SAFEND DPS FOR EU GDPR

Whitepaper

safend
a SuperCom company

EU GDPR MEANS BUSINESS

If you work in the European Union or do business with a member state, then the General Data Protection Regulation (EU GDPR) applies to you. Set in 11 chapters and with 99 articles, EU GDPR standardizes all aspects of personal data collection, its privacy and use. Initiated in 2012, EU GDPR received European Parliament and EU Council approval in 2016 and will be actual from 25th May 2018.

EU GDPR dictates that organizations must demonstrate their compliancy to regulations at any given time and there are rumors about tougher stringency for non-EU organizations.

EU GDPR, HARMONIZING PERSONAL DATA PROTECTION

GDPR creates a harmonized approach to secure management of personal data throughout the EU by enforcing organizations to be accountable for all private information they own. Before 25th May 2018 organizations must know what personal data they have on their networks, who is using it, where it is saved and how it is secured. They must also know how it is transferred internally, within the EU or abroad, if it is relevant and how it is deleted.

WHO IS WHO

Data Subject

You and me. The person to whom the personal data belongs. When collecting information, organizations must receive the person's permission and inform them how their data will be used, saved, processed, for how long and how it will be deleted.

Data Controller

The person / organization legally accountable and responsible for everything related to personal data and its processing. Data Controller responsibilities include:

- Complying with EU GDPR regulations
- Working with the SA, Data Processors and Data Protection Officers
- POC for data subjects regarding their personal data including its removal, erasure and restriction
- Deciding on the type of information saved and how it is secured
- Reporting data leakage to the SA within 72 hours after its discovery

Data Processor

Users of personal data. For example, service providers. Their responsibilities include:

- Processing the data as instructed by the Data Controller
- Maintaining data privacy
- Preventing unauthorized access and use of personal information
- Preventing data leakage
- When required, registering with the Data Protection Authority

Data Protection Officer

A DPO is appointed when Data Controllers / Data Processors regularly or systematically monitor large quantities of data subjects. A DPO has the following responsibilities:

- Monitoring compliance with EU GDPR regulations
- Updating and advising Data Controllers and Data Processors on EU GDPR issues
- Point of contact to the Supervisory Authority

Supervisory Authority (SA)

Member state's EU GDPR representative. The SA is responsible for all aspects related to the EU GDPR legislation in their state. Responsibilities include:

- Monitoring how personal data is processed in their jurisdiction
- Consultation regarding legislative and administrative measures relating to the processing of personal data
- Handling citizen complaints regarding the protection of their personal data

Personal data, information relating to an identifiable person or identified by reference to an identifier

Identifier, a name, ID, picture, location, job title, online identifier, physical, physiological, genetic, mental, economic, cultural or social identity

DO YOU KNOW?

1. The type of personal data your company saves and why?
2. Where and how it is secured?
3. How it is transferred internally / externally?
4. If your organization has leveled access permissions? Who gives them?
5. If personal data has leaked in or out of you company?

EU GDPR BASICS

ARTICLE 17: RIGHT TO BE FORGOTTEN AND ERASURE

Personal data can be removed, erased or restricted. For example when data is no longer relevant, the person objects, it is published without permission or does not comply to EU GDPR requirements. This data must also be erased from 3rd party databases.
Data can be restricted if it is inaccurate, no longer required or pending verification. Reasons for not erasing data include public interest, public health, historical or scientific research, freedom of expression or in compliance with EU law.

ARTICLE 20: RIGHT TO DATA PORTABILITY

As owners of their personal data, data subjects can permit more than one organization to collect and process it.

ARTICLE 25: DATA PROTECTION BY DESIGN AND BY DEFAULT

Following the privacy of design ethic, data controllers are required to create a protective environment for the collection, handling and storage of personal data. This includes defining access permissions, passwords and data encryption.

ARTICLE 33: NOTIFYING THE SA

Data Controllers must update the SA on all data breaches that are likely to risk the rights and freedom of individuals within 72 following their discovery. Notification should include the following:

- Nature of the breach, number of data subjects, type of information compromised
- Details of the DPO or contact person
- Consequences of the breach
- Proposed or taken actions for handling the breach

ARTICLE 34: COMMUNICATING A PERSONAL DATA BREACH TO DATA SUBJECTS

Data controllers must immediately report all incidents of breaches of unencrypted personal data to its owners (data subjects). A full description of the incident and how it is handled must appear in the report.

ARTICLE 83: ADMINISTRATIVE SANCTIONS

Organizations failing to comply with GDPR EU regulations are sanctioned. Fines have a tiered structure. For example, a company might be fined 2% of their annual turnover for not organizing their data. The fine for failing to report leakage of personal data may reach a colossal €20M or 4% of the organization's previous year's total annual global turnover, whichever is greater. If unprotected unencrypted personal data does leak, data subjects are eligible for compensation.

STEPPING TOWARDS ACCOUNTABILITY

1. Get Informed	Get educated. A list of all 99 articles appears on the EU GDPR website Train management and employees on your organization's policies regarding personal data protection
2. Be Organized	Build a professional team. Appoint Data Controllers, Data Processors and Data Protection Officers Only keep what you need. Don't hoard data. Streamline, organize, filter, categorize and map existing personal data Define processes for managing personal data
3. Know What You Need to Do	Know the following about the personal data your organization owns, uses or collects: • How it is protected and saved • Who can access it • What it is used for • Who it is transferred to internally and externally and by whom
4. Get Protective	Define protective rules and policies for personal data access, usage and collection Build permission-based password protected folders Set rules that alert on attempted access or transfer of personal data and inappropriate activities on endpoints
5. Start Encrypting	ALWAYS ENCRYPT ALL PERSONAL DATA AND ANY DATA THAT MAY IDENTIFY A DATA SUBJECT ENCRYPT ALL DATA ON COMPUTERS, LAPTOPS AND DEVICES LIKE TABLETS, USBS OR DETACHABLE HARD DISKS
6. Monitor and Control Endpoints	Monitor and control endpoints, removable devices and storage devices like USBs and SD cards
7. Get Alerts, Receive Reports	Keep continually updated. Define strong alerting and reporting policies on access / use of personal data, ports or devices Archive all reports and alerts for future use Continually audit your network activity

COMMON GDPR EU DILEMMAS

- Answering EU GDPR compliancy requirements
- Finding a solution that works and that does not disrupt daily activities
- Finding a cost-effective and granular solution
- Overcoming integration pains
- Defining profiling, policies and exceptions

Answering compliancy requirements

Safend DPS already meets EU GDPR standards and as a customizable solution, can make necessary provisions if needed. DPS also answers additional major compliance requirements like SOX, HIPAA, PCI, FISMA, BASEL II, UK Data Protection Act (DPA) and other stringent standards.

Silent operation without disrupting daily activities

Safend DPS Data Protection for EU GDPR solution is based on the Protector, Encryptor, Inspector, Reporter and Auditor modules which balance between productivity and performance without interfering with daily work activities.

When installing Safend DPS onto a network, accurate analysis of data protection requirements are made. This enables building policies and their exceptions, profiling and adding user / machine permissions - also regarding the use of USB storage drives and other external storage devices.

As a granular suite, monitoring and controlling the information flow on your organization's endpoints, the DPS enforces these policies, permissions and exceptions as it protects, encrypts, inspects and generates reports on use of ports and devices. For example, when trying to upload an Excel file holding personal data to a USB stick which is an exception to a policy blocking use of all external devices.

Cost-efficiency, leaving room for future growth

Integrating Safend DPS into your organization's data network helps side-step costs associated with data leakage through unprotected endpoints. Safend DPS currently has the capacity to support multiple endpoints via one environment.

Overcoming the integration pains

Safend DPS is designed for comprehensive installation and can be installed by both Safend certified experts or by your organization's system administrator. Depending on the solution's requirements, the entire integration process should take a short time.

Safend DPS profiles, policies and exceptions

Prior to server installation, Safend DPS can pinpoint the usage of USB, FireWire, PCMCIA, PCI, internal storage and Wi-Fi connections in your organization. Using this information provides administrators the knowledge they need to create enforced companywide preventative policies, permissions and exceptions.

This may include blocking all external devices and then assigning exceptions to different users / devices, or that specific information only can be uploaded to an external device.

Safend DPS offers the following options:

- Blocking / enabling data transfer
- Blocking data transfer and collecting information
- Blocking data transfer without collecting information
- Enabling data transfer and collecting information
- Enabling data transfer without collecting information

One Data Protection Suite, One Data Protection Agent

Built as a suite of data protection modules, DPS protects your personal information as it controls, encrypts, monitors and updates you about its whereabouts throughout its lifecycle.

Safend Data Protection Suite Modules

- Protector: controlled port and device endpoints and external media encryption
- Encryptor: transparent encryption on laptops and PCs
- Inspector: inspects, classifies and blocks sensitive data leakage
- Reporter: regulatory compliance reports and security log summaries
- Auditor: immediate risk detection on Wi-Fi ports and devices connected to endpoints

Protector, port and device endpoints control

A flexible and intuitive solution with strong rule-based file encryption capabilities, Protector averts inappropriate use of smartphones, digital cameras or memory sticks. Protector enables creation of highly granular and customizable security policies which automatically detect, permit and restrict files and selected devices according to levelled user permissions, type, model and serial number.

Encryptor, full data hard disk encryption

A full encryption solution for all personal information, Encryptor blocks inappropriate access or transfer of information. As it secures an organization's endpoints, Encryptor immediately alerts administration on all intentional / unintentional data leakage incidents.

Always one step ahead of existing and new data hacking technologies, Encryptor already protects data at rest and can cover 250,000 endpoints.

Inspector, the gatekeeper of your organization's personal data

Providing cross-channel protection based on filtered information, Inspector offers strong alerting and event management when detecting attempted data leakage. Controlling user access and activities, Inspector also enables classifying information for improved accuracy and defining level-based security policies. Inspector checks both file content and metadata without preventing the natural flow of business.

Auditor, pinpointing the real picture

Having the capacity to run on up to 60,000 computers, the clientless Auditor pinpoints the usage of USB, FireWire, PCMCIA, PCI, internal storage and Wi-Fi connections on your network. The Auditor searches for information according to Microsoft Active Directory architecture, IP Range and Computer Name and is successfully integrated into the Safend Protector.

Reporter, the knowledge to control

Giving you the knowledge you need to prevent data from leaking, Reporter provides full statistical and in-depth information about your organization's endpoints. Pinpointing intentional and unintentional misuse, Reporter automatically pulls strategic and periodic information into built-in and customized distributed reports.

Safend DPS, Keeping Personal Data Personal

Understanding where the security challenges are and by introducing proven solutions, Safend DPS protects your organization's personal data and endpoints as it monitors, encrypts, inspects, reports and updates you on where your data is and who is using it.
Safend DPS is very stable and built comprehensively and once integrated into your network, runs automatically without interrupting daily activities.
Designed as a robust solution for port and device control with a strong anti-tampering mechanism, Safend DPS has built-in compliancy provisions, including for EU GDPR, PCI, HIPAA and SOX.
Safend is already used as a cost-effective data protection solution in many organizations who have integrated it into their network to protect their sensitive information.