Securing Physical Computing Infrastructure for GDPR Compliance

SOLUTION BRIEF

The General Data Protection Regulation's (GDPR) primary intent and goal is to establish processes for the protection of personal data. The law provides explicit definitions defining personal data, how it can be used, and how it should be protected and managed. All (electronic) customer data resides on storage, is processed on servers, and accessed across a network. If you do not know where your customer's data is, or how it is physically being accessed, you are in violation of the GDPR regulation. Nlyte provides you the ability to track within the physical IT infrastructure where the data resides, how it is transported from storage, server, to end user, and who has interacted with that infrastructure.

For some time, the focus of GDPR for most commercial businesses has been on housekeeping around the data itself: what data is stored in the database, who has access to it, what are the archival and removal processes in place. The IT infrastructure teams have, until recently, ignored their role in GDPR compliance. We are learning that the physical security of the data processing infrastructure is as critical as the digital management.

The concern of physical infrastructure extends beyond an organization's data center, and includes colocation facilities, managed service providers, hosting services, SaaS vendors, and virtually any X-aaS vendor. GDPR holds you accountable for proper compliance regarding the personal data at your disposal regardless of where it resides. Not having a contract regarding data protection in place is an indication you don't know what your vendors are doing with your data. That presents itself as a more significant management issue about what infrastructure you're using and how you're treating the data. Vendor management under GDPR requires you to know how your vendors operate including their security framework and how they manage data. Without that knowledge, you don't know the risk they present.

Nlyte provides discovery, asset management, and asset integrity monitoring. This combination of functionality is key in helping any organization track data at rest and the infrastructure used for that data. Nlyte provides a consistent mechanism for the tracking of assets within an organization which includes: the physical locations of the assets; usage of the assets; end-to-end lifecycle management of the assets, both physical and logical; manual and logical auditing of assets; connection into an organization's ecosystem/ITSM systems for the logical mapping of a "data subject's" (personal/customer) data.

The GDPR Fundamentals that Nlyte Tracks

- Where is the critical data located, geographic location, devices servers/storage/network
- Where is the data replicated, geographic location, devices servers/storage/network
- What and if security tools are deployed on identified devices and enabled
- Data breach notifications i.e. what "data subjects" data ran on what assets
- Identification of secondary locations infrastructure for the safe handling of data transporting across borders

Securing Physical Computing Infrastructure for GDPR Compliance

Nlyte Support of Article 35, "Data Protection Impact Assessment"

Nlyte supports the Data Protection Impact Assessment through Nlyte Workflow. Workflow provides the ability to assign a data protection officer's review activity within any IMAC data center process. This would include a GDPR form that supports capturing the asset name, application name, and if the system is running or hosting customer data.

A second review at the end of a workflow ensures that the assets created within this IMAC process match the names requested at the start of the process and that the business applications have been captured within Nlyte's Asset Optimization database and flagged as hosting customer data.

A Nlyte GDPR report provides the count of all workflows that have a GDPR activity, and if each is active or closed. The report shows workflow name, open date, closed date, assets names, and applications names reconciled against assets within Nlyte's Asset Optimization database.

Nlyte Support of Article 17 "Right to Erasure ('Right to be Forgotten')"

Nlyte Asset Management provides the Controller the ability to flag/track the lifecycle of all assets that have been used for the storage or processing of "data subjects" (personal/customer) data. This tracking can be from the point of existence within the physical compute infrastructure through to the point of decommissioning or destruction, ensuring a complete lifecycle record of the data's physical location.

Nlyte workflow provides the controller with the ability to track who has handled or had physical access to the assets that are running the "data subjects" data.

Nlyte Support of Article 58 Investigative "Powers"

Nlyte Asset Tracking along with business applications mapped to Nlyte's Asset Optimization database support compulsorily data protection audits.

Nlyte Discovery provides Asset Integrity Monitoring by ensuring all assets and applications are aligned correctly within the physical compute infrastructure. Additionally, it identifies any assets or applications that have changed in or out of authorized workflow and compliance standards.

Securing Physical Computing Infrastructure for GDPR Compliance

How Nlyte supports Articles 59, 33, 33a "Activity Reports", "Data Breach Notification to Authorities"

Nlyte Impact Assessment Reports list assets that have been flagged for GDPR tracking providing:

Executive Summary

Number of tracked assets by location by status, active, decommissioned

Number of tracked applications by location

Operation Drill-down

List assets by location, rack, name, IP address, data last audited, mapped business applications, from discovery security software installed (name and version) and statues enabled Y/N

Nlyte Support of Article 45 "Transfers on the Basis of an Adequacy Decision" International Companies

Nlyte lifecycle tracking of assets and their moments between locations provides accountability and compliance visibility and reporting.

Nlyte takes GDPR Seriously

With 4% of a company's global revenue at stake for a breach and the impact that could have on their shareholders and reputation, every commercial organization needs to be concerned and actively building out their compliance plan. Nlyte supports the largest organizations and data centers in the world. When it comes to managing data centers and hybrid compute infrastructures Nlyte has the solutions, experience, and expertise to partner with you to protect your customer's data. Learn how Nlyte's Suite of products can help you manage your compute infrastructure and remain compliant with GDPR.

FOR MORE INFORMATION

- Contact Us: **info@nlyte.com**
- Visit Us: **www.nlyte.com**

Nlyte is a registered trademark and Nlyte Software is a trademark of Nlyte Software Limited. All other brands or products names are the property of their respective holders. Information in this document is subject to change without notice and does not represent a commitment on the part of the vendor.

About Nlyte

Founded in 2004, Nlyte Software is recognized as the industry leading data center infrastructure management (**DCIM**) solution provider. Nlyte's DCIM provides unmatched functionality that supports all data center processes across the entire "dock to decom" lifecycle. With a 98% customer retention rate, Nlyte's DCIM solution is used by many of the world's largest and most sophisticated data centers, as well as many small and medium sized organizations. Customers can quickly deploy the Nlyte DCIM solution and begin to immediately enjoy reduced costs and increased efficiency across all data center processes. For more information, visit **www.nlyte.com** or follow **@nlyte** on Twitter.