GDPR statement for Smart ID Digital Access

Nexus sees the EU's general data protection regulation (GDPR) as an important step forward in streamlining and unifying data protection requirements across the EU. We also see it as a great opportunity for us to strengthen our clear commitment to data protection principles and practices. It is as well fully in line with our recent ISO 27001 certification in Sweden.

Nexus strives to make it as easy as possible for our customers to comply with the requirements of GDPR, which was introduced on May 25, 2018. Therefore, a number of new features are included in the latest and upcoming versions of Smart ID Digital Access component. We will also continuously review the functionality of Smart ID Digital Access in terms of GDPR.

Implemented functionality

The following functionality is implemented in Smart ID Digital Access 5.12.0 and later, to help you to be compliant with GDPR:

Traceability

Smart ID Digital Access provides a wide range of reports for users, including access reports, authentication reports, authorization reports and account statistic reports. These reports rest on the user ID and do not contain any personal information.

Availability

Smart ID Digital Access minimizes storage of personal information (such as email address, name or mobile number) by receiving such kind of the data from a user storage, such as an active directory (AD) or any other LDAP-compliant directory. Smart ID Digital Access only saves data that is required to fulfill its tasks, for example OATH seeds and failed logins.

Correction

Since personal information is received from a user storage (AD, LDAP), a request for correction needs to be addressed towards these systems. In Smart ID Digital Access, it is possible to overwrite information from the user storage if required. This information is stored in the Smart ID Digital Access database and could easily be changed by the administrator or a similar role.

Security

Smart ID Digital Access uses secure layers for communication to external and internal systems. Emails containing personal information can be sent using secure Transport Layer Security (TLS) functionality.

Smart ID Digital Access does not save personal information within its database. Sensitive information such as passwords and private keys are stored encrypted.

Strong authentication can be enforced to access the administration interface of Smart ID Digital Access. Personal information is only available through this interface. Delegated management roles also restrict the ability to see personal information to certain users.

Removal

As long as a person is using Smart ID Digital Access for authentication the information is not covered with anonymous information. If a person stops using Smart ID Digital Access and wants its personal information deleted this can be done by simply deleting the entire person in Smart ID Digital Access. Since Smart ID Digital Access receives the personal information from a user storage (AD, LDAP), anonymous information in the user storage will also take effect in Smart ID Digital Access.

Related information

- Terms and GDPR Statements
- Nexus privacy policy
- Smart ID Digital Access component

Links

- EU: General Data Protection Regulation

Only the user ID of an employee will be found in log files. Therefore there is no traceability to the origin personal information if these were removed from Smart ID Digital Access. Log files will be deleted automatically due to rotation.

Important notice

A major part of GDPR is about internal routines. Organizations are responsible for personal data, regardless of whether it is a HR system, CRM system, security system, PACS system, real estate system or other. Each organization must ensure that staff handle personal data properly. This includes, among other things, having a legal basis for processing personal data, keeping track of the personal data being processed and the context in which to handle only the information necessary for the purpose expressed, deleting data when no longer required, and to inform and, where necessary, obtain consent from registered persons.

Please also observe that the GDPR acknowledges that data protection rights are not absolute and must be balanced proportionately with other rights – including the “freedom to conduct a business”. For more information on the ability of EU member states to introduce exemptions, see the section on derogations and special conditions.

As a regulation, the GDPR will be directly effective in EU member states without the need for implementing legislation. However, on numerous occasions, the GDPR does allow member states to legislate on data protection matters. This includes occasions where the processing of personal data is required to comply with a legal obligation, relates to a public interest task or is carried out by a body with official authority. Numerous articles also state that their provisions may be further specified or restricted by member state law. Processing of employee data is another significant area where member states may take divergent approaches. Organizations working in sectors where special rules often apply, for example health and financial services, should: (1) consider if they would benefit from such special rules, which would particularize or liberalize the GDPR; and (2) advocate these accordingly. They should also watch for member states seeking to introduce special rules, which may prove restrictive or inconsistent across member states.