

What you need to know about the GDPR when collecting feedback in Europe

Key Points of the General Data Protection Regulation (GDPR)

- New data protection laws for organisations that handle personal data within EU and EEA countries.
- GDPR will replace current data protection laws starting the 25th of May 2018.
- GDPR restricts how organisations can collect, store, and process personal data.
- GDPR aims to give each individual full control of how his/her personal data is handled.
- GDPR provides clear regulations regarding transparency connected to processing personal data.
- Strict sanctions for organisations that does not comply.



How Does the GDPR Affect Feedback Collection?

- Collecting and assessing feedback from individuals is a way of processing personal data under the GDPR.
- According to GDPR, the organisation that collects the feedback and determines the purpose of processing is the "Controller".
- GDPR requires that a Controller process personal data in accordance with its rules and principles.
- According to GDPR, a supplier that processes personal data on behalf of the Controller assumes the role as "Processor".
- A Controller that wants to use a Processor (for example Netigate) for their feedback collection, needs to ensure that the processor is compliant with GDPR.
- A Controller that wants to use a Processor for gathering feedback processes and procedures must enter into a Data Processing Agreement (DPA) with the Processor. Netigate has this mandatory DPA available for its customers.



PERSONAL DATA PROCESSING WHO IS WHO IN THE GDPR

The Respondent is the

DATA SUBJECT

Respondent provides input into the survey, and must provide the Controller consent for processing.

As a customer of Netigate you are the

CONTROLLER

The Controller must receive legal consent (typically consent or a contractual relationship) for processing personal data. The Controller defines the purpose as well as the data lifecycle and retention time. The Controller is always in full control of the data. The Controller is the contact point for the Data Subject.

Netigate is the

PROCESSOR

Netigate provides the software tool used by the Controller. The tool includes functionalities that allow customers to fulfill the requirements and principles in accordance with the GDPR. Netigate performs support and services. Netigate provides the required security measures. Data Processing Agreement (DPA) in place with Customer.

Netigate's hosting provider is the


SUB-PROCESSOR

Netigate uses certified hosting providers across a range of data centers to meet the highest security requirements. To ensure data confidentiality, integrity, and accessibility, Netigate takes the necessary and relevant technical and organisational security measures. Data Processing Agreement (DPA) in place with Netigate.

Other Netigate entities may be

SUB-PROCESSORS

Support and services may be provided by other entities within Netigate.



Netigate and the GDPR – be on the Safe Side With us

A business with a problem that needs a solution Collecting and assessing feedback from your customers, employees or other individuals within the EU and EEA countries is considered processing personal data. Therefore, it is your responsibility to comply with GDPR as well as document your compliance. As a customer of Netigate you're on the safe side.

GDPR Focus

One of Netigate's highest priorities is and has always been data security. Netigate's focus to comply with GDPR began in April 2016, when EU executed the new legal framework. As a result, Netigate assembled a dedicated GDPR team with the CEO as well as representatives from each department to ensure that every part of the company is compliant.

Located in Europe

Netigate's headquarters are located in Stockholm, Sweden. Netigate only uses EU-based servers to ensure data protection and security. Netigate offers server locations in Germany and Sweden for our customers. Netigate only utilises certified data centers according to the international information security standard, ISO 27001.

Security of Highest Standard

Netigate continues to be the first and safest choice for data security. Netigate strictly follows German security requirements since Germany maintains the highest security standards in Europe. Netigate has several action points in place that aligns with GDPR, which include the following:

- Maintain confidentiality with access control measures for systems and data
- Secured integrity by encrypted data transfers
- Availability is ensured by regular data and storage backups and disaster recovery plans
- Customer data is logically separated for each customer to ensure confidentiality and integrity
- Continuous penetration tests conducted by external third-party security providers
- Notification of data breach

Privacy and Consent

Netigate has implemented strategies and functions compliant with GDPR's guidelines by respecting individuals' rights to control their personal data. This is one reason why Netigate requires personal consent. As a Netigate customer (the Controller), you will always have:

- Full control of your data while using the Netigate platform. This can be accessed through the account settings. Users have the option to permanently remove all data associated with a particular Netigate account at any time.
- There are several privacy settings available, such as set data retention policies, automatic anonymising or the immediate removal of all personal data.
- There is an editable consent collection functionality available for surveys.

Detailed Documentation - for Your and our Safety

GDPR has strict requirements regarding processing documentation. The Controller is responsible for collecting documentation from the Processor. As a Netigate customer, you will have access to required documentation regarding the processing of personal data in the Netigate platform.

Employee Confidentiality

All Netigate employees operate and must abide by non-disclosure agreements. Netigate employees are also subject to privacy training and awareness. All Customer data is considered confidential. Internal access is restricted and is only granted on a need-to-know basis. Employees are not permitted to enter customer accounts or surveys without explicit approval. Our Netigate employees know how to protect your integrity.

Legal Terms

A mandatory GDPR compliant Data Processing Agreement available (if personal data is processed).

Read more on GDPR and Netigate's work on privacy at netigate.net/privacy