FUJITSU

shaping tomorrow with you

FUJITSU Cloud Service K5 Introduction to Personium Service

May 2018
Fujitsu Limited

Version 1.3

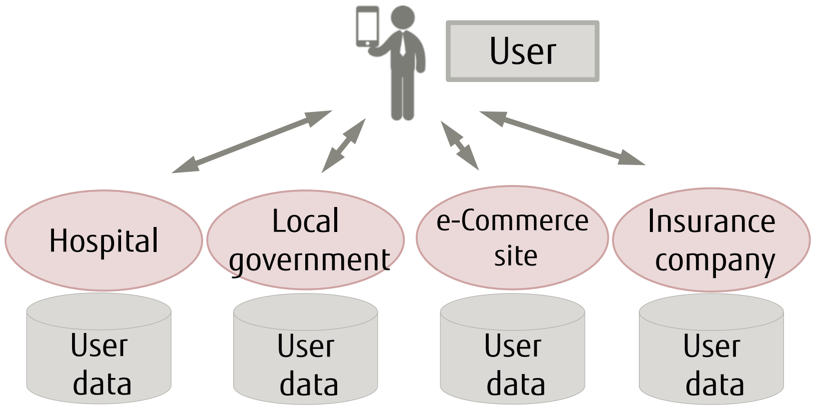
Contents

- Overview of Personal Data Store (PDS)
- Why PDS?
- Overview of PDS Business: Service Linkage - Example
- Overview of the Personium Service
- Features of the Service
- Function Overview
- Detailed Description of Functions
  - Personal Data Management
  - Event Control
  - Social Management
- API List
- Usage Scenarios
- Personium Service: Service Plan
- Restrictions and Notes
- Reference

Overview of Personal Data Store (PDS)

A PDS is a repository service for storing the personal data(*1) of individuals. It links services by becoming the hub, or central point, from which to control (i.e.: grant access rights to) the recipients of data.

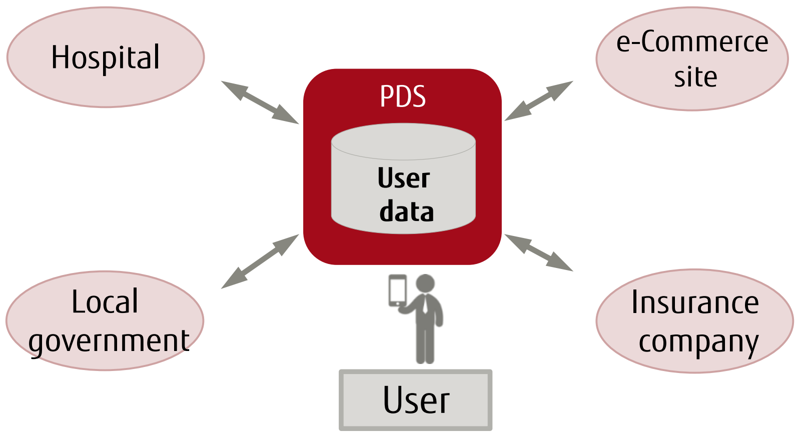
Conventional (System-centric data management)



■ Relationship between the user(*2) and user data(*3)

- The operator(*4) manages user data
- There is a risk of information leakage and data privacy issues occurring when operators attempt to link user data their respective systems.

PDS (Human-centric data management)



■ Relationship between the user and user data

- The user manages user data
- Because the PDS service only allows user data to be disclosed as permitted by the user, there is no risk of information leakage or data privacy issues.

*1: Personal data: Personal information relating to the behavior and status of a user (position information, purchase history, etc.)
*2: A user: A party using the services of an operator
*3: User data: The personal data of each individual user
*4: An operator: A party offering business services to the user

Why PDS?

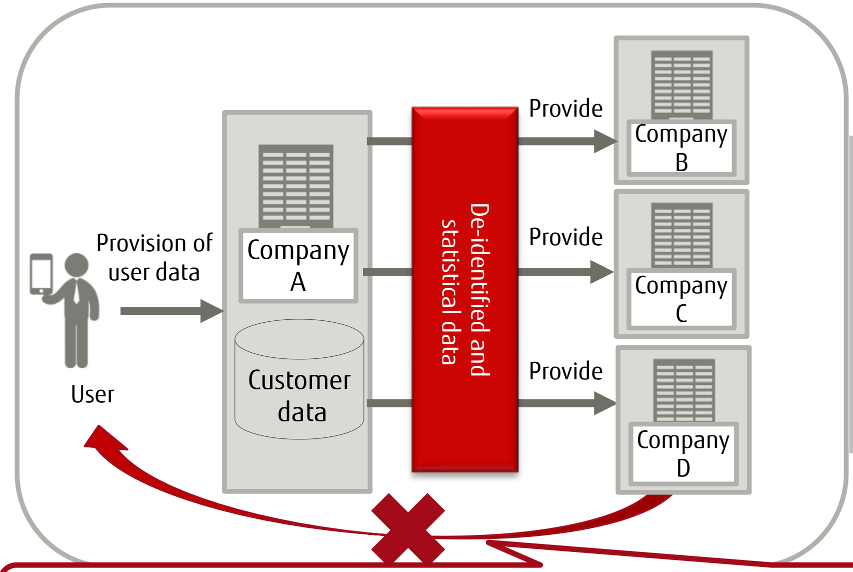
Limits to existing data circulation

Existing data trading methods require that personally identifiable information be anonymized, which means that there can be no direct remuneration to the user who provided the data. By contrast, a PDS service gives the individual control over disclosure of their personal information. This allows **data to** be traded under the individual's own name, and direct recompense provided to the individual for the use of their personal data.

Expectations of deep data

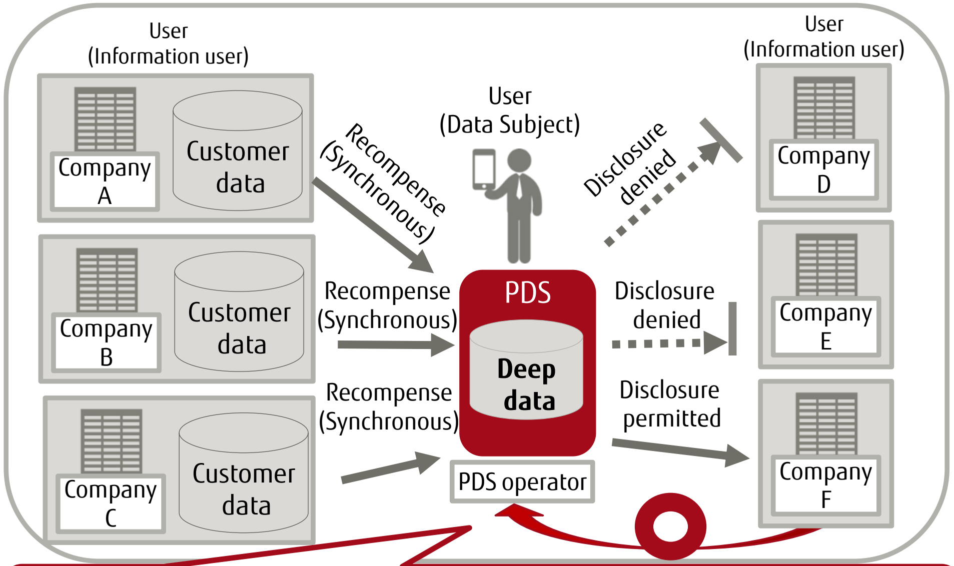
Large, rich collections of personal data that have accumulated in the PDS in the form of preference and behavior logs, over a long period of time and across a wide range of fields, are referred to as 'deep data.'
Leveraging deep data greatly increases the business value of personal data to the information user because it allows highly precise, personalized offers and recommendations to be extended to individuals.

Existing use and application of data



Data is provided anonymously, so there can be no direct recompense to the user who provided it.

Existing use and application of PDS data



Returning control over information provision to the user enables the user to freely specify who the recipients of that data will be, thus permitting the user to trade their data for a direct return.

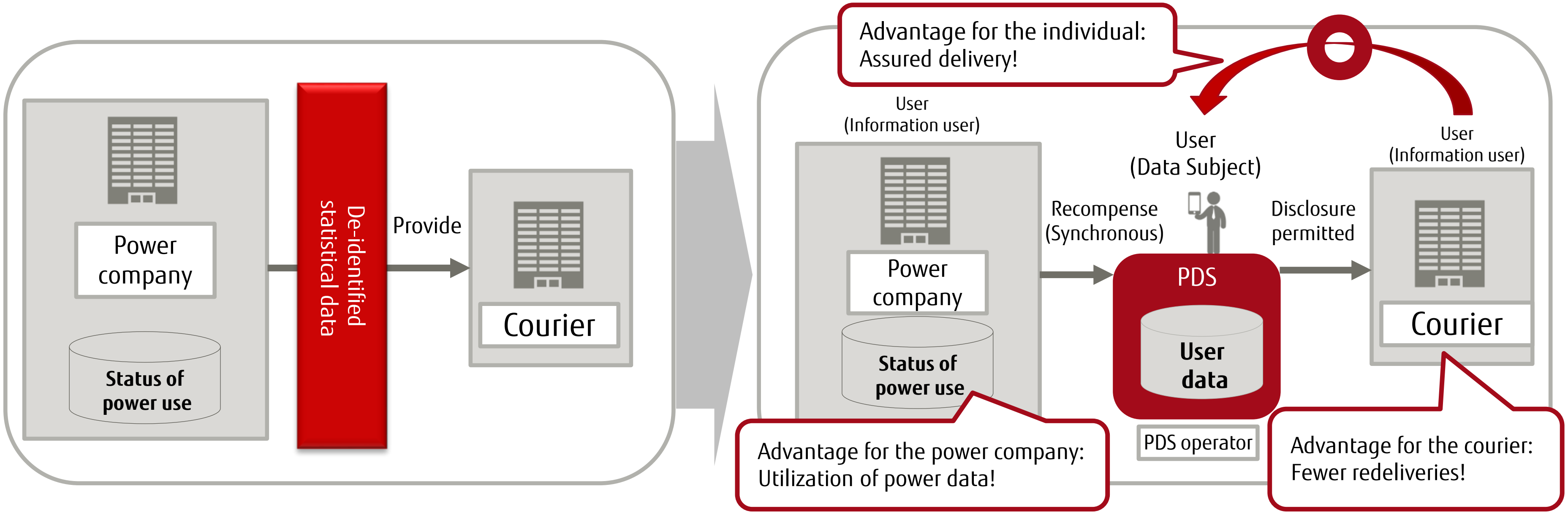
Overview of PDS Business: Service Linkage - Example

- Example: Leveraging home-based information

Scenario: Before delivering a parcel, a courier wants to confirm if there is anyone at the delivery address.

Existing use and application of data

Use and application of PDS data



Power company

Status of power use

De-identified statistical data

Provide

Courier

Advantage for the individual: Assured delivery!

User (Information user)

Power company

Status of power use

Recompense (Synchronous)

User (Data Subject)

PDS

User data

PDS operator

Disclosure permitted

User (Information user)

Courier

Advantage for the power company: Utilization of power data!

Advantage for the courier: Fewer redeliveries!

Provision of de-identified data

Power usage information indicates whether there is someone at home or not. However, this information is anonymized and therefore lacks usability.

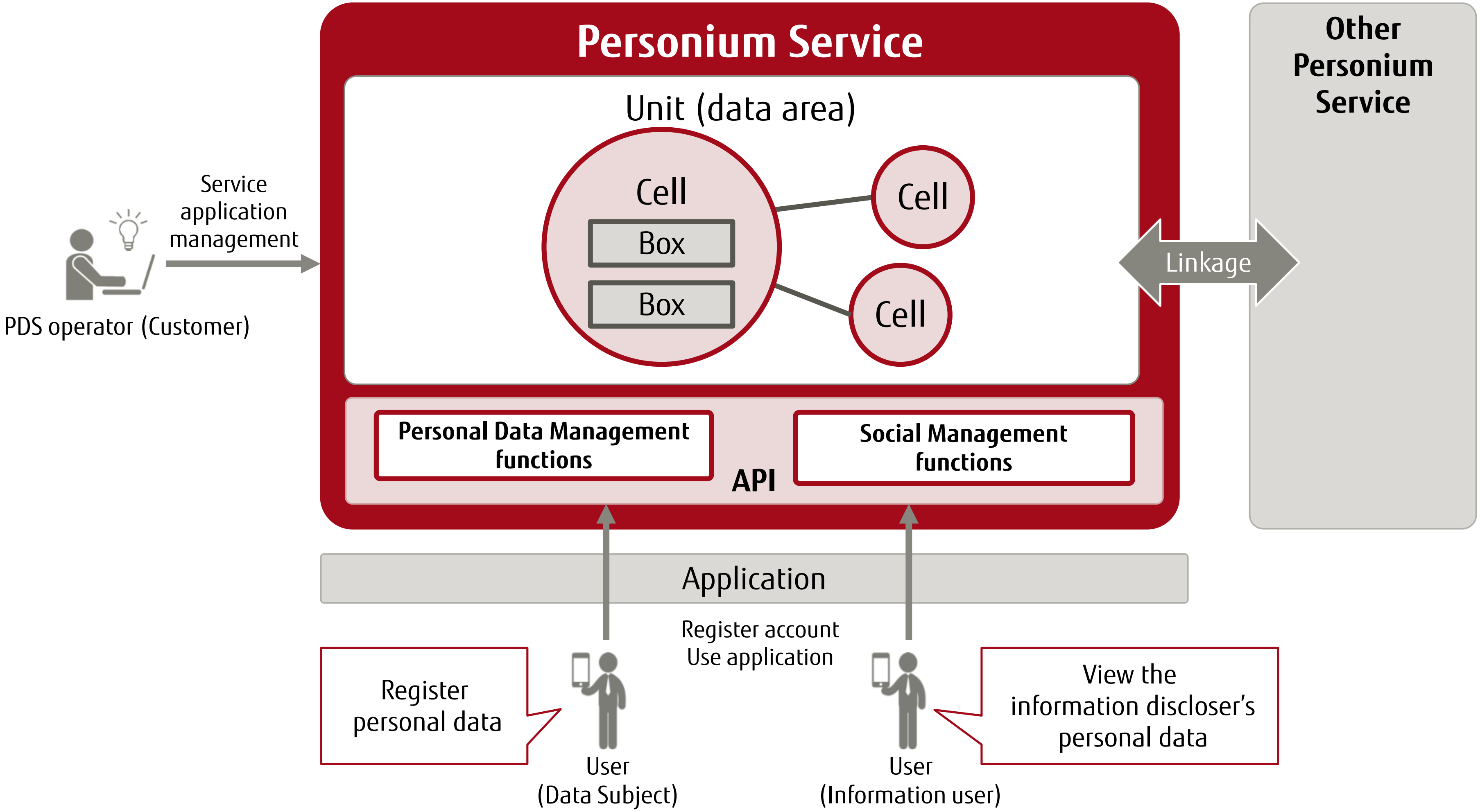
Data provision based on control over own personal information

Home-based information is provided to the courier for delivery this week “only”
Information is voluntarily provided as necessary by the individual.
Personal information is circulated safely and with the individual’s consent.

PDS is an extremely important tool

Overview of the Personium Service

- The Personium Service supports your PDS business.
- PDS uses a RESTful Web API to provide the data area necessary for PDS business, data access management functions, and functions for accessing files and data in the data area.
- Using the Personium Service enables PDS operators to rapidly build a platform for PDS business and provide the PDS services to users.



Features of the Service (1 of 2)

The Personium Service provides the personal data management functions required for PDS business applications. It supports PDS business by enabling the setting of access rights based on the data relationships between users and between PDS operators.

Uses open source Personium

Open source Personium-based services reduce the risk of being locked into a particular vendor. The Service provides the latest in technology, representing the achievements of developers throughout the world.

Provides data access functions based on the relationships between users

The Service enables each user to have both disclosure and confidentiality control over their personal data by defining, as parameters, the relationships between users.

Provides mutual access control over data between different PDS operators

The service enables data linkage between different PDS operators who deploy the Personium Service.

Features of the Service (2 of 2)

This Service provides security features for protecting user data.

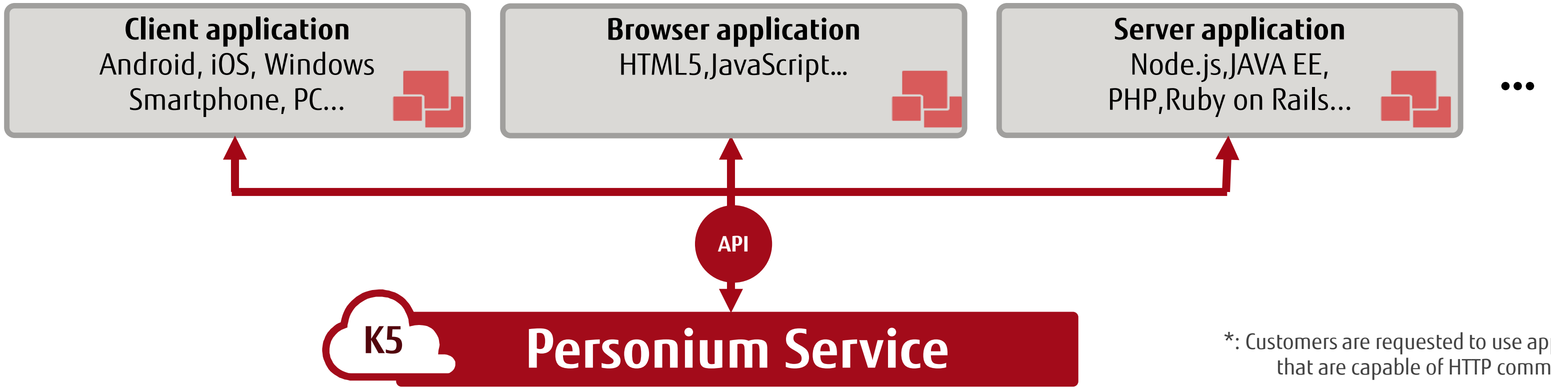
Application authentication

Application authentication enables data operations (register, read, change, delete) to be performed between the user client and user data, once certificate management using OAuth 2.0 has been completed. This protects user data from malicious users.

Functions under this Service are provided via a REST API.

Provision of a RESTful Web API

This Service uses a RESTful Web API to provide functions, enabling flexible customization.
As long as the applications are capable of HTTP communication, it can access a platform-independent environment, regardless of the programming language and execution environment(*).
In addition, customers can use their own domain names.



Client application
Android, iOS, Windows
Smartphone, PC…

Browser application
HTML5,JavaScript…

Server application
Node.js,JAVA EE,
PHP,Ruby on Rails…

…

API

K5

Personium Service

*: Customers are requested to use applications that are capable of HTTP communication

Function Overview

Personal Data Management functions

The PDS operator or PDS application provides the following functions for managing the user's personal data:

i. Cell management functions (Functions for managing the user's personal data)

(a) Cell settings (Register, read, change, delete, list the user's personal data areas)

(b) Account settings (Register, read, change, delete, list the accounts belonging to the user's personal data areas)

(c) Authentication (User authentication)

(d) Role settings (Register, read, change, delete, list the user roles)

(e) Box settings (Register, read, change, delete, list application-specific data areas)

(f) Access control (Set, read, change the access rights for users and user folders)

(g) Event acceptance (Accept events and output logs for users)

(h) Event control (executes processing or log output according to the rules set for events, such as API operation)

(i) Import/export (imports or exports all data in cells)

ii. Box management functions (Functions for managing the user's personal data in application and use-specific areas)

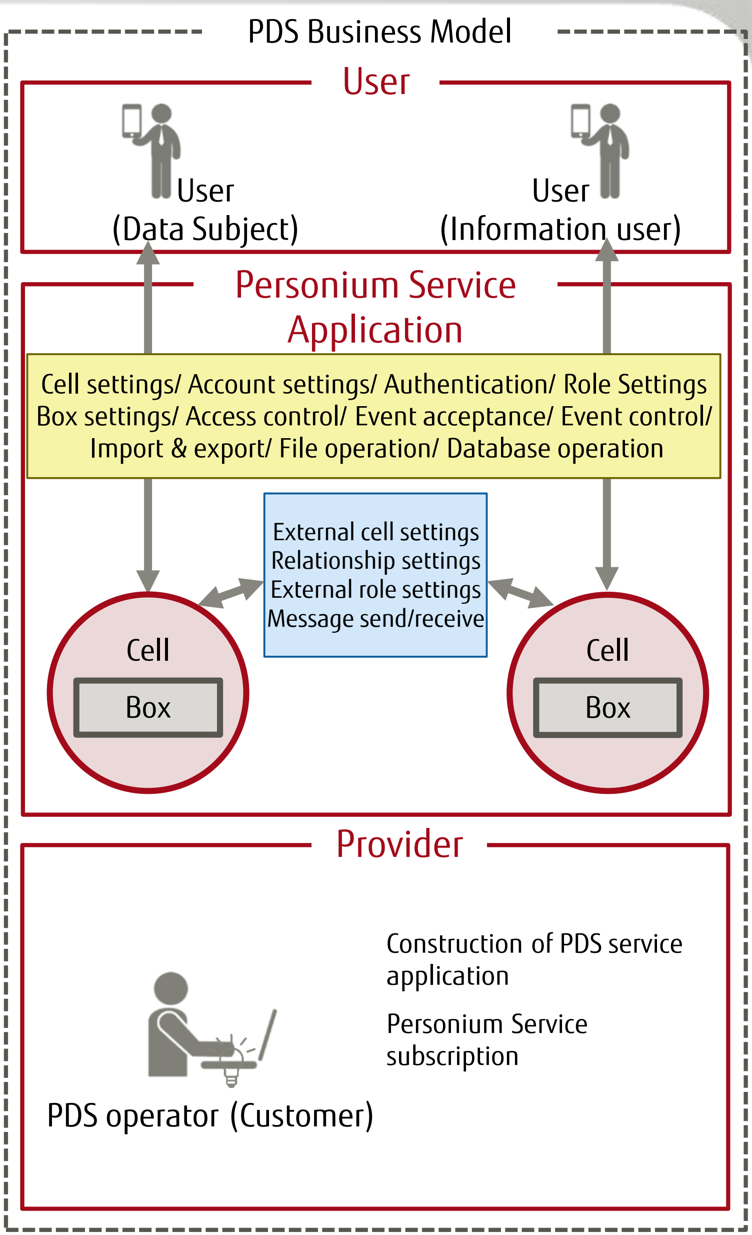
(a) File operation (Collection settings, file settings, access rights settings)

(b) Database operation (Schema settings, data manipulation)

Social Management functions

This Service provides the following functions for defining relationships between users in users' personal data, and using that for enabling disclosure control and confidentiality control of users' personal data:

- i. External cell settings (Register, read, change, delete, list users to whom disclosure can be made)
- ii. Relationship settings (Register, read, change, delete, list the relationship with users to whom disclosure can be made)
- iii. External role settings (Register, read, change, delete, list the roles of users to whom disclosure can be made)
- iv. Message send/receive (Communication function for permitting disclosure, etc. of a user's personal data)

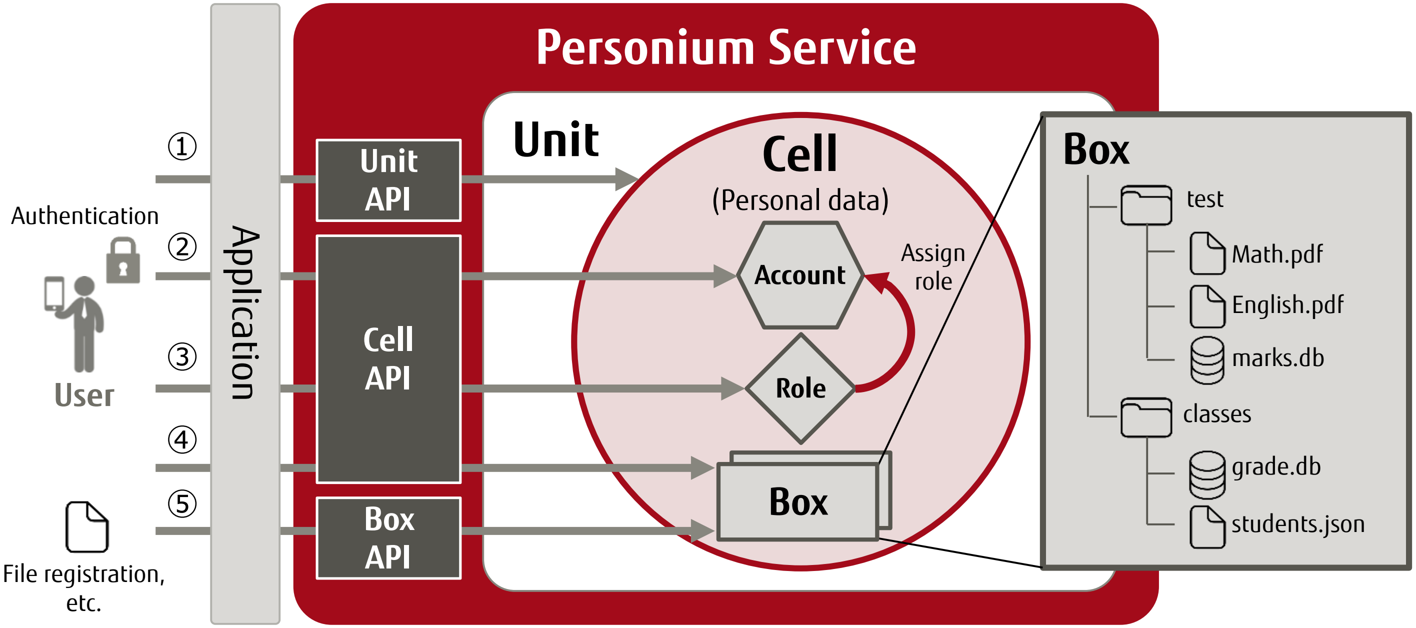

PDS Business Model
User
User
(Data Subject)
User
(Information user)
Personium Service Application
Cell settings/ Account settings/ Authentication/ Role Settings
Box settings/ Access control/ Event acceptance/ Event control/
Import & export/ File operation/ Database operation
External cell settings
Relationship settings
External role settings
Message send/receive
Cell
Box
Cell
Box
Provider
Construction of PDS service application
Personium Service subscription
PDS operator (Customer)

Detailed Description of Functions: Personal Data Management

Personal Data Management uses units, cells and boxes to manage user information and data.

Example of PDS creation and operation

① Create cell
② Create account
③ Create role and assign to account
④ Create box
⑤ To manipulate files, access the box from an account with box read or edit permissions

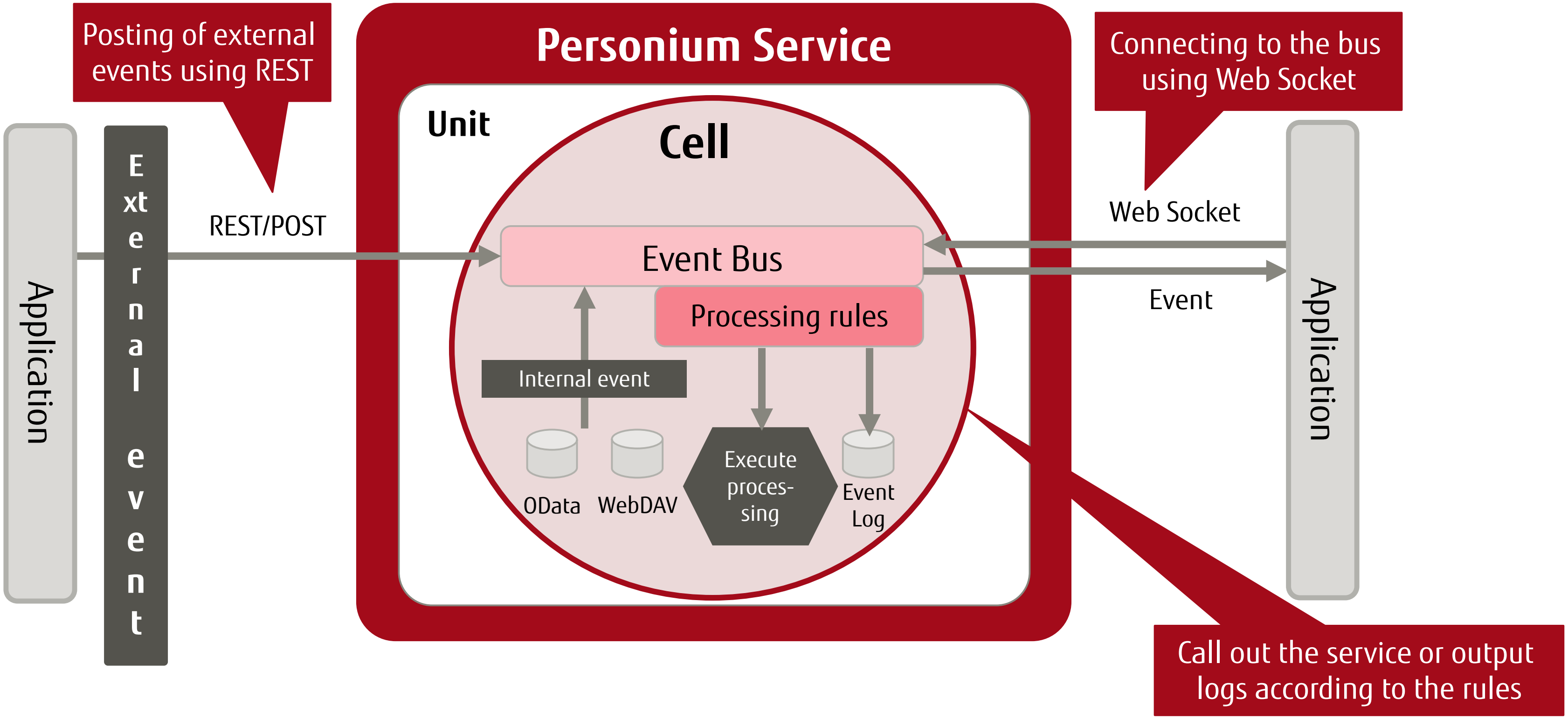


Name and containment relationship	Outline	Number that can be created	Operating privileges		
Unit	The unit for managing cells	1 unit per service environment	Unit user token	-	-
Cell	The unit for managing users and user data (personal data)	1 cell per user		Cell-level permission Note: Only a unit user token can create a cell	-
Account	The account of the user belonging to the cell	Multiple			-
Role	Defines the user's role and privileges	Multiple			-
Box	The user's data storage area	Multiple			Box-level permission - Note: Must have cell-level permission or higher to create a box

Detailed Description of Functions: Event Control

By setting the event processing rules, processing or log output is activated according to various events generated in the cell.

- Any API calls such as data manipulation issued to cells can be captured as an internal event.
- An external event can be posted from the Client, etc.
- Status of event generation can be monitored continuously using Web Socket.

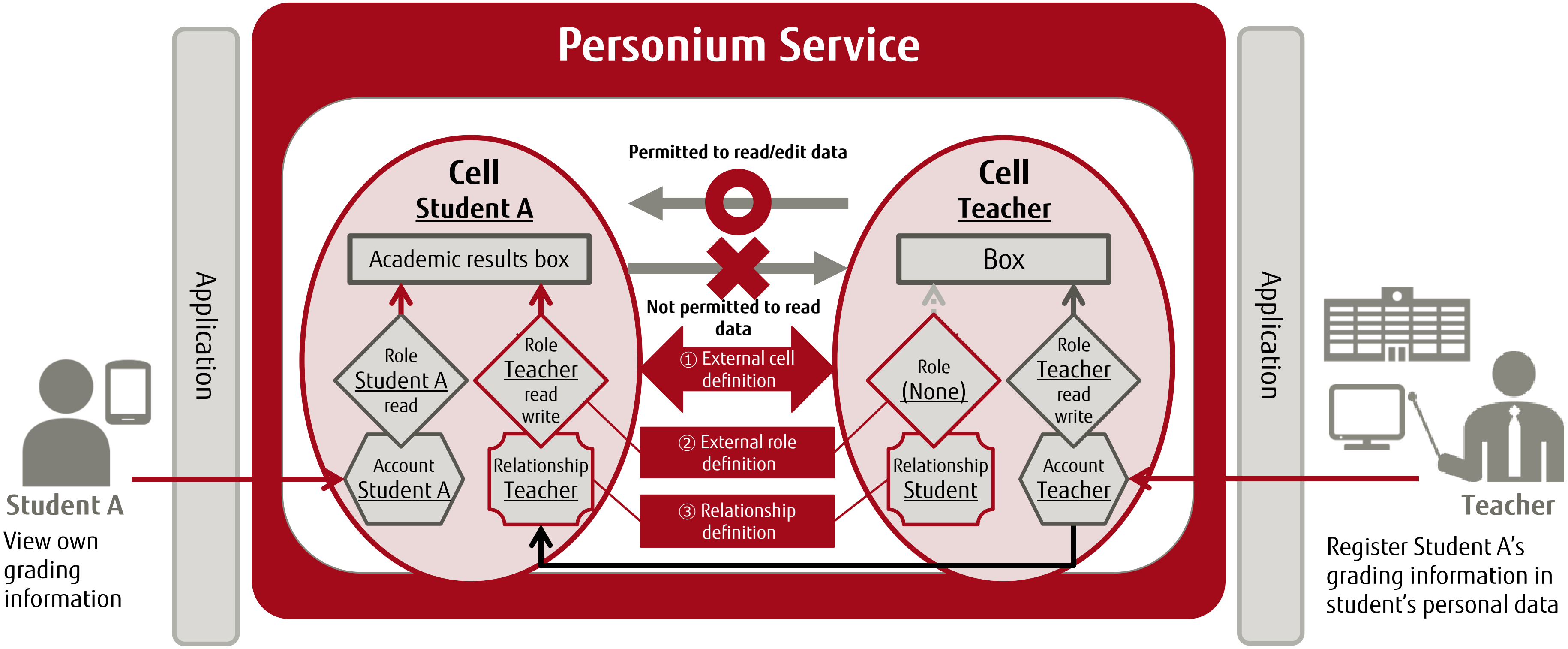


Detailed Description of Functions:
Social Management (Mutual access control between users)

FUJITSU

Enables disclosure control and confidentiality control over personal data by **defining the relationship between users** in each user's personal data (cell).

- Example: Setting mutual access rights to personal data in an education setting



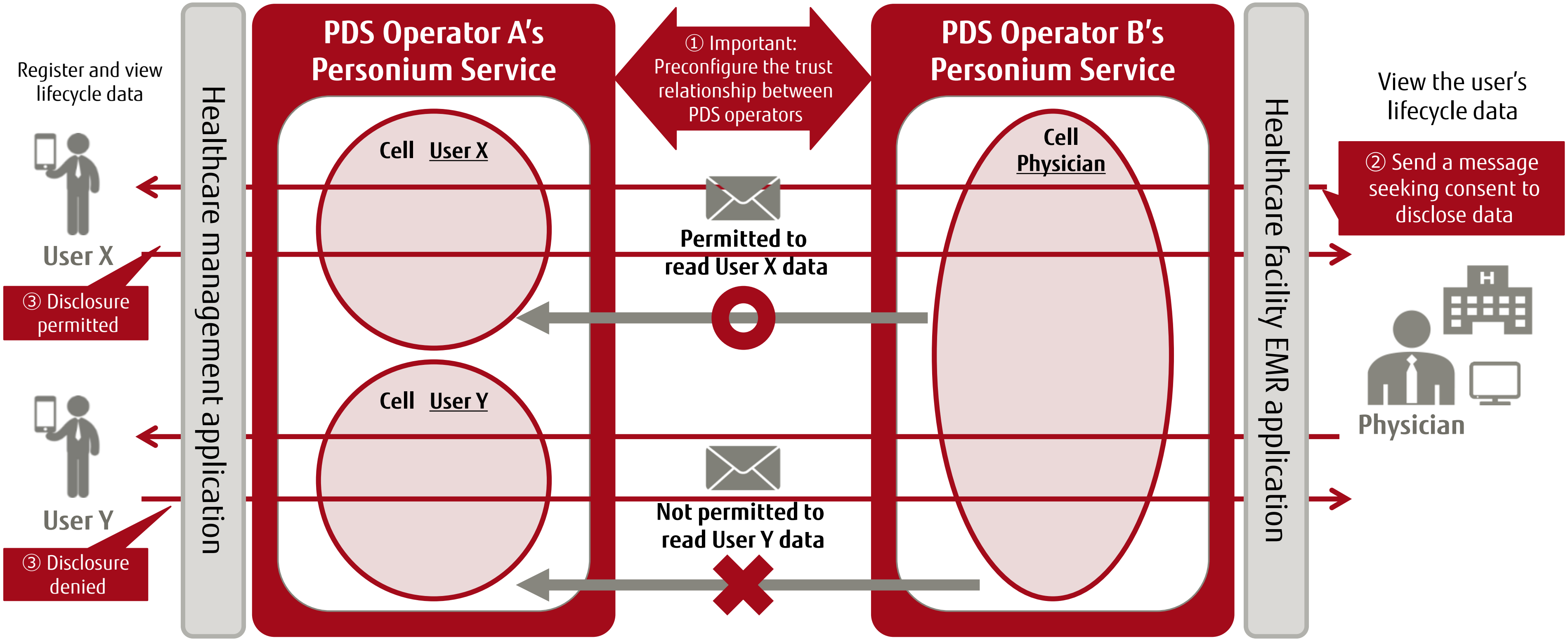
Functions provided The functions provided enable each user to have disclosure control/confidentiality control over their personal data by defining, as parameters, the relationships between users and specific access rights.

Outcome Users determine for themselves which personal data to disclose, thus maintaining confidentiality between users.

Detailed Description of Functions:
Social Management (Mutual access control between operators)

Enables data linkage between different PDS operators who deploy the Personium Service.

- Example: Linkage of health service data between healthcare facilities



Register and view lifecycle data
User X
③ Disclosure permitted
User Y
③ Disclosure denied
Healthcare management application
PDS Operator A's Personium Service
Cell User X
Cell User Y
① Important: Preconfigure the trust relationship between PDS operators
Permitted to read User X data
Not permitted to read User Y data
PDS Operator B's Personium Service
Cell Physician
Healthcare facility EMR application
View the user's lifecycle data
② Send a message seeking consent to disclose data
H
Physician

Functions provided: Users can preconfigure PDS operators as trusted identities and authorize the disclosure of data to them. This enables diverse PDS operators to access user data among themselves.

Outcome: Removing the need for a shared environment between operators means fewer deployment hurdles. This opens the way for ecosystem(*) enablement.

Note: For further details, refer to "Working with the Customer to Co-create an Ecosystem" later in this presentation

API List

The Personium Service provides the following REST API functions:

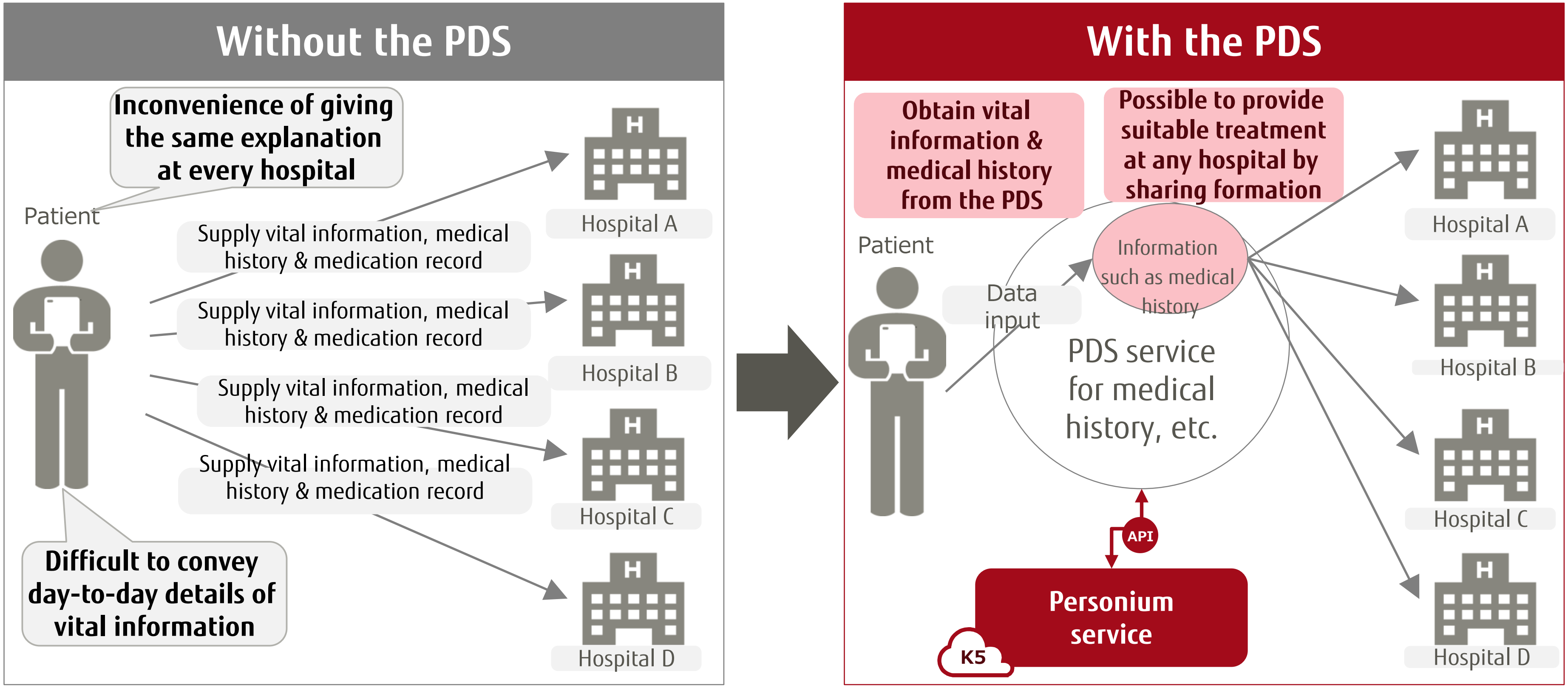
Function Name			Function Description
Personal Data Management functions	Cell management functions	Cell settings	Register, read, change, delete, list the user's personal data areas
		Account settings	Register, read, change, delete, list the accounts belonging to the user's personal data areas
		Authentication	User authentication
		Role settings	Register, read, change, delete, list the user roles
		Box settings	Register, read, change, delete, list application-specific data areas
		Access control	Set, read, change the access rights for users and user folders
		Event control	Execute processing or log output according to the rules set for events, such as API operation
		Import/export	Import or export all data in a cell
	Box management functions	File operation	Collection settings, file settings, access rights settings
		Database operation	Schema settings, data manipulation
Social Management functions	External cell settings		Register, read, change, delete, list users to whom disclosure can be made
	Relationship settings		Register, read, change, delete, list the relationship with users to whom disclosure can be made
	External role settings		Register, read, change, delete, list the role of users to whom disclosure can be made
	Message send/receive		Communication function for permitting disclosure, etc. of a user's personal data

Note: Check the following for a list of offerings:
K5 PaaS Portal > Documents > Personium Service > API Reference

Usage Scenario 1

PDS business operator	User (Data subject)	Personal data	User (Data user)
Health service	Patient	Vital information, medical history, medication records	Hospital/Clinic

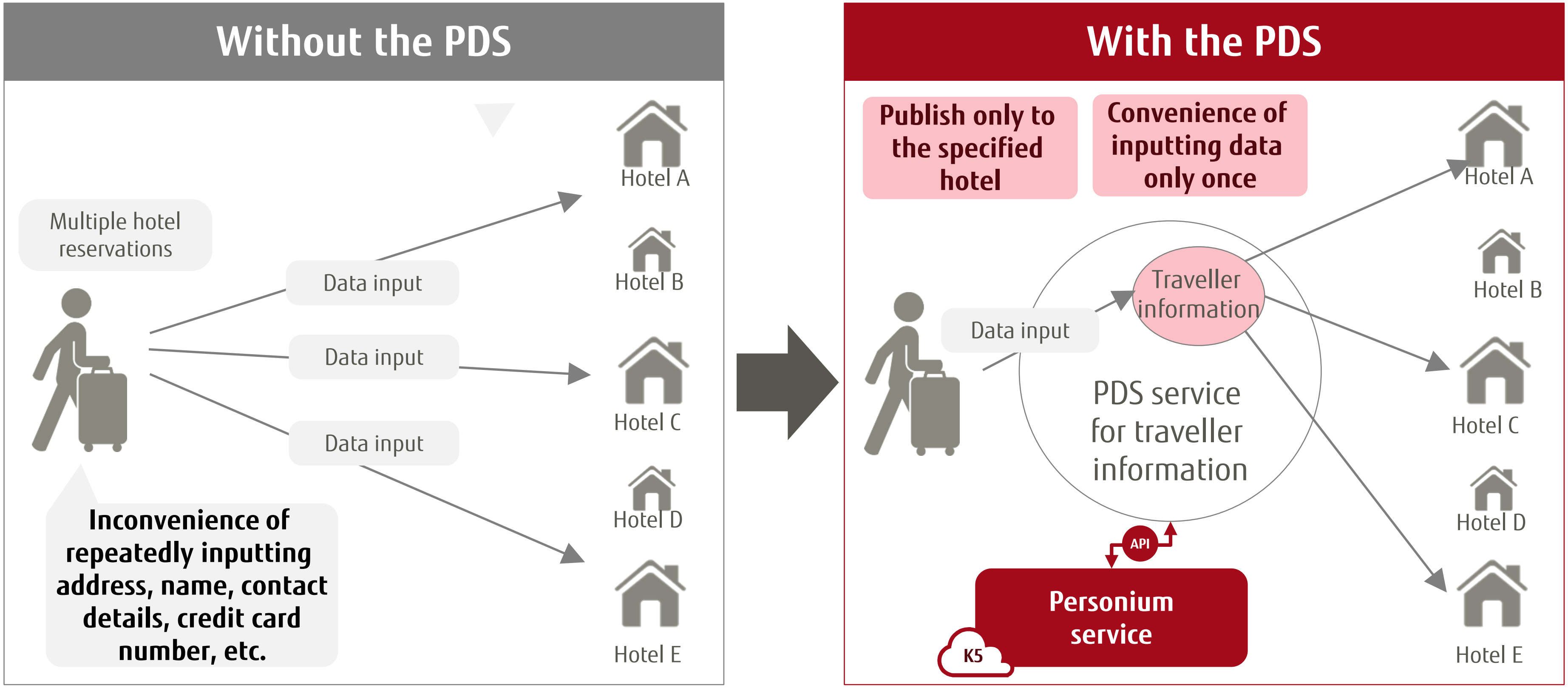
- Central management of user's vital information, medical history and medication records
- Efficient provision of suitable treatment by obtaining the required information from the PDS


Without the PDS
Inconvenience of giving the same explanation at every hospital
Patient
Supply vital information, medical history & medication record
Supply vital information, medical history & medication record
Supply vital information, medical history & medication record
Supply vital information, medical history & medication record
Hospital A
Hospital B
Hospital C
Hospital D
Difficult to convey day-to-day details of vital information
With the PDS
Obtain vital information & medical history from the PDS
Possible to provide suitable treatment at any hospital by sharing formation
Patient
Data input
Information such as medical history
PDS service for medical history, etc.
API
Personium service
K5
Hospital A
Hospital B
Hospital C
Hospital D

Usage Scenario 2

PDS business operator	User (Data subject)	Personal data	User (Data user)
Travel agent	Traveller	Traveller information	Accommodation (Hotel, ryokan, etc.)

- Remove the inconvenience of repeatedly inputting traveller information when making reservations.
- Traveller information control is enabled for the traveller.



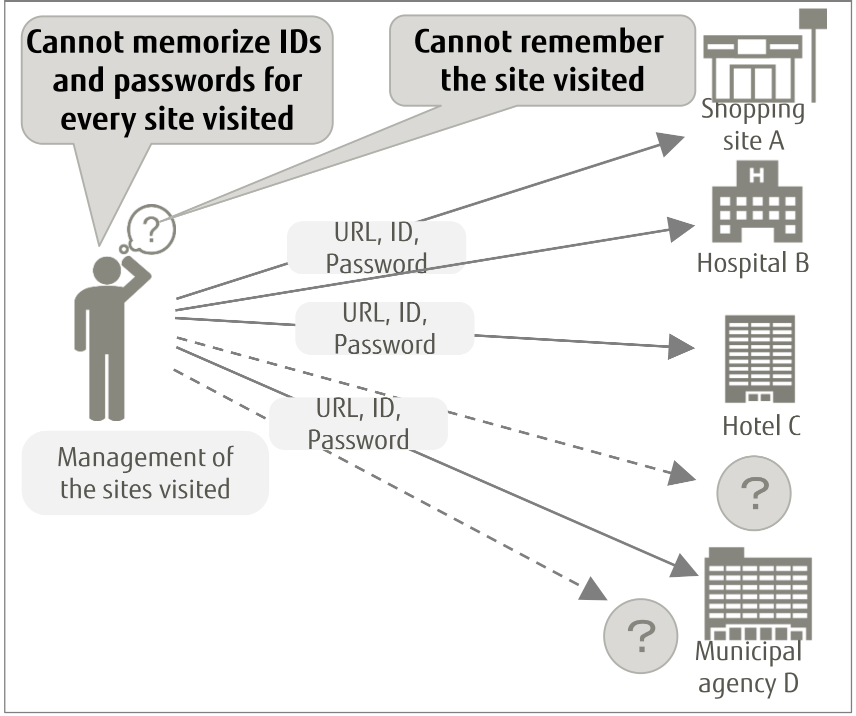
Without the PDS
Multiple hotel reservations
Data input
Data input
Data input
Hotel A
Hotel B
Hotel C
Hotel D
Hotel E
Inconvenience of repeatedly inputting address, name, contact details, credit card number, etc.
With the PDS
Publish only to the specified hotel
Convenience of inputting data only once
Data input
Traveller information
PDS service for traveller information
API
Personium service
K5
Hotel A
Hotel B
Hotel C
Hotel D
Hotel E

Usage Scenario 3

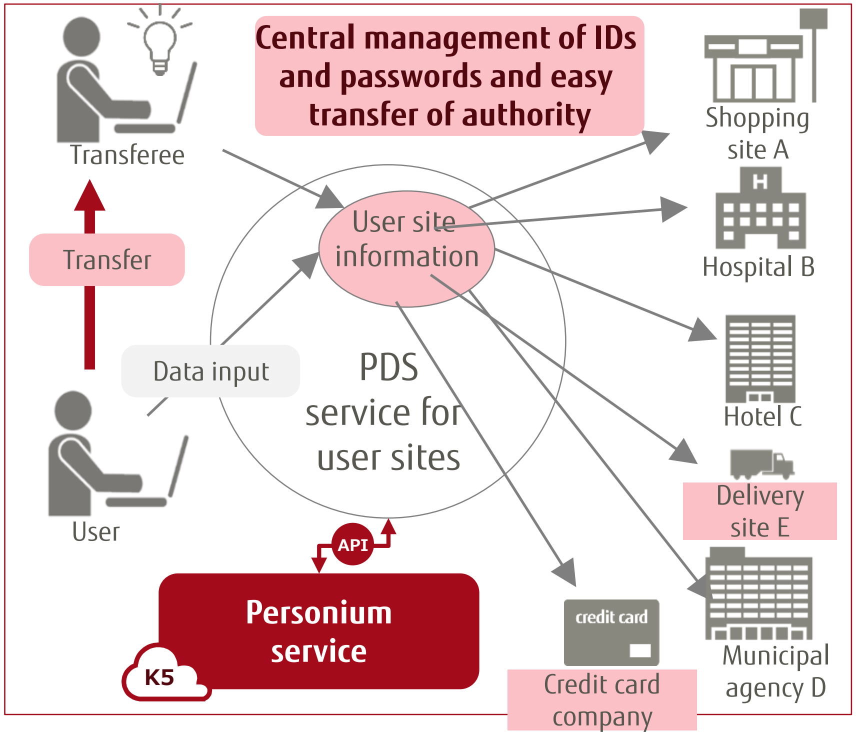
PDS business operator	User (Data subject)	Personal data	User (Data user)
Site Administrator	User	Site information	None

- Central management of URLs and account data specific to each user site.
- Proxy operation enabled when data is transferred to a close relative in an emergency, etc.

Without the PDS


Cannot memorize IDs and passwords for every site visited
Cannot remember the site visited
Management of the sites visited
URL, ID, Password
URL, ID, Password
URL, ID, Password
Shopping site A
Hospital B
Hotel C
?
?
Municipal agency D

With the PDS

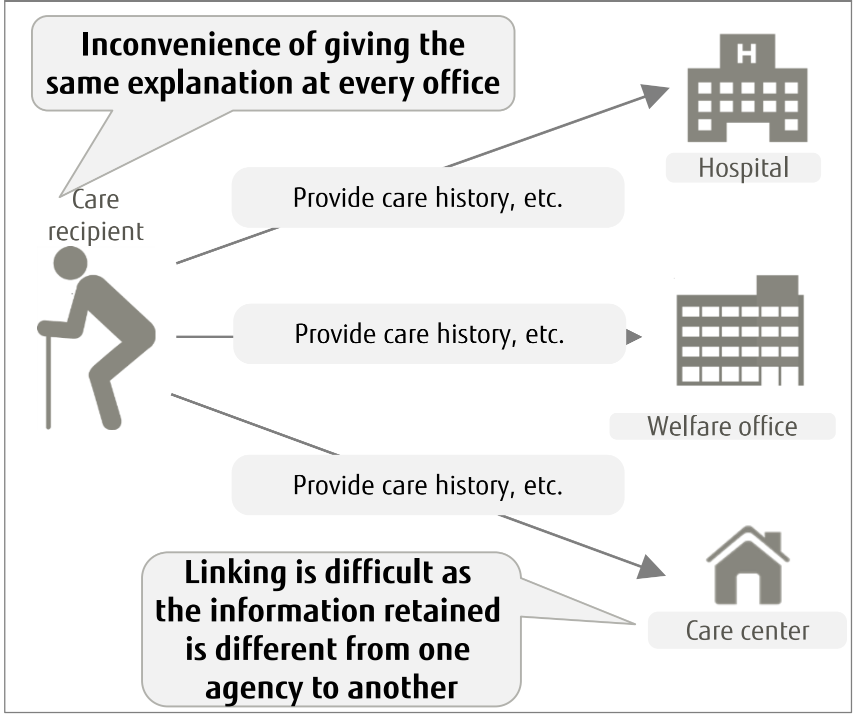


Usage Scenario 4

PDS business operator	User (Data subject)	Personal data	User (Data user)
Municipal agency/ welfare service	Care recipient	Care history/ medical history	Welfare office/ Hospital/ Care center

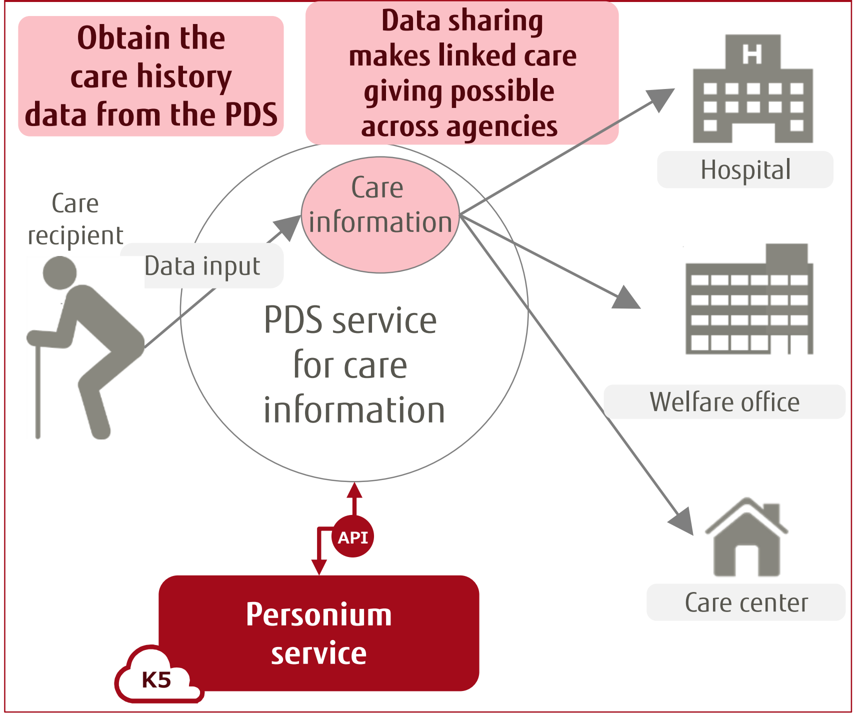
- Central management of care history, medical history, etc. of the care recipient
- Based on the information procured from the PDS, agencies can link the care they each provide.

Without the PDS



Inconvenience of giving the same explanation at every office
Care recipient
Provide care history, etc.
Hospital
Provide care history, etc.
Welfare office
Provide care history, etc.
Care center
Linking is difficult as the information retained is different from one agency to another

With the PDS

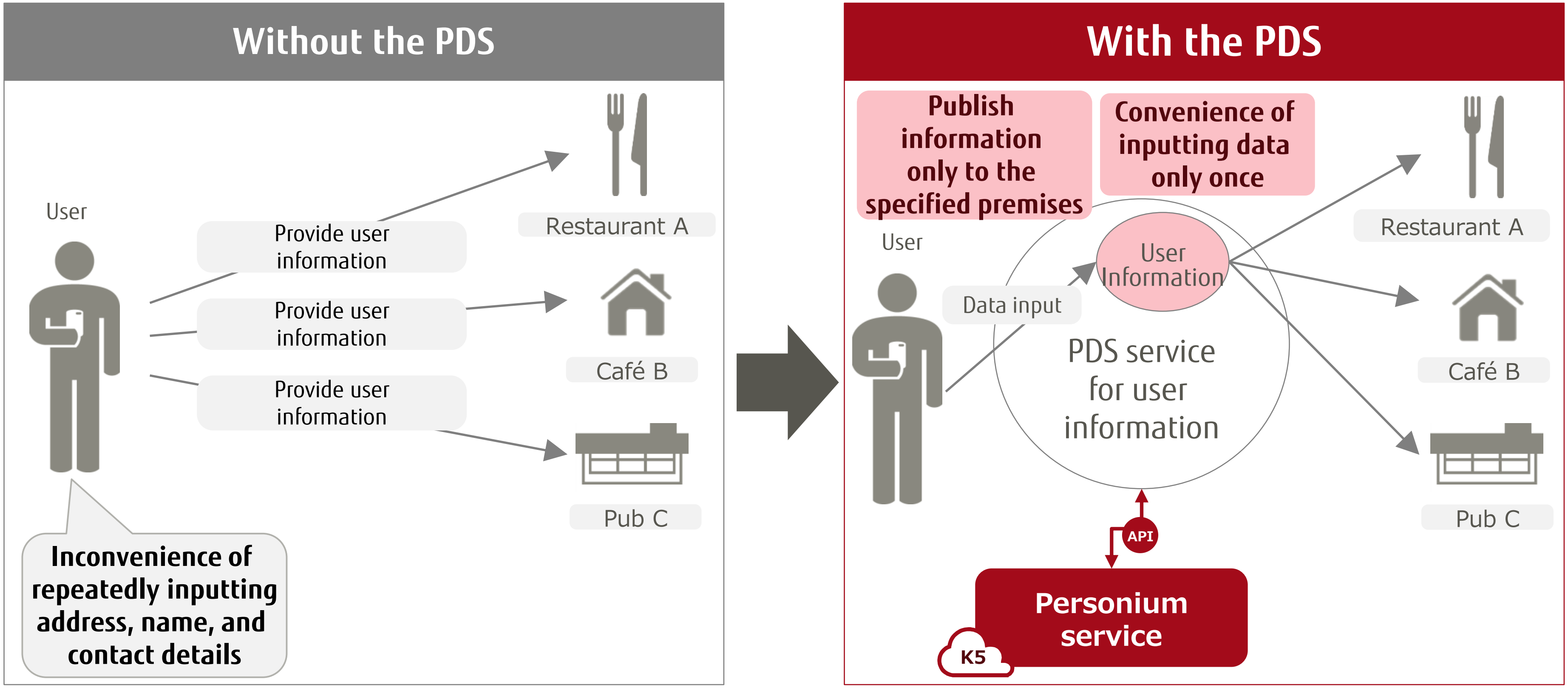


Obtain the care history data from the PDS
Data sharing makes linked care giving possible across agencies
Care recipient
Data input
Care information
PDS service for care information
API
Personium service
K5
Hospital
Welfare office
Care center

Usage Scenario 5

PDS business operator	User (Data subject)	Personal data	User (Data user)
Catering business	User	User information	Restaurant, café, pub

- Remove the inconvenience of repeatedly inputting user information when making reservations.
- User information control is enabled for the user.



Personium Service: Service Plan

Service Plan List

Menu	Unit	Note							
Basic Charge		Web Server		AP Server		DB Server		Initial Disk Size(GB)	Maximum Disk Size(GB)
		CPU	Memory (GB)	CPU	Memory (GB)	CPU	Memory (GB)		
Unit S Size	Month	1	2	1	4	2	8	300	1,300
Unit M Size	Month	2	8	4	16	8	32	1,600	3,600
Disk Addition Option									
200GB	Month	• By selecting this option, the Customer can add the disk size capacities as shown in the plans to the initial disk size provided as part of Personium Unit, up to the Maximum Disk Size. • Disk addition is reflected immediately after the application form is lodged via the K5 portal. • The Customer cannot decrease the disk size capacities added under this option. • When a basic charge plan is terminated, the service will be terminated automatically.							
500GB	Month								
1TB	Month								

Explanation of the Billing Model

- Billing by fixed monthly fee
- Fees are charged from the month in which the Personium Service start date occurs
- Fujitsu has no facility for calculating the fee on a daily pro rata basis

Restrictions and Notes

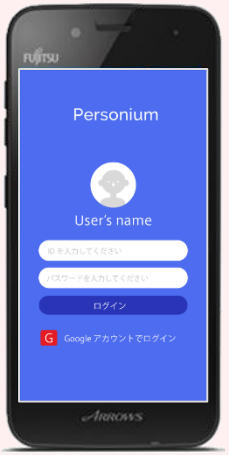
- The Customer’s PDS business application development environment and execution environment must be separately prepared by the Customer.
- The Customer shall bear responsibility for managing personal data handled by this Service, as well as any data registered independently by the Customer.
- For information on the regions in which Fujitsu offers this Service, please refer to the “Service Description” and the “PaaS Restrictions and Notes” at the Cloud Service K5 website.
- The time required from application lodgment to the start of service is:
  - Approximately 7 business days from the time an application is lodged via the Service Settings Application screen at the K5 PaaS Portal

Reference: Sample GUI Program

Standard GUI is available aimed at a range of PDS business usage scenes

- Publish key functions using sample code
- The customer is able to freely customize functions as necessary. As a result, the Service is quick to launch

Login

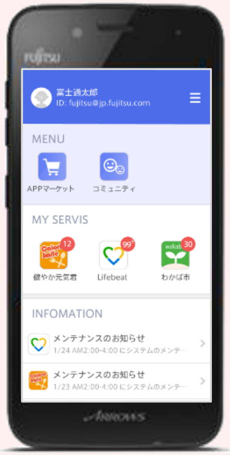

Personium

User's name

ID を入力してください

パスワードを入力してください

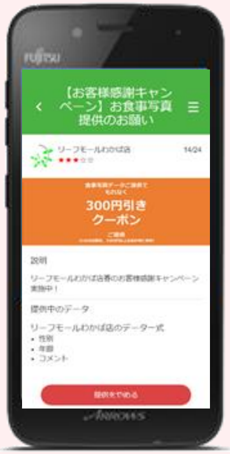
Menu screen


冨士通太郎
ID: fujitsu@jp.fujitsu.com

メンテナンスのお知らせ
1/24 AM2:00-4:00 にシステムのメンテ…

メンテナンスのお知らせ
1/23 AM2:00-4:00 にシステムのメンテ…

Data request details


【お客様感謝キャンペーン】お食事写真提供のお願い

リーフモールわかば店 14/24

300円引き
クーポン

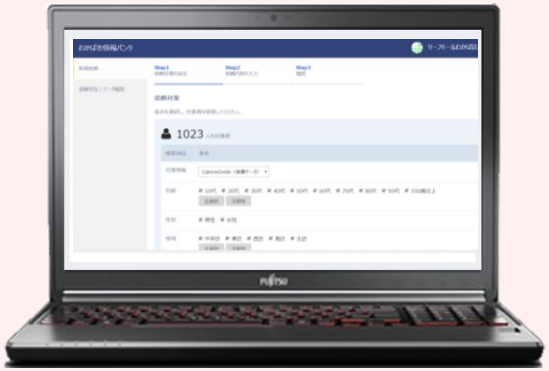
説明

リーフモールわかば店番のお客様感謝キャンペーン実施中！

提供中のデータ

リーフモールわかば店のデーター式
- 性別
- 年齢
- コメント

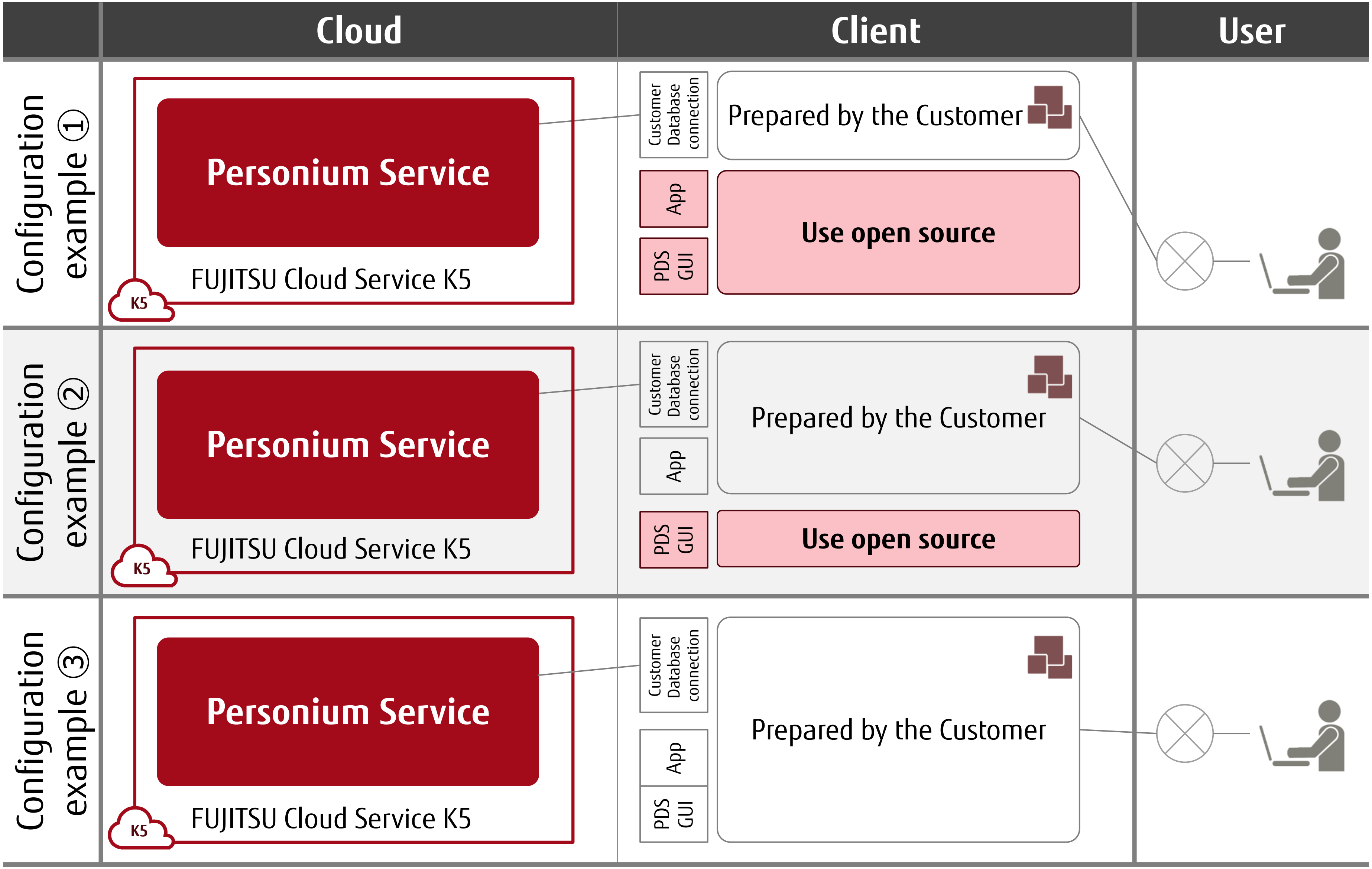
Operator's screen for requesting provision of data



Reference: Issues relating to the GDPR

- What is the General Data Protection Regulation (GDPR)?
  - A European regulation that obligates corporations, organizations and associates to protect personal data, primarily in terms of the handling of personal data. (Planned to go into effect on May 25, 2018)
    - GDPR Portal
      https://www.eugdpr.org/eugdpr.org.html
    - Fujitsu Enhances Personal Data Protections to Respond to the GDPR (Fujitsu press release)
      http://www.fujitsu.com/global/about/resources/news/press-releases/2018/0119-01.html
- The Personium-based PDS and services that use PDS provide easy-to-use capabilities in response to the newly defined rights for data subjects under the GDPR (the Right to Data Portability and the Right to be Forgotten).
  - Right to data portability
    The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format.
    - Capabilities within this service:
      By creating an application using the Cell Export API, the data subject is able to export all data in a cell.
  - Right to erasure ('right to be forgotten')
    The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay.
    - Capabilities within this service:
      By creating an application using the Cell Recursive Delete API, the data subject is able to delete cells and the data in cells.

Reference:
Examples of K5 Personium Service Usage Configuration



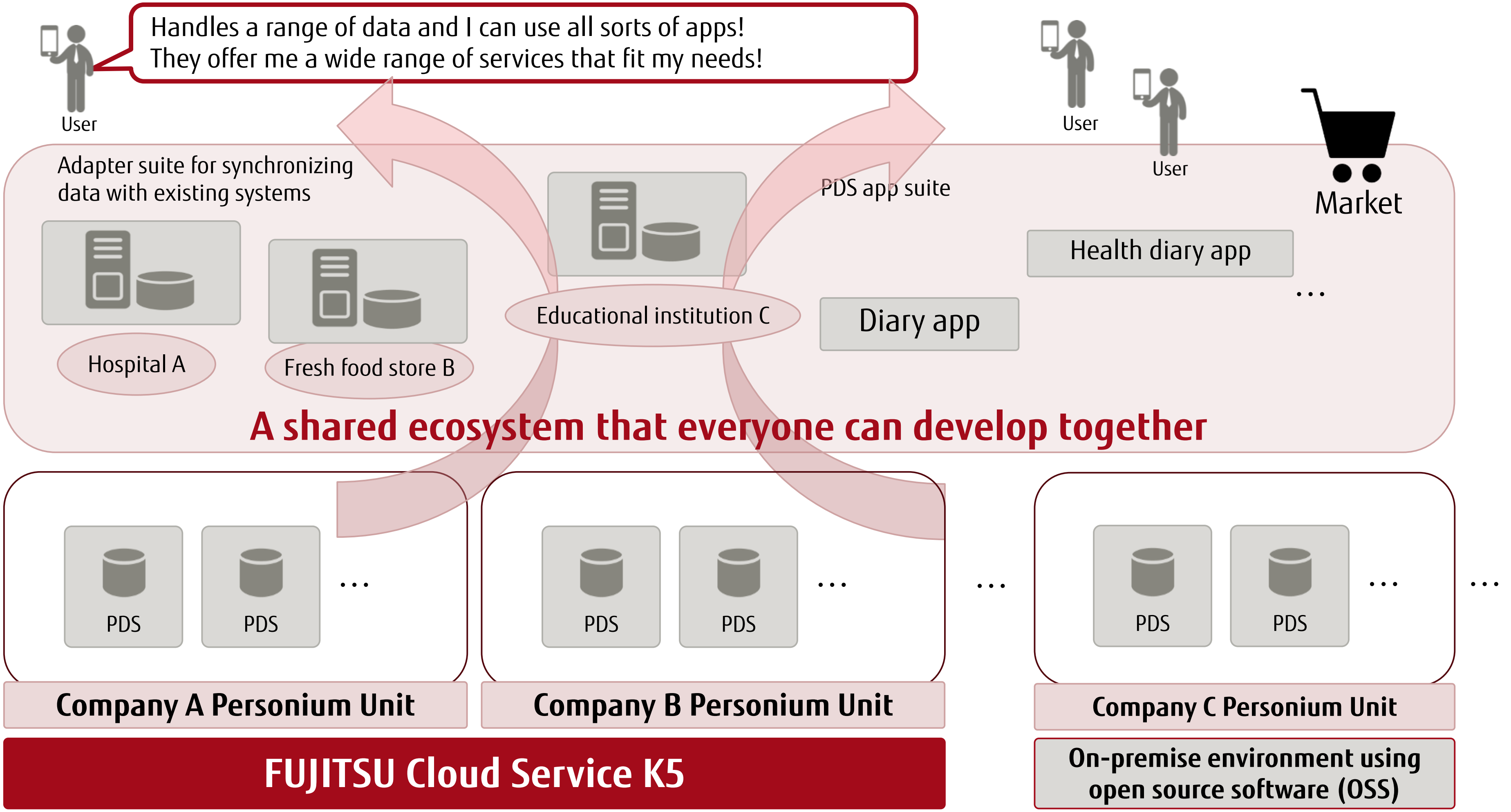
	Cloud	Client	User
Configuration example ①	Personium Service FUJITSU Cloud Service K5 K5	Customer Database connection App PDS GUI Prepared by the Customer Use open source	
Configuration example ②	Personium Service FUJITSU Cloud Service K5 K5	Customer Database connection App Prepared by the Customer PDS GUI Use open source	
Configuration example ③	Personium Service FUJITSU Cloud Service K5 K5	Customer Database connection App PDS GUI Prepared by the Customer	

Reference:
Working with the Customer to Co-create an Ecosystem

Vision of the future

Fujitsu aims to lay the foundations for an attractive market for users to publish information, using PDS applications and adaptors with existing systems. The PDS applications are created in Personium user ecosystems which include open source.

Note: You can also concentrate solely on building relationships with your customers and creating differentiators (special apps, GUI, etc.).



User
Handles a range of data and I can use all sorts of apps!
They offer me a wide range of services that fit my needs!
User
User
Market
Adapter suite for synchronizing data with existing systems
Hospital A
Fresh food store B
Educational institution C
PDS app suite
Health diary app
Diary app
…
A shared ecosystem that everyone can develop together
PDS
PDS
…
Company A Personium Unit
PDS
PDS
…
Company B Personium Unit
…
PDS
PDS
…
Company C Personium Unit
…
FUJITSU Cloud Service K5
On-premise environment using open source software (OSS)

FUJITSU

shaping tomorrow with you