Verint Community in the Age of GDPR

Verint.com

Twitter.com/verint

Facebook.com/verint

Blog.verint.com

VERINT.

Verint Community in the Age of GDPR

The General Data Protection Regulation (GDPR) takes effect in May 2018, matching fragmented data protection laws across the EU, expanding individuals' rights and increasing privacy obligations. With fines of up to €20 million or 4% of global revenue for non-compliance (whichever is greater) – now is the time for action. Verint's Community enables you to balance GDPR compliance with the continued collection of customer data to execute your customer community strategy.

What is the GDPR?

The GDPR has been introduced by the European Commission to strengthen and unify data protection for individuals within the European Union (EU). The primary objective is to give back citizens control of their personal data and simplify the regulatory environment for international business.

The GDPR will come into effect on 25 May 2018, and all companies and government organisations that offer goods and services to individuals within the EU are subject to the new legislation. The regulation also applies to any organisation based inside or outside of the EU that collects and analyses personal data related to EU residents.

What are the main requirements for GDPR compliance?

All organisations need to implement measures to ensure that customers and/or employees personal data is collected and processed according to the GDPR principles. These measures include:

- **New employee and customer or "individual" rights:** The GDPR demands increased transparency.
    - For example: Users have the ability to request the erasure of data from controllers (the 'right to be forgotten'), the correction of errors, and the right to access data in structured formats so they can switch controllers. If a data breach occurs, users also need to be notified within a critical time period.
- **New data protection requirements**
    - Organisations will need to put data protection at the centre of their information processes, including encrypting an individual's data and the execution of data protection impact assessments – in some cases administered by a data protection officer.
- **New technology strategy**
    - Organisations will need to document and report on where their data is, how it is collected, how it is stored and who can access it.

What steps should I take to help ensure compliance?

To achieve sustainable GDPR compliance, organisations can use this six-step process:

1. **Educate your organisation**

   Senior management needs to be behind the delivery of GDPR compliance. Concise briefing to senior management enforces the company's aspiration to pursue best practice and provides a platform for compliance and growth.

2. **Appoint a Data Protection Officer**

   Most organisations will require a DPO who will provide support and a single point of contact related to all matters of data protection and information security best practices.

3. **Update the way you collect data**

   Examine the data you collect from customers and employees, and where it is stored. The 'right to be forgotten' remit, for example, demands a process for erasing customer data upon request. A privacy process will also be required to allow customers to 'opt in' to having their data stored – right now they currently default to an 'opt out' position.

4. **Mitigate potential data breaches**

   Implement a cyber-security incident response and data encryption plan that both protects against breaches and adheres to the GDPR requirement to notify impacted subjects and the regulator within 72 hours.

5. **Determine your GDPR risk**

   Personal data is data that could potentially identify a specific individual. GDPR demands that personal data is subject to integrity and confidentiality measures appropriate to the nature of the personal data and the harm which could arise to the individuals to which the personal data relates should there be unauthorised access, disclosure or processing of that data. It is therefore necessary that you understand what personal data you have within your organisation, where it is located, why it is collected and processed and who has access to it.

6. **Validate your compliance**

   You need to quickly and easily demonstrate the steps taken towards meeting GDPR requirements. Establish the appropriate protective measures through appropriate organisational and technical measures and ensure you have in place audit and reporting capabilities needed to respond to compliance requests from your customers and supervisory authorities.

Why Verint?

Verint's **Community** empowers your organisation to manage the Communities you have deployed associated with implementing your GDPR policy, from tracking and managing GDPR-regulated customer SLA requirements to flagging a customer who has invoked the 'right to be forgotten' and everything in between. And Verint's **Community Product** incorporates complete, unified data 'privacy by design' best practices in support of the GDPR data protection regulations. These include only creating, capturing and storing data that is required for business processing, strictly limiting access to sensitive information within the system to suitably authenticated users**. Verint Community allows organizations to not store any customer information within the system itself, and rather to retrieve the information in real time from external systems.**

Finally, Verint's professional services team can help you strategise how to continue collecting business-critical personal data without running afoul of the GDPR.

Contact Verint to learn more about how Verint's Community supports your GDPR compliance needs.

And now for the small print

This document is not a substitute for seeking professional advice or services from legal counsel and other professional advisors, nor should it be used as a basis for any decision or action that may affect the recipient's or reader's business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor as it relates to your specific circumstances.

Not all features described in this document will be present as is and may require configuration services engagement provided by Verint or a Verint approved partner. Please speak with your Verint representative for more information.

All users of Verint solutions must be satisfied that the implementation is compliant with the laws of the relevant jurisdiction in which the solution operates. This applies irrespective of whether the Verint solution is hosted by Verint or installed in operator's own computer facility.

Unauthorized use, duplication, or modification of this document in whole or in part without the written consent of Verint Systems Inc. is strictly prohibited. By providing this document, Verint Systems Inc or its affiliates do not make any representations regarding the correctness or completeness of its contents and reserve the right to alter this document at any time without notice. Features listed in this document are subject to change. Please contact Verint for current product features and specifications.

All marks referenced herein with the ® or TM symbol are registered trademarks or trademarks of Verint Systems Inc. or its subsidiaries. All rights reserved. All other marks are trademarks of their respective owners.

Verint. Powering Actionable Intelligence.®

Verint® is a global leader in Actionable Intelligence® solutions with a focus on customer engagement optimization, security intelligence, and fraud, risk and compliance. Today, more than 10,000 organizations in 180 countries—including over 80 percent of the Fortune 100—count on Verint solutions to make more informed, effective, and timely decisions.