GDPR statement for Nexus GO PDF Signing

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 will begin on May 25, 2018. We will continuously review the functionality of Nexus GO PDF Signing in terms of GDPR.

Implemented functionality

The following functionality is implemented in Nexus GO PDF Signing, to help you to be compliant with GDPR:

Traceability

In Nexus GO PDF Signing, we log customer's and user's successful and failed logins. The log data is saved maximum 30 days. Data about signature requests that have been performed, is also logged. This data is saved maximum 1 year.

Availability

In Nexus GO PDF Signing, everyone has their own login, and access to personal data and documents is restricted to the users of the same account, or even to the user, depending on the type of request.

To gain access to the signing portal, you and your company need to be a Nexus GO customer. By a procedure in the portal, additional users are invited using a secure two-factor method. Users to sign documents may also be invited in individual signature requests. Such users can only access the documents they have been invited to sign, and the names and related data of other users that have been invited to sign the same document.

Correction

The user who has uploaded a document for a signature request is able to recall it. This means that the request, including the document, is invalidated in the portal and all users are notified. The document is deleted after maximum 30 days.

Security

All Nexus' handling of personal data is strictly confidential and with high data security. We collect only the information that our customers request.

Nexus has implemented a range of technical and organizational measures, such as establishing internal controls and information security practices to protect the data we handle on behalf of the customer. The purpose is to protect our customers' information from accidental or temporary loss, damage or change, unauthorized disclosure or access, or unauthorized destruction.

Removal

Signed documents are removed after 30 days. Data about signing transactions that have been performed, and what users have participated, are saved for a maximum of 1 year. In other cases,

Related information

- GDPR statements
- Nexus GO PDF Signing

Data processing agreement:

- Data processing agreement for Nexus GO PDF Signing

Questions and answers:

- GDPR for Nexus GO PDF Signing - FAQ

Links

- EU: General Data Protection Regulation

the customer can contact Nexus support and ask for personal data to be removed.

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.