Hewlett Packard Enterprise

Authorised Distributor

INGRAM MICRO

horizon.

GDPR
What data should be protected?

index

The GDPR.
A new step in the privacy of personal data

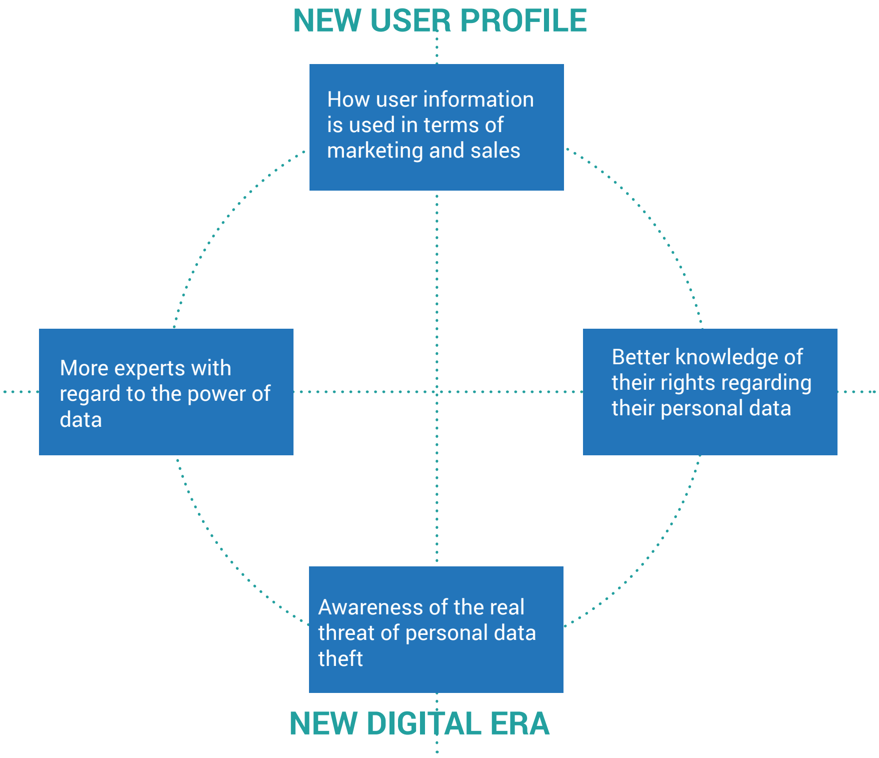
In May 2018 the new European Union General Data Protection Regulation (GDPR) comes into effect, regulating the privacy of data relating to its citizens, and which will be mandatory for all companies and institutions.

This new law provides a response to the growing volume of personal data that companies and administrations store and use, and the need for a legal framework to protect individuals against the misuse of that data and against cyber threats. The aim of the GDPR is to regulate the collection, storage and use of personal data; in short, any information that can be used to identify an individual.

The goal is to return the control over their personal data to citizens, imposing, in turn, strict rules about who stores and 'treats' these data, anywhere in the world. The Regulation also contains rules relating to the free movement of personal data within and outside the European Union.

The GDPR replaces the Data Protection Directive of the European Union, which was created in 1995, and represents the last major EU legislation regarding the privacy of personal data.

THE NEED FOR A NEW LEGAL FRAMEWORK FOR PERSONAL DATA PROTECTION


NEW USER PROFILE

How user information is used in terms of marketing and sales

More experts with regard to the power of data

Better knowledge of their rights regarding their personal data

Awareness of the real threat of personal data theft

NEW DIGITAL ERA

The GDPR.
A new step in the privacy of personal data

This new profile of users and their new awareness regarding the processing of their personal data make their protection and proper use increasingly important. The key factor for people to agree to the use of their data by organizations is the “trust” in their ability to protect the information.

Compliance to the GDPR is essential for anyone doing business in EU countries and without this trust from people, the chance to be able to continue with the business disappears.

THE GDPR ALSO REPRESENTS AN OPPORTUNITY FOR COMPANIES

Adaptation to the GDPR must be seen by companies as an opportunity and not as a mandatory regulation. The implementation of better technology gives them more competitive advantages.

GDPR Implementation → Opportunity:

✓ To provide the market with the necessary trust that a company should provide with the highest reliability in safeguarding private personal data

✓ Reach new markets and contacts with businesses that have also complied with the GDPR

GDPR Implementation → Boost competitiveness:

Profile your clients and contacts according to the GDPR regulation, as well as refining unstructured confidential information

Improve the efficiency and cost effectiveness of data protection

A path to a new regulatory framework

The thing that entities look at is the economic consequences that failure to comply with the GDPR regulations can represent, with penalties which may amount to 4% of their turnover. The most serious consequences are the effects on image and reputation that can arise, which are very difficult to quantify.

What must be avoided by all means is damaging the reputation and image of the entity due to a failure to comply with the GDPR.

All organizations must design solid plans to ensure that they comply with the rules as of May 2018. Each plan must contain the appropriate strategy for each type of entity and a roadmap for its application.

It is essential to define what requirements have to be met, categorize the data, establish how they should be protected and managed, and set the appropriate security measures, regardless of whether they are structured or unstructured data, which represent the largest volume in any entity.

THE GDPR IS AN OPPORTUNITY FOR COMPANIES

A path to a new regulatory framework

When does the GDPR enter into effect?

The GDPR officially enters into effect next May the 25th 2018.
Hence, entities must execute their plan to meet this deadline, otherwise they will be formally warned but not sanctioned.

What organizations are affected by compliance to the GDPR?

All entities established in the European Economic Community or that offer their products to citizens of the EU and therefore handle personal data, regardless of the size of the organization.

According to the GDPR, what is information of a personal nature?

For the GDPR "personal information" is any information that can be directly linked to an individual. This definition can refer to a large amount of data, many of which goes beyond common data, such as name or e-mail address, and reach personal tastes, beliefs or ideas of each person.

What can happen if you fail to comply with the GDPR?

Sanctions will vary depending on the infringement:

- If you fail to comply with the obligation to protect personal data, fines can be up to 2% of the turnover of the preceding year and up to 10 million Euros.
- If you fail to comply in terms of a serious aspect, such as the transfer of data, they can reach 4% of the turnover of the preceding year and result in a fine of up to 20 million Euros.

After two years to prepare for the new regulations, the time has come for entities to execute the appropriate measures in order to comply with the requirements of the GDPR. The time limit is running out.

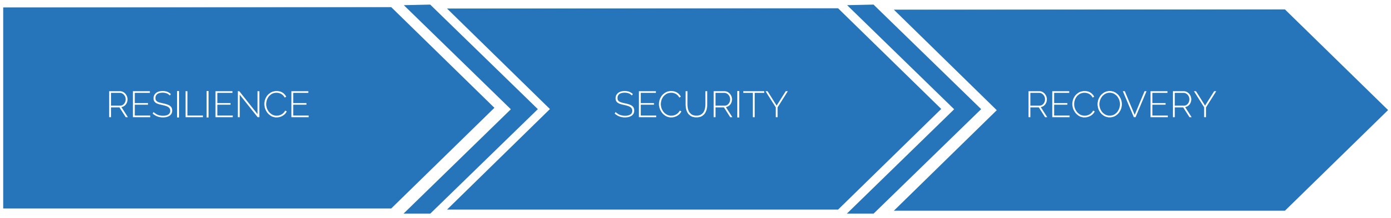
What should businesses secure?

The GDPR does not exhaustively lay out what type of IT infrastructure must be implemented. It falls to each entity to determine what technology should be used to ensure compliance.

However, the regulation determines that each organization must take the necessary security measures so as not to put the personal data that they store at risk and ensure its security at all times.

MEASURES TO ENSURE THE SECURITY OF PERSONAL DATA

IT Infrastructure for the GDPR



INFRASTRUCTURE BASED ON "RESILIENT" SOLUTIONS

BACKUP AND DISASTER RECOVERY SOLUTIONS

New security proposal for IT infrastructure

Current proposal: PROTECT

New proposal: PROTECT - DETECT - RECOVER

DATA ENCRYPTION
DATA CONFIDENTIALITY
INTEGRITY, AVAILABILITY AND FLEXIBILITY DATA PROCESSING

DATA RECOVERY AFTER A DISASTER

What should businesses secure?

In what sense and how should an organization comply with the GDPR?

An assessment of the risks must be carried out on a permanent basis, to ensure compliance with the GDPR, including IT infrastructure, just as the regulations in each country and the EU stipulate:

What personal information is protected by the GDPR?

- All information of a personal nature, in any type of format: print, audio, visual and alphanumeric.
- The concept of personal data is expanded to new sources of information, including cookies and IP addresses.
- Especially sensitive data include also genetic data and biometric data, as well as data on health, trade union membership, sex life, religion and politics.

What is the most effective management that must be performed to comply with the new regulation?

- Understand data streams, where they are used and where they move sensitive data between databases and applications.
- Ensure that all requirements set forth in all policies and legal proceedings are met.
- Continuously evaluate that the IT infrastructure used avoids all risks of data loss and meets all the requirements.
  Establish a “legal” team for the assessment of compliance with the new regulations.

How do you ensure that personal data are protected and stored safely and according to the regulation?

- The first step is to appoint a data protection officer, who will be the official contact person regarding the GDPR for both the competent authorities and the general public.
- Determine if the backup and disaster recovery systems guarantee the protection of personal data.
- Periodically review the security systems of the IT infrastructure: systems and communications.

What should businesses secure?

IT TECHNOLOGIES OF PARTICULAR SENSITIVITY FOR THE GDPR

KEY TI SOLUTIONS

NEW SECURITY RISKS

CLOUD	MOBILITY	BYoD
Is your data entirely secure?	Who has access to your network, and how?	How can you know if non-corporate devices are secure?

HPE solutions to assist in compliance with the GDPR

HPE offers a complete portfolio of solutions for organizations of all sizes and sectors to comply with the new GDPR regulations. Responsibility for the enforcement of this Regulation corresponds to each organization and its willingness to comply with it, but HPE and its distribution channel are aware that they can help all of them to do so.

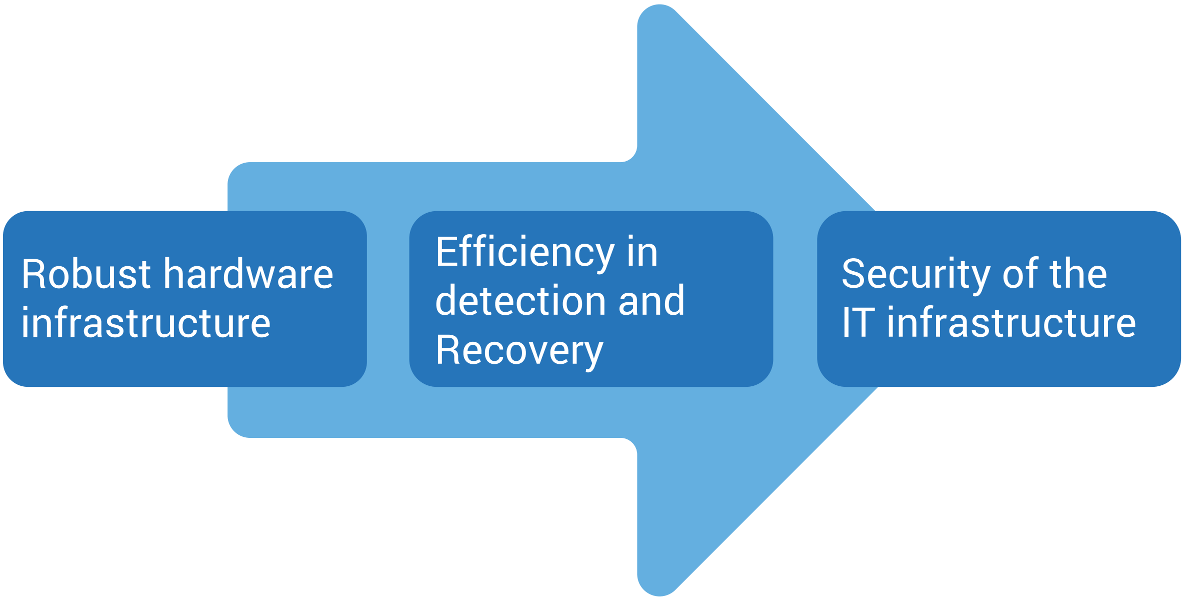
What is HPE's proposal for compliance to the GDPR based on?

The objective of HPE is to help entities manage confidential information of a personal nature, through the proposal of appropriate IT infrastructure solutions, according to the requirements of the GDPR, avoiding the risks posed to their reputation and image, in addition to possible economic sanctions.

And what IT infrastructure needs to be implemented?

GDPR legislation is very clear, and the protection of data is based on the "flow" that all of the data follows. This is really rather complex to control and it is important to have the right IT infrastructure.

HPE considers that adequate IT infrastructure for the implementation of the GDPR must ensure the following:



Robust hardware infrastructure

Efficiency in detection and Recovery

Security of the IT infrastructure

ROBUST HARDWARE INFRASTRUCTURE

Currently, the risks of cyber attacks are taking place from the application layer to the operating system and the firmware layers and, therefore, to implement a robust and reliable IT infrastructure for data security is the critical first step that needs to be addressed.

Firmware level attacks are revealing the lowest possible levels of reliability, which can be turned into trust by establishing a secure environment for rooting the operating system and applications on. HPE's proposal is based on the "Silicon Root of Trust" to ensure the safety of the firmware:

"Silicon Root of Trust"

HPE is the only vendor that provides the "Silicon Root of Trust", which creates a digital fingerprint on the silicon and ensures that the server never boots with compromised firmware.

Detection of firmware threats

With HPE's firmware threat detection, it is known on a daily basis if the firmware has been compromised. If so, this allows you to automatically recover a known and trusted state and quickly get the server up and running again.

Server data security

Data protection should not be limited just to data on the network. When deploying the highest level of security algorithms, known as CNSA-suite, you can keep your most sensitive information within a protected server.

HPE solutions to assist in compliance with the GDPR

EFFICIENCY IN DETECTION AND RECOVERY

Malware attacks and infections are becoming more numerous and inevitable. Even if you have invested in implementing a system based on "Silicon Root of Trust", the software layers have their own "security holes". Attacks intending the theft of critical data are, for the GDPR, the main focus of cyber-crimes, and detection of threats will be carried out thanks to the most advanced technologies for this purpose that will intervene before these attacks occur.

What is security supervision?

It is an automatic process that collects and analyses indicators of potential threats and then classifies them to be able to perform the appropriate actions.

Definition of security supervision

This is the definition of the types of behaviour that trigger alarms and necessary actions. Also known as "Security Information Monitoring" (SIM) or "Security Event Monitoring" (SEM), it implies the compilation and analysis of information to detect suspicious behaviour or unauthorised changes to the network system.

Why is security supervision important?

From hackers to malware; from disgruntled or not-so-careful employees to obsolete or vulnerable devices and operating systems; from mobile and public cloud computing to external service providers; most companies are routinely exposed to security threats of varying severity levels during the course of their business activities. Given the ubiquitous and inevitable nature threats, fast response times are essential for maintaining the security of the system. So automatic and continuous security monitoring is key to quick detection and response.

HPE solutions to assist in compliance with the GDPR

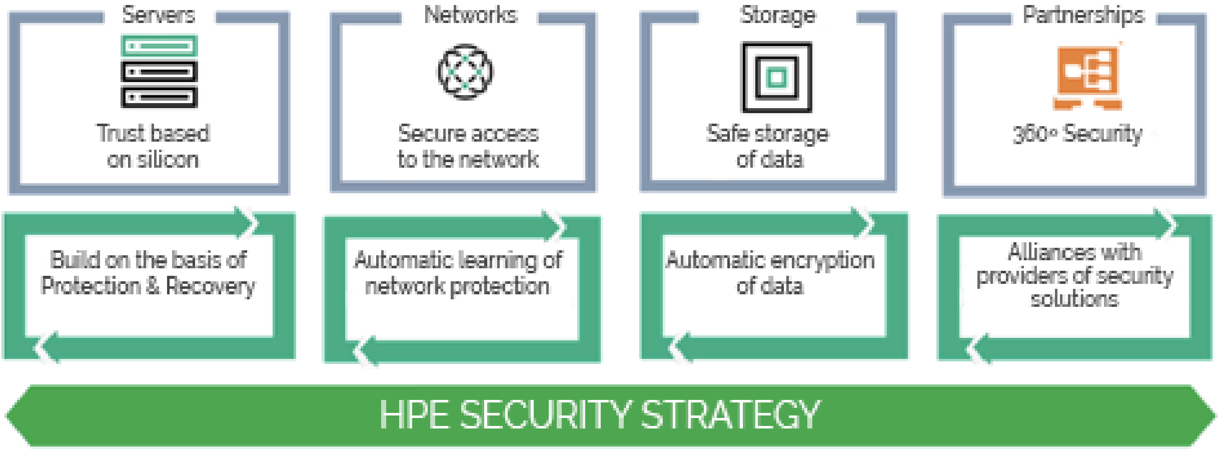
BUILT-IN IT INFRASTRUCTURE SECURITY

The fundamental goal of the GDPR regulation is to ensure the protection of personal data that is collected and used by organizations. Hence more security solutions must be implemented to reliably ensure data integrity.

One of the key solutions for the GDPR is the one in charge of protecting data and making it unusable through encryption. Entities that wish to use this solution should take care of the critical aspects of this technology:

- Compliance to Standards
- Key Management
- Key protection

HPE SECURITY STRATEGY


Servers
Trust based on silicon
Networks
Secure access to the network
Storage
Safe storage of data
Partnerships
360º Security
Build on the basis of Protection & Recovery
Automatic learning of network protection
Automatic encryption of data
Alliances with providers of security solutions
HPE SECURITY STRATEGY

Speed up EU GDPR compliance initiatives for your clients with HPE

HPE infrastructure, including servers, storage and networking has been validated against the NIST 800-53 control guidelines to accelerate compliance initiatives, such as the General Data Protection Regulation in the EU (EU GDPR).

HPE solutions to assist in compliance with the GDPR

HPE INFRASTRUCTURE FOR COMPLIANCE WITH THE GDPR

To comply with the “Silicon Root of Trust” proposal, HPE offers its HPE ProLiant Gen 10 servers, the safest on the market, alongside their storage, network, and data protection solutions, to help organizations comply with the GDPR obligations.

HPE’s complete infrastructure proposal does not ensure data and the obligations that the GDPR demands 100%, but it is the most effective tool the IT department can have to reduce the risk of attacks and provide the most reliable solutions and IT infrastructures for mandatory data protection compliance.

Secure HPE Gen10 Servers for the GDPR

HPE Gen10 Servers include the “Silicon Root of Trust” concept, which provides protection for the firmware as soon as the server is powered up.
Each time an HPE Gen10 server is booted up it compares the firmware code against the firmware code recorded from the start into the “Silicon”, detecting and avoiding any malicious code that starts with the operating system. In addition, during its operation, the HPE server has a unique real time firmware verification technology to detect any new malware implanted in critical firmware. Recovery will start with a previous version of the firmware that is known to be authentic and good.

HPE ProLiant Gen10 server platform

The world’s most secure standard servers offer high performance and safe silicon, with the aim of protecting the most confidential information.

HPE iLO Server Management

Allows easy administration for the entire server environment, including firmware security policy configuration.

HPE solutions to assist in compliance with the GDPR

HPE ProLiant Gen10 servers
New security features for Gen10

Protect

Silicon Root of Trust guarantees firmware updates via signature validation. Blocks the installation of firmware that is defective or damaged and guarantees that the executed firmware is reliable.

Authenticated Updates provides cryptographic keys to the NIC card (for HW authentication) that protects configuration and user data from unauthorized access and verifies the digitally signed firmware.

Detect

Secure Boot Safe protects the system and guarantees that rogue controllers will not run while booting.

Device-level Firewall blocks all non-administered access to memory or storage.

Recover

Audit Logs record firmware updates that are authenticated to capture the changes in the standard system records.

Sanitization (secure erase of user data) destroys both configuration and user data on the NIC and makes them unrecoverable, so that the NIC can be reused or disposed of in a safe manner.

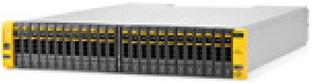
HPE solutions to assist in compliance with the GDPR

HPE storage for the GDPR

GDPR compliance depends on a scalable and reliable data protection strategy. HPE's storage proposal for the GDPR includes HPE 3PAR StoreServ, HPE StoreOnce, and HPE Nimble Storage systems to be able to create a solid basis for a comprehensive data protection strategy.

HPE 3PAR StoreServ

HPE 3PAR StoreServ storage solutions, optimized for flash and high availability, centralize and consolidate critical data of a personal nature, ensuring that it is always available and protected through the best replication snapshot features.



HPE 3PAR StoreServ 8000 Storage

The No.1 mid-range storage array on the market, available in all-flash or hybrid.

HPE 3PAR StoreServ 9000

Unified storage for the all-flash consolidation for every application and workload.

HPE 3PAR StoreServ 20000

Enterprise flash array and scalability, the industry leader, with the required resilience.

HPE solutions to assist in compliance with the GDPR

HPE Recovery Manager Central (RMC)

HPE Recovery Manager Central (RMC) integrates the all-flash HPE 3PAR StoreServ solutions with the HPE StoreOnce systems, taking advantage of the snapshots with backup protection performance for flash speed and applications protection with the lowest possible total cost of ownership.

HPE 3PAR StoreServ Data-at-Rest Encryption

Protects data from internal and external security breaches. HPE 3PAR StoreServ can be configured with self-encrypting drives (SED) and optional business secure key management. HPE 3PAR StoreServ Data-at-Rest Encryption provides data protection to ensure that access to stolen, discarded or replaced disks is not possible.

HPE StoreOnce

HPE StoreOnce devices complement the HPE 3PAR StoreServ solutions by providing the availability, scalability, and flexibility that organizations need for the preservation and retention of data in the short and long term.

HPE StoreOnce backup devices with data protection

Data growth is leading to an increase in backup times, non-compliance with Service Level Agreements (SLA) and the use of more management resources. HPE StoreOnce systems with StoreOnce Catalyst provide:

✓ A single, coherent and high-performance backup architecture that covers the whole company.

✓ A reduction in the amount of backup data that needs to be stored by 95%, choose between powerful dedicated devices for data centres or larger offices and flexible virtual devices for remote and smaller offices.

✓ High performance backup and restore speeds in order to meet Service Level Agreements (SLA) required recovery.

✓ HPE StoreOnce can deduplicate at any location as well as controlling the movement of deduplicated data across the company. HPE StoreOnce offers flexible integration for SAN, Ethernet, and Virtualized environments, reducing costs, risk and complexity.

HPE solutions to assist in compliance with the GDPR

HPE Nimble Storage

HPE Nimble solutions are ideal for advanced data services optimized with flash, which include all-flash, flash hybrid and multi-cloud support, backed by predictive analysis based on machine learning.

HPE Nimble Storage offers pure performance with unparalleled scalability.

Designed for speed and scalability, the Nimble All Flash arrays offer the performance and low latency required to run the flash data centre.

TCO from 33% to 66% lower - Absolute resilience - Horizontal scalability

HPE Nimble Storage Flash Arrays

Nimble Storage all-flash

All-flash arrays
Raw capacity from 6TB to 553TB

Useful capacity from 4TB to 238TB

Effective capacity from 20TB to 2045TB [delivers a data reduction of 5:1 resulting from deduplication and compression]

Nimble Storage adaptive

Adaptive flash arrays
Raw capacity from 11TB to 1470TB

Useful capacity from 7TB to 1185TB

Effective capacity from 13TB to 2371TB [delivers a data reduction of 2:1 resulting from compression]

Nimble Storage secondary

Secondary flash arrays
- Raw capacity from 21TB to 252TB
- Useful capacity from 16TB to 200TB
- Effective capacity from 288TB to 3600TB [delivers a data reduction of 18:1 resulting from deduplication and compression]

HPE solutions to assist in compliance with the GDPR

Aruba Solutions for a secure network ready for the GDPR

A new approach to security threats	Protect the digital workspace considering the dissolution of security perimeters	Protection begins with strict network access control	Detect attacks on the inside with UEBA
Highly organized and selective attacks are quite common. Aruba is offering a new framework for enterprise security that offers an integrated and broader way to regain visibility and control in network environments.	Mobile solutions, cloud computing and the Internet of Things (IoT) have introduced new challenges and vulnerabilities to the network. Digital work spaces based on collaboration raise new demands in terms of security.	It takes just one click to compromise a network. Aruba ClearPass provides a proactive network access control that covers a wide range of uses, from wired to wireless solutions, IoT, BYOD and corporate incorporation as well as a solution and response to attacks based on policies.	Traditional security products based on signatures, pattern matching or rules for detection are effective for known attacks. It is the unknown attacks that have the potential to cause more damage to an organization. User and Entity Behaviour Analytics (UEBA) from IntroSpect offers detection of attacks based on automatic learning for threats from inside the network.

HPE solutions to assist in compliance with the GDPR

The network should also be prepared for complying with the GDPR and mobile workplaces are a security threat. They need integrated, automatic security controls to protect data from malware and unauthorised users. Detecting and preventing
intrusions protects the infrastructure from WiFi and fake access point threats.

Wireless network

The Aruba Instant 802.11ac access points include rapid configuration, high security, integrated management control and gigabyte WiFi speeds, all at a very reasonable price.

Wired network

In the new world of WiFi, switches must offer appropriate performance. The wired solution is critical for optimal application delivery.

When installed with Aruba switches, Aruba Instant wireless access points provide businesses with a potent end-to-end secure wireless network.

Administración

Allows for the administration of a network locally, on the cloud with Aruba Central, or locally, using Aruba AirWave. Access points include a free local administration interface that provides network visibility and all authorisations for instant network administration.

HPE solutions to assist in compliance with the GDPR

HPE'S AND IT CHANNEL'S PROPOSAL TO HELP COMPLY WITH THE GDPR

Complying with the GDPR regulation is going to be really difficult for many entities, both due to the lack of time and the lack of knowledge and experience.

For this reason, HPE's goal, along with its distribution channel, is to act as a strategic partner to address this project, providing the right infrastructure to comply with the GDPR and take advantage of this juncture to improve corporate security.

HPE brings a proven server, storage, and networking and security infrastructure proposal that directly helps companies to prepare for the implementation of the GDPR.

The GDPR means an opportunity for all entities. The obligation to comply with the data protection standards in the GDPR will offer organizations the opportunity to simplify their IT, optimize security and improve the data administration.

The need to control the flow of information and its optimization –always in a safe way– will make it easier to reach new markets and digital businesses by implementing more agile and reliable IT environments that provide the necessary confidence to customers. Moreover, this awareness of required security measures will increase their reputation and improve their brand image, which in turn will attract new clients and revenue.

Hewlett Packard Enterprise and its distribution channel are prepared to help entities in this new digital era, to address their needs in terms of security and compliance with data protection regulations, such as compliance with the GDPR.

HPE IT infrastructure solutions with built-in security

HPE Gen10 servers have built-in security with Silicon Root of Trust implemented at the beginning of the production process.

HPE solutions to assist in compliance with the GDPR

Hewlett Packard Enterprise offers:

Encryption to protect data

With a full-scale encryption strategy, with HPE Smart Array encryption, HPE 3PAR self-encrypting units and compatibility with Atalla ESKM.

Resistance to recover from data loss or theft

HPE's automatic recovery features help start this process to retrieve server firmware.

Early notification security breaches

The only server manufacturer that oversees the firmware on the server every 24 hours to help quickly detect a violation and, therefore, promote notification to the authorities.

Why use Ingram Micro for your GDPR compliance security projects?

Ingram Micro helps get the most out of the technology you develop, implement, sell or use, making responding to the challenges your clients pose the goal.

With our great global infrastructure and our experience with Cloud services, mobility, production and technology, we can collaborate with you in a more efficient way and achieve greater success in the small- and medium-business market sector, in addition to accessing new clients and generating new business opportunities.

Our mission is to become your business partner and to support you wherever you need. We want you to count on us in order to offer complete and solid solutions, efficient and intelligent work processes and to shorten the sales cycle as much as possible in order to achieve greater profitability and faster adoption of the technology.

Our focus is on offering a solution able to span the whole life-cycle, from evaluations, planning and design to installation and actual deployment, through to solution management and technology obsolescence forecasting, so that they can be replaced with the best solutions on the market available at any given time.

Thanks for reading!