Accelerate your GDPR readiness

IAM a core building block for GDPR compliance

Use case

Identity and access management (IAM) is key to enabling organizations to become compliant with the GDPR, increase security and improve operational efficiency. For organisations that want to comply with GDPR, strict access controls and meticulously tracked access to data must be enforced. Security researchers point out that almost all types of cyber attacks nowadays involve privileged accounts.

Nokia NetGuard Identity Access Manager (IAM) provides unified identity access control, single sign-on with centralized policy management, address regulatory audit compliance and simplify user access.
IAM consists of tools and practices that keep an organization safe from accidental or deliberate misuse of access. A IAM offers a secure, streamlined way to authorize and monitor all privileged users for all relevant systems:

- Grant privileges to users only for systems on which they are authorized
- Grant access only when needed and revoke access when the need expires
- Avoid the need for privileged users to have or need local/direct system passwords
- Centrally and quickly manage access over a disparate set of heterogeneous systems
- Create an unalterable audit trail for any privileged operation

These capabilities give Nokia´s IAM the ability to facilitate many aspects of GDPR compliance. They also make it easier to document compliance than would be possible with ad-hoc management of privileged users. IAM provides the basis for a streamlined internal audit for GDPR compliance. NetGuard IAM can show, for example, which roles in an organization are allowed to modify, enter, copy or delete data. A typical GDPR risk might involve having a privileged user in an EU country whose access logs are not transparent. This user might, with the best of intentions, create a violation of GDPR rules. Without a pervasive privileged access management solution, that user has generated a potentially costly risk.

**GDPR use-cases**

**Central Password Management**
- Automate and centrally manage passwords across all physical or virtual network functions.
- Enforcement of password policies

**GDPR compliance logging**
- Centrally log and review activity of users and processes; supports video logging.

**Simplify user access, improve user experience**
- Removes the limitation of shared user accounts for legacy infrastructure.

**Enforcement of access controls**
- Harmonizes security access controls company wide
- Access control rights matching to each role
GDPR match

Related to the ENISA document “Guidelines for SMEs on the security of personal data processing” which shall help companies to prepare for GDPR we show below the match of Nokia NetGuard Identity Access Manager. We will focus on the Section 4.2 “Access Control and Authentication” only.

Access control and authentication are basic security measures for the protection against unauthorized access to the IT system used for the processing of personal data. They implement the access control policy of the organization (see Section 4.1.1.3) by technically enforcing it into specific components and applications:

<table>
<thead>
<tr>
<th>Controls</th>
<th>Description</th>
<th>NetGuard IAM</th>
</tr>
</thead>
<tbody>
<tr>
<td>K.1</td>
<td>An access control system applicable to all users accessing the IT system should be implemented. The system should allow creating, approving, reviewing and deleting user accounts.</td>
<td>IAM fulfills all these functions for administrators, architects, engineers, subcontractors,...</td>
</tr>
<tr>
<td>K.2</td>
<td>The use of common user accounts should be avoided. In cases where this is necessary, it should be ensured that all users of the common account have the same roles and responsibilities.</td>
<td>IAM is fully compliant</td>
</tr>
<tr>
<td>K.3</td>
<td>An authentication mechanism should be in place, allowing access to the IT system (based on the access control policy and system). As a minimum username/password combination should be used. Passwords should respect a certain (configurable) level of complexity.</td>
<td>IAM can verify the password complexity as well as automatically update/change them frequently</td>
</tr>
<tr>
<td>K.4</td>
<td>The access control system should have the ability to detect and not allow the usage of passwords that don’t respect a certain (configurable) level of complexity.</td>
<td>IAM is fully compliant</td>
</tr>
<tr>
<td>K.5</td>
<td>A specific password policy should be defined and documented. The policy should include at least password length, complexity, validity period, as well as number of acceptable unsuccessful login attempts.</td>
<td>IAM can enforce any password policy to the connected elements</td>
</tr>
<tr>
<td>K.6</td>
<td>User passwords must be stored in a “hashed” form.</td>
<td>IAM is fully compliant</td>
</tr>
<tr>
<td>K.7</td>
<td>Two-factor authentication should preferably be used for accessing systems that process personal data. The authentication factors could be passwords, security tokens, USB sticks with a secret token, biometrics etc.</td>
<td></td>
</tr>
<tr>
<td>K.8</td>
<td>Device authentication should be used to guarantee that the processing of personal data is performed only through specific resources in the network.</td>
<td></td>
</tr>
</tbody>
</table>

Related to ISO 27001:2013 - A.9 Access control
Protecting today’s and tomorrow’s networks

NetGuard IAM protects physical and virtual network assets, while providing ubiquitous Identity Access Management to infrastructure, resources, and systems for traditional, virtualized and Software Defined Networks (SDN).

NetGuard IAM is designed for critical communication networks and incorporates Nokia’s 30+ years of experience in helping utilities build operational communications networks.