# Bridging GDPR from your Application to your Cloud

Anton Aleksandrov
Chief Architect, IBM Cloud Application Identity

Gelareh Taban
Architect, IBM Cloud Application Identity

# Disclaimer

- **Notice: Clients are responsible for ensuring their own compliance with various laws and regulations, including the European Union General Data Protection Regulation. Clients are solely responsibility for obtaining advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulations that may affect the clients' business and any actions the clients may need to take to comply with such laws and regulations. The products, services, and other capabilities described herein are not suitable for all client situations and may have restricted availability. IBM does not provide legal, accounting or auditing advice or represent or warrant that its services or products will ensure that clients are in compliance with any law or regulation.**

- IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM's sole discretion.

- Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.

- The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract.

- The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.

**None of the statements contained herein constitutes legal advice – it is experience sharing only**

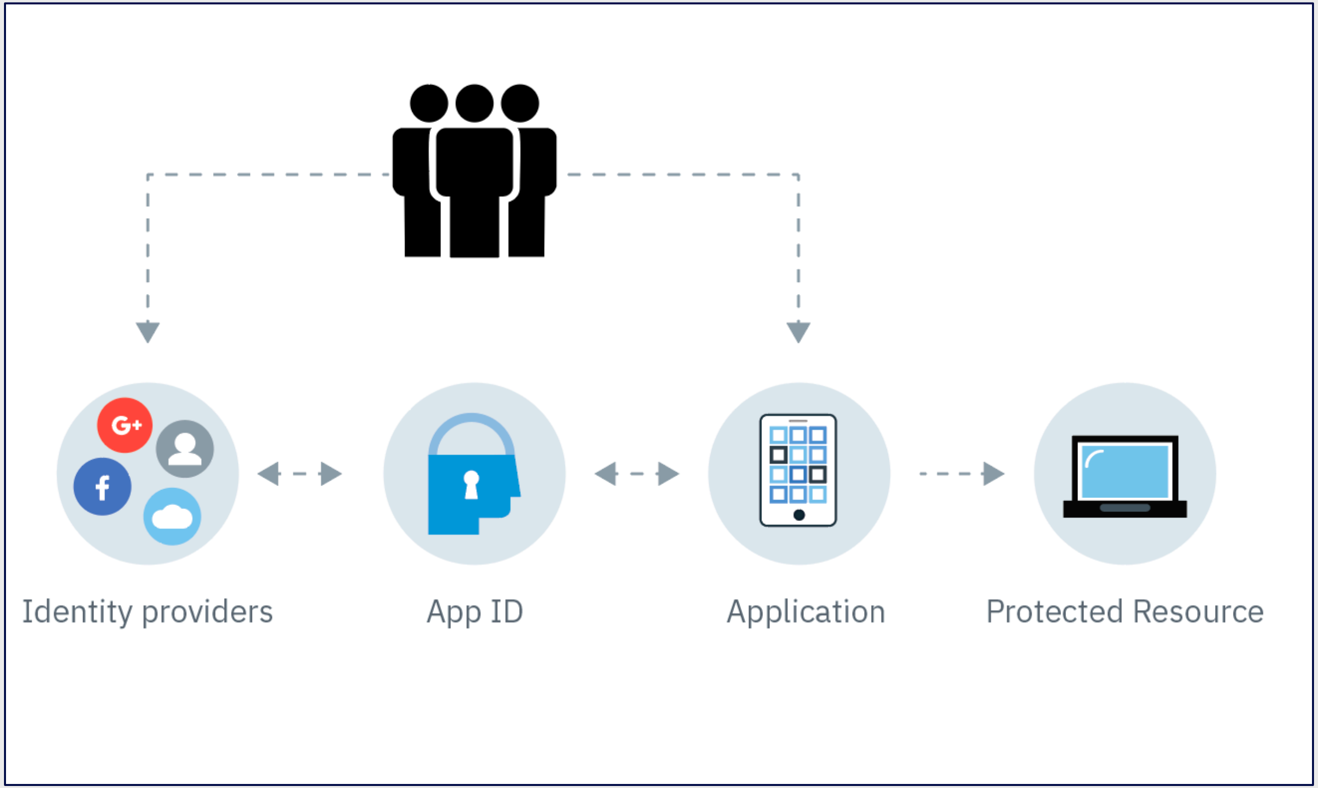
# Agenda

- Setting the context – 60 seconds overview of IBM Cloud Application Identity service
- What is GDPR?
- Terminology
- Key Issues
- Analysis of Personal Data
- Data Encryption
- Handling the Replicas
- Access Tracking
- Data Management
- Q&A

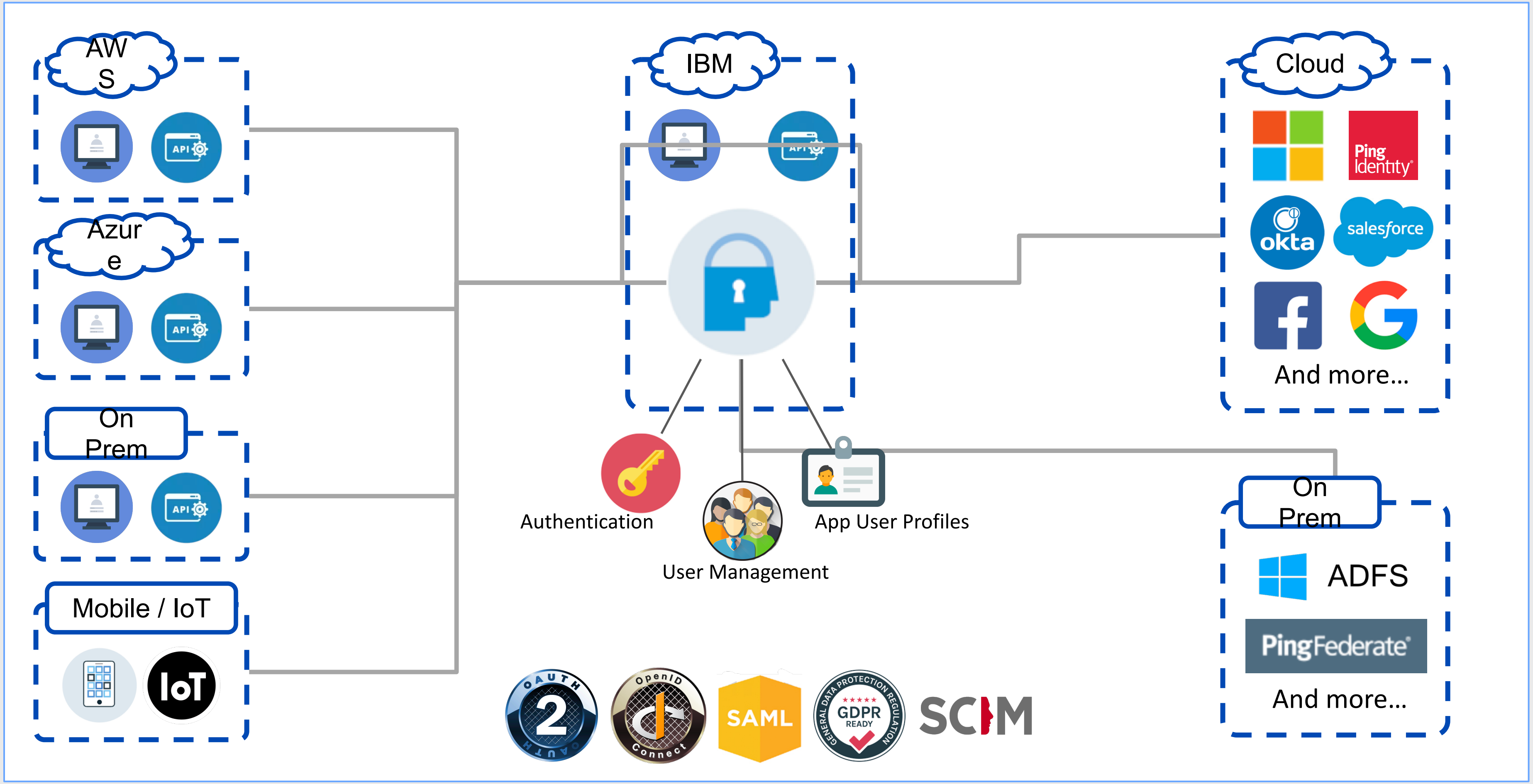
Anton Aleksandrov
Chief Architect, IBM Cloud Application Identity

Gelareh Taban
Architect, IBM Cloud Application Identity

# App ID in a nutshell

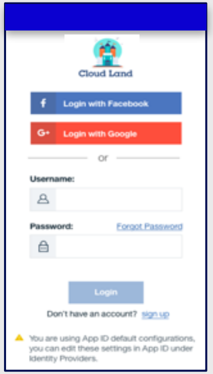


# App ID in a nutshell



# App ID Value to Developers of any app on any cloud

Add authentication to your mobile and web apps and protect your APIs and back-ends running on cloud. Add email/password based sign-up and sign-in with App ID's scalable user registry - Cloud Directory, or social log-in. For employee apps, use SAML 2.0 federation for enterprise sign-in. For all app users, enrich their profiles with additional info so you can build engaging experiences.



Don't have an account? sign up

You are using App ID default configurations, you can edit these settings in App ID under Identity Providers.

## Authentication

- Email/Password, Social sign-in, Enterprise sign-in
- Use Client SDKs for iOS and Android, Server SDKs for node.js and Swift, REST APIs called from any language, a customizable sign-in widget, and App ID starter app
- Secure your apps running on Kubernetes or your managed APIs with no code changes
- Open standards based (OAUTH2, OIDC, SCIM, SAML 2.0)

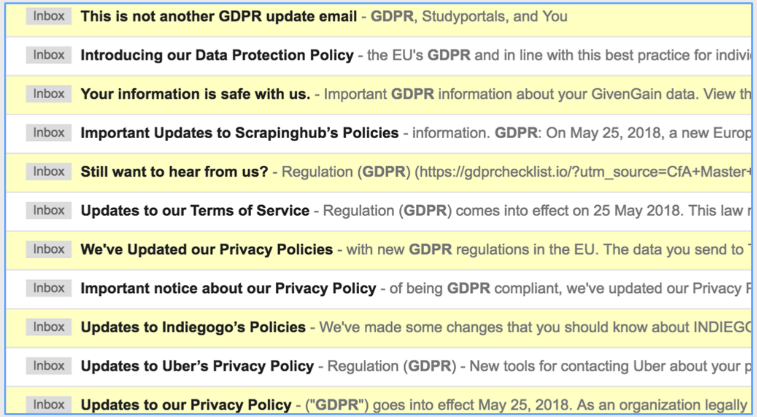
## User Management

- Sign-in, sign-up, email verification, change password, forgot password
- Default UI and flows, or replace with your own branding and custom flows
- Default email templates you can customize and brand

## Application User Profile Management

- Store end user data, like app preferences, to personalize app experiences
- Leverage data from user repositories, or add your own custom attributes
- Continuity for users who start out anonymously and sign-in later

# May 25th, 2018. Every inbox on the planet…



Inbox **This is not another GDPR update email** - **GDPR**, Studyportals, and You

Inbox **Introducing our Data Protection Policy** - the EU's **GDPR** and in line with this best practice for indivi

Inbox **Your information is safe with us.** - Important **GDPR** information about your GivenGain data. View th

Inbox **Important Updates to Scrapinghub's Policies** - information. **GDPR**: On May 25, 2018, a new Europ

Inbox **Still want to hear from us?** - Regulation (**GDPR**) (https://gdprchecklist.io/?utm_source=CfA+Master+

Inbox **Updates to our Terms of Service** - Regulation (**GDPR**) comes into effect on 25 May 2018. This law r

Inbox **We've Updated our Privacy Policies** - with new **GDPR** regulations in the EU. The data you send to T

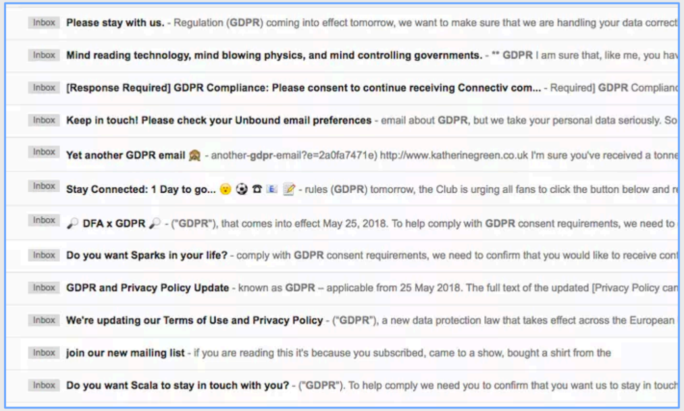
Inbox **Important notice about our Privacy Policy** - of being **GDPR** compliant, we've updated our Privacy P

Inbox **Updates to Indiegogo's Policies** - We've made some changes that you should know about INDIEGO

Inbox **Updates to Uber's Privacy Policy** - Regulation (**GDPR**) - New tools for contacting Uber about your p

Inbox **Updates to our Privacy Policy** - ("**GDPR**") goes into effect May 25, 2018. As an organization legally

(source - Business Insider South Africa)



Inbox **Please stay with us.** - Regulation (GDPR) coming into effect tomorrow, we want to make sure that we are handling your data correct

Inbox **Mind reading technology, mind blowing physics, and mind controlling governments.** - ** GDPR I am sure that, like me, you hav

Inbox **[Response Required] GDPR Compliance: Please consent to continue receiving Connectiv com...** - Required] GDPR Complianc

Inbox **Keep in touch! Please check your Unbound email preferences** - email about GDPR, but we take your personal data seriously. So

Inbox **Yet another GDPR email** 🙈 - another-gdpr-email?e=2a0fa7471e) http://www.katherinegreen.co.uk I'm sure you've received a tonne

Inbox **Stay Connected: 1 Day to go...** 😮 ⚽ ☎ 📧 📝 - rules (GDPR) tomorrow, the Club is urging all fans to click the button below and r

Inbox 🔎 **DFA x GDPR** 🔎 - ("GDPR"), that comes into effect May 25, 2018. To help comply with GDPR consent requirements, we need to

Inbox **Do you want Sparks in your life?** - comply with GDPR consent requirements, we need to confirm that you would like to receive cont

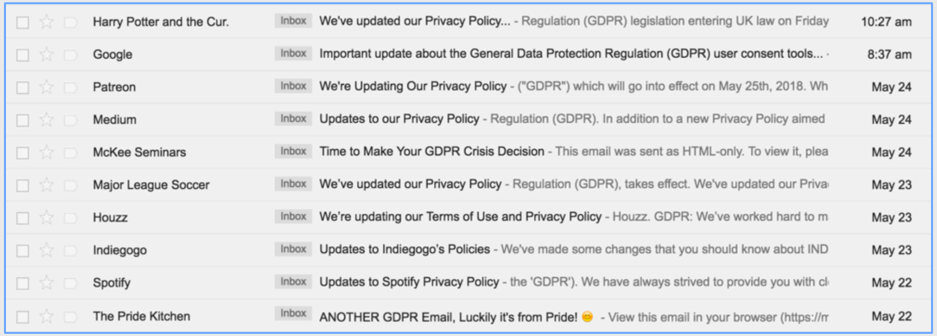
Inbox **GDPR and Privacy Policy Update** - known as GDPR – applicable from 25 May 2018. The full text of the updated [Privacy Policy can

Inbox **We're updating our Terms of Use and Privacy Policy** - ("GDPR"), a new data protection law that takes effect across the European

Inbox **join our new mailing list** - if you are reading this it's because you subscribed, came to a show, bought a shirt from the

Inbox **Do you want Scala to stay in touch with you?** - ("GDPR"). To help comply we need you to confirm that you want us to stay in touch

(source - The Guardian)



| | | | | |
|---|---|---|---|---|
| □ ☆ | Harry Potter and the Cur. | Inbox | We've updated our Privacy Policy... - Regulation (GDPR) legislation entering UK law on Friday | 10:27 am |
| □ ☆ | Google | Inbox | Important update about the General Data Protection Regulation (GDPR) user consent tools... - | 8:37 am |
| □ ☆ | Patreon | Inbox | We're Updating Our Privacy Policy - ("GDPR") which will go into effect on May 25th, 2018. Wh | May 24 |
| □ ☆ | Medium | Inbox | Updates to our Privacy Policy - Regulation (GDPR). In addition to a new Privacy Policy aimed | May 24 |
| □ ☆ | McKee Seminars | Inbox | Time to Make Your GDPR Crisis Decision - This email was sent as HTML-only. To view it, plea | May 24 |
| □ ☆ | Major League Soccer | Inbox | We've updated our Privacy Policy - Regulation (GDPR), takes effect. We've updated our Priva | May 23 |
| □ ☆ | Houzz | Inbox | We're updating our Terms of Use and Privacy Policy - Houzz. GDPR: We've worked hard to m | May 23 |
| □ ☆ | Indiegogo | Inbox | Updates to Indiegogo's Policies - We've made some changes that you should know about IND | May 23 |
| □ ☆ | Spotify | Inbox | Updates to Spotify Privacy Policy - the 'GDPR'). We have always strived to provide you with cl | May 22 |
| □ ☆ | The Pride Kitchen | Inbox | ANOTHER GDPR Email, Luckily it's from Pride! 😊 - View this email in your browser (https://r | May 22 |

(source – BookNet Canada)

# **G**eneral **D**ata **P**rotection **R**egulation – Simply… Why?

## Compliance

A single regulation to rule them all - policies, processes, organizational changes

## Data Protection

EU term for data security, encryption, access control, monitoring, reporting

## Personal Data

What is Personal Data, what companies can do with data, more controls to users, how's data collected and used

# GDPR – What is it?

The EU General Data Protection Regulation (GDPR) came into effect on **25 May 2018** and presented the biggest change in data privacy in two decades. The legislation aims to give control back to individuals located in the EU over their Personal Data and simplify the regulatory environment for international business.

May 25, 2018

Global Impact

4% or €20M

Potential penalty for non-compliance

## 5 Key General Data Protection Regulation Obligations

- Rights of EU Data Subjects
- Security of Personal Data
- Consent
- Accountability of Compliance
- Data Protection by Design and by Default

# GDPR – What is it?

The EU General Data Protection Regulation (GDPR) came into effect on **25 May 2018** and presented the biggest change in data privacy in two decades. The legislation aims to give control back to individuals located in the EU over their Personal Data and simplify the regulatory environment for international business.

May 25,
2018

Global
Impact

4% or €20M

Potential pena ty f n
compli

PER
INCIDENT !!
!

## 5 Key General Data Protection Regulation Obligat

- Rights of EU Data Subjects
- Security of Personal Data
- Consent
- Accountability of Compliance
- Data Protection by Design and by Default

# GDPR – Key Terminology

Data **Subject**

(Individual)

An identified or identifiable living natural person

Data **Controller**

(e.g. you/client)

Legal entity that determines the purpose and means of processing of Personal Data

Data **Processor**

(e.g. IBM)

Legal entity that processes Personal Data on behalf of the Controller

Personal Data

Any information relating to a Data Subject, regardless where it is stored

Processing

Any operation performed on Personal Data  (includes storage, access), anywhere in the world

Data Privacy

The rights of individuals to control how their public and non-public Personal Data is collected and used

Data Security

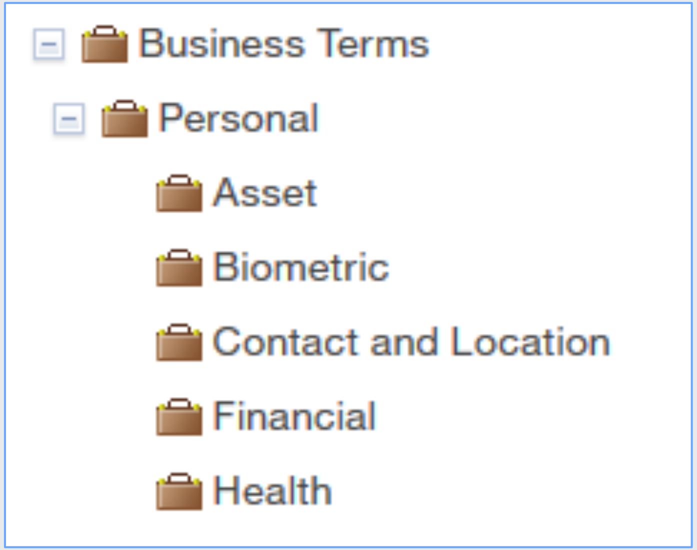
The protection of Personal Data against loss, unauthorized access, destruction, use, modification, disclosure etc == encryption, access controls etc.

Data Governance

Defines who can take what actions with what Personal Data, when, under which circumstances, and using what methods

# Personal Data ?

“*any information relating to an identified or identifiable natural person*” (Art. 2(a))



- Business Terms
  - Personal
    - Asset
    - Biometric
    - Contact and Location
    - Financial
    - Health

**Personal Data:**
an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

**Sensitive Personal Data:**
data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation. The commission or alleged commission by them of any offence; or any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

# The GDPR strengthens and unifies data protection across the EU

## Definition of “Personal Data”

- All Information relating to an identified or identifiable natural person
  - Behavioural-, derived- and self-identified data
  - Physical
  - Genetic
  - Cultural
  - Social
  - Economic
- Unstructured data
- Format and technology agnostic

## Enhanced, harmonized and extended rights for individuals located in the EU

- Inform / access / rectify / erase / object
- Give or withdraw data specific consent
- Insight in automatic decision making
- Transfer Personal Data to other provider (portability)

# Key Impacts of GDPR

## Organizational Impact

- Controllers and Processors liable for breaches
- Controllers legally bound to validate Processor’s compliance
- Data Protection Officer obligatory
- Stringent data security and breach management
- Processors jointly responsible for cross-border data transfers
- All relationships, transactions, and data flows must be transparent, documented, and auditable

## Increased cost of non-compliance

- Fines up to 4% of annual turnover or 20 million Euros (whichever is the greater)
- Data Privacy Authorities empowered
- Increased activist and court activity
- Risk / ¨Cost¨ of reputation loss

The GDPR applies to Controllers, and Processors located in the EEA. It also applies to Controllers and Processors located outside the EEA if they are processing Personal Data in relation to the offering of goods and services to individuals located in the EEA, or for purposes of monitoring their behavior.

# Key Issues

- Consent
- Data Protection Officer
- Email Marketing
- Encryption
- Fines / Penalties
- Personal Data
- Privacy by Design
- Privacy Impact Assessment
- Processing
- Records of Processing Activities
- Right of Access
- Right to be Forgotten
- Right to be Informed
- Third Countries

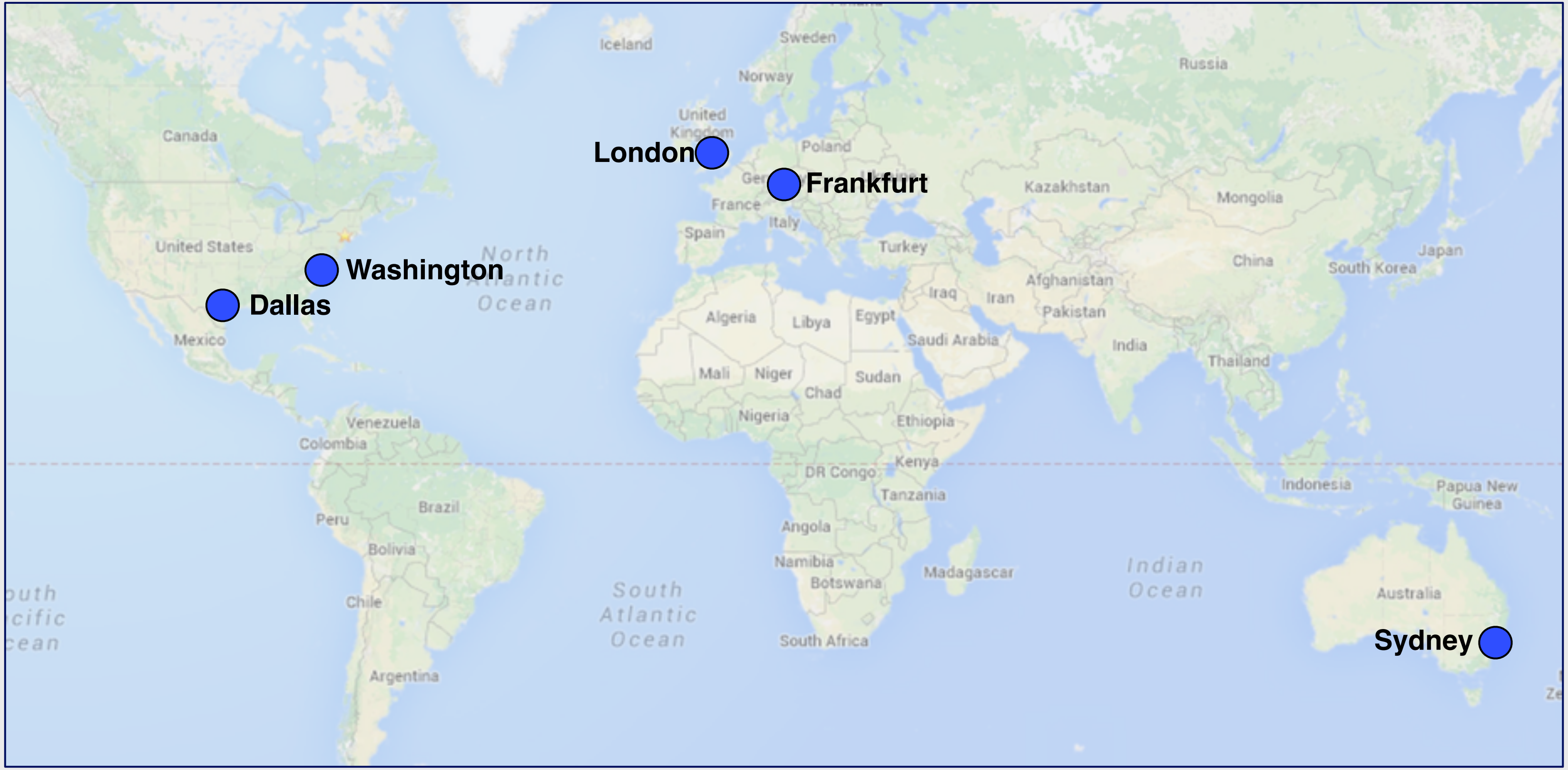
https://gdpr-info.eu/issues/

# Key Issues

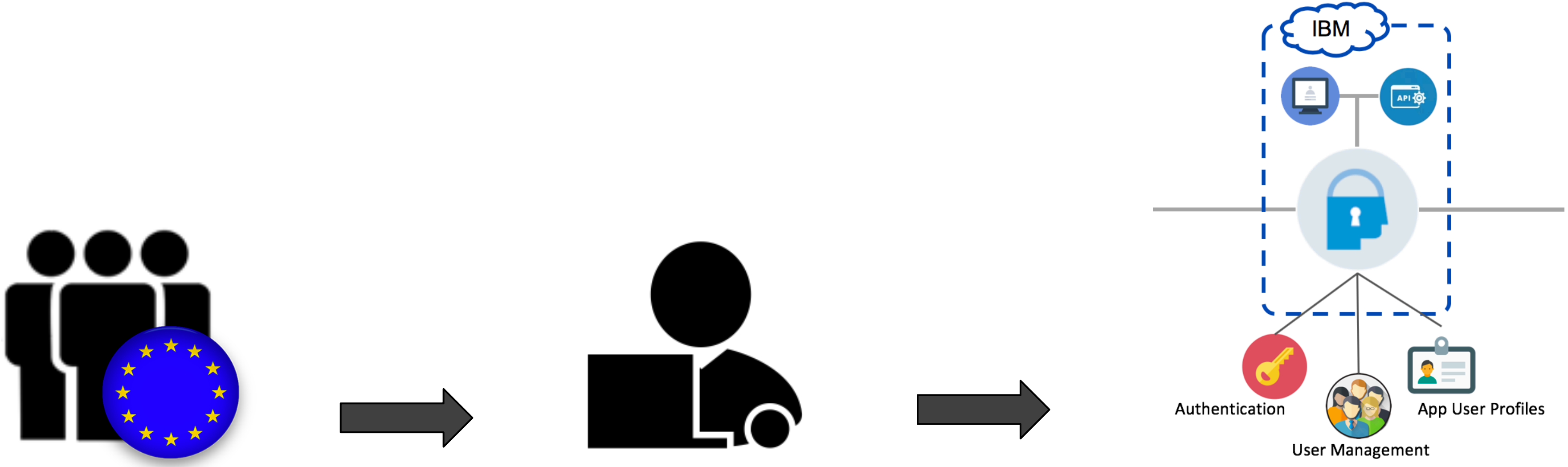
- Consent
- Data Protection Officer
- Email Marketing
- **Encryption**
- Fines / Penalties
- Personal Data
- **Privacy by Design**
- **Privacy Impact Assessment**
- Processing
- **Records of Processing Activities**
- **Right of Access**
- **Right to be Forgotten**
- Right to be Informed
- Third Countries

https://gdpr-info.eu/issues/

# Regional availability – data never leaves a particular region



# App ID – Data Controller or Data Processor?



**EU Citizen**

Personal Data

**App Developer**

Data Controller

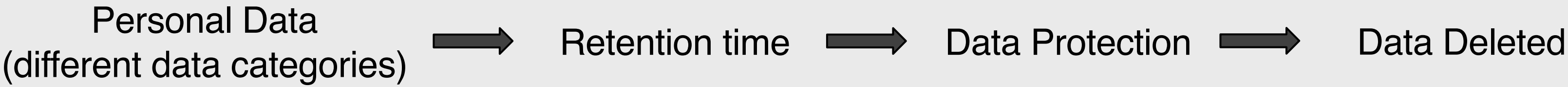
- Collect
- Manipulate

**App ID**

Data Processor

- Store
- Process

# Analysis of Personal Data



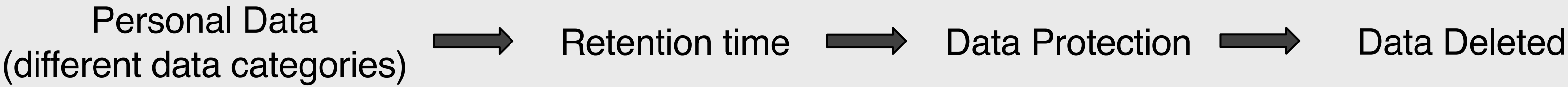
Personal Data
(different data categories)

Retention time

Data Protection

Data Deleted

# Analysis of Personal Data - Examples



Personal Data
(different data categories) → Retention time → Data Protection → Data Deleted

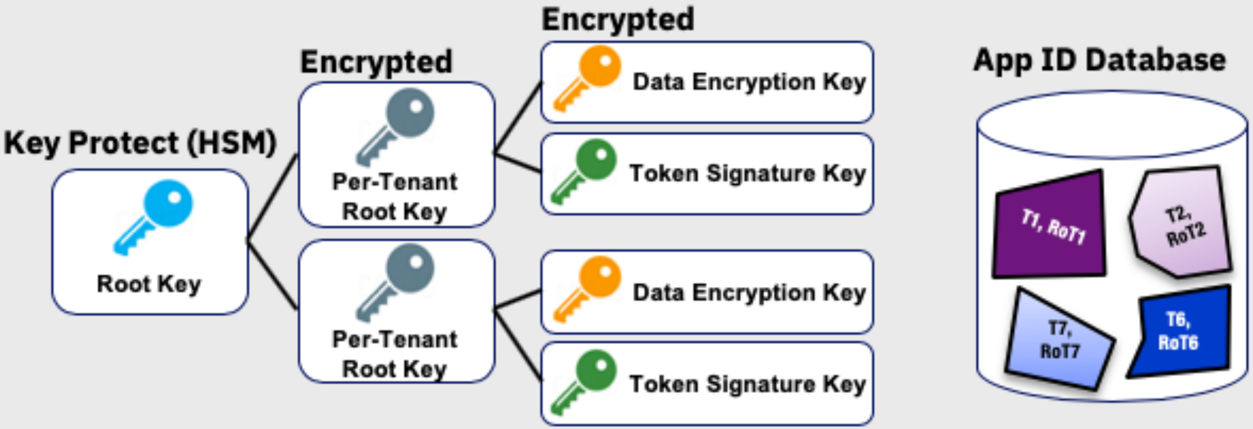
- User authentication info
- User account details
- Custom Attributes
- etc

Customer decision

- TLS in transit
- Field-level encryption at rest (more details to come)

- Delete APIs
- Cryptographic destruction

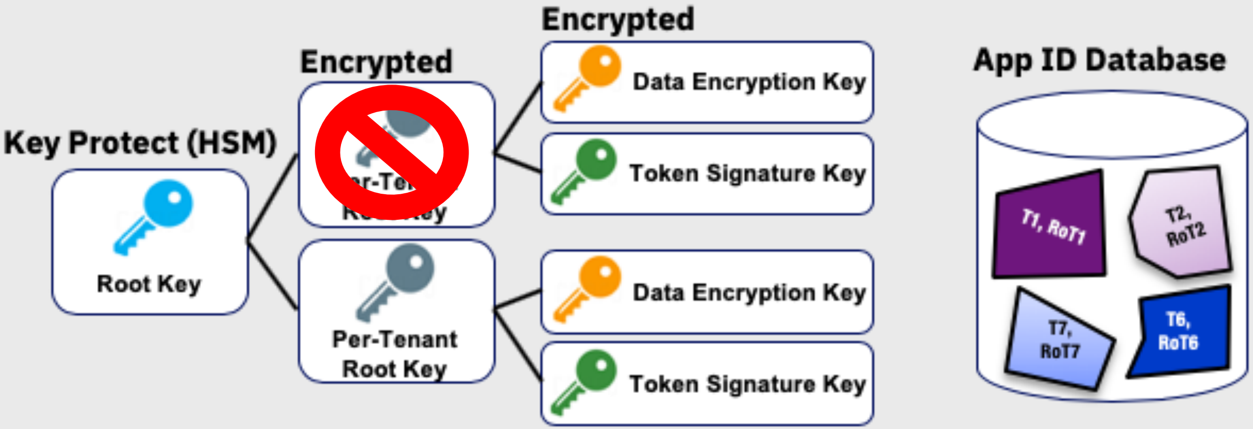
# Data protection at rest – Data encryption



Per-tenant

- key encrypting keys (KEKs)
- data encryption keys (DEKs)
- tokens signature keys (TSKs)
- cryptographic data isolation

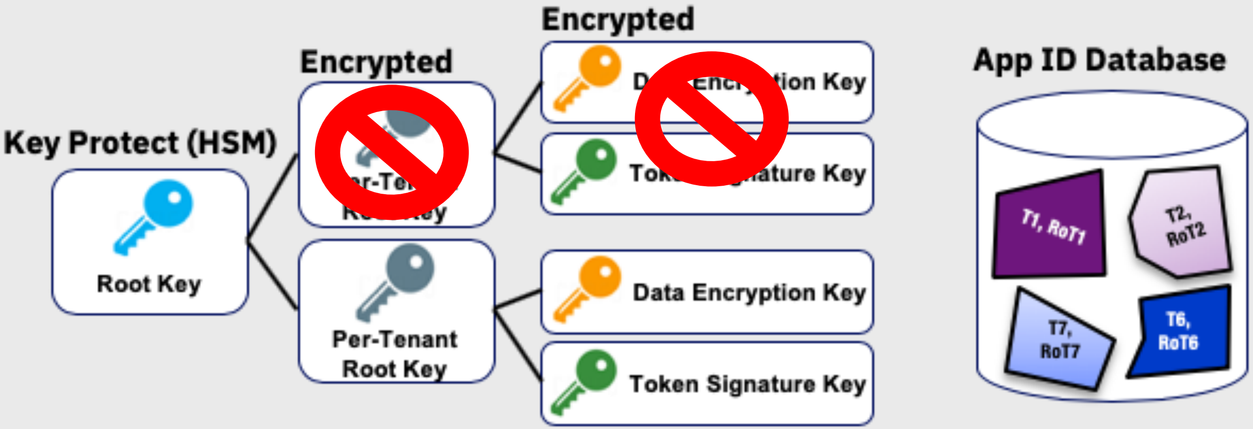
# Data protection at rest – Data encryption



Per-tenant

- key encrypting keys (KEKs)
- data encryption keys (DEKs)
- tokens signature keys (TSKs)
- cryptographic data isolation

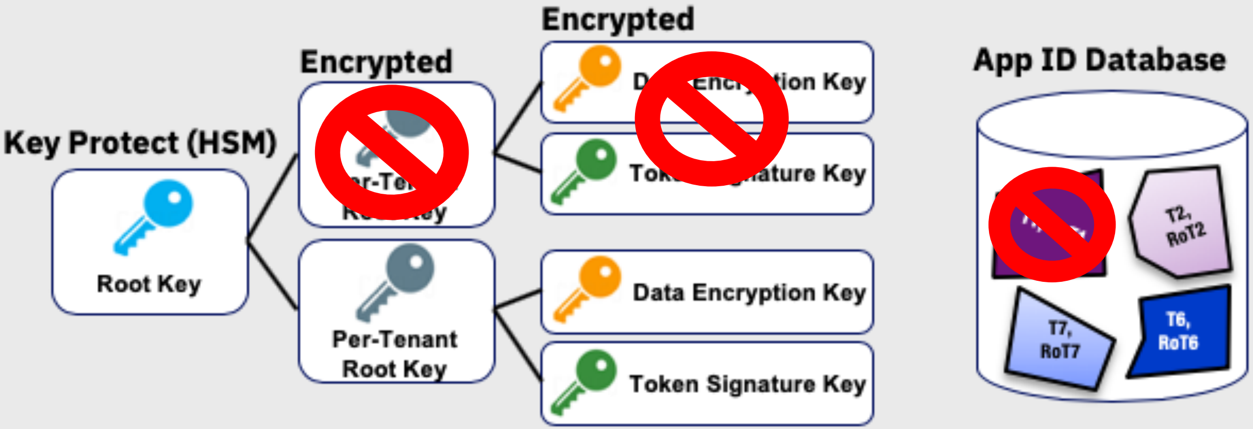
# Data protection at rest – Data encryption



Per-tenant

- key encrypting keys (KEKs)
- data encryption keys (DEKs)
- tokens signature keys (TSKs)
- cryptographic data isolation

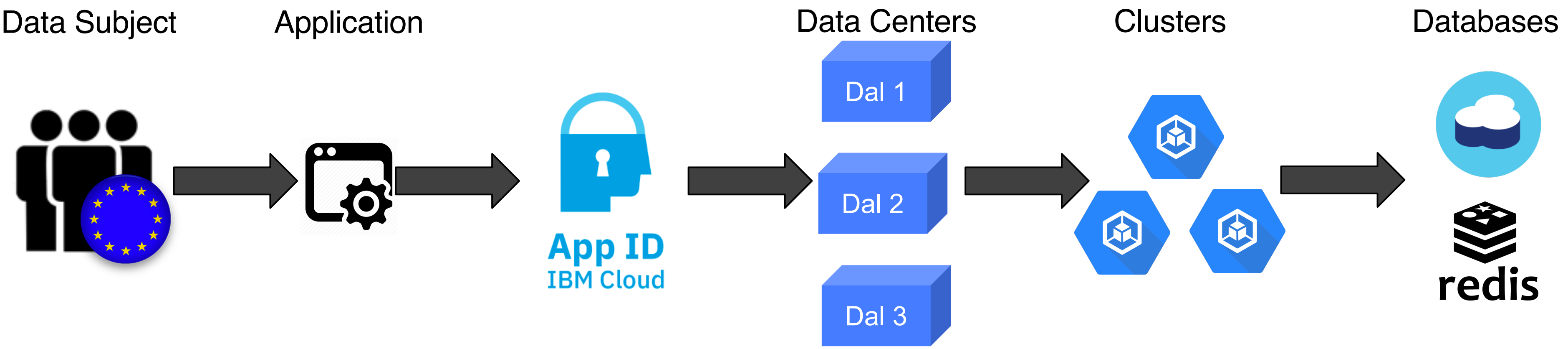
# Data protection at rest – Data encryption



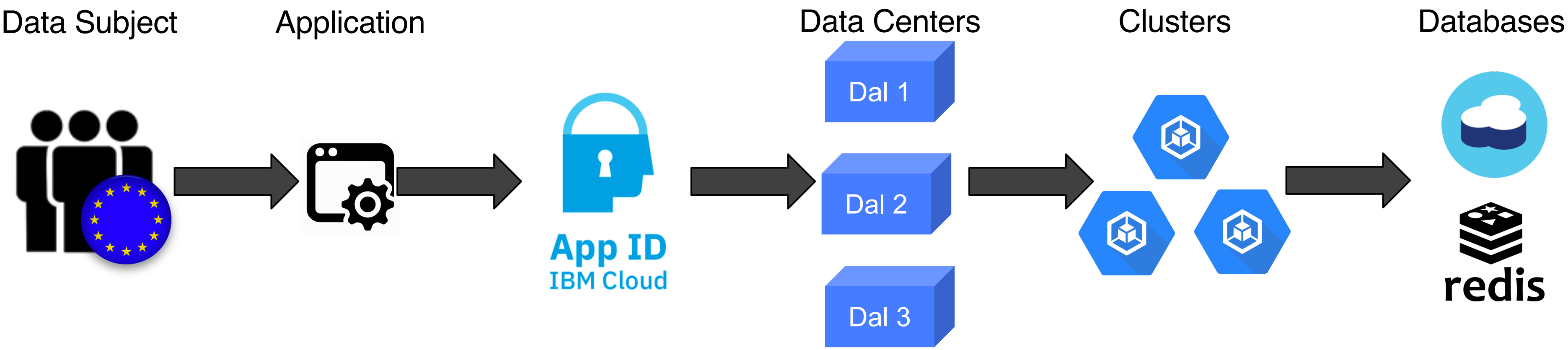
Per-tenant

- key encrypting keys (KEKs)
- data encryption keys (DEKs)
- tokens signature keys (TSKs)
- cryptographic data isolation

# Analysis of Personal Data - "Copies"



# Analysis of Personal Data - ”Copies”



Data Subject

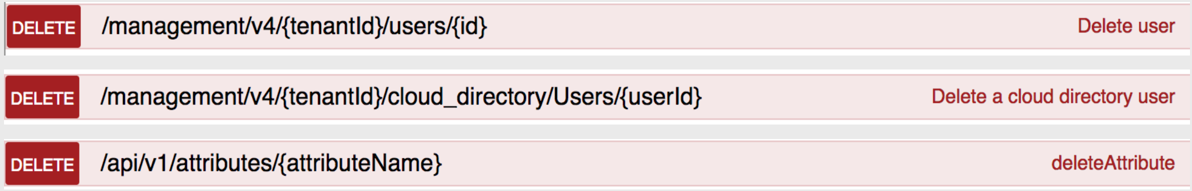
Application

Data Centers

Clusters

Databases

## Examples of Available APIs

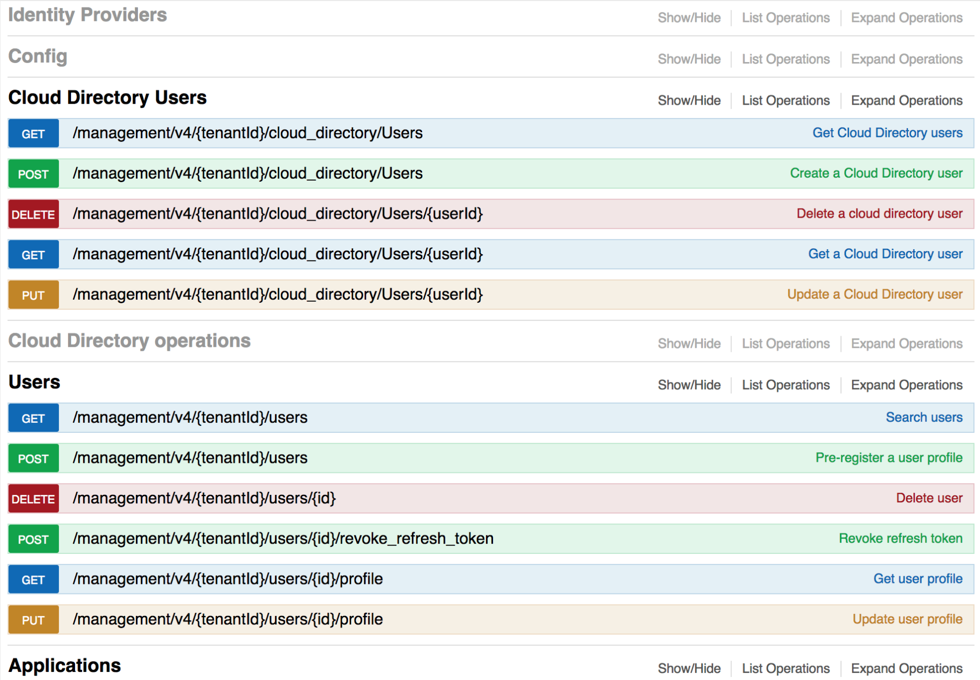


DELETE /management/v4/{tenantId}/users/{id} Delete user

DELETE /management/v4/{tenantId}/cloud_directory/Users/{userId} Delete a cloud directory user

DELETE /api/v1/attributes/{attributeName} deleteAttribute

# Analysis of Personal Data – Management



Identity Providers

Config

Cloud Directory Users

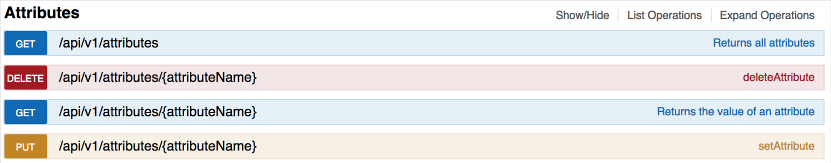
| | | |
|---|---|---|
| GET | /management/v4/{tenantId}/cloud_directory/Users | Get Cloud Directory users |
| POST | /management/v4/{tenantId}/cloud_directory/Users | Create a Cloud Directory user |
| DELETE | /management/v4/{tenantId}/cloud_directory/Users/{userId} | Delete a cloud directory user |
| GET | /management/v4/{tenantId}/cloud_directory/Users/{userId} | Get a Cloud Directory user |
| PUT | /management/v4/{tenantId}/cloud_directory/Users/{userId} | Update a Cloud Directory user |

Cloud Directory operations

Users

| | | |
|---|---|---|
| GET | /management/v4/{tenantId}/users | Search users |
| POST | /management/v4/{tenantId}/users | Pre-register a user profile |
| DELETE | /management/v4/{tenantId}/users/{id} | Delete user |
| POST | /management/v4/{tenantId}/users/{id}/revoke_refresh_token | Revoke refresh token |
| GET | /management/v4/{tenantId}/users/{id}/profile | Get user profile |
| PUT | /management/v4/{tenantId}/users/{id}/profile | Update user profile |

Applications



Attributes

| | | |
|---|---|---|
| GET | /api/v1/attributes | Returns all attributes |
| DELETE | /api/v1/attributes/{attributeName} | deleteAttribute |
| GET | /api/v1/attributes/{attributeName} | Returns the value of an attribute |
| PUT | /api/v1/attributes/{attributeName} | setAttribute |

# Thank you