How TIBCO LogLogic Helps with Data Privacy Protection Compliance

While the European Union's General Data Protection Regulation (GDPR), and the new California Consumer Privacy Act of 2018 (CCPA), have dominated regulatory headlines, organizations should anticipate the pace of privacy regulations to accelerate. Already, more states in the US and other countries are working on their own data privacy regulations.

As your organization faces more and more regulations, it's essential that you understand the ins and outs of each regulation and adjust your tactics and strategies to be compliant. To prepare for these new laws, your company must first determine what data it has and how it's being used. Both GDPR and the CCPA require obtaining consent from individuals to collect and use their data and disclosing how you will use it. Of course, to do this, you must know what sort of information you currently have.

THREE WAYS TO SUPPORT YOUR DATA PRIVACY PROTECTION NEEDS

TIBCO LogLogic® Operational Intelligence provides complete visibility into your on-premises and cloud IT infrastructure via advanced analytics, including browser-based pre-packaged dashboards, detailed reports, real-time alerts, and faster search. Within seconds, not days, its real-time forensics engine can quickly get to the root cause of incidents enabling effective and efficient decision-making.

The LogLogic® Compliance Manager provides customizable report workflow that simplifies the review and audit process for adherence to internal and external policies for major mandates like COBIT, FISMA, GDPR, HIPAA, ISO, ITIL, NERC, PCI DSS, and SOX.

Here are three ways the LogLogic® platform can support your data privacy protection needs:

SECURE PROCESSING

Ensure that data both in transit and at rest is properly secured and can only be accessed by authorized personnel.

The LogLogic platform gives you the ability to quickly monitor, report on, and alert for:

- Risky and suspicious traffic
- Unsecured data transports
- Access control list changes on your file servers and datastore
- Much more

Insights from machine data provide early warning of threats to your digital infrastructure.

BREACH NOTIFICATION

In the event of a personal data breach, rapid notification without undue delay, and if feasible, within a defined time period of becoming aware of the breach must occur. The notification must contain, among other information, the nature of the breach, including the number of data owners affected and your steps for remediation.

For example, an online retailer could be responsible for a personal data breach if a customer's contact information and preferences are inappropriately accessed due to lack of appropriate internal controls. Machine data allows organizations to quickly detect, investigate, and scope breaches.

Detailed forensics can be run to track how and when the breach occurred, which systems and data were accessed and when, how many people and records were affected, and what remedial measures need to be taken.

The LogLogic platform provides the ability to quickly run forensic and monitoring reports for activity such as:

- File server and database access reports
- Web access and traffic reports
- User access reports
- Infrastructure

These LogLogic reports and others can help you meet your notification requirements.

SEARCH AND REPORT ON PERSONAL DATA PROCESSING

Nowadays it is becoming ever more important for organizations to ensure that only authorized personnel have access to personal data. And that they are able to make available to auditors all information necessary to demonstrate compliance with the applicable data privacy mandates.

The LogLogic platform gives you the ability to run scheduled reporting audits on your machine data as well as a compliance workflows that track assigning, completing, and defining a review schedule, and other tasks.

As we are seeing now with mandates like GDPR and CCPA, citizens now have the right to know what personal data is being processed about them, with whom it is shared, and where it is processed. Consumers can now ask that their personal data be corrected or deleted. Those processing the data are required to ensure that only authorized persons are involved with processing personal data, and when the processing is complete, a request can be made for all personal data to be deleted or returned, including, in some cases, backup copies.

Data privacy protection compliance dashboard.

Some examples of areas where the LogLogic system can help:

LATIN AMERICA

Mexico: Protection of Data Held by Private Parties (the Data Privacy Law)

Argentina: Personal Data Protection Law (25,326), regulatory Decree 1558/2001

Colombia: Decree 1377/2013 (Articles 13, 23, 26, and 27)

NORTH AMERICA

Canada: Personal Information Protection and Electronic Documents Act ("PIPEDA")

CCPA: California Consumer Privacy Act 1798.105,1798.110,1798.112,1798.115,

1798.120,1798.130,1798.135, 1798.140 and 1798.150

EU

GDPR: Article 15,24,25,28,32,33,34 and 58

UK

DPA: Data Protection Act

SUMMARY

Machine data gives organizations end-to-end visibility into their infrastructure and processing activities, which is critical information for data privacy protection compliance. TIBCO LogLogic Operational Intelligence can help you leverage your machine data to provide documentation about what personal data was accessed, by whom, how it was used, and when it was deleted.

To learn more about TIBCO LogLogic and how it can help you with compliance and other business challenges, contact TIBCO at www.tibco.com/contact-us.