

Safend for EU GDPR

Why run when you can walk

EU GDPR means business, and if you work in the European Union or do business with a member state, then it applies to you. Actual from 25th May 2018 and enforcing a structured chain of accountability, EU GDPR (General Data Protection Regulation) harmonizes the security of our personal data, its privacy and use.

11 Chapters with 99 articles of enforced accountability

Personal Data:

Any information relating to an identifiable person.

Data Subject:

You and me... the person to whom the personal data belongs.

Data Controller:

Person / organization legally accountable for everything related to collecting, protecting, processing, saving, using and transferring personal data.

Data Protection Officer:

Optional and appointed by the Data Controller. Point of contact to a state's Supervisory Authority.

Supervisory Authority:

Member state's EU GDPR representative.

Data subject rights

- People have the right to not share their information, request its removal and erase or strict its usage.
- People can permit more than one organization to collect and process their data.

Privacy by design

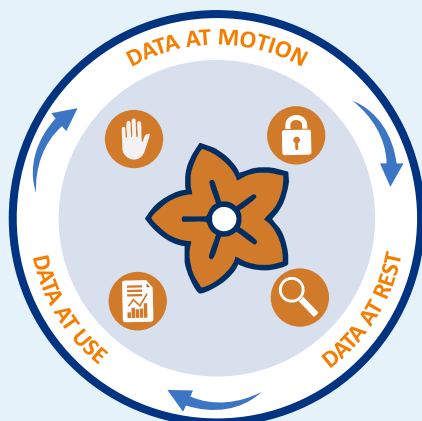
Data controllers must create a protective environment for the collection, handling and storage of personal data. This includes defining access permissions, passwords and data encryption.

Data breach notifications

- Data Controllers must report all data breaches to the Supervisory Authority within 72 hours after an incident is discovered.
- If encrypted data is compromised, no action is required by the Data Controller. Data Controllers may later need to provide proof of encryption to the Supervisory Authority.
- If unencrypted personal data is compromised, the Supervisory Authority can force Data Controllers to inform the data subjects.

Sanctions and fines

Organizations failing to comply with EU GDPR regulations may be sanctioned. The fine for failing to report a personal data breach may reach €20M or 4% of an organization's previous year's total annual global turnover, whichever is higher.



Talk it, Walk it

Get Informed	Learn more about EU GDPR and how it may effect your organization.
Get in the know	USE SAFEND AUDITOR and DISCOVERER Know exactly which ports, devices and Wi-Fi connections are used on your endpoints. Know what, where and how sensitive data is saved on your networks.
Get Encrypting	USE SAFEND ENCRYPTOR and PROTECTOR Always encrypt all personal data and any data that may identify a data subject. Encrypt all data on computers, laptops, tablets, USB keys and external hard disks.
Get Protecting	USE SAFEND PROTECTOR and INSPECTOR Avoid inappropriate use of Wi-Fi connections on endpoints by setting rules and policies that limit personal data transfer from private devices.
Get Encrypting	USE DPS ENCRYPTOR 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.
Get Monitoring	USE SAFEND PROTECTOR and INSPECTOR Monitor transfer of personal data on endpoints to external devices via channels like email, FTP, websites, the cloud or printers.
Get Alerts and Reports	USE SAFEND Data Protection Suite Be continually updated. Define strong alerting policies on access / use of personal data, ports or devices. Archive all alerts. Define strong reporting policies that generate reports on access / use of personal data, ports or devices.

About Safend, a SuperCom Company

Safend are providers of security products designed to protect against corporate data loss via comprehensive data encryption, port control, device control and content inspection solutions.

With over 3,000 customers worldwide and 3 million licenses sold, Safend software is deployed by multi-national enterprises, government agencies, healthcare organizations and small to mid-sized companies across the globe.



Herzliya, Israel, Tel: +972 (9) 889-0880, Fax: +972 (9) 889-0814
New York, USA, Tel: +1 (212) 675-4606