CODE42

TECH OVERVIEW | PRODUCT

INCYDR PRIVACY BEST PRACTICES

Code42 is the leader in Insider Risk Management, allowing organizations to protect corporate data from loss, leak and theft and mitigate insider threats without disrupting collaboration. We do this by detecting, collecting, preserving, analyzing and reporting on files and file activity. We believe our customers should benefit from cloud solutions without compromising their privacy and compliance requirements.

What data does Code42 collect?
The Code42 Incydr™ data risk detection and response product monitors all file activity. Incydr collects data pertaining to the creation, deletion, modification and movement of files, including browser upload activity, connected device activity, machine-generated file activity and metadata about other file transfer methods. Incydr also collects the contents of certain files.

Is this personal data?
Many jurisdictions consider data that is associated with a person to be personal data, even if that data alone may not identify a specific individual. Because all data collected by the Code42 Incydr product is associated with individual users, we consider all of the data to be personal data for compliance purposes.

Is this sensitive data?
Code42 is unaware of any regulatory regime that considers file activity data to be sensitive personal data. File contents may contain sensitive personal data, but because files are encrypted before transmission to Code42, we have no knowledge of which files may contain sensitive personal data.

Is the data encrypted?
Yes, all data collected by Incydr is encrypted in transmission and at rest.

Where is the data stored?
Code42 allows customers to choose the region where certain types of data are stored. File contents are stored in the data center you have configured for your backup destination. Code42 uses Amazon Web Services (AWS) data centers located in the United States or Ireland for storage of file activity data.

How does Code42 use the data?
Code42 collects only the data that is needed to provide our services, and we only use the data as described in our customer agreements. Code42 uses file activity data to provide you the services and to analyze, characterize, attribute and identify data loss events for generalized product improvements. Code42 uses file contents solely to provide you the services.

Does Code42 sell the data?
No. Code42 does not sell the data.

How long does Code42 keep the data?
File activity data is retained for a period of 90 or 30 days, depending on the Incydr subscription purchased. File contents are retained until the file is deleted from a user's endpoint device and then according to the retention period you have configured. File activity data that is part of a case and file contents of any user included in an active Legal Hold matter will not be deleted and will be retained indefinitely. Code42 permanently deletes all data at the end of your subscription.

Privacy compliance model

Data protection laws and regulations have comprehensive requirements, including how a service is used and the notice that must be provided to individuals whose personal data you're using. The same service can be used in both compliant or non-compliant manners. The Code42 Incydr product can be deployed, configured and used in a manner that enables you to comply with the requirements applicable to you. Below are some considerations for using Incydr.

This is provided for informational purposes only and not for the purpose of providing legal advice.
You should contact your attorney to obtain advice with respect to any particular information or situation.

Be transparent with your employees:

- Notify employees about your monitoring practices and the personal data being collected. You may consider providing notice in your acceptable use policy, your employee privacy policy, by adding a disclaimer to corporate devices or all of the above.
- Be explicit in the notice about what you're using the data for. Incydr is an Insider Risk Management solution to help secure your organization's data.
- Address your organization's policy on personal use of company devices. Should employees refrain from using company devices for personal use? Is personal use permitted but with the understanding that the devices are being monitored?
- Have a process to ensure employees read the notice, such as by requiring all employees acknowledge the policies on a periodic basis.

Limit access to Incydr data to employees who need access:

- Implement role-based access controls to limit who in your organization can access the data collected by Incydr and when. For example, access is only given to:
    - Security analysts who are using Incydr to manage insider risk.
    - Security managers, if required based on the insider risk activity.
    - Legal counsel, only if the insider risk activity requires legal advice.
    - HR specialist, only if the insider risk activity requires HR assistance.
- In each case, document the reasons for broadening access in the Cases functionality for a particular investigation.
- Consider implementing further controls to limit which security analysts are permitted to investigate which employees.
    - By position in the organization.
    - By geographic location of the employee.
- Use roles to only allow specific security members to view file contents during an investigation and to limit permissions based on business use cases.

Limit the data accessed to the least amount required for each step in an investigation:

- Establish guidelines for when an investigation will occur. For example, do you investigate every departing employee? Every activity that triggers an alert?
- Focus the initial investigation on the file activity data and not the contents of the file. Roles can be used to limit who has access to file contents, but considering implementing policies for when security users should access file contents during an investigation and limit to only investigations that warrant it.

Limit use of the data for the security purposes communicated to employees:

- Incydr is a data detection and response product. It collects data to be used for security purposes.
- Unless the file activity itself is a violation of a security policy, the data is not collected for purposes of managing employee performance.

Consider whether certain groups of employees require additional steps:

- Consider requiring permission from a privacy specialist before accessing file contents of an employee in a jurisdiction with stringent privacy laws (ex. the European Union.)
- Consider asking the employee for permission before accessing file contents.

Train and audit administrators to ensure compliance:

- Train all employees who will have access to data. Training may include:
  - Applicable data privacy laws and regulations.
  - Operating procedures for using Incydr, including guidelines for acceptable and unacceptable use of Incydr and the data collected.
- Just as security teams use Code42 Incydr to ensure employees are not putting the organization's data at risk (intentionally or inadvertently), security management should review the Incydr audit logs to ensure security analysts are following your organization's procedures.

Learn more about getting started with insider risk management.

CODE42

Corporate Headquarters
100 Washington Avenue South
Minneapolis, MN 55401
612.333.4242
code42.com

Code42 is the leader in insider risk detection and response. Native to the cloud, Code42 rapidly detects data loss, leak, theft and sabotage as well as speeds incident response – all without lengthy deployments, complex policy management or blocking employee productivity. With Code42, security professionals can protect corporate data and reduce insider risk while fostering an open and collaborative culture for employees. Backed by security best practices and control requirements, Code42's insider risk solution can be configured for GDPR, HIPAA, PCI and other regulatory frameworks.

More than 50,000 organizations worldwide, including the most recognized brands in business and education, rely on Code42 to safeguard their ideas. Founded in 2001, the company is headquartered in Minneapolis, Minnesota, and backed by Accel Partners, JMI Equity, NEA and Split Rock Partners. Code42 was recognized by Inc. magazine as one of America's best workplaces in 2020. For more information, visit code42.com, read Code42's blog or follow the company on Twitter. (OV2105266)