Horizon 2020
European Union Funding
for Research & Innovation

CPaaS.io
City Platform as a Service – Integrated and Open

NICT

H2020-EUJ-02-2016
H2020 Grant Agreement Number 723076
NICT Management Number 18302

Deliverable D2.3

First Ethics Report

Version V1.0

June 30, 2017

ABSTRACT

Protection of personal data is the only potential ethics issue in the use cases of the CPaaS.io project. This report summarizes the findings of the ethics analysis performed for each project use case and gives an outlook what will be necessary for the upcoming use case implementations.

Disclaimer

Document Information

Editors	Stephan Haller (BFH)
Authors	Martin Strohbach (AGT), Alexander Overtoom (TTN), Toshihiko Yamakami (ACC), Hiroshi Amano(MSJ), Noboru Koshizuka (UoT), Chiaki Ishikawa (YRP), Katsunori Shindo (YRP)
Reviewers	Stefan Gessler (NEC)
Delivery Type	R
Dissemination Level	Public
Contractual Delivery Date	June 30, 2017
Actual Delivery Date	
Keywords	June 30, 2017

Revision History

Rev.	Date	Description	Contributors
0.1	16/05/2017	Table of Contents and initial	Stephan Haller (BFH)
0.2	01/06/2017	Added text for section 2.1 and section 3 (EUE)	Martin Strohbach (AGT)
0.3	02/06/2017	Description of ethics added by TTN	Alexander Overtoom (TTN)
0.4	13/06/2017	Description of ethics added by ACC	Toshihiko Yamakami (ACC)
0.5	13/06/2017	Description of ethics added by MSJ	Hiroshi Amano(MSJ)
0.6	14/06/2017	Description of ethics added by UoT and YRP	Noboru Koshizuka (UoT), and Chiaki Ishikawa (YRP), Katsunori Shindo (YRP)
0.7	20/06/2017	Introduction, Abstract and final editing	Stephan Haller (BFH)
0.8	27/06/2017	Description of ethics modified by MSJ	Hiroshi Amano(MSJ)
0.8r	30/06/2017	Review	Stefan Gessler (NEC)
1.0	30/06/2017	Final editing	Stephan Haller (BFH)

Table of Contents

1 Introduction

Some of the use cases in CPaaS.io deal with personal data. Protecting of such data is not only important to get people's acceptance of such a platform and the related applications and services, but it is also a legal requirement. How CPaaS.io is generally dealing with this issue, as well as respective procedures and policies have already been described in D1.1, Protection of Personal Data (POPD) Requirements, and the initial plan of how to apply this in the concrete use cases have been outlined in the initial Data Management Plan (D7.2).

This deliverable now describes how the concrete activities undertaken in order to protect personal data in the use case implementations for CPaaS.io.

2 Personal Data in Current Prototype Releases

2.1 Event Management – Enhanced User Experience

As part of the event management use case, AGT has collected personal data from 8 participants at the Color Run in Utrecht in the Netherlands (see Deliverables D2.1 and D2.2). According to German law AGT has informed and reviewed the activity with his data protection officer. Informed consent forms have been provided to each participant. All participants have signed the forms. The form is attached in the Appendix of this deliverable.

As described in the first version of the CPaaS.io data management plan (D7.2) AGT has, quote, "implemented appropriate technical and organizational measures to ensure generated data is protected from unauthorized or unlawful processing, accidental loss, destruction or damage. We review our information collection, storage and processing practices regularly, including physical security measures, to guard against unauthorized access to our systems. We restrict access to generated data to only those employees, contractors and agents who strictly need access to this information, and who are subject to strict contractual confidentiality obligations."

2.2 Event Management – Sapporo Visitor Experience

The Open Data Distribution Platform System manages visitors experience information which is related to tourism and sports events organized by Sapporo city. We don't have any personal information in the system.

To deal with information of Sapporo city we adopt a Create Commons (CC) license. CC licenses are a tool for copyright holders to define under what can terms and conditions their creation can be used. Most interesting is the CC-BY license which only requires to name the author of the creation in order to use it.

Security measures for the Open Data Distribution Platform System are to adopt a segmentation architecture between the global segment and the private segment from the network point of view. Access to the global segment is like accessing the Internet network environment through a firewall and Internet gateway. Access to the private segment is limited by authorization.

The system and network environment above is structured under the Microsoft Azure service environment. It is certified by cloud security and operations standards under ISO and public market organizations:

- ISMS : ISO/IEC 27001
- International Privacy Standard : ISO/IEC 27018
- Security management standard for cloud services: JASA CS mark as Gold
- Common information security standard for government agency in Japan : NISC common standard
- Online service system and account settlement with financial institution : FISC security standard

2.3 Event Management – Tokyo Management of Service Vehicles

As part of the Tokyo Management of Service Vehicles, we are currently investigating use cases for field tests. We are not collecting any personal data or any data to be protected so far.

The ethics issues will be appropriately addressed when new contexts that require ethics consideration are identified and dealt with in our platform.

2.4 Waterproof Amsterdam

As part of the Waterproof Amsterdam application, we are currently collecting data from one pilot water buffer device in Amsterdam. This concerns a so called 'smart rooftop', with a water buffering mechanism that controls the outflow of rain water from the rooftop to the sewerage. Additionally, sensors are measuring temperature, humidity and wind speed on the rooftop.

The data we are collecting from the device's API consists of sensor readings and metadata such as geolocation. We are not collecting any personal data (e.g. name and residential address of the buffer device owner). Concerning the geolocation of the water buffer, while the location is stored into the FIWARE IoT Broker, there is no direct relation to any person or company. In the near future, the data access will be secured via SSL encryption.

Further, the backend of the Waterproof application, which currently runs stand-alone from CPaaS.io, does not actually use the data that is published on the device APIs of the water buffer manufacturers. These data are for the time being merely formatted and stored into the FIWARE IoT broker.

So, the data processed by the Waterproof application are anonymous. Any personal data remains in the database of the retailer of the buffer devices. This also applies to any following locations and devices we are connecting to the Waterproof application.

2.5 Yokosuka Emergency Medical Care

The on-going Yokosuka Emergency Medical Care project is to introduce modern ICT, such as IoT technology, in the emergency medical care practice. Currently, it has installed a camera inside ambulances and sends the images of the patients to doctors at the hospitals for early diagnosis and selection of proper hospital wards depending on the condition of the patients. The system also plans to streamline the dispatching of ambulances, but that aspect does not have any privacy concern for now.

The medical practice inside the ambulance adopts the ordinary privacy protection policy and procedure in the general medical community. So there is nothing new in that regard except for one thing.

The image of the patient is considered private data. So before the system was installed, the City of Yokosuka which operates the ambulances for emergency medical care reported the usage of the system to the "Committee to evaluate the protection of privacy data" of the City of Yokosuka for the committee's opinion. Today the system's principles of operation require that an ambulance with this system needs a visible sticker that explains that the live image of the patient is transmitted to doctors in remote hospitals, and the consent from the patient or the party who accompanies the patient needs to be obtained before the image is thus taken and transmitted. The committee did not object the usage of the system because it regards the operation as being in compliance with the Japanese privacy protection laws and regulations. Also no party who has been transported by these ambulances objected to the taking and transmission of the live images.

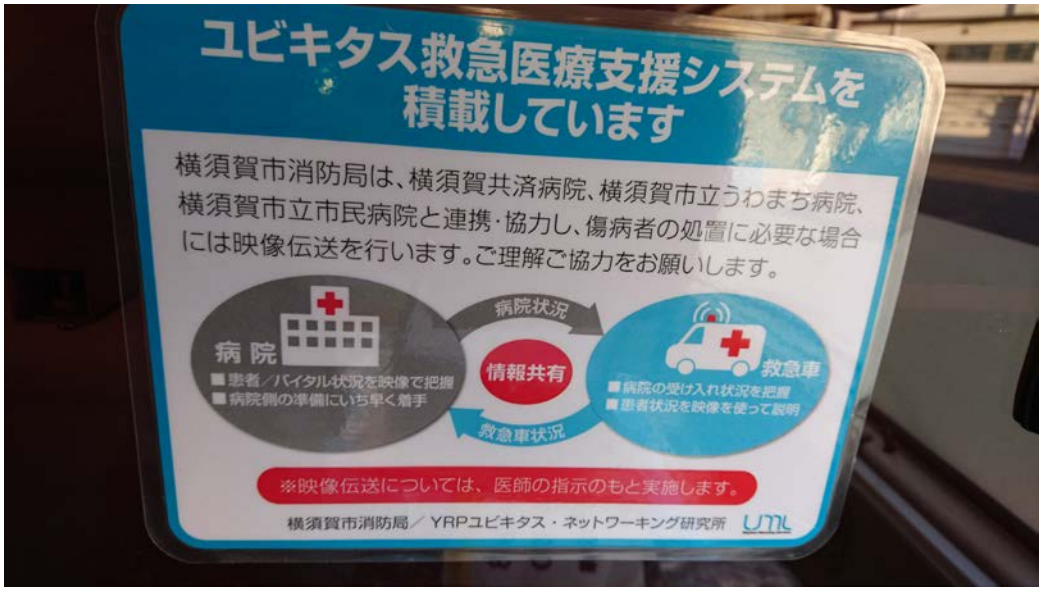

Figure 1: sticker inside the ambulance in the City of Yokosuka which explains the transmission of images.

This privacy angle regarding the live image transmission in an ambulance can be generalized. There is a school of thought that suggests emergency medical care sometimes needs to be allowed to override the privacy concerns. What if the patient in an ambulance or in emergency ward is unconscious, say, under coma, and no one seems to have the power of attorney, so to speak, to give the permission to let others to research and retrieve the patient's past history from the hospitals the patient may have visited before, for example. The patient may die due to improper care caused by the scarcity of past medical history. This is not an idle philosophical question and often heard outside Yokosuka, too. This issue needs to be formulated and solved once and for all before the real benefit of emergency medical care in ICT age is enjoyed by everyone including an unconscious patient carried by an ambulance. Unfortunately, the current laws and regulations are not clear on this issue. That was why the City of Yokosuka was forced to consult its Committee to evaluate the protection of privacy data before the system was installed.

Based upon our experience in Yokosuka and the ongoing discussion about this emergency vs. privacy protection mentioned above, the template of the consent form discussed by the Japanese partners to be used in CPaaS.io Japanese prototypes (more about this in the next section: "3 Future Plans") includes the following clause:

The Association shall not disclose or provide the Member's Personal Information to a third party unless one of the following conditions is met

…

(3)when there is a pressing need to protect the life, body or the property of the Member and obtaining the agreement from the Member in question in a timely manner is difficult

Solving this privacy issue regarding one's medical information in case of medical emergency in a legally satisfactory form completely is beyond CPaaS.io itself. However, YRP and its partners will be ready to create input to proper legal and government bodies if asked for an opinion on this matter.

3 Future Plans

Later this year AGT is planning to conduct a deployment at another Color Run in which similar data will be collected as in the Utrecht Color Run. We will review this activity with our data protection officer and provide updated informed consent forms targeted at this specific activity to the participants.

For the EU-Japan joint use case we are currently discussing the possibility to apply Color Run analytics at the Sapporo Snow Festival. The scenarios under discussion would also involve the collection of personal data and using signed informed consent forms. We would also need to clarify the regulations on how personal data collected in Japan can be made available to European partners.

Aside from the EU-Japan joint use case, the Japanese partners have been discussing a possible generic template for consent form for the collection of personal data to be used in Japan. That is attached as appendix 3.2 (translated from the original Japanese so that it can be shown to visiting tourists who understand English.)

This template has been created by adhering to the requirements of the Japanese laws and regulations regarding the online privacy data (Act on the Protection of Personal Information in particular[1]). We have strived to make this template compatible with the law, and also make it easily agreeable by the majority of service recipients (i.e., the individuals who will consent to provide personal information to receive some ICT services) based on the partners' experience in the Sapporo trial and other experiences. The Japanese partners intend to base future consent forms on this template during CPaaS.io. The law has been modified and a new version has been announced and put into effect since May, 2017. So the Japanese partners will accommodate the necessary changes to bring the template into a form compatible with the May, 2017 version of the law. We hope to report the successes/failures of the usage of the template in the future prototypes in the next version of this deliverable.

[1] For details about this act, see http://www.japaneselawtranslation.go.jp/law/detail_main?id=130

Appendix A: Consent Forms used by AGT in Color Run Utrecht

CONSENT FORM

Event members

Thank you for agreeing to be supplied with smart bracelets, smartphones, smart chest straps and a mobile camera that will collect information about you when you are wearing it ("the wearables") during your attendance at the **Color Run Event on 11th September 2016 starting 11:00am at Haarrijnseplas, Utrecht, The Netherlands**.

This notice sets out how AGT Group R&D GmbH, Hilpertstrasse 35, 64295 Darmstadt ("we" or "us") will use the information collected from the wearables ("your data"). Your data will only be collected, used, retained, disclosed, transferred (together: "processing") and secured in accordance with applicable data protection law.

The wearables and smartphone sensors will collect information about your location, motion (hand and body movements based on acceleration and gyroscope sensors), heart rate and inter-beat (RR) intervals, data on breathing, emotional arousal (based on galvanic skin response/skin conductance), distance travelled, step counts, calories consumed, contact data, skin temperature, environmental conditions (UV light, ambient light, barometric pressure, altitude). The wearables will also collect video data about other participants running with you and collect audio information about yourself. Video data about yourself may be collected by other participants using the wearables during the event. We will require your email address in order to contact you about your data.

The purpose of the data collection effort is to compare the performance of wearables for detecting your activities and emotional responses throughout the event. We will only use your data for (i) research regarding the development of new products and services, (ii) user experience optimization, (iii) improving event operations, and (iv) statistical analysis. Your data will be collected using the provided wearables and after the event will be transferred to our servers and to third party cloud storage Amazon S3 operated by Amazon Web Services, seated in 410 Terry Avenue North, Seattle WA 98109,United States. The data will only be processed in an environment on servers within the European Economic Area (EEA). Please note that your data will not be processed in order to make decisions about you in a personal capacity. After your data has been initially collected, your data will be linked with a pseudonym. Your email address will be stored separately from the data collected by the wearables but may be linked to the pseudonym. Your email address will only be used to ask you questions that will help us better understand your data. The remaining data will be anonymized insofar possible. Your data will be deleted from our servers in 5 years.

We have implemented appropriate technical and organizational measures to ensure that your data is protected from unauthorized or unlawful processing, accidental loss, destruction or damage. We review our information collection, storage and processing practices regularly, including physical security measures, to guard against unauthorized access to our systems. We restrict access to your data to only those employees, contractors and agents who strictly need access to this information, and who are subject to strict contractual confidentiality obligations.

We may share your data with consortium members of the EU (grant agreement number 723076) and "National Institute of Information and Communications Technology" from Japan (management number 18302) jointly funded project CPaaS. (Current members of the consortium are: "Bern University of Applied Sciences", Falkenplatz 24, 3012 Bern, Switzerland; ‘‘AGT Group (R&D) GmbH", Hilpertstrasse 35, 64295 Darmstadt, Germany; "NEC Europe Ltd", West end road Athene Odyssey Business Park South RUISLIP, London HA4 6QE; "Odin Solutions S.L.", Poligono Industrial Oeste, Calle Perú, 5, 30820

Alcantarilla, Murcia, Spain; “University of Surrey”, Institute for Communication Systems, Stag Hill Campus, Guildford, GU2 7XH, United Kingdom; “The Things Network”, Herengracht 182, Amsterdam 1016 BR, The Netherlands; “YRP Ubiquitous Networking Laboratory”, YRP Center No.1 Building, 3-4 Hikarino-oka, Yokosuka-City, Kanagawa-Prefecture, 239-0847, Japan; “Microsoft Corporation”, One Microsoft Way, Redmond, WA 98052-7329 USA; “ACCESS CO.”, Daito Building, Kandaneribei-cho 3, Chiyoda-ku, Tokyo 101-0022, Japan; “Ubiquitous Computing Technology Corporation”, 2-12-3 Nishi-Gotanda, Shinagawa-ku, Tokyo 141-0031, Japan; “The University of Tokyo”, 7 Chome-3-1 Hongo, Bunkyo, Tokyo 113-8654, Japan.) We will only share data containing pseudonyms as described above, but not share any personal identifiers such as emails.

By default we will not disclose your data to any other third party. However, some of the wearables use third party software of TomTom International B.V. (De Ruijterkade 154, 1011 AC Amsterdam, The Netherlands), Carré Technologies Inc. (5800 Rue Saint-Denis #402a, Montréal, QC H2S 3L5, Canada), and Polar Electro Oy (pääkonttori, Professorintie 5, 90440 Kempele, Finland) which may process your location and movement, heart rate, data on breathing, and calories to servers outside of our control. This processing is subject to the terms and conditions of the applicable third party. We will not enrich the sensor data uploaded by this software with any other personal data such as your email address.

Some of the operators of third party software as well as some consortium members of the project CPaaS.io may store your data in countries which may not have the same level of data protection as in the European Union (Third Countries). Recipients of data in Third Countries are not bound to the regulations of the German Federal Data Protection Act (Bundesdatenschutzgesetz) and the European data protection rules. Therefore, it is possible that Relevant Data might be transferred to other authorities; governmental control mechanisms; other third parties and judicial protection might not be available.

Your consent is voluntary and can be revoked at any time with effect for the future by notifying us via userinfo@agtinternational.com. You can also at any time return the wearables to AGT representatives, Hilpertstraße 35, 64295 Darmstadt, if you no longer agree to the processing of your data and wish to revoke your consent to the processing.

If you wish to access, correct or delete the personal information which we have collected about you, or if you have any questions regarding this notice, please contact us at userinfo@agtinternational.com

By signing below you confirm that you have read this notice and you agree that your personal information may be collected, processed and used as set out in this notice.

SIGNATURE

PRINT NAME _____

DATE _____

EMAIL: _____

Appendix B: Consent Forms used in Japan – Draft Standard on agreement on the handling of personal information

The parties who wish to use the Service register their own personal information (hereinafter referred to as Personal Information) to the Service. (Hereinafter these parties are referred to as Members.) This agreement (hereinafter referred to Agreement) defines the proper handling of Personal Information between the Association and the Members. Members shall offer the Personal Information ONLY AFTER they understand the content below and agree to it. The Association shall handle the Personal Information properly according the "Basic Policy of Handling Personal Information" of the Association to prevent the leak of personal information.

Article 1: The overview and goal of the Service

This goal of this Service is to enable the Members to receive high-quality service that fits the preference or likes/dislikes of the Members from the service providers (hereinafter referred to as Servicer), by providing the individual attributes, preference and wishes (these are collectively called personal information in this Service) of the Members to the Servicer. This Service is not for the CRM (Customer Relationship Management) of the Member's personal information done by corporations, etc. This service is for letting the Members perform VRM (Vendor Relationship Management) by controlling the provision of Personal Information to Servicers on their own in order to receive customized service from the Servicers. The handling of Personal Information in the Service is done on the principle that the Members have the ultimate authority over the handling based on this agreement, relevant laws and regulations.

Article 2: The Objective of the Use of Personal Information

The Association uses the Personal Information properly as the need arises in order to execute the Service and the following projects (hereinafter referred to as Project).

(1) *****

(2) *****

Article 3: Voluntary Nature of Information Provision

The range of the provision of the Personal Information by the Members is arbitrary and is up to the Members. Members shall understand that if there is personal information that is not provided by the Members, the feasibility study experiments in the Project may not be executed fully, and the Members may not be able to receive the Service and the service provided by the Project.

Article 4: Accuracy of Personal Information

Members shall not provide false Personal Information.

2 Members shall upgrade the Personal Information to keep it current when the information changes as often and timely as reasonably possible.

3 Members shall understand that if the Personal Information provided by the Members is not correct or inexact, the Service provided by the feasibility experiment in the Project to the Members may not have a satisfactory quality.

Article 5: The Right to Provide the Personal Information

The right to decide whether or not to provide the Personal Information of a Member belongs to the Member. The right to correct or delete the Personal Information, or decide to which Services the Personal Information is provided belongs to the Member who has provided the Personal Information.

Article 6: Provision of Personal Information to the Third Parties

The Association shall not disclose or provide the Member's Personal Information to a third party unless one of the following conditions is met.

(1) when there is an agreement from the Member to provide the information to Servicer in a manner defined in Article7

(2) when the data is published as a statistical data by which an individual identification is impossible

(3) when there is a pressing need to protect the life, body or the property of the Member and obtaining the agreement from the Member in question in a timely manner is difficult

(4) when the information is requested on legal ground by the courts of law, prosecutor's offices, and police offices and other government offices

(5) when laws and regulations mandates such provision

(6) when Article11 and/or 12 apply

Article 7: The Method of Provision, etc.

The Association shall provide "CPaaS.io Portal App" in the form of a website or in the form of an application to make it easy for Members to provide, review, correct, and delete Personal Information, and also to agree to the provision of the Personal Information to Servicers. Members shall be able to perform the following actions any time using the CPaaS.io Portal App.

(1) Provision, correction and deletion of the Personal Information of the Member's own to the Association

(2) Agreement to provide the Personal Information to a Servicer, and the withdrawal of such agreements

Article 8: Transparency of Provision

By using the CPaaS.io Portal App, Member can identify the Servicers to which the Member has provided the Member's own Personal Information by using the App any time.

Article 9: Disclosure, Correction and Deletion of Personal Information

When the request for disclosure, correction, stopping the usage, withdrawing the provision to Servicers, deletion, the disclosure of the purpose of the usage, etc. of a Member's Personal Information is received from the Member who has provided the information via CPaaS.io Portal App and other means, the Association responds according its internal rules as much as possible in a reasonable time.

2 The person in charge of the management of the Members' Personal Information is the Managing Director of the Association.

Article 10: Security Management

The Association shall continue to apply the proper security measures, both technical and organizational, to avoid the risks of illegal access, loss, erasure, unwanted alteration, leak, etc. of Members' Personal Information.

Article 11: Shared Use of Personal Information in the Execution of the Project

The Association may use the Personal Information in a shared manner among the main contractor of the Project and its partners in the Project listed in the Association's website in order to execute the Project.

(1) Purpose of the usage: to be used during the execution of the Project

(2) Personal Information that will be shared: all the information provided as Personal Information

(3) The scope of the partners who will share the information: the main contractor of the Project and its partners in the Project listed in the Association's website

(4) The responsible party for the management of Personal Information: Association for IoT Services Coordination, a general incorporated association.

Article 12: Escrow of Personal Information for the Execution of the Project

The Association may put the Personal Information in an escrow at corporations that satisfy the reasonably high information management criteria defined by the Association (the corporations shall be listed in the Association's website) for the execution of the Project.

Article 13: Disposal

The Association shall dispose the Personal Information after applying security measures such as protection against illegal access by the third party, etc. according to the internal procedure of the Association.

Article 14: Inquiry

Inquiry regarding the Personal Information, or the request for disclosure, correction and deletion of the Personal Information can be done by using the CPaaS.io Portal App. Other inquiries should be addressed to the following:

Address.....
Organization Name.....
TEL：+81-3-****-****
E-mail：*****@***.***

Article 15: Miscellaneous

(1) The formation, validity and performance of this Agreement shall be, in all aspects, governed by and interpreted under the laws of Japan.

(2) This Agreement shall be created in Japanese. It is free to create the reference translation of the Agreement in other languages in so far as the interpretation of the Agreement is concerned, the Japanese language version shall prevail.

(3) Matters not stipulated in this Agreement and any other ambiguities which arise in relation to this Agreement shall be settled through consultation in good faith by the parties involved.

(4) If the consultation does not settle issues, any proceedings relating to the content and execution of this Agreement shall be subject to the exclusive jurisdiction of the ***** Court or ***** Court as the first instance.

Article 16: Agreeing to this Agreement

When a Member agrees to this Agreement, the Member shall perform one of the following actions below.

(1) If this Agreement is displayed electronically, please enter the date and your name in the designated fields and push the "Register" button.

(2) If this Agreement is provided on paper, please enter the date, and put your name and a seal or put your signature and send the agreement to the Association.

Day: Month: Year:		Name in Full	