NEXTLABS

SOLUTION BRIEF

NextLabs and the GDPR

Automated, Integrated, Pervasive Protection of Personal Data

According to the GDPR, data subjects have the right to:

- **Access** the personal data being collected on them and understand how it's been processed and distributed
- **Rectify** incorrect personal data
- **Erase** their personal data (the "right to be forgotten")
- **Restrict** how they use their personal data
- **Receive** data that they have previously provided
- **Be notified** "without undue delay" when their personal data is involved in a breach that is likely to result in high
  risk to their "rights and freedoms"

Ensure the Expanded Rights of Data Subjects

If your organization captures, processes, and/or controls the personal data of people residing in the European Union (EU), you are certainly aware of the General Data Protection Regulation (GDPR). This is the most important data privacy change in 20 years, and non-compliance can lead to sanctions, fines (up to 4% of annual global turnover or €20 Million, whichever is greater), reputational damage, and individual private claims.

The GDPR protects the rights of EU residents (both citizens and non-citizens) to determine whether, when, how, and to whom their personal information is revealed and how it can be used. The regulation expands protection for special categories of personal data such as racial origin, religion, political beliefs, genetic/biometric/health data, sexual orientation, and more.

OVERVIEW

NextLabs' attribute-based policy platform secures sensitive personal information at the data level—regardless of whether it resides inside or outside your organization; in structured or unstructured formats; or in applications, the cloud, or mobile devices. NextLabs solutions help you automate the consistent enforcement of GDPR-related compliance and security policies across the enterprise to protect personally identifiable information (PII); monitor and control access to PII; and prevent security violations caused by information sharing, external breaches, and internal misuse.

GDPR Impact on IT, Security, and Compliance

To meet all the requirements specified in the regulation (including data subjects' expanded rights), IT, Security, and Compliance leaders must be able to:

- **Identify and classify all sources of personal data** the organization has in its control, and know where that data is at all times
- **Control access to personal data**, so that only those with proper authorization are able to view or perform actions on it
- **Document compliance with the GDPR**, and have an audit trail of how, when, and where the personal data is used —both within and outside the organization

To ensure full compliance with the GDPR, organizations need a system that can automate policy enforcement to remove the chance for user error. The solution must also keep user attributes up to date without human intervention. In order to adequately protect PII, data must be secured directly, protecting data that is shared across the extended enterprise (customers, partners, service providers, users) and no matter which device is used to access it.

NextLabs has these capabilities built into its platform, data protection, and application security solutions. Out of the box, NextLabs offers the "data protection by design and by default" required by Article 25 of the GDPR.

Identify and Classify Personal Data

Accurately classifying data is key to ensuring adequate protection of PII. It is not possible to comply with the requests of data subjects to access, rectify, erase, restrict, and receive their personal data unless you first know precisely which data is sensitive and where that data resides—both inside and outside the organization, whether on premise or in the cloud.

Besides tracking the location of PII, data classification also lets you set up the actions people can take when they access it. You can define access and usage policies associated with each type of classification.

NextLabs works with any file type and automatically classifies large file repositories based on your predefined rules, keywords, and metadata. For example, because the GDPR has restrictions on handling PII as it relates to children, you'll want to track data subjects' age and set permitted actions on the data. (Note that you can categorize personal data by any of the protected categories, whether religion, gender, or more.) NextLabs can categorize personal data whether it resides in structured or unstructured data formats. It can also:

- Automatically do **batch classification** based on your rules, using content analysis to search for your desired keywords and metadata
- Apply **rules-based protection** to sensitive files
- **Segregate** sensitive data into certain classified directories
- **Scan incremental changes** at time intervals you specify, to ensure data is always properly classified
- **Centrally manage** your rules, and create reports to show how your organization is distributing and storing personal data

Control Access to Personal Data

In the extended enterprise, where we share sensitive data across organizations, over external systems, and with unknown users and devices, implementing authorization policies consistently can seem an impossible challenge. In a typical scenario, each application and system silo has authorization policies that are redundant, difficult to change, and costly to maintain. NextLabs' centralized policy management accelerates data protection and compliance.

The NextLabs platform is **identity-aware, content-aware**, and **context-aware**. It automatically applies protections to data based on its content—rather than relying on end users to manually apply policies to each and every document.

The system makes authorization decisions at runtime, using contextual information—or attributes—about the **user** (for example, title, department, project); the **data** (classification, category, type, content); and **environment** (device, location, time of day). This enables fine-grained decisions to ensure that only the right people gain access to sensitive information.

These data protections are persistent. NextLabs secures sensitive personal information at the data level, whether that data resides inside or outside your organization; in structured or unstructured formats; or in applications, the cloud, or mobile devices. In addition, you can:

- **Mask, delete, and redact fields** to comply with Article 9 (increased protection for special categories of PII)
- **Filter data** so users see only the information they're authorized to see
- **Fulfill a data subject's request to be forgotten** by setting attributes for a specific time period/end date (followed by deletion or inability to access)
- **Encrypt data** so that PII is securely protected, even in the case of a breach
- **Segregate data** to ensure only those who have rights can see the data
- **Protect across multiple systems** based on the same user attributes

Document Compliance with the GDPR

The GDPR requires that organizations report data breaches to the supervisory authority within 72 hours, and report which data was compromised and how many data subjects it affected. In addition, you must be able to demonstrate compliance with all relevant articles of the GDPR and verify that your value chain partners are in compliance as well.

An added complication for compliance is that individual EU countries may have other data protection regulations on top of the GDPR mandate, which makes adhering to regulations across country lines more complex. NextLabs' fine-grained policies can account for local or country-specific differences and grant access rights accordingly—making the process streamlined and easy to enforce.

NextLabs helps you comply with the GDPR and document your compliance by centralizing policy management with full visibility and control. Organizations can centrally control the creation, enforcement, and management of security policies across all applications and systems—ensuring that policies are aligned with business objectives and are applied consistently across the enterprise

Comprehensive monitoring and reporting on user activity and data access provides enhanced audit and compliance capabilities and allows organizations to detect anomalies in access patterns and alert administrators of suspicious behavior—even before a breach occurs

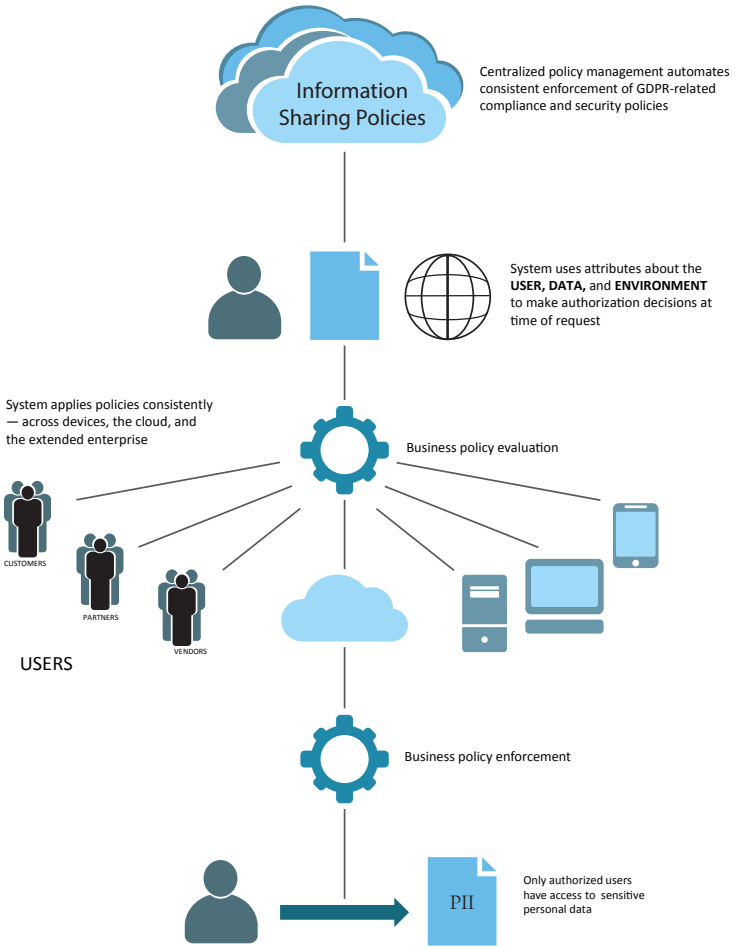
The NextLabs platform supplies always-on event monitoring and logging across your extended enterprise, so that users with the proper access can view:

- Usage patterns
- Authorization decisions
- Trend analysis
- Audit trails for all data usage

How NextLabs Ensures GDPR Compliance

Simply putting data security tools and processes in place does not ensure that an organization is actually protecting sensitive data to the degree required by the GDPR. NextLabs uniquely ensures full GDPR compliance through its automated, integrated, and pervasive protection of PII:

- GDPR policies are created and managed in a single platform, and are enforced consistently and automatically across the enterprise. Organizations have full visibility into which policies are enforced.
- Protection of PII is pervasive, no matter where the data resides: cloud, laptops, mobile devices, or file servers. Data protection is persistent throughout the lifecycle regardless of where it goes.
- Policies are easily amended or updated and the system automatically enforces the new policies across the extended enterprise.
- As user status changes (for example, team members leave a project), the system automatically takes status changes into account when evaluating access requests so the most current information is used to determine whether access should be granted.
- Centralized visibility and reporting provides a real-time view of data access and usage, regardless of where the data goes.



ABOUT NEXTLABS

NextLabs®, Inc. provides data-centric security software to protect business-critical data and applications. Our patented dynamic-authorization technology and industry-leading attribute-based policy platform help enterprises identify and protect sensitive data, monitor and control access to the data, and prevent regulatory violations—whether in the cloud or on premise. The software automates enforcement of security controls and compliance policies to enable secure information sharing across the extended enterprise.

NextLabs has some of the largest global enterprises as customers and has strategic relationships with industry leaders such as SAP, Siemens, Microsoft, and IBM.

For more information on NextLabs, please visit http://www.nextlabs.com.