GDPR Compliance with NICE

The EU's General Data Protection Regulation (GDPR) is to be enforced by 25 of May 2018 at which time the organizations that are not compliant will face heavy fines, of up to 4% of their annual turnover – or 20 million EUR - whichever is greater. The aim of the regulation is to protect EU citizens' data and privacy. This will bring tremendous change to the way organizations record, archive and process their data.

What are the main changes brought by the GDPR?

The GDPR sets a list of key principles which all define requirements for better data governance. While not all of them are prescriptive, they encourage organizations to move away from the "tick the box" paradigm in which they practiced compliance, to make privacy a central guiding principle.

Privacy by Design

Each new service or business process that makes use of personal data must take its protection into consideration. Indeed, an organization needs to be able to show that it has adequate procedures in place and that compliance is regularly monitored. Furthermore, "Privacy by design" requires that the system and policies in place be proactive – in the sense that they should be able to detect violations, and that the strictest privacy settings be applicable by default. "Privacy by design" also requires strict security settings in which the private data is encrypted and/or uses pseudonyms.

Right to be forgotten

Also known as "Data Erasure", the right to be forgotten entitles customers to have their personal data erased, and to cease further dissemination. It is important to note the definition given to personal data in the GDPR encompasses any information relating to an identified or identifiable natural person: a name, an identification number, location data, online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. For organizations regularly processing exabytes of data regularly, the challenge is almost similar to finding a needle in the haystack. In order to be able to identify, retrieve and delete such granular information in a reasonable timeframe, organizations must tag interactions and data in ways that enable them to comply with the right to be forgotten and the right to access, described below.

Right to access

Your customers have the right to request and obtain information so as to whether or not personal data concerning them is being processed, where and for what purpose: whether to improve quality, business processes or even for compliance purposes. Further, your organization should be able to provide a copy of the personal data, free of charge, in an electronic format. In this respect, the regulation also requires for a thorough data trail to be followed so as to understand and communicate upon what is done with the data concerned at any given time, making it paramount for organizations to be able to understand and communicate their data practices.

Opt-in data processing consent

Data processing consent should be freely given, specific, and withdrawable. Meaning that customers should be made aware of any types of processing foreseen with their personal data, and must be able to withdraw their consent, and require that their data be erased, at any given time.

Personal data breach notification

Personal data breach notification is mandatory in within 72 hours of first having become aware of the breach. Organizations must inform the supervisory authority as well as the affected customers whose personal data's security may have been compromised. Under the GDPR, this includes "the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."

Global applicability

GDPR is applicable even if your organization is not in the EU. As long as an organization processes EU citizens' data, it should abide by the text of the regulation.

With NICE's Compliance Center, GDPR is easy!

A Unique End-to-End Compliance Solution

The Compliance Center is a unique end-to-end compliance solution for contact centers, bringing together the abilities to visualize data, take action on policies, and bridge siloes between data systems to efficiently manage interactions and policies. With the Compliance Center, users obtain actionable intelligence on their GDPR related activities and can directly take proactive or corrective actions to ensure that their practices are aligned with the principles of the regulation.

The Compliance Center offers an innovative "Compliance Assurance" application displaying multiple dashboards to gauge the adherence of the organization to the best data governance practices for capture and retention. Whether organizations need to verify that all data concerned is adequately encrypted, prevent breaches by detecting abnormal behavior, verify that consent has been recorded and is discoverable, or track the quantity and the quality of the data stored, the Compliance Center delivers a tailored solution.

Indeed, by applying thresholds onto the aggregated data, users can specifically focus on the policies and campaigns that include or process private data and effectively monitor these activities so as to detect vulnerabilities or accommodate the requests of their customers to delete their data or obtain a copy of the latter. With the "Policy Manager" application, which centralizes all retention policies and comprises mission-critical mechanisms to manage the data archived, authorized users can take direct action and dramatically reduce the time needed to detect breaches or delete/extract specific interactions.

Simplifying GDPR Compliance

To accommodate requests to exercise the Right to Be Forgotten, the Compliance Center makes use of advanced data tagging which can retrieve the data associated with any customer ID. It also comprises dedicated workflows for authorized users to perform deletions and/or extractions without the need for 3rd party or professional services. As such, these actions are performed promptly and in strict adherence with the organizations procedures for policy enforcement.

Based on the market leading Engage platform, the Compliance Center provides an end-to-end media encryption approach protecting information during every stage of its lifecycle: capture, use, transmission, and storage. Encryption can also be performed on historical interactions, as a corrective measure.

Overall the Compliance Center offers a single solution for GDPR compliance and a wealth of features and applications that address the needs of all stakeholders in the Call Center – IT, agents, and compliance, in order to power the adoption of a "compliance by design" approach without creating additional overheads.

Contact us today to hear more about how NICE can help you comply with GDPR, or visit us here to schedule a Compliance Center demo

About NICE

NICE (Nasdaq: NICE) is the worldwide leading provider of both cloud and on-premise enterprise software solutions that empower organizations to make smarter decisions based on advanced analytics of structured and unstructured data. NICE helps organizations of all sizes deliver better customer service, ensure compliance, combat fraud and safeguard citizens.
Over 22,000 organizations in more than 150 countries, including over 80 of the Fortune 100 companies, are using NICE solutions.

www.nice.com