PRODUCT OVERVIEW

Code42 Incydr & Data Privacy

Code42 Incydr is a data loss and insider threat protection solution, allowing organizations to see and stop corporate data leakage and theft without disrupting employees. 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.

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.

WHAT DATA DOES CODE42 COLLECT?

The Code42 Incydr product monitors all file activity and collects data pertaining to the modification and movement of files. This includes endpoints, browsers, cloud, and metadata about other file transfer methods (“File Event Data"). Code42 Incydr also collects the contents of exfiltrated 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 Incydr 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 Event 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 uses Amazon Web Services (AWS) data centers for storage of customer data. Customers can choose to have their data stored in a data center located in the United States or Ireland.

ARE THERE CROSS-BORDER DATA TRANSFERS?

Code42 operates in the United States. Depending on where a customer is located, there may be cross-border data transfers. A customer can elect for their data to be stored in Ireland; however, data may still be transferred to the United States as part of a support engagement.

Our Data Processing Addendum incorporates Standard Contractual Clauses for transfers of personal data from the EEA, UK, and Switzerland.

HOW DOES CODE42 USE THE DATA?

Code42 collects only the data that is needed to provide the services and uses the data only as described in our customer agreements. Code42 uses File Event Data to provide the services and analyzes it along with usage data for generalized product improvements. File contents are used solely to provide you the services and not for Code42's internal purposes.

DOES CODE42 SELL THE DATA?

No. Code42 does not and will not sell any customer data.

HOW LONG IS DATA RETAINED?

Customer data is only retained for a limited period (i.e. 30 days, 90 days, etc.) dictated by the product plan purchased. Data can be retained for longer if a customer uses the Cases feature. Data associated with a Case is retained for between 90 and 365 days, based on the product plan.

All customer data is permanently deleted once a customer no longer has an active subscription.

CODE42 PRIVACY CERTIFICATIONS

Code42 is currently certified under the following:

- EU-US Data Privacy Framework
- Swiss-US Data Privacy Framework
- UK Extension to the Data Privacy Framework
- APEC Privacy Recognition for Processors

PRIVACY COMPLIANCE GUIDANCE

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. Code42 enables you to deploy, configure, and use the Code42 Incydr product in a manner that enables you to comply with the requirements applicable to you. Below are some considerations for using Incydr in accordance with legal and/or organizational privacy requirements.

Be transparent

- Notify your employees about your organization’s monitoring practices and about the data being collected.
- Notice can be included in an acceptable use policy, employee privacy policy, and/or a login banner.
- Be explicit about how you’re using the data. Incydr is a data loss and insider threat protection solution that collects data to help protect your organization’s data.
- Address your organization's policy on personal use of company devices.
  - Should employees refrain from using their company device for personal use?
  - Are employees permitted to use company devices for personal use but with the understanding that devices are monitored?
- Ensure employees read the notice, such as by requiring all employees to review and acknowledge the policies on a periodic basis.

Limit access to the data

- Implement access controls. Use Roles for Incydr to limit who in your organization can access the data.
- Determine who and when others in the organization should be given access. For example:
  - Security analysts who are using Incydr to manage insider risk.
  - Security managers, if required based on the security event.
  - Legal counsel, only if the activity requires legal advice.
  - HR specialist, only if the insider 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 of your security analysts are permitted to investigate which employees.
  - By position in the organization
  - By geographic location of the employees.

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

- Establish guidelines for when an employee investigation will occur.
  - Do you investigate every departing employee?
  - Do you investigate every activity that triggers an alert?
- Focus the initial investigation on the File Event Data. Only permit analysts to open file contents if and when the File Event Data warrants further investigation into the file contents.

Only use the data for security purposes

- Incydr is a data detection and response solution. It collects data to be used for security purposes only and is not intended for monitoring employee performance.
- Unless the file activity itself is a violation of the organization’s security policy, the data should not be collected and used for purposes of managing employee performance.

Consider whether certain groups of employees require additional steps

- Establish a policy where permission from legal or privacy is required before an analyst can access 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.

Training and audit compliance

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