PIa | Privacy impact assessment

| MY PIAS ⌄ | PIA TEMPLATES | KNOWLEDGE BASE | | Settings ⌄ | Help ⌄ | 🌐 |

My PIAs > Current PIAs > Data Pipeline for New Feature

Data Pipeline fo… ✕

CONTEXT
— Overview
— Data, processes and supporting …

FUNDAMENTAL PRINCIPLES
— Proportionality and necessity
— Controls to protect the personal …

RISKS
— Planned or existing measures
— Illegitimate access to data
— Unwanted modification of data
— Data disappearance
— Risks overview

VALIDATION
— Risk mapping

Edition

Context

This section gives you a clear view of the treatment(s) of personal data in question.

OVERVIEW
This part allows you to identify and present the object of the study.

What is the processing under consideration?

Collection of Behavioral Data and Analytics of Flight Taxi App (incl. Desktop Version) to evaluate Mulitvariate Testing approaches. Based on that we want to customize and enhance User Experience for each User. Data is furtermore used to build Machine Learning Models (linear regression) to estimate probable time of usage of the app so that promotions and notifications can be send out in advance.

0 comment(s)

1/20/22   💬 Comment ⌄

What are the responsibilities linked to the processing?

data subject: product user (data collection),
processor: AWS (data mgmt & retention),
controller: Taxi Flight Inc. (Analytics and ML solution)

📑 ⤓
Knowledge base

Choose your knowledge base

| CNIL's knowledge base ▾ |

🔍

⌄ **Principle**
Processing's description

⌄ **Definition**
Controller

⌄ **Definition**
Processor

CONTEXT
— Overview
— Data, processes and supporting …

FUNDAMENTAL PRINCIPLES
— Proportionality and necessity
— Controls to protect the personal …

RISKS
— Planned or existing measures
— Illegitimate access to data
— Unwanted modification of data
— Data disappearance
— Risks overview

VALIDATION

Edition

Context

This section gives you a clear view of the treatment(s) of personal data in question.

DATA, PROCESSES AND SUPPORTING ASSETS
This part allows you to define and describe the scope of the processing in detail.

What are the data processed?

Stakeholder: Customer Care
Use-Case: Provide personalized responses to the customer
Entity Data: **Customer Data** (Customer ID, Name, email)
Event Data: **Customer Feedback Data** (Feedback ID, Type of Feedback, Content)
Justification: Customers should feel treated as a valuable customer. This plays a big part in customer retention which results into a good CLV.

Stakeholder: Product Mgmt
Use-Case: Analyzes customer interaction data on website and app (potential big-data use case)
Entitiy Data: **Customer Data** (Customer ID, Name, email)
Event Data: **Interactions Data** (Event ID, Timestamp, Event Type, OS)
Justification: To stay competitive & improve our service this use case is supporting the business goals the most.

0 comment(s)

📑 ⤓
Knowledge base

Choose your knowledge base

| CNIL's knowledge base ▾ |

🔍

⌄ **Principle**
Data and processes

⌄ **Principle**
Recipient

⌄ **Definition**
Personal data

⌄ **Definition**
Recipient

How does the life cycle of data and processes work?

1. Data is collected from the user (either through usage of desktop or app version) & from Taxi Drones
2. Data is transferred through an Load Balancer to our Servers who are writing entity data to a structured database and event data into an unstructured database (S3 bucket as Data Lake)
3. Data Storages are hosted through AWS. Location is Frankfurt (Germany).
4. Both data storages will send their information regularly to the Data Warehouse.
5. Databases and the Data Warehouse are mirrored in another AWS data center (Milan) for Disaster Recovery purposes.
6. Flight Taxi Inc. is evaluating the information with Tableau, MS Excel and an Integrated Development Environment for applying Machine Learning Frameworks like Scikit-Learn, Keras/Tensorflow. Access is enabled through an authorization concept and custom build APIs.

Data is collected with each User2Product and Drone Interaction (aka not time dependent)

Storage Duration: 1 year and unlimited after anonymization

see attachement 1_aws for support

0 comment(s)

1/20/22   💬 Comment ⌄

📑 ⤓
Knowledge base

Choose your knowledge base

| CNIL's knowledge base ▾ |

🔍

⌄ **Principle**
Data and processes

⌄ **Principle**
Recipient

⌄ **Definition**
Personal data

⌄ **Definition**
Recipient

PIa | Privacy impact assessment

Press F11 to exit full screen mode.

MY PIAS ⌄   PIA TEMPLATES   KNOWLEDGE BASE   Settings ⌄   Help ⌄   🌐

My PIAs > Current PIAs > Data Pipeline for New Feature

Data Pipeline fo... ✕

CONTEXT
— Overview 📝
— Data, processes and supporting ... 📝

FUNDAMENTAL PRINCIPLES
Proportionality and necessity 📝
— Controls to protect the personal ... 📝

RISKS
— Planned or existing measures 📝
— Illegitimate access to data 📝
— Unwanted modification of data 📝
— Data disappearance 📝
— Risks overview

Edition

Fundamental principles
This section allows you to build the compliance framework for privacy principles.
PROPORTIONALITY AND NECESSITY
This part allows you to demonstrate that you are implementing the necessary means to enable the persons concerned to exercise their rights.

Are the processing purposes specified, explicit and legitimate? ⌃

We want to improve our services so that the user has a better experience. By using our services the user agrees to be tracked via cookie banner or already acknowledged terms of service which results in an successful user sign up.

0 comment(s)

1/20/22   💬 Comment ⌄

🗐 ⬇
Knowledge base

Choose your knowledge base

CNIL's knowledge base ▾

🔍

⌄ Principle
Justification of lawfulness

⌄ Principle
Principles relating to processing of personal data

⌄ Principle
Data minimisation

Are the data accurate and kept up to date? ⌃

Data is collected based on action and stored in the connected database/ data lake. From there the data will be forwarded to the Data Warehouse during night (supports completeness & accuray of data throug usage of low latency timeframes). Data Validation after transfer is automatically done via scheduled job between data sources and Data Warehouse. Deviation will be investigated & solved by employees.

0 comment(s)

1/20/22   💬 Comment ⌄

What are the storage duration of the data? ⌃

1 year, data will be anonymized afterwards and held unlimited (personal data will be replaced by dummy data, data like start of session and when the user dropped off will be held)

0 comment(s)

1/20/22   💬 Comment ⌄

🗐 ⬇
Knowledge base

Choose your knowledge base

CNIL's knowledge base ▾

🔍

⌄ Principle
Justification of lawfulness

⌄ Principle
Principles relating to processing of personal data

⌄ Principle
Data minimisation

⌄ Principle
Storage Durations

My PIAs > Current PIAs > Data Pipeline for New Feature

Data Pipeline fo... ✕

CONTEXT
— Overview 📝
— Data, processes and supporting ... 📝

FUNDAMENTAL PRINCIPLES
— Proportionality and necessity 📝
Controls to protect the personal ... 📝

RISKS
— Planned or existing measures 📝
— Illegitimate access to data 📝
— Unwanted modification of data 📝
— Data disappearance 📝
— Risks overview

VALIDATION
— Risk mapping
— Action plan
— DPO and data subjects' opinions 📝

Edition

Fundamental principles
This section allows you to build the compliance framework for privacy principles.
CONTROLS TO PROTECT THE PERSONAL RIGHTS OF DATA SUBJECTS
This part allows you to demonstrate that you are implementing the necessary means to enable the persons concerned to exercise their rights.

How are the data subjects informed on the processing? ⌃

Information is provided through terms of service when user signs up and through Cookie Banner. We inform our visitors and users after the data storage limit is reached (1 year) regularly

We have a self service portal which helps to get information like this and the information according to the Rights of the data subject (Art 15 -22 including 77).

0 comment(s)

1/20/22   💬 Comment ⌄

If applicable, how is the consent of data subjects obtained? ⌃

Through specific acknowledgment of the terms of service and cookie consent. Acknowledgment and Cookie Consent will be documented in a specific data table which can be related through unique identifier (User ID/ Cookie Data) to the specific person.

🗐 ⬇
Knowledge base

Choose your knowledge base

CNIL's knowledge base ▾

🔍

⌄ Principle
Subcontracting

⌄ Principle
Transfers

⌄ Principle
Informing data subjects

⌄ Principle
Consent