It governs the rights of the person, whose data are being processed.

It details the data security requirements under the risk-based approach.

It formulates the responsibilities of administrators and entities processing the personal data (e.g. in the scope of incident reporting).

It specifies the penalties which can be imposed for violation of the regulation (up to EUR 20 million or 4% of company's annual turnover).

Axence nVision®

will help you to comply with

GDPR
requirements

General Data Protection Regulation (GDPR) – is a regulation in EU law on the processing of personal data;

GDPR came into force on May 25, 2018

How will **GDPR** affect your company?

- ✓ GDPR affects all companies which collect and use the data of natural persons – both large corporations and small enterprises.

- ✓ Due to the enforcement of GDPR, a company which is a data administrator must pay more attention to data security within their organization.

- ✓ The company is obliged to implement the necessary technical (e.g. IT tools) and organizational tools (e.g. procedures) to guarantee that data are processed in compliance with the regulation, in particular in the scope of security, and must be able to prove it.

- ✓ Complying with GDPR security requirements forces the company to guarantee the confidentiality, integrity and availability of personal data; therefore, data must be protected against leaks, destruction, accidental loss or unauthorized access.

- ✓ In order to guarantee data confidentiality, integrity and availability, data access control mechanisms (technical or organizational means) must be implemented.

- ✓ The administrator must know who can access personal data and how long these will be processed.

- ✓ Along with the security issues, the need to fulfill the various requests of the persons whose data are being processed is an important requirement.

- ✓ The administrator shall guarantee each person, whose data are at their disposal, the right to acquire, transfer, correct or remove the data and the right to "become forgotten".

- ✓ Each company is obliged to implement suitable technical protection measures and suitable organizational means to immediately identify any personal data violation and rapidly inform the supervising body and the person involved.

How can Axence nVision® help you to meet the **GDPR** requirements?

Axence nVision® was developed to assist you in the management of your network infrastructure and take care of the security of your data. The answer to GDPR requirements are the DATAGUARD module and selected functions of USERS module. The remaining modules will also help to satisfy the GDPR-related requirements.

Axence nVision® will help you comply with GDPR requirements in the following areas:

Security

- ✓ Checking potentially dangerous software and applications.
- ✓ Secure data storage.
- ✓ Limiting the risk of personal data leaks by controlling data media access – detecting their connection and blocking them.
- ✓ Blocking unauthorized websites and dangerous processes.
- ✓ Protection of data against access by unauthorized users.
- ✓ The ability to define the policy for transferring corporate data by the employees with relevant authorization.
- ✓ Alarms in the case of undesirable and potentially dangerous user actions, e.g. connection of USB data media.
- ✓ Option to notify employees about new data security threats.
- ✓ The product is designed and developed with the latest IT security know-how in mind.

Supervision/Audit

- ✓ Monitoring all data file operations – auditing of the file creation, deletion and copying.
- ✓ Monitoring, which allows supervision over users' logging in to machines.
- ✓ Full file access audit allows the administrator to quickly verify and diagnose potential incidents (gathering evidence with the identification of the person responsible for the violation).
- ✓ The HelpDesk module features will help you to conduct an educational policy within the company and allow the users to report dangerous behaviors on workstations.
- ✓ Printing audits.
- ✓ Audit (history) of connecting and operations on portable devices and network devices.

Administration

- ✓ Axence nVision® does not collect sensitive data.
- ✓ It enables the management of access rights (writing, executing, reading) for devices, computers and users.
- ✓ Personal data and monitoring data can be accessed only by the specified administrators within the organization.
- ✓ It is possible to assign specific rights to selected users.
- ✓ The HelpDesk module can be used to report incidents to the IT department (or the respective specified person, e.g. ABI).

Even more corporate data security with **Axence nVision®** − Comply with **GDPR**!

We constantly work on our software, adding more security features. Axence nVision®, has been designed in compliance with the approaching changes in the law, resulting from the Regulation.

By exploiting the synergies between nVision modules, you can obtain even more tools to ensure the optimum and safe work environment within your company.

You can enhance your company's security by using AdminCenter, get a full live visibility of events and incidents on the corporate network and verify anomalies in user behavior.

Meet the features of Axence nVision®, which fully satisfy the **GDPR** requirements

- ✔ Axence nVision® has been designed with great attention to security, especially in scope of personal data collection (in compliance with GDPR's privacy by design/by default requirement).

- ✔ All personal data (including employee activity monitoring data) have been separated from the information on the configuration of the device operated by the user.

- ✔ All connections between agents, server and console, and the Web-based access are protected with full SSL/TLS encryption with the option of using a Signet/BPTP-signed certificate.

- ✔ Only the selected administrators and specified employee groups have access to personal data and monitoring data. Access to personal data is granted on the basis of rights assigned to specific persons within the company.

- ✔ Axence nVision® fully supports the virtualized environment. In organizations applying virtual machine servers with terminals, nVision enables the easy and automatic management of the data of the monitored employees − without the need of any configuration if virtual machines are changed.

- ✔ Axence nVision® introduces an object, who is a user (data will be collected and assigned to a specific user, not to a host, as it was before). Therefore all access, rights, application and website policies and the monitoring policy will automatically follow the employee, regardless of the machine he/she uses to log in.

- ✔ Collecting data per user allows it to be stored in one location, which helps to maintain data integrity. Due to the obligation to respond to the requests of an individual to whom the data pertain, and the right to "be forgotten", introduced by GDPR, it will be possible to effectively and fully remove all data related to a specific user (regardless of hosts).

- ✔ Axence nVision® in compliance with GDPR requirements related to data retention limitation, allows the administrator to define how long the data is to be stored.

- ✔ Axence nVision® supports compliance in the scope of responding to the requests of individuals, whose data are being processed (employees), e.g. by issuing copies of the data or removing the data.

- ✔ Axence nVision® supports compliance with the requirement to minimize the data, allowing it to be accurately defined in the scope of processed data.

- ✔ Replacement of the employee's machine is not an issue − monitoring data are kept, regardless of the machine on which the user is currently working. If Active Directory is used, the entire process is performed in a fully automatic manner and requires no input from the administrator.

If you are interested in the latest Axence nVision® version, contact your Business Consultant or write to us at sales@axence.net