# TyDIDs

A user-friendly JavaScript library for easy implementation of secure Self-Sovereign Identity and Consent Management, featuring strong encryption and decentralized control.

# Introduction

**In the world of Ethereum blockchain transactions, it's important to verify the identity of the person signing the transactions. To meet Know Your Customer (KYC) requirements, we need a way to prove that the person behind an Ethereum account is who they claim to be. Our service provides a solution by allowing individuals to use their eID card to sign their Ethereum account, creating a verified link between their identity and their blockchain transactions. This ensures that third parties can trust the identity of the account holder, even when interacting through smart contracts on the Ethereum network.**

# Use Case: John the Freelancer

John is a freelance developer who often engages in projects with various companies. Recently, he started working with Acme Corp., a company that specializes in creating decentralized applications on the Ethereum blockchain. As part of his contract, John needs to sign a smart contract to receive his payments and other project-related transactions.

Acme Corp. has strict KYC requirements to ensure the authenticity of their collaborators. To meet these requirements, John uses Tydids that allows him to link his real-world identity to his Ethereum account using his eID card.

1. **Setup and Verification:**
   - John logs into Tydids and uses his eID card to digitally sign his Ethereum account. This process securely binds his verified personal identity to his Ethereum address.
   - The service generates a digital certificate that confirms John's identity and associates it with his Ethereum account.
2. **Signing the Smart Contract:**
   - John accesses the smart contract provided by Acme Corp. through their decentralized application.
   - Before signing the contract, the application prompts John to prove his identity using the digital certificate generated by the Tydids service.
   - John selects his verified Ethereum account and uses his eID card to sign the transaction. This action confirms his identity to Acme Corp.
3. **Transaction Execution:**
   - The smart contract on the Ethereum blockchain receives John’s signed transaction along with his identity verification.
   - Acme Corp.’s smart contract validates the digital certificate and confirms that the transaction is indeed from John.
   - Once verified, the smart contract executes the transaction, ensuring John receives his payment and any other agreed-upon benefits.

4. **Trust and Security:**
    - Acme Corp. is assured that the person signing the transaction is truly John, fulfilling their KYC requirements.
    - John can now seamlessly continue his work with Acme Corp., knowing his identity is securely verified on the blockchain.

By using this Tydids  verification service, John and Acme Corp. can engage in secure, trusted transactions on the Ethereum blockchain, enabling efficient collaboration and compliance with KYC regulations.

# Use Case: Alice sells CO2 savings

Alice is an environmentally conscious homeowner who has installed a rooftop solar PV system to generate electricity. By doing so, she reduces CO2 emissions, contributing to a cleaner environment. Alice has accumulated significant CO2 savings and wants to sell these savings to Acme Corp., a company with a Corporate Social Responsibility (CSR) directive to lower its Scope 2 emissions.

To facilitate this transaction and ensure that Acme Corp. remains audit-safe and compliant, a smart contract on one of the Ethereum based blockchain is used. This contract handles the "deal" between Alice and Acme Corp., ensuring transparency and anonymity while providing the necessary validation for Acme Corp.'s audits.

1. **Generating CO2 Savings:**
    - Alice’s rooftop solar PV system continuously generates electricity, reducing her reliance on grid power and saving CO2 emissions.
    - The total CO2 savings are recorded and verified through a trusted environmental monitoring service, which provides a digital certificate of the savings.
2. **Setting Up the Smart Contract:**
    - Acme Corp. posts an offer on an Ethereum blockchain to buy verified CO2 savings to meet their CSR goals.
    - Alice sees the offer and decides to sell her verified CO2 savings to Acme Corp.
    - Both Alice and Acme Corp. agree to the terms of the deal through a smart contract. The contract specifies the amount of CO2 savings, the price, and the verification requirements.
3. **Identity Verification:**
    - To ensure compliance and audit readiness, Alice uses her eID card to sign her Ethereum account. This verifies her identity without revealing it publicly on the blockchain.
    - Acme Corp. also uses its verified Ethereum account to sign the smart contract, ensuring both parties are authenticated without exposing their identities.
4. **Executing the Transaction:**

- The smart contract on the Ethereum blockchain executes the deal once Alice’s CO2 savings are verified.
- The digital certificate proving Alice’s CO2 savings is linked to the transaction, ensuring that Acme Corp. can later prove the source of their CO2 reductions.
- The agreed-upon payment is transferred from Acme Corp.’s Ethereum account to Alice’s Ethereum account.

5. **Transparency and Anonymity:**
   - The transaction details, such as the amount of CO2 savings and the payment, are recorded on the Ethereum blockchain, ensuring transparency.
   - However, the actual identities of Alice and Acme Corp. remain anonymous to the public. Only Alice and Acme Corp. know each other's real-world identities.
6. **Audit and Compliance:**
   - Acme Corp. can now use the verified CO2 savings to report lower Scope 2 emissions, fulfilling their CSR requirements.
   - During an audit, Acme Corp. can present two key documents to streamline the process:
     - The blockchain transaction record, which details the CO2 savings transaction.
     - A PDF document proving Alice's identity, linked to the digital certificate used in the transaction.
   - This simplified documentation makes the audit process more efficient, ensuring compliance with minimal paperwork.

By using this system, Alice can monetize her environmental contributions, and Acme Corp. can meet their emission reduction targets in a transparent, anonymous, and compliant manner, with streamlined audit processes.

# Use Case: KYC Validation on an existing customer base

Acme Corp. is a global company with a diverse customer base. To comply with international regulations, Acme Corp. needs to ensure the strong eValidation of all their customers. Currently, every customer is assigned a unique customer number, but this alone is not sufficient for compliance.

To address this, Acme Corp. implements a new process to validate customer identities securely and efficiently.

1. **Customer Onboarding:**
   - Acme Corp. informs its customers about the new identity validation process.
   - Each customer is given a unique URL to initiate their eValidation. The URL contains the customer’s unique number, ensuring that the validation process is linked to the correct account.
2. **Initiating eValidation:**

- When a customer logs into their account on Acme Corp.’s website, the system automatically generates and displays a personalized eValidation link.
- For example, for a customer with the number 1337, the URL would be automatically generated as: `https://tydids.com/?return_to=https%3A%2F%2Facme.com%2Fvalidation%3FcustomerID%3D1337&key_1=customerID&value_1=1337`.
- The customer simply needs to click on the provided URL without needing to manually replace any part of it.

3. **Validation Process:**
   - The customer clicks on the provided URL and is redirected to the eValidation service of tydids.
   - At `tydids.com`, the customer undergoes an identity verification process, in form of a eID verification and signing.
4. **Completion of eValidation:**
   - Once the eValidation process is completed successfully, the customer is redirected back to Acme Corp.'s validation endpoint.
   - The URL for the redirection will look like this: `https://acme.com/validation?customerID=1337&validationID=abc123`, where `abc123` is the unique validation ID generated during the eValidation process.
5. **Processing the Validation at Acme Corp.:**
   - Acme Corp.’s system receives the validation ID along with the customer ID.
   - Acme Corp. uses the validation ID to retrieve the validation results from `tydids.com`, ensuring that the customer’s identity has been verified.
   - The customer’s account is then updated to reflect the successful validation, ensuring compliance with regulatory requirements.
6. **Benefits and Compliance:**
   - This process ensures that Acme Corp. has a robust and reliable method for verifying the identities of its global customer base.
   - The use of a unique customer number and validation ID ensures that the process is secure and that each customer’s identity is accurately verified.
   - During an audit, Acme Corp. can present  the verifications to streamline the process:
     - A PDF document proving the customer’s identity, linked to the digital certificate used in the transaction.
     - This simplified documentation makes the audit process more efficient, ensuring compliance with minimal paperwork.

By implementing this eValidation process, Acme Corp. can efficiently and securely verify the identities of their worldwide customers, meeting compliance requirements and enhancing trust in their customer database.

---

# Use Cases and Receipts

In this chapter, we will explore the best practices for working with the Tydids framework. Through practical examples and real-life scenarios, you will learn how to effectively use the framework’s validation and cryptographic processes. This chapter aims to equip you with the knowledge to seamlessly integrate Tydids into your projects, ensuring robust security and reliable performance.

# Lending a drilling machine

**In this scenario, Alice, a homeowner, wants to lend her drilling machine to Bob, a neighbor who needs to perform some home improvement tasks. To ensure transparency and trust, Alice will receive a digital receipt confirming that she has lend the drilling machine from Alice.**

## What should be achieved?

Transparency and trust between Alice and Bob about the lending of a drilling machine.

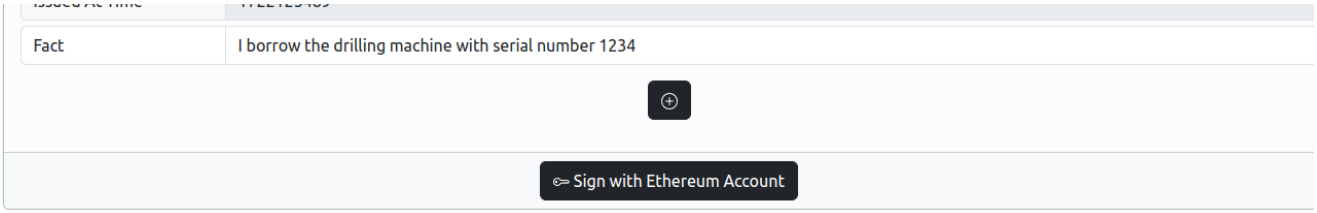
## What should not happen?

- Alice and Bob do not want to make their real identities transparent to others.
- The fact that it is a lending process should not be exposed.
- The fact that a drilling machine should not be exposed.

## How to do this?

For simplicity, both Alice and Bob know the ID of each other from the past. *(Hint: You get your ID by clicking on the upper right Icon. It will give your ID and allow you scanning the ID of someone else to see it).*

- Bob opens https://tydids.com/
- Creates a new validation
- Using the "+" adds a field named "Fact" with the value "I borrow the drilling machine with serial number 1234"




- Bob signs the validation and gets a PDF document that he will give to Alice.

- Alice opens the Verifier of Tydids and validates the signatures and gives the drilling machine to Bob.

## Important: Do only trust if you trust

Basic rule: "Zero Trust"

The example has a single point where trust is needed: It relies on the past/history knowledge of the IDs (=*consensus*).  But what if this does not exist? What if Bob just moved to the new house? A technical answer to this is "strong qualified signatures".

# Getting freelancer work signed off and paid

**Alice works for a multinational corporation and needs to sign a new consulting agreement with Bob, a contractor providing services to her company. The agreement outlines the terms of Bob's freelance work, and payment should be made directly to his designated wallet.**

## eIDAS in a Nutshell

The eIDAS (electronic IDentification, Authentication and trust Services) regulation simplifies secure electronic interactions within the European Union. It ensures businesses, citizens, and governments can interact digitally with standardized identification methods and trust services – all seamlessly working across EU member states. This regulation promotes trust in electronic transactions, fostering a more integrated digital market within the EU.

## Goal

To securely sign the consulting agreement in a way that can be verified by a third party if necessary.

## How to do this?

1. **Bob Prepares the Contract:** Bob creates and shares the contract electronically, attaching it to a validation request.
2. **Alice Signs the Contract:**
   - Alice visits https://tydids.com/.
   - She creates a new validation request.
   - Uploads the contract as a PDF document (using the "Attach" button).

- Signs the document electronically.
- To ensure highest security, she then uses the "Request eID validation" button to finalize the signing with her electronic ID (eID).

3. **Verification and Payment:**
   - Once signed, Alice shares the eID-validated document with Bob, who can view it under "Verifications" in the online system.
   - Upon confirmation of the agreement and completion of Bob's services, Alice's company uses the verified eID information to transfer the payment directly to Bob's designated wallet.

# How ACME Corp uses Self-Sovereign Identity (SSI) to give customers full control over their personal data

Showcase: https://energychain.github.io/tydids-validation/public/DataIdentity/

## Scenario

Experience how ACME Corp. uses Self-Sovereign Identity (SSI) to give you full control over your personal data. With SSI, you can manage and revoke consent anytime, ensuring compliance with GDPR and other privacy regulations.

## Key Benefits

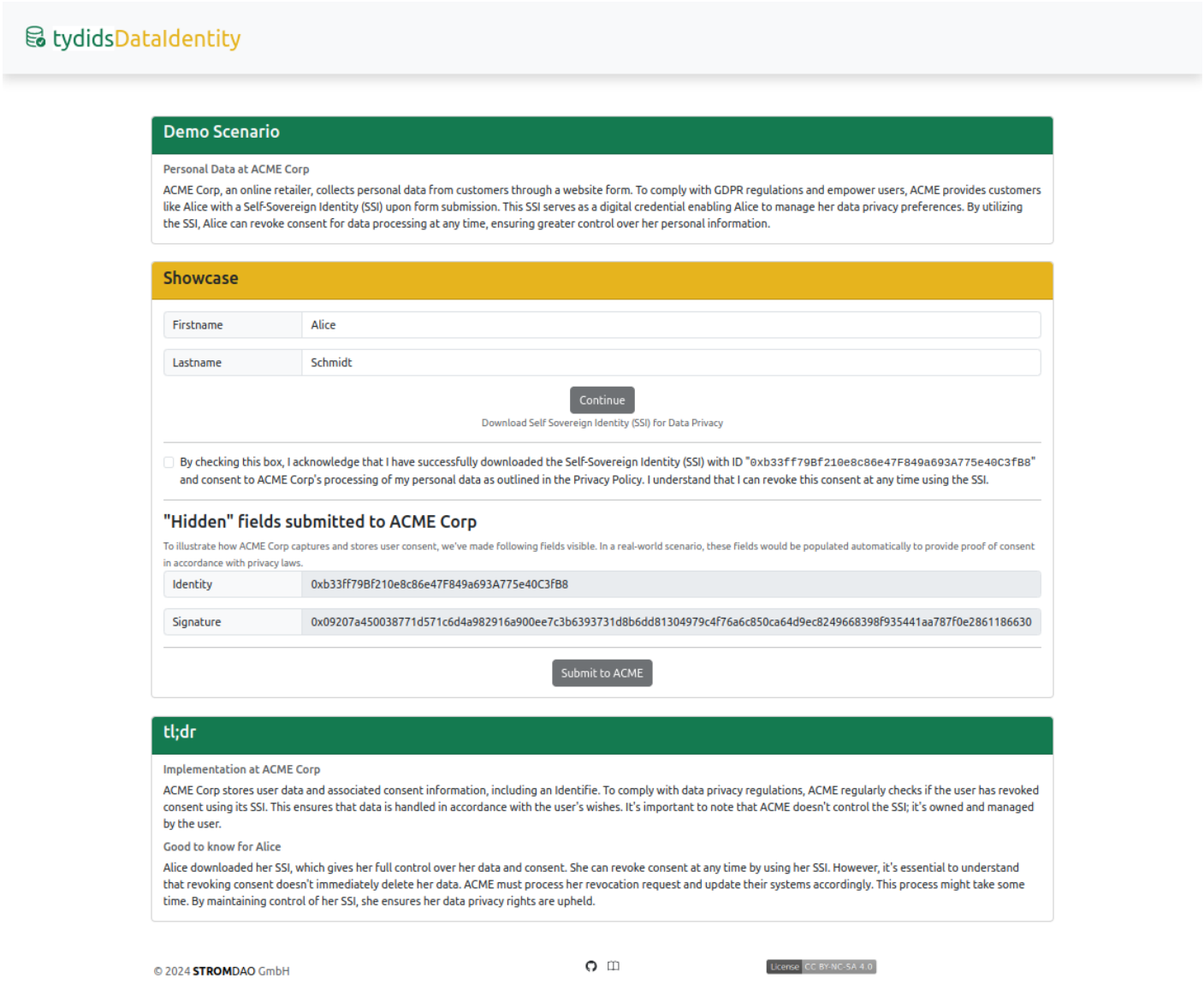
- **Full Data Control:** Download your SSI to manage consent preferences easily.
- **Privacy Compliance:** Ensure your data is handled according to GDPR and other privacy regulations.
- **User Empowerment:** Maintain ownership of your data and revoke consent at your discretion.
- **Seamless Integration:** ACME Corp. processes your revocation request efficiently, maintaining data privacy and security.

## Demo Instructions

1. **Download Your SSI:** Click "Download Self Sovereign Identity (SSI) for Data Privacy."
2. **Acknowledge and Consent:** Check the privacy checkbox to consent to ACME Corp.’s processing of your personal data.
3. **Submit Your Data:** Click "Submit to ACME" to see how your consent is securely handled.

# Why It Matters

By using SSI, you have unparalleled control over your personal information. Protect your privacy, ensure regulatory compliance, and experience the future of data consent management with TydidsDataIdentity.



# Check Grant Status via REST API

This document describes a simple REST API call to check the revocation status of a specific identity on Currently.io. This functionality is useful for organizations that implement the TyDIDS Trust Framework for GDPR compliance.

## API Endpoint

- **URL:** https://api.currently.io/v2.0/tydids/status?identity=<identity>
- **Method:** GET
- **Path Parameter:**
  - `<identity>`: Replace this with the identity you want to check the revocation status for. The identity is typically an SSI (Self-Sovereign Identity) identifier string.

## Response

The API responds with a JSON object containing information about the revocation status and consensus value. The HTTP status code of the response indicates the overall status of the request.

- **HTTP Status Code 200 (OK):**
  - **Body:**
    JSON

    ```
    {
      "status": "granted",
      "consensus": 40856
    }
    ```

    Verwende den Code mit Vorsicht.
  - **Description:** The identity has **not** revoked data approval.
    - `status`: String indicating the approval status. In this case, the value is `"granted"`.
    - `consensus`: Integer representing the number of the latest consensus reached at the time of the request.

- **HTTP Status Code 403 (Forbidden):**
  - **Body:**
    JSON

```
{
  "status": "revoked",
  "consensus": 40850,
  "revoked": 1722722789
}
```

    Verwende den Code mit Vorsicht.
  - **Description:** The identity has **revoked** data approval.
    - `status`: String indicating the approval status. In this case, the value is `"revoked"`.
    - `consensus`: Integer representing the number of the latest consensus reached at the time of the request.
    - `revoked`: Integer representing the timestamp (in Unix time) at which the approval was revoked.

# Example Usage

- **Checking an identity that has not revoked data approval:**
  - API Call:
    https://api.corrently.io/v2.0/tydids/status?identity=0x95Bee09c395c60883Fa8bb95F05404a71f7ee7F7
  - Response Body:
    JSON

```
{
  "status": "granted",
  "consensus": 40856
}
```

    Verwende den Code mit Vorsicht.
- **Checking an identity that has revoked data approval:**
  - API Call:
    https://api.corrently.io/v2.0/tydids/status?identity=0xa8CD7c57c144be63852Da3C44D97088A740D43Cd
  - Response Body:
    JSON

```
{
  "status": "revoked",
  "consensus": 40850,
  "revoked": 1722722789
}
```




# GDPR Compliance

Organizations implementing the TyDIDS Trust Framework for GDPR can use this API to regularly check the revocation status of identities. If an identity revokes data approval, the organization can take appropriate actions, such as stopping data processing or informing the user.

# Concept

Concept

# Traditional Data Collection

## Defining Sensitive Data

Understanding what constitutes sensitive data is fundamental for organizations aiming to comply with regulatory frameworks and ensure robust data protection. Sensitive data, as defined by various regulatory bodies, involves types of information that, if compromised, could lead to significant harm or discrimination against individuals. This chapter will delve into the specifics of sensitive data categories guided by the General Data Protection Regulation (GDPR) and other relevant frameworks.

- **Personal Information:** Names, addresses, email addresses, phone numbers, and other identifying details.
- **Financial Data:** Credit card numbers, bank account information, and transaction history.
- **Health Data:** Medical records, genetic information, and biometric data.
- **Biometric Data:** Fingerprints, facial recognition, and voice patterns.
- **Racial or Ethnic Origin:** Information about an individual's race, ethnicity, or nationality.
- **Political Opinions:** Information about an individual's political beliefs or affiliations.
- **Religious or Philosophical Beliefs:** Information about an individual's religion or philosophical beliefs.
- **Trade Union Membership:** Information about an individual's membership in a trade union.
- **Sexual Orientation:** Information about an individual's sexual orientation.
- **Criminal Convictions:** Information about an individual's criminal history.

## Traditional Data Collection Models

The methodologies for collecting sensitive data have evolved considerably over the years. Traditional data collection models serve as the foundation for understanding current practices and the inherent vulnerabilities that necessitate robust data protection measures. This chapter outlines some of the key traditional methods organizations have employed to gather and manage sensitive data.

- **Centralized databases**
  represent one of the earliest and most widely-used methods for data collection and storage:
  - **Single Repository**: Sensitive data is stored in a unified location, simplifying data management.

    - **Organizational Control**: The organization maintains direct control over data access and security measures.
    - **Advantages**: Simplifies data management, facilitates integrated analytics, and ensures consistent data governance.
    - **Disadvantages**: Presents a single point of failure, making it a prime target for cyberattacks and data breaches.
- **Data brokers**
  specialize in collecting and aggregating data from various sources to sell to third parties:
    - **Aggregated Data Sources**: These entities compile data from public records, online activities, purchases, and other available sources.
    - **Commercial Transactions**: Data is sold to businesses seeking targeted marketing, risk assessment, and other purposes.
    - **Advantages**: Provides organizations with extensive datasets without investing in their own data collection efforts.
    - **Disadvantages**: Raises ethical and privacy concerns, and often lacks transparency about data origins and consent.
- **Third-Party Data Collection**
  Relying on third-party services for data collection has become a common practice among organizations:
    - **Outsourced Services**: Third-party providers, such as analytics services and advertising platforms, collect data on behalf of the organization.
    - **Specialized Expertise**: These providers offer advanced tools and methodologies for efficient data collection and analysis.
    - **Advantages**: Reduces operational burden, leverages specialized expertise, and allows access to comprehensive data analytics tools.
    - **Disadvantages**: Complicates data governance, introduces dependency risks, and may engender compliance issues due to varying data protection standards.
- **Cookies and Tracking**
  Websites and applications often utilize cookies and tracking technologies to gather data on user behavior and preferences:
    - **Cookies**: Small text files stored on users' devices, tracking their online activities, preferences, and session information.
    - **Tracking Technologies**: Includes web beacons, pixels, and fingerprinting methods to monitor user interactions across multiple sessions.
    - **Advantages**: Enhances user experience through personalization, provides valuable insights for targeted marketing, and tracks user engagement.
    - **Disadvantages**: Invokes significant privacy concerns, necessitates transparent consent mechanisms, and faces increasing regulatory scrutiny.

# Data Lifecycle

Understanding the data lifecycle is crucial for organizations to manage sensitive data responsibly, ensuring privacy and compliance with regulatory frameworks. The data lifecycle encompasses various stages, each with its own set of processes and challenges. This chapter delves into the

typical stages of the data lifecycle and highlights a critical issue related to data collection and context retention.

1. **Collection:** Data is gathered from various sources, including user input, public records, and third-party providers.
2. **Storage:** Data is stored in databases, data warehouses, or other storage systems.
3. **Processing:** Data is analyzed, transformed, and used for various purposes, such as marketing, personalization, and decision-making.
4. **Sharing:** Data may be shared with third parties, such as business partners or service providers.
5. **Disposal:** Data is eventually deleted or anonymized when no longer needed.

**A critical issue arises at the very beginning of this lifecycle.** While data is often collected through specific interactions (e.g., filling out a form), the link to this original source is frequently lost. This means that data becomes detached from its context, making it difficult to trace its origin and for individuals to exercise control over its usage.

# Data Ownership and Control

In the traditional model, organizations typically assert ownership over the data they collect. This grants them significant control over data usage, sharing, and retention. Individuals have limited rights to access, modify, or delete their data.

# Privacy Concerns

Traditional data collection practices raise substantial privacy concerns:

- **Data Breaches:** Centralized databases are vulnerable to cyberattacks, potentially exposing sensitive information to unauthorized parties.
- **Unauthorized Access:** Employees, contractors, and third-party service providers may have access to sensitive data, increasing the risk of misuse.
- **Data Retention:** Organizations often retain data for extended periods, even when it is no longer necessary, creating ongoing privacy risks.
- **Lack of Transparency:** Individuals often lack visibility into how their data is collected, used, and shared.
- **Data Monetization:** The practice of collecting and selling user data for commercial purposes raises ethical concerns.

**The GDPR, among other regulations, has introduced stricter data protection measures.** It grants individuals specific rights, including the right to access, rectify, erase, and restrict the processing of their personal data. However, enforcing these rights can be challenging under traditional data collection models due to the lack of data traceability and control.

**To address these challenges, we propose a new approach based on the concept of Data Identities (DIDs).**

**A DID represents a unique identifier linked to a specific data collection event.** It acts as a container for associated data and provides individuals with granular control over their information. By establishing a clear link between data and its origin, DIDs enable greater transparency, accountability, and user empowerment.