Workforce Optimization and Data Privacy Compliance

Data privacy and protection regulations are proliferating and maturing quickly. Governments around the world are protecting customer rights with new and enhanced legislation to provide individuals with personal data security and privacy protection.

The European Union's General Data Protection Regulation (GDPR) is setting the standard by giving people the right to access and control their personal data, and implementing penalties for violations. Similar measures have been introduced in a number of countries, including Canada, China, Japan and Australia.

Now is the time for action. Verint® Workforce Optimization™ solutions can empower you to comply with these measures as you implement your customer engagement strategy.

Why Now?

With at least five such regulations already in place around the globe and more expected, your organization will likely need to address the requirements of multiple regulations and put processes and technology in place to comply. Since there are similarities within the regulations, consider developing a coordinated approach to their requirements, rather than addressing each regulation individually.

What are the common requirements for data privacy compliance?

Many existing and proposed data privacy laws embrace a number of common principles, and organizations will need to implement measures to ensure that personally identifiable data is collected and processed in accordance with them.

They include:

- **New employee and customer or "individual" rights:** These demand increased transparency. For example, individuals can request the erasure of data, the correction of errors, and the right to access data in structured formats. If a data breach occurs, it is a common demand that individuals and regulators be notified within a critical time period.
- **Data usage statements:** Organizations must explicitly state how data they collect will be used. This can range from a statement on the company's website to more complex scenarios in which customer consent must be obtained.
- **New data protection requirements:** Organizations will need to put data protection at the center of their information processes. This may include encryption of an individual's data and the execution of data protection impact assessments — in some cases, administered by a data protection officer.
- **New technology strategy:** Organizations will need to put in place comprehensive measures to ensure compliance is maintained and be prepared to report on where their data is processed and by whom, how and why it is collected, how it is stored, and who can access it.

VERINT®

Executive Perspective

What steps should I take to facilitate compliance?

Each regulation will have its own unique components that must be accounted for in any compliance initiatives — for example, GDPR requires the appointment of a data protection officer. That said, to help achieve sustainable compliance, organizations can consider this five step process:

1. **Determine your risk.**
   Personal data is information that could potentially identify a specific individual. Most regulations demand that personal data is subject to integrity and confidentiality measures. These should be 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 unauthorized access, disclosure, or processing of that data. It is therefore necessary that you understand what personal data you have within your organization, where it is located, why it is collected and processed, and who has access to it.

2. **Educate your organization.**
   Senior management must stand behind the delivery of data privacy compliance. Provide them with a concise briefing that spells out the potential costs and negative impacts of non-compliance, and clearly sets out your organization's aspiration to pursue best practices and provide a platform for compliance and growth.

3. **Update the way you collect data.**
   Examine the data you collect from customers and employees, and where it is stored. Many regulations provide for deletion of customer data upon request, for example, so being able to identify and consolidate data by individual is critical.

4. **Mitigate potential data breaches.**
   Ensure that data is encrypted at rest and in transit to protect it from external threats. Additionally, restrict access internally to only those users who need it to conduct business.

5. **Validate your compliance.**
   You need to quickly and easily demonstrate the steps taken towards meeting the requirements of the regulations you are subject to. Establish the appropriate protective measures through organizational and technical measures, and ensure you have in place audit and reporting capabilities for responding to requests from your customers and supervisory authorities.

Why Verint?

Verint offers a portfolio of workforce optimization solutions — including recording, automated quality management, speech analytics, desktop and process analytics, workforce management, and performance management — that can support your customer engagement efforts by capturing and processing customer and employee personal data. Our unified administrative components incorporate robust, end-to-end data protection and security capabilities that help ensure adherence to data "privacy by design" practices, and our encryption solution helps protect your customer and employee data in the event of breach.

Verint solutions also include configurable capabilities to address the requirement for customer and employee rights of access, rectification, erasure, and portability over their personal data. And because our solutions are part of a unified set, the process to address these requirements is streamlined.

The Customer Engagement Company™

Americas
info@verint.com
1-800-4VERINT

Europe, Middle East & Africa
info.emea@verint.com
+44(0) 1932 839500

Asia Pacific
info.apac@verint.com
+(852) 2797 5678

verint.com
twitter.com/verint
facebook.com/verint
blog.verint.com

VERINT®