Demonstrating **GDPR** Compliance

Veriato

www.veriato.com

The biggest challenge in ensuring security of personal data is people.

At its core, GDPR compliance is simply about protecting personal data of EU citizens that is necessary and appropriate to collect. Applications hosting personal data may provide some level of detail around when personal data is accessed, but without visibility into what users do with personal data after they access it, the risk of data breaches, compliance violations, and the investigations, fines, and reputational damage that comes with them, is significantly increased.

Veriato provides contextual user activity detail and screen recordings necessary to satisfy GDPR requirements. By logging all user activity and capturing screen detail for video playback, Veriato creates an indisputable audit trail that will satisfy the evidence requirements of even the most scrutinizing supervisory authority.

This brief discusses the challenges of safeguarding personal data, and how Veriato uniquely creates the audit detail necessary to meet GDPR compliance objectives.

Introduction

Effective on May 25, 2018, the General Data Protection Regulation (GDPR) of the European Union stands to change how many companies worldwide do business involving European Union citizens. For the first time, the concept of what constitutes personal information has been expanded by GDPR. According to the regulation, personal data includes any information "that can be used to directly or indirectly identify the person. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address." It is this data that must be protected, regardless of where the data, or the organization processing or controlling the data resides.

There are material penalties for a breach – as much as 4% of a company's annual worldwide revenue or €20 million (approximately $24.8 million), whichever is greater. Avoiding these penalties depend solely on an organization's ability to demonstrate proper processing, security controls, and the lack of breach. And with breach notification required within 72 hours, organizations need an audit trail that provides the detail necessary to document the scope of a breach.

So, what's needed is a means to have complete visibility into every action performed by a user with access to personal data – every application used, webpage visited, record copied, file saved, print screen generated, and page printed. Only then will a controller or processor truly know whether personal data has been appropriately accessed and used.

But, compliance to GDPR isn't just a technical battle; it's one filled with administrative policies and procedures that, in conjunction with technology, ensure users are trained, access to personal data is correctly granted, use and processing thereof is appropriate, and compliance can be demonstrated.

GDRP Challenges for Key Stakeholders

While GDPR only breaks down responsibilities to an organizational level, and to one new role – the Data Protection Officer (DPO), traditional stakeholders in the organization each have different needs around the goal of adhering to GDPR:

CEO – Needs a proactive approach leveraging people, processes, and technology that ensures adherence to GDPR requirements around protecting personal data.

CFO – Can't afford the cost of a breach in compliance. Would rather spend budget on preventative measures, than on responding to a breach.

CCO – Wants a plan in place of how to easily and quickly demonstrate compliance.

DPO - Desires to ensure personal data processes, activities and systems conform to GDPR by design.

CSO – Desires for personal data to remain secure, and a way to know personal data isn't being misused.

IT Manager – Needs to understand what data resides where, as well as any redundancies. IT also needs to provide a means of visibility into exactly how GDPR's expanded definition of personal data is used, regardless of application.

What's needed is a technology that cost-effectively addresses GDPR requirements by monitoring the processes involving personal data, aligning with established policy and processes, providing visibility into how personal data is used or misused, and providing context around either demonstrating compliance or determining the scope of a breach.

How Veriato Helps Address GDPR Challenge

Veriato helps organizations of all kinds satisfy the GDPR obligations related to assessing risk, ensuring safeguards are in place, demonstrating access is appropriate, and providing context should a breach occur. It does so by recording and providing access to detailed user activity data – both within applications used to process personal data, as well as in any other application – combined with robust screen recording and video-like playback. Customizable policies and alerts help enterprises craft appropriate responses to their unique environments.

Veriato can be used to assess the security of a process, that all access to personal data is appropriate, and to replay actions involved in a data breach. All activity data is searchable, making it easy for the DPO, an auditor, security teams, or IT to find suspect actions, with the ability to playback activity to see before, during, and after the process activity in question. Alerts can inform the enterprise about suspicious user activities and minimize risks of breaches. Reports can be produced in minutes – typically a fraction of the time needed – and don't require pulling critical resources from other tasks.

Veriato assists with a number of specific articles in the regulation, utilizing its detailed visibility into specific user actions related to accessing and processing personal data. The following sections outline how Veriato can assist with meeting specific GDPR requirements.

ARTICLE 24

Controller Responsibilities

One of the key responsibilities of the controller under GDPR is to ensure the data is only accessed and used for business-related processing. Veriato can be used to monitor user interaction with specific data, systems, and applications related to the processing of GDPR-protected personal data.

Below are some examples of how Veriato can assist in addressing the Controller responsibilities:

- **Demonstrate Proper Processing (Paragraph 1)**
  Veriato records every user action, providing the DPO with activity detail used to demonstrate that processing is performed in accordance with GDPR.

ARTICLE 25

Data Protection by Design and by Default

The DPO is mandated to ensure security within systems and applications used to process personal data is in place and part of the intent, the implementation, and the process. Veriato provides unmatched visibility into who is accessing personal data, what applications are being used, which data is being accessed, and what's being done with it – all factors in testing to see if data protection is implemented as an inherent part of the process.

Below are some examples of how Veriato can assist in addressing some of GDPR's data protection design standards:

- **Validate Data Protection Principles (Paragraph 1)**
  Activity data can serve as the basis for verifying the necessary safeguards have been put into the processing. By reviewing how users access and process data, an understanding of whether safeguards are in place or not can be quickly ascertained.

Ensure Data Inaccessibility (Paragraph 2)
By monitoring user access to personal data, Veriato can detail when and what personal data is being accessed, used to ensure that data is only accessible to the appropriate internal users by default.

ARTICLE 30

Records of Processing Activities

GDPR requires the processor and controller to maintain a record of several different categories of detail around each and every processing activity. The ability to record, report on, and playback user activity provides organizations with specific details and context around each processing activity. Customizable policies can help processors and controllers manage these different categories and provide easily understood reports.

ARTICLE
32

Security of Processing

Akin to most data security standards, GDPR mandates the establishing, assessment, and validation of security around the processing of personal data. Aligning with the assessment of risk in Article 35, this article seeks to ensure a level of security commensurate with the risk should an organization's personal data be breached.

Below are some examples of how Veriato can assist in establishing and maintaining the security of processing:

- **Ensure Ongoing Security (Paragraph 1d)**
  Meet the need for regular evaluation of the technical and organizational controls around security of the processing by comprehensively providing access to a review of user activity. Activity detail is provided both within the processing-related applications, as well as within any other application that can be leveraged to steal, expose, or otherwise misuse personal data.

- **Evaluating Risk of Processing (Paragraph 2)**
  Whether accidental or malicious, activity details help with the assessment of appropriate levels of security and the risks presented through a user's ability to destroy, lose, alter, disclose of, or access personal data while being transmitted, stored or otherwise processed.

- **Validate Appropriate Process (Paragraph 4)**
  Monitor and audit application usage, with the ability to notify the DPO or other appropriate staff of access to personal data both as alerts and through reporting. This audit detail can be used as part of validating that access to and processing of personal data does not occur without instruction from the controller.

ARTICLE
33

Notification of a Personal Data Breach to the Supervisory Authority

GDPR mandates notification of a personal data breach within 72 hours of it occurring. This means the organization needs to be continually monitoring for personal data breaches. Additionally, should a breach occur, GDPR requires organizations to define the scope of the breach or be required to report all effected personal data, likely resulting in a larger fine if found inadequate. Veriato assists with both detecting potential breach activity, as well as providing activity detail should it be determined a breach has occurred.

Below are some examples of how Veriato can assist in addressing some of personal data breaches:

- **Detecting Potential Risk of Breaches**
  Veriato's user and entity behavior analytics (UEBA) identifies users demonstrating a potential breach threat through monitoring and analyzing behavior and communication changes. IT and the DPO can be notified of any risk potential, at which time a review of user activity can be made.

- **Detecting Potential Breaches**
  Monitor for, detect, and alert on specific user activity that the controller deems inappropriate. This can be based on application use, keyword searches, and more.

- **Defining the Nature of the Breach (Paragraphs 3a and 5)**
  Should a breach occur, Veriato's video playback of user activity provides clear context around the actions before, during, and after the breach. These details can be used as part of the controller's documentation of the personal data breach.

ARTICLE 35

Data Protection Impact Assessment

Impact assessments are intended to either expose risk in the process, or to establish that the process protects personal data end-to-end. Veriato's activity monitoring uniquely assists with assessing the current state of operations and its adherence to GDPR..

ARTICLE 41

Monitoring of Approved Codes of Conduct

Periodically, supervisory authorities may review the policies, processes, and documentation of an organization to review its adherence to GDPR. Veriato's user activity logging can provide needed detail throughout any audit of user conduct.

Below is an example of how Veriato assists in monitoring conduct:

- **Periodic Operations Review (Paragraph 2b))**
  As part of an operations review, the supervisory authority will need to audit the actual processing of personal data. Veriato not only empowers supervisory authorities to examine recorded user activity within systems containing protected personal data, but also within any other application, providing unmatched visibility into actions involving the processing of personal data.

Demonstrating GDPR Compliance with Veriato

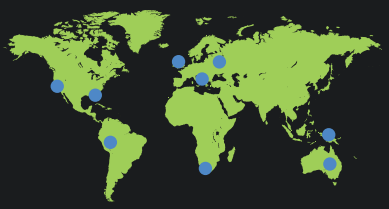
GDPR is a far-reaching, bold piece of legislation that impacts any business with customers in the European Union. Ultimately, GDPR is designed to ensure the privacy of personal data. And, as long as the only access to and processing of a given personal record is performed by someone who both has a legitimate need and only uses that information for the purposes of the organization, your organization will remain compliant.

But, because users with access to personal records utilize that access every day, it becomes nearly impossible to tell if and when your organization may be out of compliance. For example, the access to a record may seem appropriate, however the cutting and pasting of that information into a separate document saved up on a cloud drive certainly isn't. This means your organization needs to be monitoring and recording all user activity, regardless of application.

Veriato assists with establishing compliance with GDPR requirements by providing IT, the DPO, security teams, and supervisory authorities alike with complete visibility into every action taken by the organization's users. Veriato solutions help to analyze risk, test processing security, and review activity in an effort to identify breaches and their scope.

To learn more about how Veriato can help you with **GDPR Compliance**, contact a Veriato representative today.

Over 3,000 enterprises, & thousands of SMBs have placed their trust in our solutions



Our solutions are deployed in **110+ countries**

Veriato USA

4440 PGA Boulevard , Suite 500

Palm Beach Gardens, FL 33410

Veriato EMEA

3rd Floor, Crossweys House

28-30 High Street

Guildford, Surrey

GU1 3EL United Kingdom

https://plus.google.com/+Spectorsoft

https://www.linkedin.com/company/veriato

https://twitter.com/veriato

https://www.youtube.com/SpectorSoft

https://www.facebook.com/VeriatoInc/