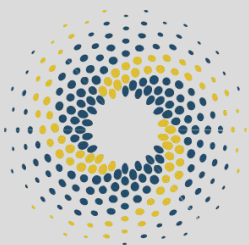




# Data Protection Overview

Safeguarding Your Data  
with Advanced Security  
Measures



**4impactdata**

# Table of Contents

- 1** Introduction to Data Protection at 4impactdata
- 2** Key Data Protection Methods
- 3** Key Data Protection Methods: Data Transit Security, Separation of Information & Data Deletion
- 4** Key Data Protection Methods: File Handling Process, Power BI Security & Data Usage
- 5** 4ID Compliance
- 6** 4ID Architecture
- 7** 4ID Process
- 8** Frequently Asked Questions (FAQ)
- 9** Frequently Asked Questions (FAQ)
- 10** Conclusion



# Introduction

- At 4impactdata, we prioritize the security and privacy of our clients' data.
- As a business guidance system leveraging AI, our data protection methods are designed to safeguard sensitive information through every stage of its lifecycle—whether in transit, at rest, or during processing.
- We are committed to implementing robust security protocols to ensure data integrity, confidentiality, and compliance with industry standards.



# Key Data Protection Methods

## 1. Azure Hardened Cloud Environment

- We utilize **Microsoft Azure**, which is SOC 1 Type 2 certified, for hosting our data. This ensures the highest level of security for infrastructure and data handling, with rigorous auditing and control standards.
- All data processed within our system is secured within the Azure framework, offering compliance with international security protocols and standards.

## 2. Anonymization of Data

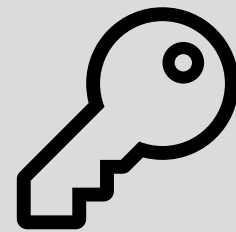
- All descriptive and identifying information is **anonymized both at rest and during processing** within the 4impactdata cloud. This means that even if data is accessed, it cannot be linked back to any individual or organization without the appropriate re-identification process.



# Key Data Protection Methods

## 3. Data Transit Security

- Data is encrypted in transit to ensure that any data transfers are protected from interception or unauthorized access.
- Only specific, authorized IP addresses and credentials are allowed to access our systems, reducing exposure to unauthorized parties.



## 4. Separation of Descriptive Information and Data

- To enhance security, **descriptive information and data are stored separately**. They are only joined together within the secure Power BI environment to generate insights. This further protects the integrity of the data and prevents unauthorized access to full datasets.

## 5. Data Deletion

- After processing, **all transit data and descriptive information are permanently deleted**, ensuring that there is no lingering risk of data exposure after it has been used.



# Key Data Protection Methods

## 6. File Handling Process

- Files are processed into the Azure environment where any descriptive information is removed.
- Data and descriptive information are stored in **different, secure locations** and only joined during analysis in the Power BI service, reducing the risk of data compromise during processing.

## 7. Power BI and Entity-Level Security

- We implement **row-level security (RLS)** within Power BI to ensure that only authorized users have access to specific data segments.
- **Azure/365 authentication protocols** further secure access, ensuring that only credentialed and verified users are able to interact with the data.

## 8. Data Usage and Deletion

- No payment card information is collected or stored by 4impactdata, and therefore **PCI DSS compliance does not apply** to our operations.
- We adhere to strict data management policies, ensuring that any processed data is securely deleted once it has served its purpose.





# 4ID Compliance



## Azure SOC Type 2

Power BI Service

Azure Cloud Service

## PCI DSS

Power BI Service

Azure Cloud Service

■ [System and Organization Controls \(SOC\) 1 Type 2 - Microsoft Compliance | Microsoft Learn](#)

■ [System and Organization Controls \(SOC\) 1 Type 2 - Microsoft Compliance | Microsoft Learn](#)

■ 4ID DOES NOT store any Payment Card Industry Data (PCI)





# 4ID Architecture

## 4ID Load Process



- All transit data and descriptive information is deleted after load.
- Data is anonymized at rest and during processing in 4ID Cloud.
- Identity is established in Power BI framework.

### 4ID Cloud – Azure Hardened Environment



Clean / Validate



Codify Wisdom



AI Enablement

### Power BI Service



Azure/365 Auth



Entity Row Level Security



Individual Custom Content



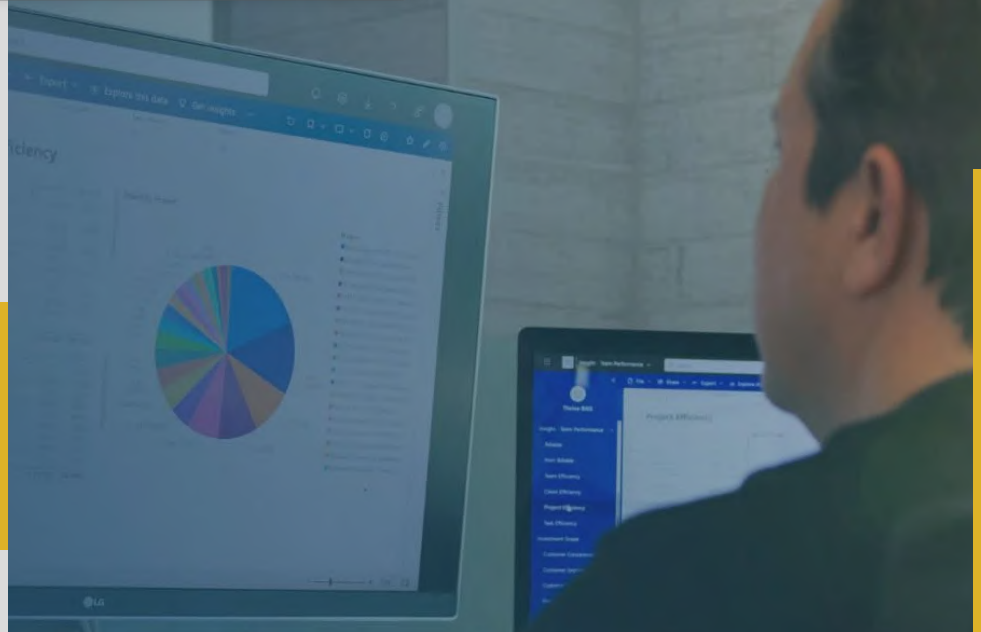
Individual AI Insight







# 4ID Process



## Data Load into 4ID

- Files Extracted
- Files Processed into Azure
  - Descriptive information Removed
  - Connections only accepted from Select known IPs and Credentials
- Files Deleted
- Descriptive Information and Data is stored in different locations

## Data Loaded into Power BI

- Data Loaded in several Stages
- Descriptive information and Data are loaded separately
- Data "Joined" with Descriptive information in Power BI Environment



# Frequently Asked Questions (FAQ)

## Q: How do you ensure my data is safe during transfer?

A: We use encryption for all data in transit, ensuring that it cannot be intercepted or accessed by unauthorized parties. Additionally, only specific, known IP addresses and credentials can access our system.

## Q: Is my data anonymized?

A: Yes, all descriptive and identifying information is anonymized at rest and during processing. This ensures that your data cannot be linked to your organization or individuals without proper re-identification protocols.

## Q: What happens to my data after it is used?

A: Once data processing is complete, all transit data and descriptive information are permanently deleted, minimizing the risk of data exposure.

## Q: Do you handle payment information, and are you PCI compliant?

A: We do not collect or process any payment card information, so PCI DSS compliance does not apply to our operations. Our focus is on the secure processing and handling of business-related data only.



# Frequently Asked Questions (FAQ)

## Q: What measures are in place to prevent unauthorized access?

A: We implement row-level security within Power BI and use Azure/365 authentication protocols to ensure that only authorized users with verified credentials have access to specific data sets.

## Q: How do you store and process data?

A: Descriptive information and data are stored separately and only joined during analysis in Power BI. Data is processed in stages, and all sensitive information is handled securely in Microsoft Azure's SOC 1 Type 2 compliant environment.

## Q: Are you compliant with international data protection standards?

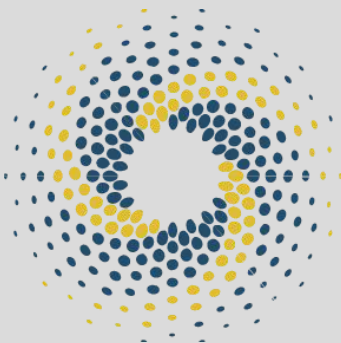
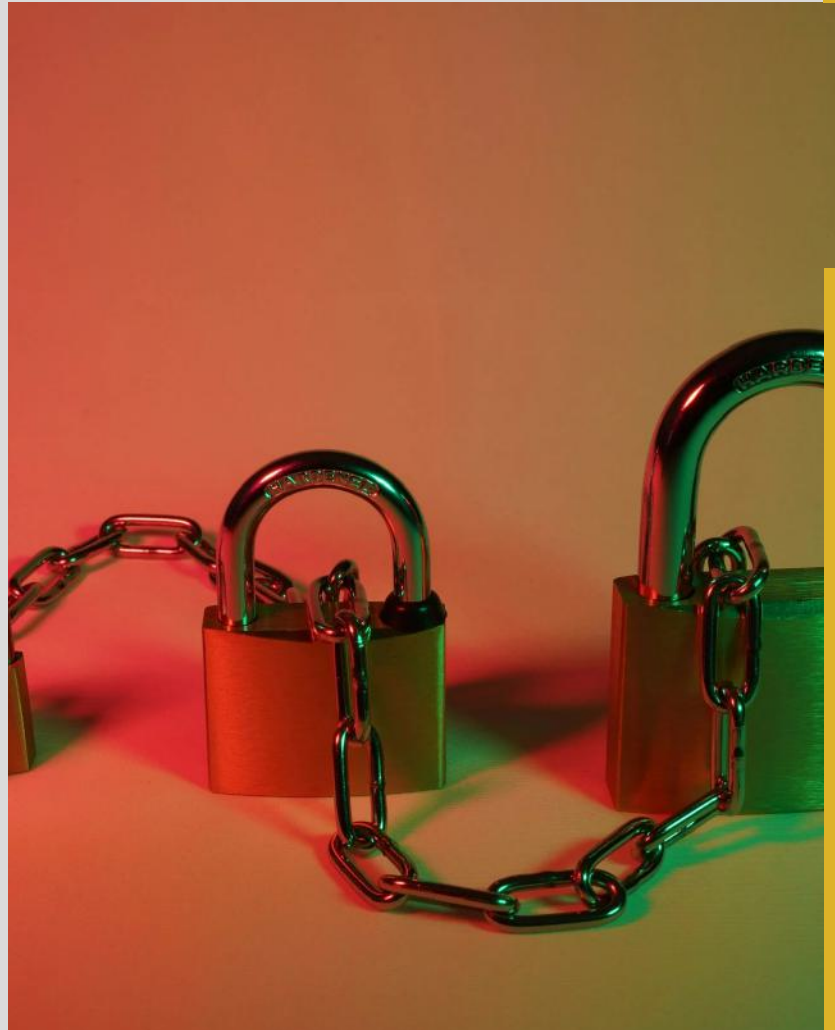
A: Yes, we utilize Microsoft Azure's SOC 1 Type 2 certification to ensure our infrastructure and data management practices comply with stringent international security standards.



# Conclusion

By utilizing these methods, 4impactdata ensures that all client data is handled with the utmost care and security, providing peace of mind to all stakeholders.

If you have any additional concerns or questions, feel free to reach out to our team for more information.



# 4impactdata

