Agenda Netadmin GDPR Webinar

→ Netadmin as supplier / product

→ Our work with GDPR

→ How you ensure GDPR compliance in Netadmin

→ How personal data is handled

→ Our Netadmin GDPR Compliance offer

→ Next steps

→ Appendix – Best Practices

Our work with GDPR

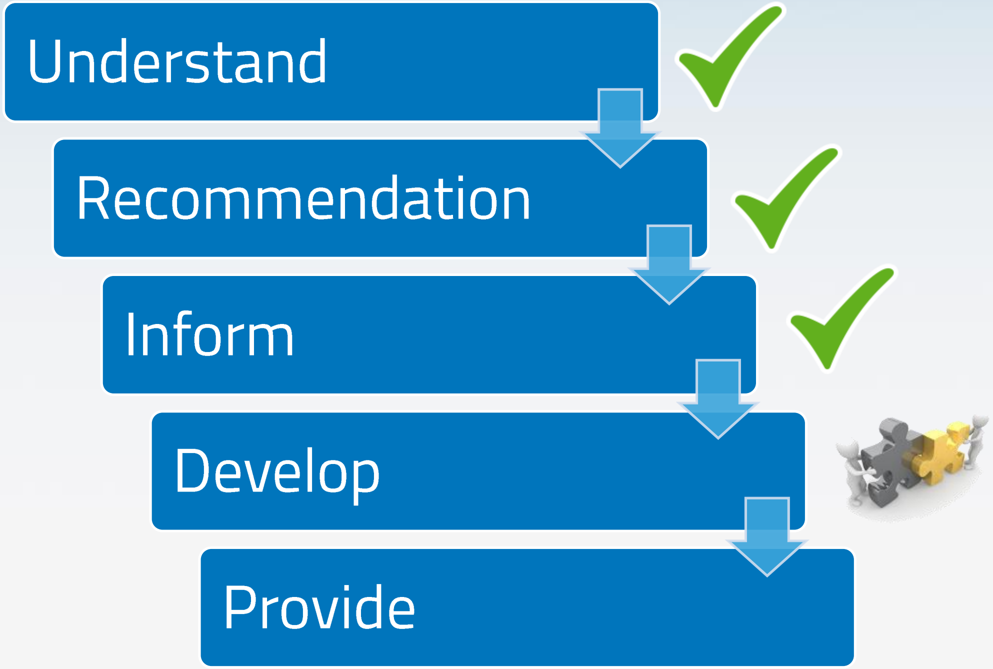
→ **Understand** how GDPR affects our customers in relation to the Netadmin system - policies, routines, usage

→ Make a **recommendation** of how you can be compliant with GDPR through a combination of best practices, system functionality and system analysis

→ **Inform** our customers how GDPR affects their use of Netadmin and how we as a supplier support them in complying with the regulation

→ **Develop** and **provide** necessary compliance offering with system functionality and associated services (analysis, implementation, verification)

→ **"Privacy by design"** approach in future product development



Understand ✓

Recommendation ✓

Inform ✓

Develop

Provide

Step 1 (Analysis) – Book now!
Step 2 (Measures & Verification) - April 2018

How you ensure GDPR compliance in Netadmin

→ ***Article 7:*** Conditions for consent

- → The requirement is fulfilled by registering in Netadmin when Customer has given or withdrawn his consent. This can be done through API, customer import, directly in the GUI and via the Netadmin customer portal.

→ ***Article 15:*** Right of access by the data subject

- → The requirement is fulfilled et by using the default search function in Netadmin. Access the corresponding customer in Netadmin and retrieving stored personal information either by copying or exporting. Mask / remove any third party data (personal data derived from a person other than the one requesting an extract).

→ ***Article 16:*** Right to rectification

- → The requirement is fulfilled by changing the personal data stored on the customer object.

→ ***Article 17:*** Right to erasure ('right to be forgotten')

- → For customers, the requirement is fulfilled by deleting the customer object. The GDPR Compliance Add-on will anonymize customer personal data in the customer history after reaching the configurable life span, clear logs referring to the customer as well as anonymize tickets related to the customer.
- → For alert and system users, the requirement is fulfilled by manually deleting the required data as needed.
- → Please see the slide "How personal data is handled" for detailed information about how personal data should be handled in Netadmin and how it is removed / anonymized.

netadmin
Enabling Growth

How you ensure GDPR compliance in Netadmin

- ***Article 19:*** Notification obligation regarding rectification or erasure of personal data or restriction of processing
  - The requirement is fulfilled by the fact that, in cases where Netadmin automatically forwards personal information, it also notifies the receiving party of corrections and deletions. This is handled within the framework of GDPR Compliance Services.
- ***Article 20:*** Right to data portability
  - This requirement is fulfilled by exporting a customer's personal data through Excel export, which meets the requirement for machine-readable electronic format.
- ***Article 25:*** Data protection by design and by default
  - The requirement is fulfilled by not storing personal data more than is required and following Netadmin's GDPR best practices, specifically regarding system security and user authentication.

How personal data is handled

- Tickets
  - Only store personal data in cases related to corresponding customer objects
  - Anonymized in connection with customer thinning
- Messages
  - Only store personal data in the sender and recipient fields
  - Erased periodically (configurable life span)
- Alert users
  - Only store personal data in the usernames and recipient addresses fields
  - Not erased automatically, needs to be manually deleted if necessary
- Alerts
  - Created by the system and may contain personal data
  - Erased periodically (configurable life span)
- Sites
  - Only store personal information in the site owner and contact information fields
  - Not erased automatically, needs to be manually deleted if necessary
- Customers
  - Only store personal information in the names, social security, billing and contact information fields
  - Erased either manually or through the automatic thinning functions for inactive customers
  - Customer history is periodically anonymized (configurable life span)
- System log
  - Created by the system and may contain personal data
  - Erased periodically (configurable life span)
- System users
  - Only store personal information in the names and contact information fields (phone number, email address, fax)
  - Not erased automatically, needs to be manually deleted if necessary
- Service providers
  - Only store personal information in the contact details fields (phone number, email address, contact person)
  - Not erased automatically, needs to be manually deleted if necessary

Our Netadmin GDPR Compliance offer

Step 1, Analysis

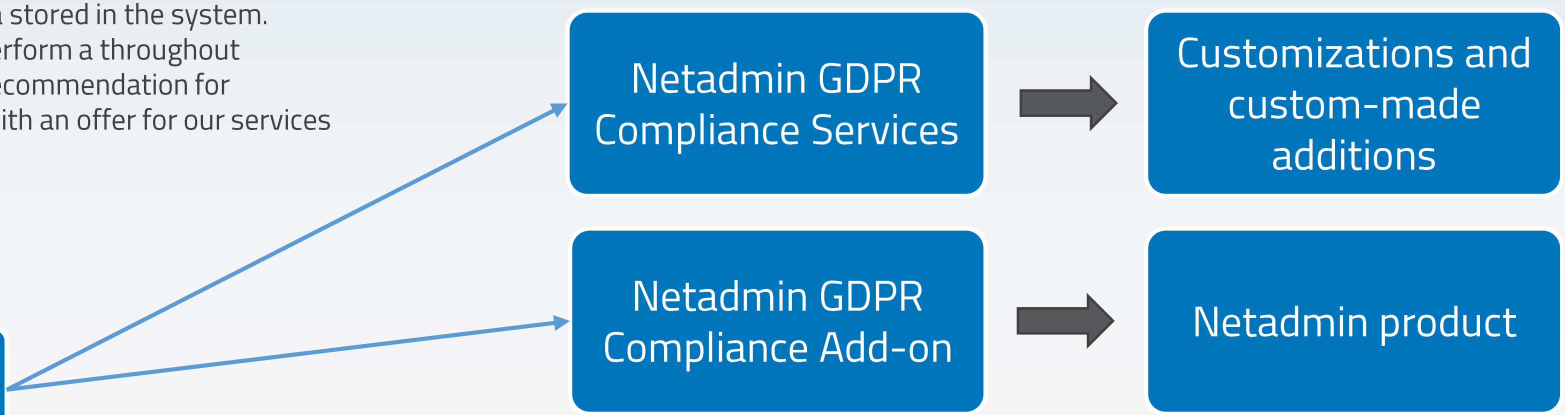
Initial 2-hour web conference to get a clear picture of your Netadmin installation and use of Netadmin, such as customizations, integrations, and data stored in the system. After that, we log into your system, perform a throughout system analysis, and then provide a recommendation for necessary measures in combination with an offer for our services / efforts.

Price: 1.000€

Step 2, Measures & Verification

We carry out measures and verification with scope and division of labor as agreed. Here we install Netadmin GDPR Compliance Add-on.

Price: An offer is made during the analysis

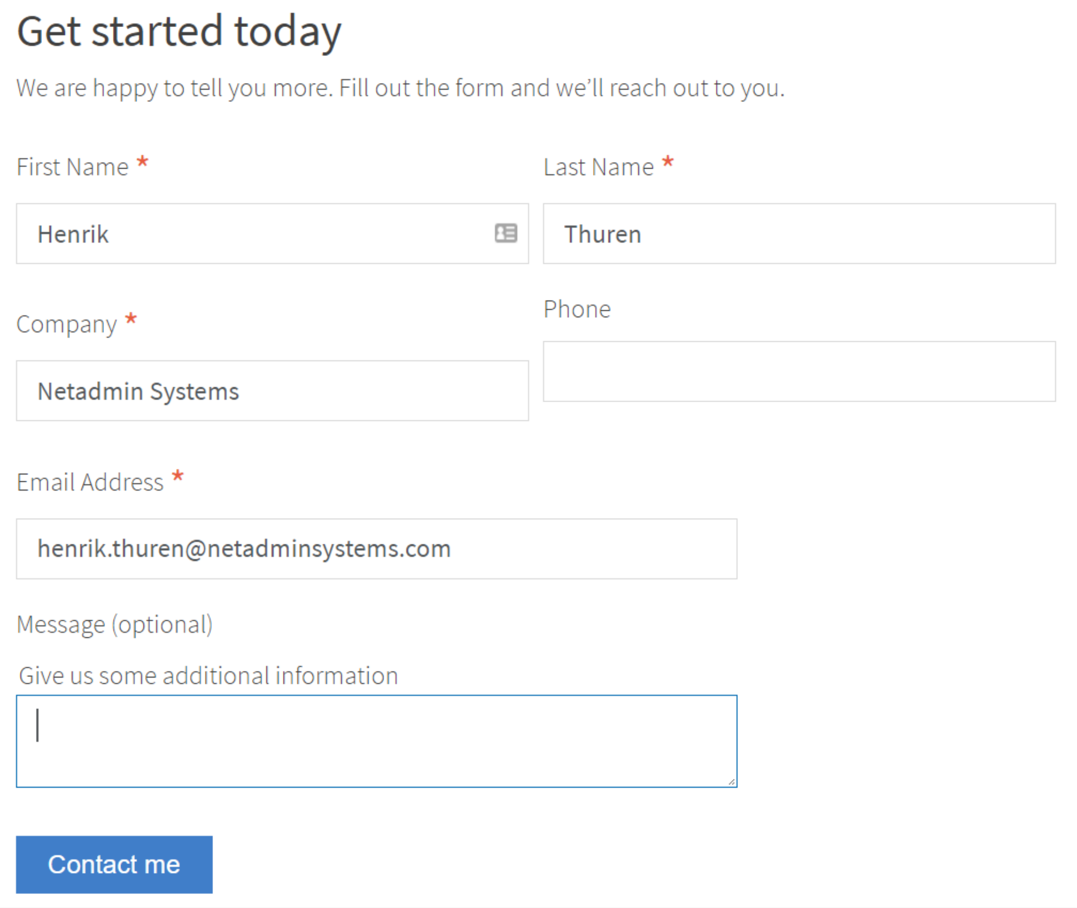

Netadmin GDPR Compliance Services
Customizations and custom-made additions
Netadmin GDPR Compliance Add-on
Netadmin product

- Management of consent
- Automated erasure and anonymization of personal data

Next steps

- → Step 1 – Analysis (can be ordered and delivered immediately)
- → Step 2 – Measures and verification (can be ordered after completion of analysis)
  - → GDPR handling of any customizations and additions can be delivered immediately
  - → GDPR Compliance Add-on will be delivered from April
- → Delivery related questions – Fredrik Holmberg, fredrik.holmberg@netadminsystems.com
- → Product related questions – Henrik Thurén, henrik.thuren@netadminsystems.com

http://www.netadminsystems.com/solutions/gdpr



Get started today

We are happy to tell you more. Fill out the form and we'll reach out to you.

First Name * Henrik

Last Name * Thuren

Company * Netadmin Systems

Phone

Email Address * henrik.thuren@netadminsystems.com

Message (optional)

Give us some additional information

Appendix – Best Practices

System security

- In order to avoid data breaches, it is recommended to following strict IT security policies and procedures. In addition to any existing internal IT security policy the following is a list of recommended measures:
- The servers on which Netadmin is installed should be secured in terms of both physical and network access
- The operating systems running on the servers should be continuously updated with security patches etc.
- System user password should consist of at least 8 characters including both lower case letters, upper case letters, digits and special characters
- System user password should be changed regularly (at least annually)
- The Netadmin ACL authorization framework should be configured and applied to ensure that users have appropriate access
- Inactive system users which no longer need access should be removed
- Valid SSL certificates for web portals and services

Managing customer consent

- Consent should be documented in the system which is the master of customer data unless a specific system is used to manage consent. If Netadmin is the master system for customer data, it is recommended to document consent in Netadmin. If not, it is recommended that consent is registered in another system and any necessary handling including erasure of personal data is initiated by that system.

Managing personal data in multiple systems

- Erasure of personal data should be initiated from the system which is the master of customer data. Such an erasure procedure should be propagated to all systems which contain personal data and completion of the propagated request should be ensured by the master system.

Data maintenance

- Erasure of personal data should not take longer than 180 days from the point when there is no long a lawful basis to process it. It is therefore not recommended that backups of Netadmin data is contain data older than 180 days in order to avoid unnecessary work of removing data from backups.
- According to GDPR personal data should only be stored and handled under certain circumstances, for example if you have an agreement with a customer which requires you to handle their personal data. In the case that a broadband customer has cancelled his or her services it is advised that the following standard Netadmin features are utilized:
- Automatic removal of inactive customers with no services
- Automatic removal of inactive customers which have disconnected all of their previous services

Development and testing systems

- Non-production Netadmin deployments should preferably not contain any personal data of real customers. Both because it is not needed to but also because it can make erasure of personal data more complicated and costly. In the case that personal data exists in such systems you should make sure that it is resynched with the production system or purged within 180 days.