compliance measures* in line with what is expected in the GDPR. More emphasis is required from companies, especially those with a multinational footprint, to get ahead of impending global regulations and risks. They can start by conducting risk assessments and investing in new technologies, such as encryption, as well as considering appointing a data protection officer to oversee compliance."[3]

An All-Encompassing Territorial Imperative

Likely the most sweeping change in the new regulations is the extended jurisdiction of the GDPR, now applicable to any company selling or offering goods or services or monitoring the behavior of individuals in the EU. Previously, the territorial boundaries specified for protections focused only on companies with establishments in the EU. By this reckoning, any company offering businesses or services in the EU must adhere to the data protection measures in force. Because of this, many companies are opting to handle all personal data in the same manner, without trying to identify the country of origin. This policy is good insurance, as many other countries around the world are instituting laws similar to GDPR. Enterprises that have already implemented effective data security measures will be ready for the inevitable change.

The Definition and Handling of Personal Data

GDPR has adopted a broad definition of personal data. The regulation uses this definition:

> *Personal data* means any information relating to an identified or identifiable natural person (data subject); an identifiable natural person 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, an online identifier to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.[4]

Because of the rash of large-scale data breaches in recent months, organizations are facing a serious lack of public trust in the handling of personal data. For example, an ICO survey found that only one-fifth of the UK public have trust and confidence in the companies that handle and store their personal data. The transparency required by GDPR represents a strong step in bolstering the public's attitude toward personal data privacy.

Steve Wood, the Deputy Commissioner of ICO, commented, "As personal information becomes the currency by which society does business, organisations need to start making people's data protection rights a priority. Putting data protection at the centre of digital businesses strategies is the key to improving trust and digital growth."[5]

Wood continued, "Changes to data protection legislation, which includes the introduction of the GDPR, offer organisations an opportunity to re-engage with their customers about data. The new laws require organisations to be more accountable for data protection and this is a real commitment to putting the consumer at the heart of the business."

Companies must ensure that personal information is:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant, and not excessive
- Accurate and up to date
- Not kept for longer than is necessary
- Processed in line with a person's rights
- Secure
- Not transferred to other countries without adequate protection

Understanding the GDPR provisions that apply to personal data is an essential requirement when devising system and infrastructure protection mechanisms to guard against breaches and malicious intrusions.

GDPR Protections and the Hybrid Cloud

As revealed by the industry study conducted by Experian Data Breach Resolution and the Ponemon Institute, mentioned earlier in this document, even data breach occurrences on a global scale often don't motivate CIOs and CSOs to prioritize compliance measures. The penalties that GDPR can impose, as well as the equally damaging risks of losing stature in the industry and forfeiting customer trust, provide strong incentives to strengthen security measures. One effective way to do this is by taking advantage of the flexibility and functionality of the hybrid cloud. Smart applications of the latest technologies can serve as a mechanism for compliance, as well as an effective way to achieve business goals.

Hybrid cloud implementations offer numerous choices for managing risk in a cost-effective way and instituting controls over the movement, storage, and use of personal data. As a means of helping to achieve compliance with GDPR, hybrid cloud solutions provide functionality to enable accountability, transparency, centralized management, and oversight, as well as flexible security options that risk practitioners and data protection officers can easily and effectively implement.

Reducing risk to manageable levels is always a balancing act. Information security professionals must weigh the tradeoffs that exist among the available controls, factoring in cost, effectiveness, efficiency, and long-term utility. The most visible controls, those on the frontlines of data protection, generally present clear-cut benefits and more easily measurable costs, including intrusion prevention systems, data encryption of stored data and transferred data, virus scanners, malware solutions, data classification tools, and so on.

Other controls can be equally important, but aren't always as easy to evaluate with a straightforward cost-benefit analysis. Some examples of these controls include:

- Auditing the enterprise IT group and data processors, including CSPs and software-as-a-service vendors, on a regular basis
- Establishing physical protections for the data center facility
- Controlling access to the data center using badges, passwords, and biometric readers
- Wiping or destroying physical media when it is appropriate to purge the data
- Disabling USB ports on servers to prevent theft or illicit access to data

- Applying Content Security Policy mechanisms to deter cross-site scripting (the primary vulnerability in modern web applications)

The Art and Science of Applying Controls

Skilled IT architects and security professionals recognize that applying controls to strengthen data protection is both an art and a science. Any weak points in a security system need to be identified and vulnerabilities removed. Otherwise, the effectiveness of the entire system becomes compromised, subject to failure and possible breach. The best defense-in-depth practices follow the principle that applying controls at a single layer is insufficient to protect assets; a multi-layered approach to instituting controls is much more effective at mitigating risk. Technologies that are used as part of a data protection solution should be applied across the hardware infrastructure and the software stack, whether the IT operations are on-premises, in the cloud, or part of a hybrid solution.

To protect personal data, security professionals within an organization need to ask relevant questions about the compute environment, such as:

- Do we adequately control who has access to the physical servers?
- Is there a media wiping or destruction policy in force to govern data purging?
- Is there a security risk from any of the applications running on the same servers as the with personal data subject to GDPR?
- Are there tracking and auditing measures in place to manage and confirm that protections are effective and meeting compliance mandates?
- Is data in each of its states (at rest, in transit, in use) being encrypted? Are compute, storage, and network resources fully secured using the latest-generation encryption tools?
- Have all required controls been activated and tested successfully and regularly?

As part of a comprehensive security evaluation, other considerations should be addressed, with the goal of always seeking to discover vulnerabilities at each of the layers of the system infrastructure.

Security Components of Software-Defined Infrastructure

Hybrid clouds and multi-cloud environments offer the richest breadth of control choices. Public and private clouds are part of the environment that may contain personal data subject to GDPR, as are on-premises servers residing within enterprise facilities, as shown in Figure 2. Some security components are common to all forms of cloud computing; others are unique to specific implementations.

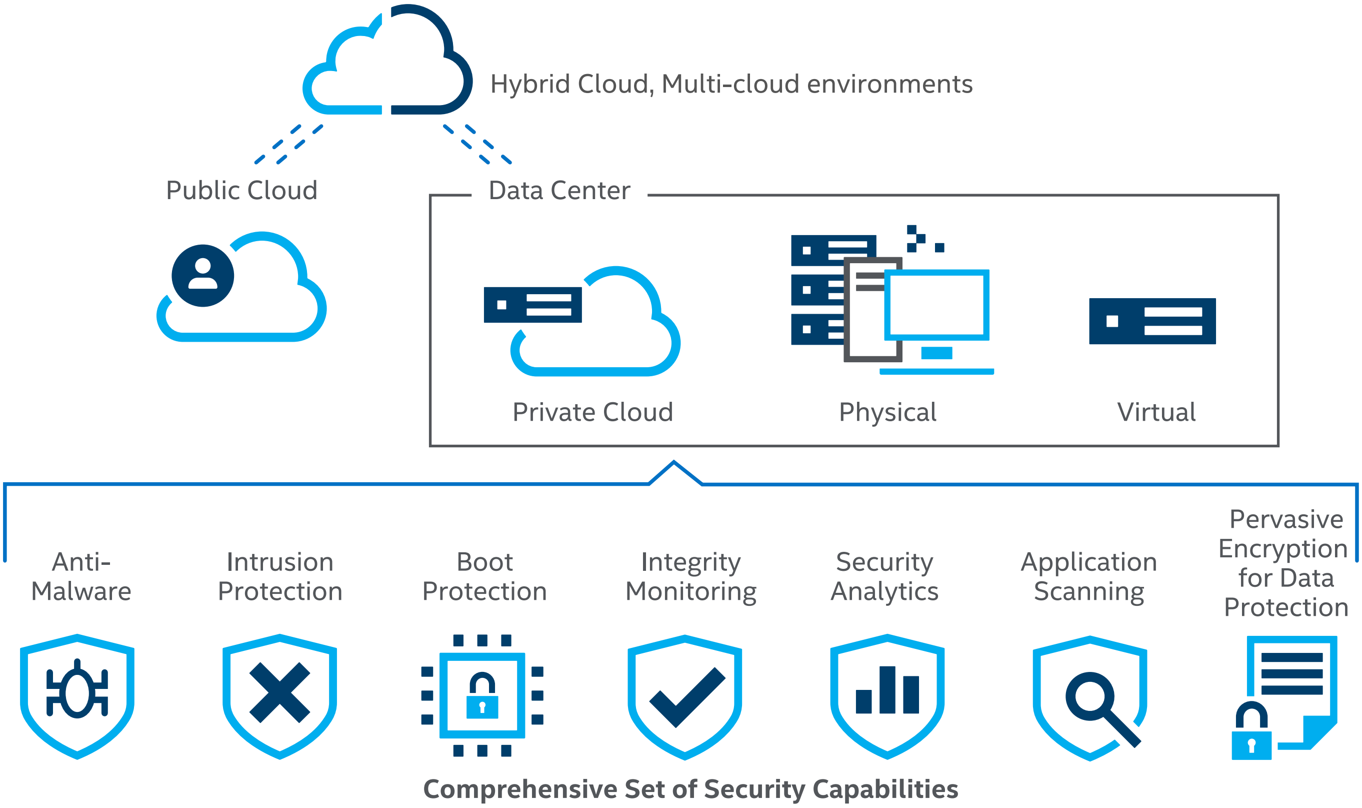

Figure 2. Available security capabilities for cloud deployments.

Technologies available with a software-defined infrastructure have the advantage of full visibility across compute, network, and storage assets, all of which can be observed and administered from a centralized, single-point console. Security tools can be applied to protect all assets, using measures such as:

- Micro-segmentation
- Boot protection
- Anti-malware software
- Intrusion protection
- Integrity monitoring and validation of vital components prior to use
- Security analytics
- Application scanning
- Data protection through pervasive encryption

Controls for Private Cloud Deployments

The critical controls and their uses to private cloud owners are discussed in the following sections.

Establish a root of trust

The foundation for a hardware-based root of trust begins with *boot protection*, enabled by Intel® Trusted Execution Technology (Intel® TXT) and a trusted platform module (TPM). To enable a secure environment for trusted cloud operations, Intel TXT inspects the system environment during the boot operation, comparing measurements of the BIOS, operating system, hypervisor, and modules with known good measurements from a prior boot. Discrepancies in the measured values can interrupt the boot process before malware code can be run or illicit system configuration changes can be made.

Intel TXT can be used to create trusted pools with policy-driven security-enabled protections, as shown in Figure 3, delivering fine-grained control over sensitive workloads being run, particularly those that contain personal information.

The technology is based on an initiative by the Trusted Computing Group (TCG) to promote safer computing. As a first line of defense in a private cloud or on-premises, you can deploy this technology directly within your systems. If using a public CSP, you can often request this protection as an option. In some cases, it is a built-in capability freely provided by the CSP. (For more details, download this white paper, The Road to a Secure, Compliant Cloud.) For more information about Intel TXT and other silicon-based security technologies from Intel, visit the landing page Trusted Infrastructure Enabled by Intel® Technology

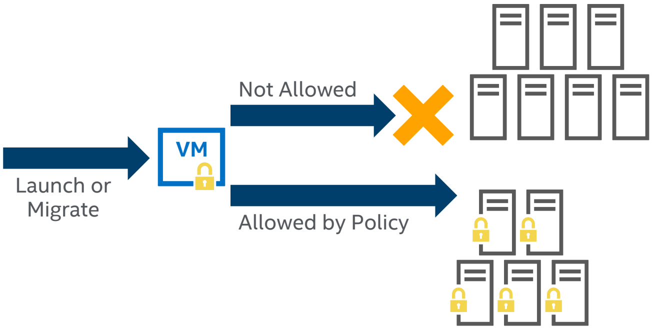

Figure 3. Policy-driven workload distribution.

Apply encryption liberally - everywhere

In modern system security scenarios, cryptography plays a vital role for protecting data in each of its states. Cryptography uses algorithms to convert data from readable forms to unintelligible forms, preserving the confidentiality of data whenever theft or intrusion presents a risk. Experienced security professionals tasked with meeting GDPR data protection requirements encrypt data liberally, the only drawback being that the algorithms that perform encryption and decryption have historically been processor intensive, as shown in Figure 4. However, by leveraging Intel® Advanced Encryption Standard New Instructions to encrypt data at rest, in use, or in motion, you can accelerate the operations involved to reduce processor cycles while gaining confidence that many attacks against the physical files are mitigated. An effective solution includes protecting files as they are being stored, as well as when they reside on any type of backup media.

Another aspect of sound data management is to ensure that the private cryptographic keys needed to unlock encrypted data are never exposed during their life cycle. Intel® QuickAssist Technology (Intel® QAT) with Intel® Key Protection Technology provides this functionality—when keys are being generated, used, and stored. This capability is included with the Intel® Xeon® processor Scalable family. To further boost the performance of cryptographic operations, Intel QAT offloads encryption of data packets to relieve the processor of these operations. Besides availability on Intel® Xeon® Scalable processors, Intel QAT is available in select Intel® network products.

Accelerated encryption in the private cloud can often be extended to public CSPs as an optional or bundled capability. Check with your public CSP to ensure that your data is protected with cryptography at rest, in use, and in transit. CSPs that support Intel QAT will increase the performance benefits as well.

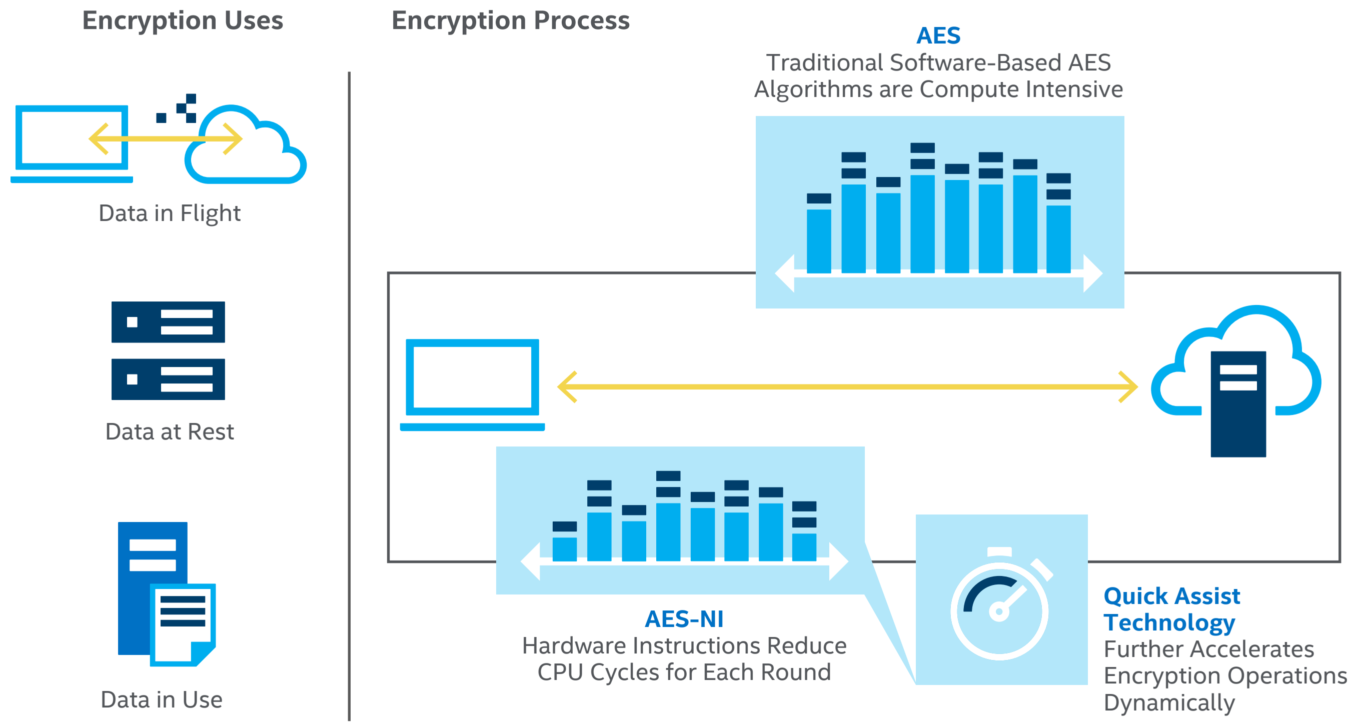
Encryption Uses
Encryption Process
Data in Flight
Data at Rest
Data in Use
AES
Traditional Software-Based AES Algorithms are Compute Intensive
AES-NI
Hardware Instructions Reduce CPU Cycles for Each Round
Quick Assist Technology
Further Accelerates Encryption Operations Dynamically

Figure 4. Accelerating encryption operations.

Ensure controls are current, active, and have relevance to GDPR

The controls discussed are typically considered vital components to ensure strong security when protecting personal data. It is also essential—even after controls are deployed—to validate that the controls are providing the necessary and intended risk reduction without interruption. Many recent examples of breaches have shown that while organizations have installed appropriate controls, failure to deploy them and maintain them has led to compromise.

Controls for Hybrid Cloud Deployments

Techniques for expanding controls into a hybrid cloud are discussed in the following sections.

Pseudonymization

Pseudonymization is a technique that minimizes potential exposure of required personal data by replacing identifying fields in a data record with one or more tokens or artificial identifiers. As shown Figure 5, there is a difference between what is considered pseudonymous data and anonymous data (one is linked by a token, for example "User X," and the other has no link between the data and the individual).

Personal data stored in the private cloud can be better protected by selected application of necessary controls. Appropriate IAM (Identity and Access Management) controls allow authentication and authorization—along with the appropriate amount of personal data and pseudonyms—to complete processing.

<table>
<tr><td colspan="2">Personal data:
"Jane Doe's eyes are green."</td><td colspan="2">Annonymous data:
"People's eyes are green."</td></tr>
<tr><td>Identified data:
"Jane Doe's eyes are green."</td><td colspan="2">Pseudonymous:
"User X's eyes are green."</td><td>Anonymized:
"A User's eyes are green."</td></tr>
<tr><td>Identifying data:
"Jane Doe"</td><td colspan="3">Attributed data: "green eyes"</td></tr>
</table>

Figure 5. Pseudonymous compared with anonymous data.

Advanced Data and Key Protection

Intel® Software Guard Extensions (Intel® SGX) provides tools for application developers to protect code, encryption keys, and data from exposure or alteration during use, an important factor for helping to ensure compliance with the GDPR strictures. This set of Intel® architecture extensions helps increase security by making it possible to run selected code and data in enclaves (protected regions in memory).

Special instructions available in the Intel SGX SDK give developers a means to designate specific application code or sensitive data to be moved into the protected region of memory. Creating and debugging tools are provided in the SDK, as well as APIs, libraries, documentation, and sample code. Visit the Intel SGX homepage for more information.

Limiting Sensitive Workloads to Appropriate Platforms

Open Cloud Integrity Technology (Open CIT) is an open source project originally developed as an Intel® product. Open CIT provides trusted computing and attestation across cloud infrastructures and enables visibility and compliance in data centers residing in public and private cloud environments. Intel TXT is used to establish a root of trust at the hardware level and then to build a chain of trust across hardware and software components, including asset tagging. With the platform trust and asset tagging confirmed, Open CIT enables controlled geofencing of data and workloads, referencing physical geography as well as virtual segmentation of computing and storage assets. This video provides an overview of Open CIT capabilities.

Through Open CIT, systems administrators can tag host systems with specific properties and administrators can tag data volumes and compute virtual systems with distinct classifications. By combining these characteristics and referencing policy controls, sensitive workloads (such as those processing personal data) can be designated to run only on specific hardened platforms. Audit tracking and recording of the cloud infrastructure for compliance is also accomplished.

Complying with GDPR

Businesses established in the EU or selling or offering goods or services to or monitoring the behavior of individuals in the EU—which includes storing, transferring, or otherwise processing this data—are mandated by GDPR to demonstrate the implementation of technical and organizational measures to ensure a level of security appropriate to the risk presented by the processing operations. This is an ongoing obligation. A change in the processing operations may require additional or different security measures. The types of data covered are all encompassing, including information stored by human resources, data about consumer purchases and identities, business contact information, details about website visitor identities, data carried over the IT network, and virtually any data that discloses details about an individual's life, records, and personal transactions. In addition, businesses must ensure that rights have been granted to collect an individual's data and permission obtained for processing it.

To help accomplish these goals, a number of Intel technologies offer capabilities that can help address the GDPR requirements to have in place appropriate security measures, starting with solutions embedded in silicon at the lowest hardware levels ranging upward to protections that help guard against data breaches that might occur anywhere within the software stack. Chief security officers, data protection officers, chief technology officers, and other staff members involved with corporate security in the enterprise IT infrastructure have a responsibility to assess current practices, identify potential vulnerabilities in their networks and data handling processes, and implement protections in advance of the GDPR deadline. Doing this not only will strengthen security as a compliance measure, but can also bolster customer confidence, solidify the brand reputation, and lead to modernization of the enterprise IT infrastructure to incorporate the latest productivity technologies.

Generally, always apply the most capable and most advanced controls to the most sensitive data. These advanced controls typically cost more and should be used judiciously. To take maximum advantage of available resources, analyze the tradeoffs and base your decisions on where controls are best deployed to help ensure that your hybrid cloud will be cost effective, as well as secure.

Many data protection issues can be simplified and risk minimized by separating the most sensitive personal data from all the other data. Explore the available solutions and be prepared to be compliant when that big date—May 25, 2018— arrives. Bear in mind also that compliance is an ongoing obligation. A change in processing operations may require additional or different security measures.
In addition, the GDPR, like most modern data protection regulations, assumes the state of the art will change, and, so, assessment of available and appropriate solutions to help secure personal data will be an ongoing process, beyond May 25, 2018.

> Hybrid cloud implementations provide security and data protection by offering a broad range of control choices to IT professionals tackling GDPR compliance issues. Intel architecture-based solutions offer the flexibility and built-in capabilities to address many GDPR challenges effectively.

Learn More

The ICO has created a guide—Preparing for the General Data Protection Regulation: 12 steps to take now—that is available here: https://ico.org.uk/media/for-organisations/documents/1624219/preparing-for-the-gdpr-12-steps.pdf), explaining the essential requirements every company should consider before the regulation is enacted.

[1] "Pulse Survey: US Companies ramping up General Data Protection Regulation (GDPR) budgets." PwC. 2017. https://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/pwc-gdpr-series-pulse-survey.pdf

[2] Stone, Adam. "The 10 Worst Data Breaches of 2017." Security Magazine. 2017. https://www.securitymagazine.com/articles/88568-the-10-worst-data-breaches-of-2017

[3] "Report Says Organizations Are Not Ready for Global Security Risks and Regulations." Security Magazine. 2017. https://www.securitymagazine.com/articles/88118-report-says-organizations-are-not-ready-for-global-security-risks-and-regulations

[4] "Regulation (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016." Office Journal of the European Union. 2016. http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf#page=33

[5] "ICO survey shows most UK citizens don't trust organisations with their data." Information Commissioner's Office. 2017. https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/11/ico-survey-shows-most-uk-citizens-don-t-trust-organisations-with-their-data/

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document. You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a non-exclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at www.intel.com.

The products described may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.