CYERA

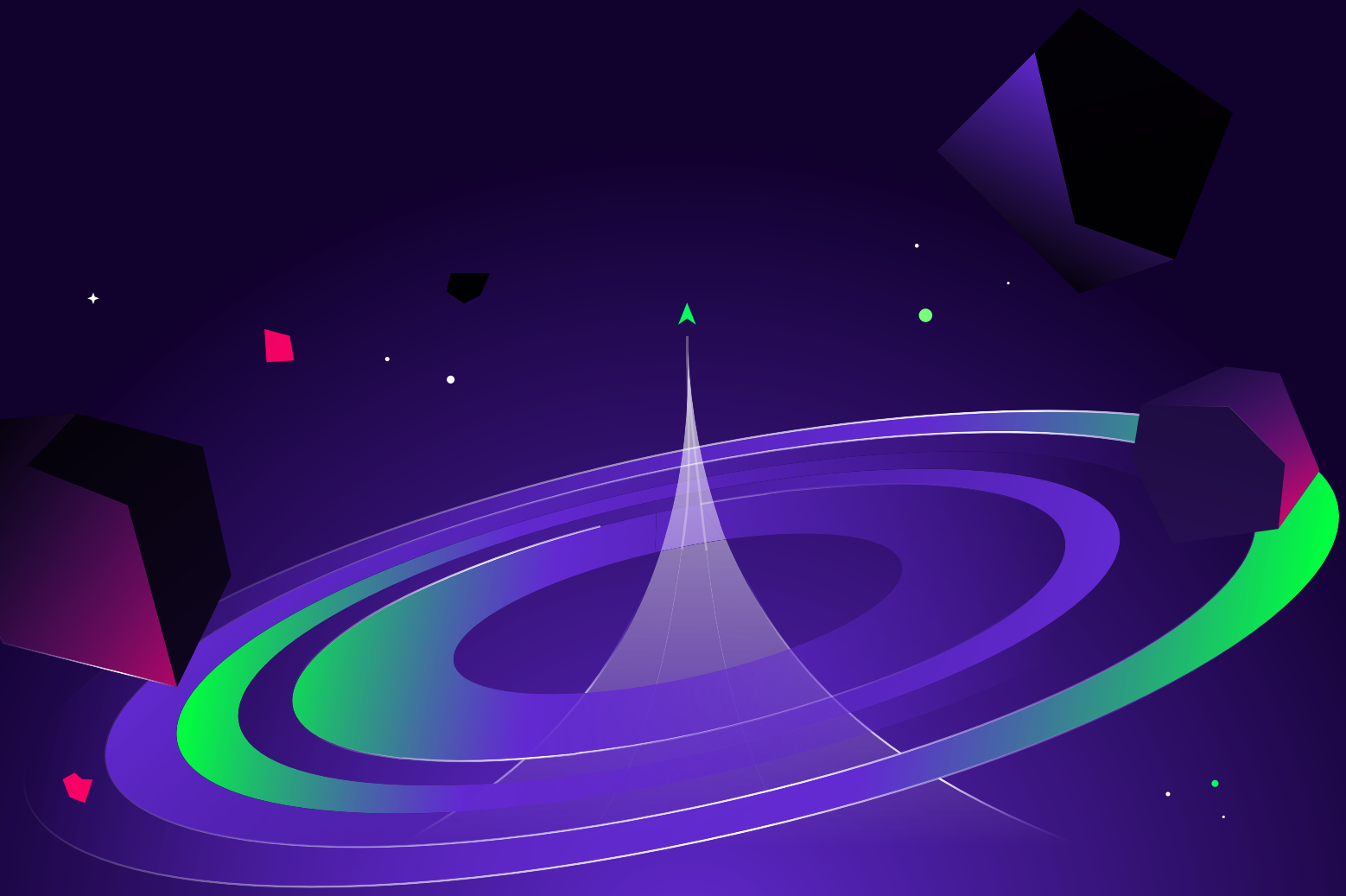
GUIDE

Protecting Personal Data in Brazil

# How Cyera Supports Compliance with the LGPD

# Table of Contents





# Introduction

## About the LGPD

The Brazilian General Data Protection Law (Lei Geral de Proteção de Dados, or LGPD) was enacted in 2018 and came into effect in September 2020. Inspired largely by the EU's GDPR, it was created to unify Brazil's fragmented privacy rules and regulate the processing of personal data in both public and private sectors.

The LGPD establishes principles such as purpose limitation, necessity, and transparency. It grants individuals rights to access, correct, delete, and transfer their data, while requiring organizations to obtain clear consent, implement security measures, and report breaches. The law applies broadly to data processing activities involving Brazilian citizens, regardless of where the business is located. Enforcement is overseen by the National Data Protection Authority (ANPD).

The LGPD is significant for advancing data security in Brazil, aligning the country with international privacy standards, and reinforcing accountability, consumer trust, and cybersecurity practices in the digital economy.

## About Cyera

Cyera is a unified, AI-native data security platform that empowers businesses to manage sensitive data across highly permissive and widely distributed environments with precision and efficiency.

The platform's non-invasive, automated data discovery provides a comprehensive view of sensitive data across structured and unstructured sources. This capability enables organizations to address critical challenges like data proliferation. Powered by AI-driven classification, Cyera goes beyond traditional methods by understanding context, intent, and nuance. This deep insight helps uncover ghost data, reveal data risks, reduce false positives, and mitigate threats like data breaches and ransomware — areas where conventional data loss prevention and data governance tools fall short.

By combining advanced technology with ease of use, Cyera empowers organizations to confidently secure personal data, support LGPD compliance, and safely enable AI use cases.

# Principles for the Processing of Personal Data

Chapter II (Articles 7 through 16) sets out the basic guardrails for processing personal data. Similar to the GDPR, the LGPD enshrines core principles, defines categories of sensitive personal data, and establishes heightened consent requirements for processing sensitive personal data and the personal data of children.

Under the LGPD, the principles for the processing of personal data include the following:

- **Lawfulness:** Data controllers must obtain consent to process data subjects' personal data, unless some exception to the consent requirement applies.

  Consent requirements are stricter for the collection and processing of sensitive personal data or children's personal data.

- **Transparency:** Data controllers must provide a privacy notice that informs data subjects of the purpose for which their data is being collected, the form and duration of any processing activities, contact information for the data controller, information about entities with whom data will be shared and for what purposes, and information about data subjects' rights under the LGPD.

- **Purpose Limitation:** Consent for collection and use of data subjects' personal data must be for specified purposes only. Generic authorizations to collect and process a data subject's personal data are void.

- **Minimization:** Data controllers may only process data that is necessary to fulfill the legitimate purposes for which it was collected.

- **Storage Limitation:** Data controllers may not retain data subjects' personal data longer than authorized by law. The retention period is terminated when the purpose for the data's collection has been achieved, at the end of the stipulated processing period, when the data subject revokes consent, or when determined by the relevant authorities.

The cornerstone of lawful data collection and processing is consent. Cyera Privacy will soon be equipped with consent management, allowing your organization to manage user consent for cookies, tracking technologies, mobile software development kits (SDKs), and other processing activities.

Data minimization is a key use case for the Cyera data security platform. Many Cyera customers are discovering petabytes of data they didn't realize they had, not only saving them tens of thousands of dollars per month in cloud storage costs, but also reducing their attack surface and improving their compliance posture.

Similarly with storage limitation, Cyera discovers dormant personal data and orphaned data stores. It allows you to review datastore and file age and pinpoint retention issues. And it can validate secure deletion of files and datastores to demonstrate compliance with organizational and regulatory data retention policies.

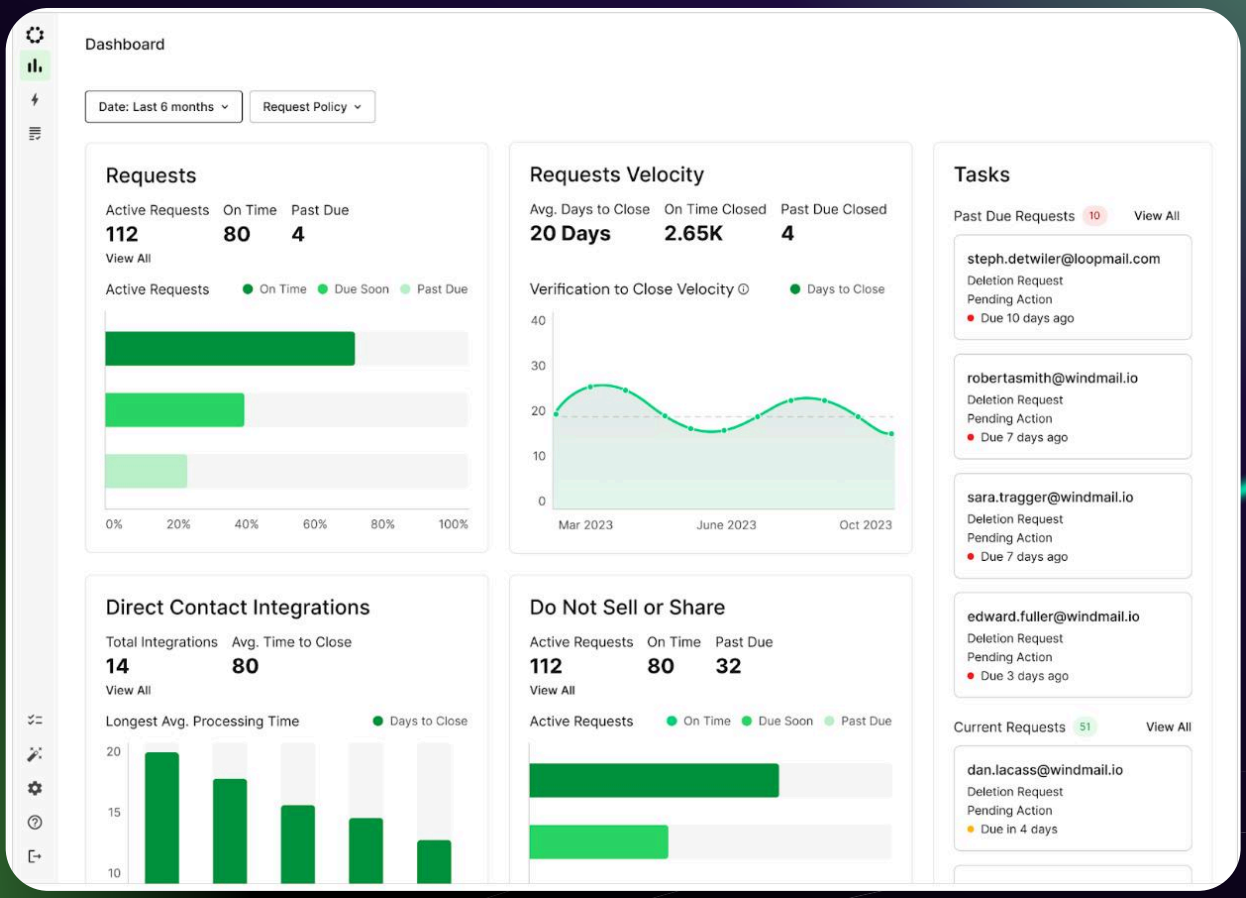
# Data Subjects' Rights

Chapter III (Articles 17 through 22) enumerates the rights of data subjects in Brazil. Similar to the GDPR, these rights include:

- **Right to be Informed:** Data subjects have a right to know whether their data is being processed, with whom it is being shared, that they have a right to refuse consent to processing, and the consequences of revoking or refusing consent to processing.
- **Right to Access:** Data subjects have a right to access their personal data held by a data controller or operator.
- **Right to Correct:** Data subjects have the right to correct inaccurate, incomplete, or outdated data.
- **Right to Delete:** Data subjects have the right to request the deletion of data that had previously been processed with their consent.
- **Right to Data Portability:** Data subjects have a right to request a copy of their data to provide to a different product or service provider.
- **Right to Revoke Consent:** Data subjects have a right to revoke their consent to any further processing of their personal data.
- **Right to Object:** Data subjects have a right to object to the continued processing of their data, or to request the anonymization or deletion of their data, when they believe it has been collected or processed in violation of the law.
- **Right to Review Automated Decisionmaking:** Data subjects have a right to request a review of decisions made solely on the basis of automated processing of their personal data.

Cyera can help your organization streamline the process of fulfilling DSRs in a timely manner. Cyera's DSPM discovers and classifies personal and sensitive personal data in your IT ecosystem, allowing your organization to create an up-to-date personal data inventory.

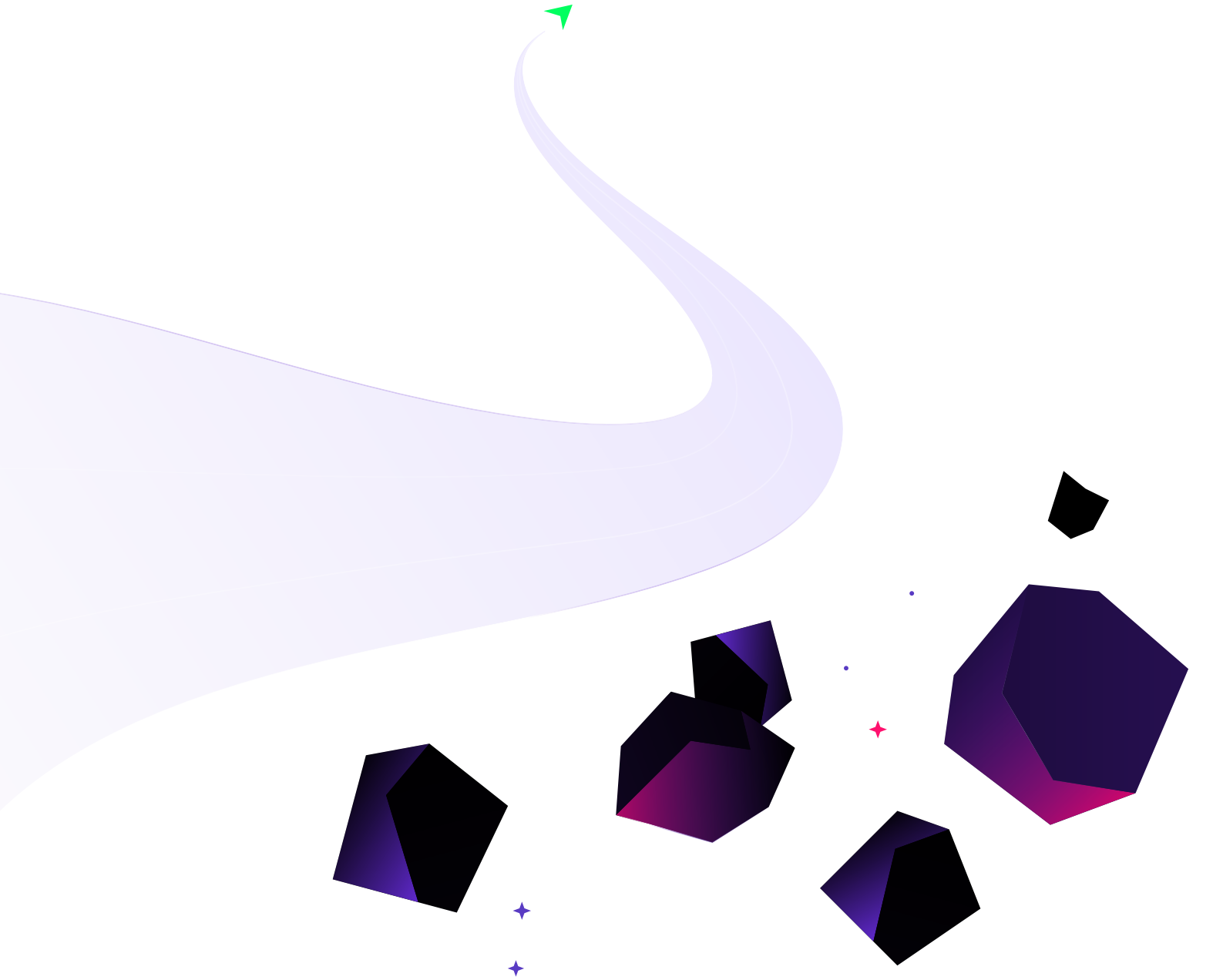
Cyera Privacy (see graphic below) also enables data subjects to submit requests easily through a structured web form. The form helps automate requests for access, deletion, correction, objection to processing, and transfer of data. Cyera verifies requesters' identities and automatically executes data collection or deletion to securely fulfill the subject access request.



# International Data Transfers

Chapter V (Articles 33 through 36) governs the transfer of Brazilian data subjects' personal data to other jurisdictions. Such transfers are generally restricted except in certain enumerated circumstances, or where the relevant authorities have determined that the target country has sufficient data privacy protections in place. The law also empowers relevant authorities to determine the content of Standard Contractual Clauses to govern contractual relationships involving the transfer of personal data to foreign businesses or individuals.

Cyera's DSPM enables filtering by data subject residency, allowing you to build an inventory specifically of Brazil data subjects. It also enables you to monitor which third parties are accessing personal data, and set policies to flag non-Brazilian vendors accessing Brazilian data subjects' data.



# Duties of Data Controllers

Chapters VI and VII (Articles 37 through 51) impose certain obligations on data controllers and operators (analogous to processors under the GDPR). These obligations include things like keeping a record of data processing activities, appointing a DPO or other responsible person for data security, implementing adequate security controls to protect data subjects' personal data, and rules for notifying data subjects and authorities in the event of a breach.

The table below lists the obligations of data controllers and operators under the LGPD, and describes how Cyera can help you comply with them.

| LGPD Requirements | Cyera Capabilities |
| --- | --- |
| **Record of Data Processing Operations**<br>Controllers and operators must keep a record of data processing activities that they perform. | Cyera's data discovery and classification capabilities help your organization build a comprehensive and up-to-date personal data inventory.<br><br>By pre-filling the data-focused sections of a Record of Processing Activity (RoPA) - including things like categories of personal data, categories of data subjects, categories of recipients, data transfers, and technical security measures in place - Cyera accelerates the process of completing RoPAs.<br><br>Cyera can help inform the process of performing Data Protection Impact Assessments by creating an inventory of your organization's personal data and analyzing the impact of security configuration changes on sensitive data.<br><br>Cyera's Data Risk Assessment and AI Risk Assessment services can also help surface data security risks - in particular those associated with AI deployments - and recommend strategies for mitigating risk, including timelines and milestones. |
| **Data Protection Impact Assessments**<br>When required by the relevant authorities, controllers must prepare a Data Protection Impact Assessment (DPIA) that will include:<br>• A description of the types of data collected;<br>• The method used for the collection;<br>• The methodology used for assurance of information security; and<br>• The controller's analysis of the measures, safeguards, and other risk mitigation mechanisms it has adopted. | |

| LGPD Requirements | Cyera Capabilities |
| --- | --- |
| **Appointment of Data Protection Officer**<br>Controllers must appoint a Data Protection Officer and provide their contact information to the public. | While it is each organization's responsibility to appoint a DPO or other responsible person for data protection, Cyera can provide services - such as its Data Risk Assessment, Breach Readiness, or AI Risk Assessment - to help those persons better understand the organization's data security posture and develop a plan for improving your security posture going forward, including timelines and milestones. |
| **Data Security Controls**<br>Organizations must implement appropriate technical, organizational, and administrative controls to protect the confidentiality, integrity, and availability of data subjects' personal data. | Cyera's data security platform discovers and classifies personal data across cloud and on-prem resources. It can identify unencrypted personal data at rest or in motion, and apply policies to obfuscate unencrypted data and alert data owners to take remedial actions.<br><br>Cyera integrates with identity providers like Okta to create a catalog of identities with access to your data estate, including internal and external users. Cyera can identify stale or ghost identities that should no longer have access, and can see which entities have disabled multifactor authentication.<br><br>Cyera's AI Guardian (including AI Security Posture Management and AI Runtime Protection) can identify embedded AI apps, homegrown AI tools, and public AI apps in use in your organization, and enforce policies to prevent AI from ingesting sensitive data, as well as blocking sensitive data from leaking through AI outputs.<br><br>Through its integration with Cohesity, Cyera enhances your cyber resilience by helping you prioritize your backup policies based on the sensitivity and criticality of your data.<br><br>Finally, Cyera offers a number of professional services - including its Data Risk Assessment, Breach Readiness, and AI Risk Assessment, that can help you evaluate the effectiveness of the technical and organizational measures you have implemented for data security. |

| LGPD Requirements | Cyera Capabilities |
| --- | --- |
| **Breach Notification**<br>Controllers must report significant breaches of personal data to the data subjects and the relevant authorities.<br>The notification must include:<br>• A description of the data affected;<br>• Information about the data subjects;<br>• The technical and security measures used at the time of the incident;<br>• Risks related to the incident;<br>• Reasons for delayed notification, if applicable; and<br>• Measures that have been taken to mitigate the impact of the incident. | Cyera's data security platform helps your organization simplify breach response by quickly identifying all impacted personal data - including unstructured personal data - generating reports and determining the materiality of a breach.<br>Cyera helps you protect data integrity and supervise third party processors by giving you visibility into which identities are accessing your data and what actions they have taken. |
| **Supervising Third Parties**<br>Operators must perform data processing in accordance with instructions provided by controllers.<br>Controllers must ensure that operators guarantee the security of data shared with them. | |


CYERA