NICE Satmetrix

NICE Satmetrix and the GDPR

Easy Controls and Security by Design Help Companies Comply with Data Privacy Regulations

What Is the GDPR?

The General Data Protection Regulation (GDPR) has been called the most important change for data privacy protection in years. Taking effect May 25, 2018 across the European Union (EU), GDPR replaces and consolidates existing data protection regulation by introducing several new requirements that strengthen control over an individual's personal data. It also introduces significantly higher penalties for non-compliance.

Who's Affected?

Almost every company needs to pay attention to the GDPR. The regulations apply directly to companies located in the EU and extends to all companies that do business in the EU or have customers with EU citizenship. That means every business could be subject to the requirements if they handle interactions with EU residents or citizens, no matter where the business or citizen is based and regardless of whether the business has a physical presence in the EU. The specific impact that the GDPR will have on a business will vary depending on a number of factors. Some of the most important are covered below.

GDPR and NICE Satmetrix Customers

NICE Satmetrix has long served the EU market and has always taken a proactive stance with respect to complying with EU privacy laws and supporting our customers with strong personal data protections. We are committed to continuing that support and vigilance, including responding to all individual needs under the GDPR and maintaining full compliance with the regulation. We've made compliance easy within our software, NICE Satmetrix NPX.

Four Facts You Should Know About the GDPR

1. If You Do Business Online, You're Probably Subject to the Regulations.

While the GDPR applies directly to companies located in the EU, it can extend any business that has interactions with EU residents.

2. Non-Compliance Can Get Very Expensive.

Fines for non-compliance can cost up to 4% of annual global turnover (or gross revenues) or €20M, whichever is greater.

3. The GDPR Does NOT Require Your Servers to be Located in the EU or the Data Subject's Home Country.

The GDPR debunks one of the most prevalent myths about EU privacy regulations. The regulations don't care where your servers are located, as long they're secure and take every measure to protect individuals' PII.

4. Your Verbatim Comment Fields May Put You at Risk.

While NICE Satmetrix does not intentionally capture personal data beyond what companies provide to us for survey administration, we have no control over what respondents enter into open text comment fields, and it is not uncommon for them to submit personal information about themselves or their accounts as part of their commentary. We recommend you speak to your NICE Satmetrix team about strategies you can deploy to minimize the risk.

Customer Rights Granted by the GDPR

The countries of the EU have always taken a proactive approach to individual privacy, and many of the protections codified by the new regulation have been in effect for years in one form or another throughout the region. With the GDPR, the protections will be strengthened and applied consistently throughout the EU, so regardless of where a customer lives, they will have the same confidence that their personal data will be secured regardless of where they live or go online.

Essentially, the GDPR is a Bill of Rights for the internet age and requires businesses to prioritize the security and protection of Personal Data by extending RIGHTS to individuals in the following eight areas:

Right to Security

Businesses must put in place "technical and organizational measures" to ensure personal data is appropriately secured, including anonymization and encryption and a privileged-based system that limits access to only specifically defined roles.

Right to Data Minimization

The collection and processing of data must be limited to ONLY what is necessary for processing purposes, and personal data should only be stored for as long as the purpose requires. Processes and procedures should also be put in place for the periodic deletion/destruction of personal data no longer needed.

Right to Be Forgotten

GDPR gives individuals the right to have their personal data deleted upon request at any time, and businesses must put in place procedures to accommodate the request without delay and document it for future reference. If deletion is not possible, the software must support a block to prevent future processing of the information.

Right of Rectification

Businesses must give individuals a way to quickly correct inaccurate or incomplete information in their personal data record.

Right to Access

GDPR gives individuals the right to access their personal data and supplemental information (including the legality of its use) about its processing at any time, and businesses must comply by accommodating the request without delay.

Right to Data Portability

Businesses must be able to provide individuals and/or their designated third-party with their personal data upon request and without delay in a structured, easily readable format.

Right of Consent

Data cannot be processed without the individual's explicit consent. Businesses must clearly state the purpose of the processing when requesting consent, retain proof of consent, and provide the individual with a way to remove consent at any time.

Right to Be Notified in the Event of a Breach

Data Processors must notify the Data Controller within 72 hours of a personal data breach occurrence, as well retain a record of the breach for a specified time period.

NICE Satmetrix NPX Software and GDPR Compliance

While NICE Satmetrix cannot make a customer solution GDPR compliant, we do help customers in their efforts to comply with the GDPR. In the following section, we'll look at the GDPR and the rights it grants to individuals within the context of the NICE Satmetrix software and specifically what we've done and are doing to support our customers and remain compliant with the new regulation.

Security by Design

As a data processor, NICE Satmetrix does not collect any personal data itself and so is not subject to the regulations covering data controllers. As part of our service, however, we do store and process the personal data provided by our customers, and thus we have multiple security controls in place to protect every individual's PII from theft and/or unauthorized access. Those include only using Class A data centers with bulletproof physical security and deploying a three-tiered network architecture protected by disk-level data encryption and multi-factor authentication protocols. We also place controlling access to your customers' data entirely in your hands, and allow you to completely lockout NICE Satmetrix staff from gaining access to your data. In addition, NICE Satmetrix participates in the EU-US Privacy Shield, complies with the US-EU and Swiss Safe Harbor framework, and regularly performs audits to meet the security and privacy standards of the global industry and governmental organizations that regulate our business.

Data Minimization

NICE Satmetrix encourages its customers to provide only the minimum amount of personal data needed to perform our services. We also have put in place a policy and process that ensures all of a customers' individual personal data is removed (deleted) from the system 30 days after terminating the NICE Satmetrix service.

Personal Data Anonymization

A new GDPR compliance feature for the NPX software gives NICE Satmetrix customers the ability to anonymize or delete all their personal data stored on the system. With the simple controls, program administrators can create aging rules to anonymize selected data in bulk after a specific time period or use the import function to upload individual contacts to be deleted or anonymized.

Agile Controls for Rectification, Access, and Portability

NPX is built for hands-on use and provides program administrators with all they tools they need to schedule or manually export data in multiple formats to any individual or destination. The simple admin controls also make it easy to edit or update any individual's contact data on demand.

Consent Management

As NICE Satmetrix does not collect the personal data, securing consent is the responsibility of our customers and must be obtained prior to porting the data to NPX. If needed, NICE Satmetrix could assist with obtaining and documenting consent. For example, the form feature could be used to obtain consent. Then, integration with your CRM could track that consent and demonstrate compliance.

Breach Response Team

NICE Satmetrix has an established breach notification process in place with its hosting partners – Rackspace and AWS. If a personal data breach were to occur, the host would immediately notify the internal team at NICE Satmetrix responsible for investigating and managing data breaches. That team would investigate the breach, identify the individuals and accounts affected, and then notify the customers within 72 hours as stipulated by the regulation.

What's Next

The GDPR is complex and businesses should dedicate time to understand their specific requirements and prepare for compliance. The requirements for each business will be unique and should be determined by consulting with lawyers or other GDPR experts to understand which specific GDPR requirements apply and what needs to be done to address them.

Glossary -- The Key Terms of the GDPR

The GDPR introduces terminology and concepts that may be new to some businesses. To help guide you through the new regulation and its requirements, we've included the following glossary of the key terms you should understand and take note of.

Data Subject

An individual who is the subject of Personal Data.

Personal Data

Any information related to the Data Subject that can be used to directly or indirectly identify the person (e.g. name, photo, online identifiers, location, political opinions, ethnic origin and more).

Data Processing

Any operation that is performed on Personal Data (e.g. recording, profiling, structuring, storage).

Data Controller

Entity (bank, internet company, etc.) that collects the Personal Data and determines the purposes and means of its processing.

Data Processor

Entity (e.g. IT outsourcer, marketing vendor, etc.) that processes Personal Data on behalf of the Data Controller.

Data Protection Officer (DPO)

The individual employee at the Data Controller or Data Processor responsible under Article 39 of the GDPR for ensuring compliance with the new regulation.

Pseudonymisation

Processing of Personal Data in such a manner that it can no longer be attributed to a specific Data Subject.

Opt-in Consent

A higher threshold that requires the Data Controller to obtain an unambiguous affirmative action, such as the tick of a clearly marked box, agreeing to consent before collecting Personal Data. Banks for instance, or operators, will no longer be able to rely on a customer failing to untick a box in order to collect and keep their data.

NICE Satmetrix

INTERNATIONAL +44(0) 845.371.1040 | NORTH AMERICA 888.800.2313
sales@satmetrix.com | www.satmetrix.com