INFORMATION TECHNOLOGIES FOR SHIFT TO RAIL

D7.8 – White Paper on Ethics, Privacy and Security Aspects of IT2Rail

Due date of deliverable: 30/11/2017

Actual submission date: 27/06/2018

Leader/Responsible of this Deliverable: THALES

Reviewed: Y

Document status		
Revision	Date	Description
01	07/11/2017	First issue
02	29/01/2018	Document updated after adding EPS experts contributions
03	17/06/2018	Document updated after adding IT2Rail partners contributions
04	27/06/2018	Final Version after TMC approval and Quality check

Project funded from the European Union's Horizon 2020 research and innovation program		
Dissemination Level		
PU	Public	X
CO	Confidential, restricted under conditions set out in Model Grant Agreement	
CI	Classified, information as referred to in Commission Decision 2001/844/EC	

Start date of project: 01/05/2015 Duration: 36 months

REPORT CONTRIBUTORS

Name	Company	Details of Contribution
Rui Lourenço	THALES	Document originator
Cristina Hernandez	UITP	Contributor
Yves Amsler	UITP	Contributor
Franck Dumortier	EPS Expert	Contributor
Javier Warleta	EPS Expert	Contributor
Stefano Persi	EPS Expert	Contributor
Mary Sharp	EPS Expert	Contributor
Marco Ferreira	THALES	Reviewer
Maria Laura Trifiletti	RINA C-BE	Quality check

EXECUTIVE SUMMARY

This White Paper introduces the Ethical, Privacy and Security (onwards EPS) challenges raised during the development of IT2Rail[1], one of the Shift2Rail lighthouse projects. Therefore, it analyses and proposes some paths to ease the future implementations of the so-called "Web of Transportation"[2] while assuring a respectful EPS service for all the European society.

Indeed, these topics are a cornerstone of any sustainable multimodal[3] system. Making transport seamless all across Europe is a complex task where the system needs to be flexible, while establishing an efficient flow of travellers. At the same time, these activities face a broad spectrum of threats, from cyber-attacks to ethical risks and potential concerns and misuses of personal data rights and interests.

IT2Rail provides a preliminary technical demonstration based on the application of semantic technologies in the transport sector, a test of the future so-called "Web of Transportation". The application of a semantic web may leverage the path for a seamless multimodal travel in Europe. However, it may also create new challenges, in particular EPS challenges which need to be properly and accurately addressed.

Some of the main questions are focused on data collecting and sharing issues: (1) the ethics and privacy issues related to the recording of user preferences and other personal data stored, (2) the needs for data protection when it comes to exposing travellers and operators data (in different measures), which opens the way to hacking and interference with privacy valuable information, (3) the security aspects related with the publishing of services and products into a common Interoperability Framework[4] (onwards IF), (4) the anticipation of potential problems resulting from data sharing and interaction with law enforcement agencies, as well as (5) the consequences of the implementation of the recently announced General Data Protection Regulation (onwards GDPR[5]) and Directive on Security of Network and Information Systems (onwards NIS EU[6] Directive).

[1] "IT Solutions for Attractive Railway Services": http://www.it2rail.eu/

[2] Term used in the "Shift2Rail - Multi Annual Action Plan" (Brussels, November 2015). See explanation on paragraph 3 of this section.

[3] "Multimodality is the possibility to shop and book and to travel using a combination of different modes of transport combined to offer a full travel solution for a customer's door-2-door mobility query. It includes 2 business models: co-modality and multimodality". Source: IT2Rail newsletter, September 2016.

[4] "An interoperability framework is an agreed approach to interoperability for organisations that wish to work together towards the joint delivery of public services. Within its scope of applicability, it specifies a set of common elements such as vocabulary, concepts, principles, policies, guidelines, recommendations, standards, specifications and practices". Source: Annex 2 to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions "Towards interoperability for European public services" (COM(2010)744 final), chapter "Definitions".

[5] http://ec.europa.eu/justice/data-protection/

[6] Directive on security of network and information systems: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

It is important to stress that EPS issues have a high value for citizens, because they are perceived as “directly linked” to individuals’ dignity. Technologies like the IF could benefit individuals, for example, when it facilitates access to new tailored services with an added value while ensuring their personal rights. However, the benefits of these systems may be perceived as ”with drawbacks”. That’s why it is key to ensure the protection of these rights and to explain how the IF could benefit the citizens, in particular avoiding the loss of privacy, blocking any type of un-ethical consequences derived and ensuring a security network. European society is particularly susceptible to EPS challenges, thereby they need to be ensured. Indeed, the work developed in IT2Rail should ensure how the implementation of the IF technology does not increase the risk of suffering any of the previously listed challenges, while it may contribute to ensure the security and privacy of the systems and services that would emerge within a Shift2Rail IP4[7] ecosystem.

Many of these concerns already exist in other sectors of today’s digital economy. Internet payment systems, social networks, internet hotel booking companies and a lot of other internet based solutions that every one of us is using today are already dealing with similar ethics, security and data privacy concerns.

The main conclusions that can be derived from this White Paper point out that:

- (1) privacy should be achieved by compliance with the EU privacy and data protection legislation, ethical and societal acceptance, as well as any other aspects that are at stake, and
- (2) the interoperability framework may offer new technical possibilities to effectively ensure the compliance with the EU legislation. Since the Interoperability Framework acts as “a wire” regarding its involvement in privacy, it does not collect any data, leaving the whole responsibility to comply with GDPR to the interconnected actors. So, it is recommended to add additional services based on this regulation, e.g. to allow travellers to ask to delete/modify their own personal data in all the nodes requesting data portability.

Moreover, to join the (semantic) web of transportation ecosystem, a partner just needs to publish its service on the internet. However, there is not yet a mechanism to ensure the trustfulness of the actors joining the system. The IF sets out a new arena where to develop different solutions to guarantee this level of trustfulness. E.g. mechanisms such a Service Registry, a place where the joining party is able to describe who is authorized to use their services, could be implemented to guarantee a certain level of trust.

[7] IP4: Innovation Programme 4 of Shift2Rail. For more information, please click on the link: https://shift2rail.org/research-development/ip4/

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

EC	European Commission
ECHR	European Convention of Human Rights
EPS	Ethics, Privacy and Security
EU	European Union
GDPR	General Data Protection Regulation
IF	Interoperability Framework
IP	Innovation Programme (as part of the Shift2Rail work programme)
ISO	International Organization for Standardization
IT	Information Technology
KPI	Key Process Indicator
MaaS	Mobility as a Service
NIS	Directive on Security of Network and Information Systems
UITP	International Association of Public Transport

INTRODUCTION

The recommendations made on this White Paper may affect not only the case of the IT2Rail, but also all other projects which are part of the Shift2rail IP4, as well as the later implementation of these services into real-life environments to the benefit of travellers, suppliers, operators, public authorities and the civil society at large. In some occasions, in particular when addressing ethical issues, potential challenges[8] may be described. When possible, it is recommended to implement the suggested solutions at the very beginning of the projects to ensure their right development.

When figuring out the challenges faced by IT2Rail, it is important to note that many of them are not new and are already being addressed in other areas, such as Online Hotel Booking Services, Online Flights Booking Services and many other Internet Payment Services. Throughout this White Paper, references are made to studies on how these challenges are being considered in other areas. However, special focus is given to the novelties brought by IT2Rail, i.e. the creation and availability of an open published Semantic IF based on transport ontologies, allowing transport incumbents and newcomers to join and publish their services and products in the future "Web of Transportation" in a very simple manner[9], considering mechanisms to guarantee a certain level of privacy and security trust when joining this ecosystem.

Two key observations follow:

- Privacy is achieved by compliance with the EU privacy and data protection legislation. Privacy and protection of personal data are fundamental rights, which ensue from Article 8 of the European Convention on Human Rights (ECHR). These rights are now included in a wide range of pieces of legislation at European level. Protection of personal data is currently mainly regulated at European level by Directive 95/46/EC[10] (hereafter "the Directive") as implemented by the Member States' national law[11]. However, after over four years of discussion, a new EU data protection framework has finally been reviewed and adopted in May 2016. It takes the form of a Regulation – the General Data Protection Regulation[12] (hereafter "GDPR") –, which repeals the current Directive and is directly applicable in all Member States as from 18 May 2018 (without the need for implementing national legislation which is the case for a Directive). Both the Directive and the GDPR contain principles applying to the processing of personal data: these must be processed

[8] At this stage it was possible to identify additional challenges that may be analysed throughout the upcoming stages of the IP4 Shift2Rail projects.

[9] See IT2Rail White Paper on Business Ecosystem.

[10] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[11] Other relevant legislation applies: Regulation (EC) No 45/2001 establishing the European Data Protection Supervisor; Directive 2002/22/EC (Universal Service Directive); Directive 2002/58/EC (Directive on privacy and electronic communications); Regulation (EC) No 2006/2004 (the Regulation on consumer protection cooperation); Directive 2009/136/EC amending the three latter legislation.

[12] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), (OJ L 119, 4.5.2016).

according to the following principles: 1) lawfulness, fairness and transparency, 2) purpose limitation, 3) data minimisation, 4) accuracy, 5) storage limitation, 6) integrity and confidentiality, and 7) accountability.

- Attention should also be paid to resilience of interoperable IT systems in the sector of transport/and or using cloud computing solutions. These systems should take into account the security requirements and incident notification procedures of the NIS directive[13] where applicable. Indeed, operators in air transport, rail transport and road transport are considered as "operators of essential services" under article 5 of this Directive, but it is not the case of local public transport (e.g. for rail, only mainline operators are in the scope, and urban rail systems are not). Indeed, the interpretation of the scope of the NIS Directive depends upon Member States. Moreover, cloud computing services are considered as "providers of digital services" as per article 16 of this Directive.

1. CHALLENGES

The current background for travelling[14] within and across Europe is that different transport operators providing services on different modes use different and often heterogeneous systems to support/implement their travel services. Furthermore, many new travel services on demand – like Mobility as a Service (MaaS) - are quickly developing. Specifically referring to the digital aspect of transport systems, a number of standards, specifications and conventions indeed already exist. Despite their eventually large implementation they lack a broad and general interoperability when addressing the whole transport system (therefore including all transport modes). In addition, making transportation seamless all across Europe is a complex task, always in development, where the system needs to be flexible to allow the entrance of new high added value services.

A first analysis of the "Web of Transportation" concept[15], from the ethical perspective, raises several challenges that should be taken into account when designing the actual IP4 solutions, but also may be helpful to identify some opportunities to introduce an overall technical solution to overcome particular ethical problems (specially related to privacy but not only) in the relationship between travellers and services providers in the transportation chain. In other words, from the EPS point of

[13] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

[14] Travel includes transport services, when a "traveller" is on-board (then, as "passenger"), and travel services which can be offered either in departing, transfer or arrival multimodal stations, or even outside of the transport systems (like hotel booking, access to a museum, participation to a big event, etc.…).

[15] Indeed, different organizations have understood the benefits of establishing a real European wide implementation of semantic technology to achieve interoperability within a Single European Transport Area. This future scenario where companies and organizations could just plug-and-play into this new transport ecosystem based on Semantic is called "Web of Transportation". It is envisioned, for the benefits of everyone that the "Web of Transportation" will be a new European digital ecosystem easy to join that foster the appearance of new tailored services to the European citizens.

view, there is a crucial design decision that has to be made as soon as possible: how may the Web of Transportation play an active role by providing technical mechanisms which will help all players to implement privacy friendly services, ensuring the travellers' rights?

Of course, privacy is not the only ethical aspect that should be assessed here, but other ethical and security issues that could arise (e.g. any kind of discrimination based on gender, digital divide, etc.) seem to be either out of the scope of the Web of Transportation or so generic as not to be dealt with in this paper.

It is important to remark that one of the aims (probably the key one) of the Web of Transportation is to become a business facilitator / accelerator for all the traveller transportation ecosystem, and its success or failure will mostly rely on the acceptability of this system from all stakeholders, including travellers. Purely legal compliance could not be enough to guarantee it.

1.1 HANDLING DATA

With the clear need to address the ethical and legal requirements linked to the privacy and data protection issues, special emphasis is given to the aspects of collection, control, processing, sharing and storage of personal data made available by the travellers.

In addition to the Data Management Plan [16]of IT2Rail, some specific considerations are necessary in the context of data sharing, in terms of challenges and opportunities.

In the next real implementation of the IP4 results, when building on the outcomes of IT2Rail, data collected by any entity will have to be declared (in terms of type and criticality for privacy and business) to the National Authorities/Agencies responsible for Data Protection. Every entity involved in handling data in some way has to do this at national level, not only the entities collecting data, but also the ones in charge of storing or processing it.

It is important to take into account the data producer of each dataset[17]. In fact, the different entities that are part or are related with the Shift2Rail IP4 ecosystem, and in particular IT2Rail, will often have a very diversified and relevant set of data. It must be made clear what each entity (including the traveller) will receive in exchange for sharing their data. The traveller, for instance, could receive some extra functionality in exchange of the login and specific preferences information (and indirectly habits). This will be requested to be compliant to the GDPR but could also motivate the user to join, in a context where more users start wondering if it is worthwhile and necessary to share certain information. In a similar way, if we consider public and/or private transport operators, MaaS operators, specific service providers and others, they all have pieces of information concerning the travellers and their services. The sharing of such information is essential to improve the knowledge about the traveller's preferences, habits and needs, as well as to improve the global

[16] ITR-T8.1-D-UNI-001-01: D8.1 – Document Management Plan

[17] The EC now refers to this in contraposition to the data owner concept, since in some case the concept of ownership is rather complicate[17] and the subject is in continuous evolution.

offer and integration of services across the semantic IF. However, for this to work, innovative business models and a clear definition of their governance mechanisms are necessary[18].

A specific mention is necessary concerning the data storage, both for long term as well for specific real-time operations. In fact, while for the GDPR the main distinction is when the data is crossing or not the European Borders, in many cases the business related entities (in particular private companies) may operate crossing national borders. Being aware that the data is stored in the cloud by a national entity doesn't mean that data is stored at national level, unless specifically agreed with the provider. Even if this seems to be more a concern rather than a real threat, it is important to consider the data storage level to improve transparency and increase trust.

As mentioned before, GDPR and previous Privacy and Data protection related legislation regulates extensively how personal data may be collected and processed in the EU. Besides, electronic transfer of information (including personal data) between travellers and transportation services providers has existed for years in the EU under strict compliance of these regulations. In this sense, it can be concluded that the introduction of a new Web of Transportation ecosystem will not change the situation in this aspect, providing that it will act exclusively as an *intermediary* between all stakeholders, so that all responsibilities for data protection compliance would rely on these stakeholders and not on the regulation of the ecosystem itself.. This would be of course an acceptable approach from the legal perspective, but in certain extent it would be also missing an opportunity to provide all Web of Transportation clients with a technical solution to deal with privacy and data protection issues at platform level. This technical opportunity is what could be considered as part of the future IP4 challenges.

Basically, this second approach seeks to take advantage of the role played by the platform by implementing mechanisms to guarantee the compliance with data minimization or purpose limitation principles (e.g. the so-called case of the need to reveal all ID card data just to ensure that someone is a legal adult). Recent research on "*Attributes Based Credentials*" schemes based on trusted entities could be applied, in case this second approach is eventually followed. This approach, if well designed, can also be helpful to keep track of all personal data transactions, so that it would facilitate customers to exercise their withdrawal rights in an effective manner.

Under GDPR, EU citizens will benefit from new or stronger rights, such as being informed about how their data is used, the data portability across service providers, the ability to erase or delete their personal information, the access to the personal data an organization holds about them, the ability to correct inaccurate or incomplete information and over automated decisions and profiling.

The GDPR also includes mandatory breach disclosure that will help citizens to understand serious incidents concerning confidentiality and security, and it acts as a transparency mechanism as well as a mechanism to help those affected mitigating any harm.

It is also important to highlight the positive effect that the GDPR will have in the effective opening of borders for the EU travellers as personal data subjects. In an increasingly digitized world, this

[18] Note that this topic is further developed in the follow-up of IT2Rail: the GOF4R project: http://www.gof4r.eu/

"European" traveller perspective would be impossible without previously removing all the already existing digital borders between EU countries. This is exactly the aim of the GDPR, by harmonizing all data protection regulations throughout the EU.

1.1.1 Interoperability Framework

One of the IP4 Shift2Rail challenges consists in the establishment of a Semantic "Interoperability Framework" (IF). The IF will enable new business applications to 'interoperate' in an easy and fast way so as to provide the customer with comprehensive information on available travel options, corresponding processes for their booking, payment, ticketing (including consumption and/or modification), etc. More exclusively, the IF could also provide the arena where to build other particular valuable business services such as business analytics.

Thanks to the activities and projects developed in IP4, Shift2Rail would like to embrace the opportunity to achieve interoperability at semantic level by developing a shared model of the meaning of the exchanged information in the transport domain and by fostering the adoption of multilateral solutions.

The IF developed in IT2Rail is an enabler for the interoperability of a number of rich traveller-centric applications operating on a distributed "Web of Transportation". This IF represents the core of the IT2Rail architecture. It is based on:

- The creation of a shared domain Ontology - an explicit, formal, shareable, machine-readable and computable description of the associated data and exchanges. It will allow a higher degree of automation of distributed processes across multiple data formats and protocols, spanning unspecified actors;
- The provision of a set of semantic interoperability services that can be deployed in multiple architectures and configurations. For this, they do not mandate a specific set of communication protocols or frameworks, leaving the choice to partners: they may opt to re-use a shared enterprise service bus, perhaps on a virtual private network protected by specific security and authentication protocols, or decide to engage in pure peer-to-peer exchanges over the web, or a mixture of these or other options.

It is worth noticing that the IF could be seen as "a wire" regarding its involvement in privacy, in a way that it can be seen as neutral, not collecting any data and leaving the whole responsibility to comply with GDPR to the interconnected actors.

This will allow the building of a one-shot trust service (the future S2R IP4) because in the end the IF knows where all the data is being communicated to and from. To reassure the transport stakeholders, especially those Transport Services Providers concerned about the eco-system exposing them to indiscriminate access of their services and data, it is important to highlight the potential of the Service Description which is registered together with the annotated services in the a Service Registry: this capability allows the joining party to describe who is authorized to use their services thanks to ontology tags. It is also important for Transport Services Providers which have

very specific distribution strategies which may, for example, use exclusively direct or proprietary distribution channels (perhaps due to higher cost of indirect distribution channels) to reflect them in this new ecosystem.

A Service Registry Scan capability could work as a standard Interoperability Framework service, available to any Transport Service Provider, to scan the Service Registry to see what is actually on offer that they could use to come up with innovative new products or features of existing products by using or combining with new services and business areas that they may discover in the ecosystem.

As such it could provide some support to these actors for compliance (and beyond), at the expense of collecting and processing some personal data under strict “informed consent” rules.

1.1.2 Travel Companion

The Travel Companion app is the easiest ‘entrance path’ to access the Web of Transportation for the travellers. This app is accessible through a preferred smart device (e.g. a mobile device) which should be protected and secured against unauthorized access and external threats. On top of it, the traveller may use this app to create and store his/her profiles (e.g. professional profile, personal profile, etc...) and login with a unique digital ID. These credentials and preferences are organized in a cloud data store[19] within a set of secured compartments containing, among others, customer preferences, pre-selected payment means and credentials, itineraries obtained from a Travel Shopper, and entitlements from Ticketing processes.

By customizing his/her Travel Companion, the traveller can build a personal and dedicated virtual ‘travel environment’ where he/she can feel shielded from the complexity of the transportation system. Indeed, the goal of this Travel Companion is to decrease the travellers’ cognitive efforts when using the app so as to make the travel experience easier and more comfortable. Interaction with the Travel Companion can be customized according to personal choice, e.g. language and other ‘local’ properties, whilst indoor navigation and other capabilities as made available by local instrumentation may be discovered automatically by the IF.

[19] Article 4(19) defines ‘cloud computing service’ as “digital service that enables access to a scalable and elastic pool of shareable computing resources”. Those computing resources include resources such as networks, servers or other infrastructure, storage, applications and services. The term ‘scalable’ refers to computing resources that are flexibly allocated by the cloud service provider, irrespective of the geographical location of the resources, in order to handle fluctuations in demand. The term ‘elastic pool’ is used to describe those computing resources that are provisioned and released according to demand in order to rapidly increase and decrease resources available depending on workload. The term ‘shareable’ is used to describe those computing resources that are provided to multiple users who share a common access to the service, but where the processing is carried out separately for each user, although the service is provided from the same electronic equipment.

For a description of cloud services from a legal perspective, see the Annex of Opinion 05/2012 on Cloud Computing of the Article 29 Working Party, which is available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf

ENISA’s report on Incident Reporting for Cloud Computing is available at https://www.enisa.europa.eu/publications/incident-reporting-for-cloud-computing/at_download/fullReport

To offer their customers a unique and personal travel experience tailored to their preferences, it is common for most transport operators to store information in relation to customers travel behavior, such as their favorite means of transport, travel companions, luggage and insurance options, automatic check-in, travel destinations, departure airport, ancillary products such as car and hotels, seats, duty free products, food and drinks at airports, hobbies on holidays and data roaming usage. They may also store details of the travellers such as their credit/debit card or other payment details.

Travel Companion apps should disclaim in a clear and easy to read and understand a Privacy Statement about what information is collected, how it is collected, what is done with it and how it is protected. It shall also claim that any personal data is collected and processed in accordance with EU data protection laws[20]. Generally speaking, this item is already being addressed, for instance, in the transportation sector by airline travel companies which disclaim and describe how they collect, use and protect their customers privacy data[21].

1.1.3 The Travel Shopper Block

Thanks to the IF implementation, the Travel Shopper accesses distributed travel and transportation resources as a service of the IF as well as customer preferences, stored in the Travel Companion. This provides the capability to build a set of integrated door-to-door, multi-modal itineraries in answer to a traveller mobility query. The shopper has for ambition to become a seamless one-stop shop servicing all travellers' itinerary requests including the all-important first and last miles of the European journeys. This is an example of how innovative and expert or 'niche' shopping related applications can be orchestrated at relatively low cost.

It is common for travel companies that deploy Travel Shopper apps to collect personal details from travellers together with other pieces of information about them, such as how they use their website and / or app, as well as other websites accessible through their website and / or app. These details may include (where applicable) travellers' names, addresses, passport or Government issued EU National ID card numbers, telephone numbers, e-mail and IP addresses, credit/debit card or other payment details. In some instances, these companies may also collect information regarding medical conditions (only for travellers who have special medical requirements) which may affect the chosen travel arrangements. To provide location-based services, these companies and their trusted partners may collect, use, and share precise location data, including the real-time geographic location of travellers' computer or device through GPS, Bluetooth, IP Address, along with crowd-sourced Wi-Fi hotspot and cell tower locations. This location data is collected anonymously, unless travellers provide their consent. Generally speaking travellers are provided with the possibility to withdraw consent to travel companies and their partners' collection, use, transmission, processing and maintenance of location and account data at any time by not using

[20] All current and future EU legislation about privacy is available at: http://ec.europa.eu/justice/data-protection/law/index_en.htm

[21] https://www.ryanair.com/gb/en/corporate/privacy-policy

the location-based features and turning off the Location Services settings (as applicable) on travellers' devices and computers.

The data collected may be e.g., used for the following purposes: providing products and services requested by travellers, contacting travellers in the event of a travel time change or cancellation, credit or other payment card verification/screening, immigration/customs control safety, security, health, administrative, crime prevention/detection, legal purposes, statistical and marketing analysis, systems testing, customer surveys, customer relations communications and offering services and products that may interest the travellers.

Travel Shopper apps should also disclaim in a simple and easy to read format the consequences for people of accepting the terms described.

In addition to Travel Shopper apps there are many apps available that will help to keep travellers safe while travelling. However many of them have security issues. For example in many cases the personal data is still not encrypted and could be easily intercepted.

1.1.4 Trip Monitoring

Using the Interoperability Framework, IT2Rail monitors relevant events available on the 'web of transportation' that could affect the traveller's journey. Matching those events with the traveller preferences and door-to-door itineraries, stored in the Travel Companion, the Trip Monitoring module aims to update the traveller about any disruption that could impact on his/her traveller experience, and by enabling seamless re-arrangements. To this end, it may invoke Travel Shopper to create alternate itineraries and through the Travel Companion display alerts, offer alternative routings where applicable and desired.

For this purpose the traveller must explicitly give his/her consent to start receiving these notifications. In other words, it is the traveller the person that, first instance, allows the modules to update him/her. Trip Monitoring apps should also disclaim in a simple and easy to read format the consequences for people of accepting the terms described.

1.1.5 Business Analytics

The IT2Rail Business Analytics module allows the operators to adapt their transport environment and services with greater accuracy by listening to traveller's feedback, thus contributing to the ease and seamlessness of the traveller's travel experience. Integration with Social Networks may be a valuable source of traveller's feedback. The Business Analytics module uses 'big data' technologies to access the "Web of Transportation" and leverage the data published by the multimodal services to generate analytical insights (e.g., service disruptions risk). The created analytical data sets are, in turn, semantically annotated and published back to the "web of transportation" thus contributing to its enrichment. Selected analytics can also be accessed by the traveller through their Travel Companion.

If the processing of personal data is based on consent of the travellers, the systems developed within IT2Rail should ensure that data subjects are provided with a clear explanation of the processing for which they are granting their consent, ensure that the consent mechanism is genuinely voluntary and of an 'opt-in' nature, ensure that data subjects can withdraw their consent easily and ensure that consent is not based on unresponsiveness or inactivity. For this purpose data encryption and pseudo-anonymization are highly recommended.

1.2 DATA QUALITY

GDPR, when defining the principles relating to the processing of personal data (Article 5), states that:

> "[*Personal data shall be*] *accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')"*

Compliance with this principle, as explained before, is a sole responsibility of each stakeholder dealing with personal data, but when using a platform to collect data, as presented above, it could as well provide them with some mechanisms to help to fulfil this responsibility.

1.3 CREDIBILITY OF NEWCOMERS

The credibility of the new comers will be extremely important considering the critical exchange of information involved, including payment details, preferences of the users, etc. Similarly, it would be useful to measure the quality of the service offered. This can be done comparing the service performance to specific KPI's or similarly to WAZE, MOOVIT and MyTaxi, relying to crowdsourcing feedback, therefore asking for the direct feedback of the users (that becomes relevant when the number of uses starts being high, to avoid voluntary or arbitrary (subjective opinions) influence of few users).[22] The mechanism chosen will have to be in accordance with the governance of the IF.

As explained before, there is not yet a mechanism to ensure the trustfulness of the actors joining the system. The IF sets out a new arena where to develop different solutions to guarantee this level of trustfulness. E.g. mechanisms such a Service Registry could facilitate this process. This new service could potentially lead to a place where the joining party is able to describe who is authorized to use their services, could be implemented to guarantee a certain level of trust

[22] Different mechanisms can be used, as highlighted in FP7 and H2020 projects Co-Cities and MyWay (amongst others), with the support of TomTom and other important industrial stakeholders.

2. RECOMMENDATIONS FOR FURTHER STEPS IN THE AREA

The following section deals with guidelines and directions on topics that can specifically impact future developments on Shift2Rail IP4 projects.

2.1 GDPR

In our increasingly interconnected world with its growing volumes of personal data and ever-faster transmission rates, the protection of personal data and their subjects' privacy has become a major concern.

A new European Union Regulation, the GDPR, sets stringent requirements to be met by all enterprises (i.e. any organization that processes personal data). Personal data is defined by article 4(1) in a broad manner as:

> "*Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*".

Recital 26 confirms this broad interpretation by indicating that:

> *"Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments".*

It should also be noted that Recital 30 clearly states that:

> *"Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them".*

Such online identifiers should be considered as being personal data.

When such personal data are processed, to be GDPR compliant, the systems developed within the IT2Rail project and follow-ups must ensure that the personal data are:

- Processed legally and appropriately and with a clear view of how the information will be used;
- Collected for specified, explicit and legitimate purposes;
- Relevant and limited to the respective purposes;
- Accurate and kept up to date; retained for no longer than is necessary for the relevant purposes;
- Only processed if the data are kept appropriately secure.

Moreover, accountability considerations require the systems' operators being developed to demonstrate that:

- They compile a data register for all processing activities (inventory);
- Ensure that they only process the minimum volume of personal data necessary to achieve the legal purposes of doing so;
- Draft a privacy notice, i.e. A statement issued to a data subject that describes how the organization, among other things, collects, uses, retains and discloses personal data;
- Develop an internal policy for informing and training the staff; appoint an employee who is in charge of data protection;
- Use data protection impact assessments where appropriate (these pinpoint the most effective means of compliance and allow enterprises to identify and fix problems at an early stage);
- Establish effective (protection) procedures to ensure the enterprise's compliance with the privacy legislation.

If the processing of personal data are based on consent of the consumer, the systems developed within IT2Rail and Shift2Rail IP4 should ensure that data subjects are provided with a clear explanation of the processing for which they are granting their consent, ensure that the consent mechanism is genuinely voluntary and of an 'opt-in' nature, ensure that data subjects can withdraw their consent easily and ensure that consent is not based on unresponsiveness or inactivity.

Furthermore, the GDPR provides data subjects with a wide array of rights that can be enforced against organizations that process personal data. These rights may limit the ability of organizations to lawfully process the personal data of data subjects, and in some cases these rights can have a significant impact upon an organization's business model. The exercise of these rights should be taken into account in the development phase of the systems being developed within IT2Rail and Shift2Rail IP4, in particular the rights to access and the right to data portability.

Importantly, special attention should be taken to the implementation of appropriate technical and organizational measures to appropriately protect the security of the personal data. Encryption and pseudonymization are highly recommended. Indeed, in case of data breach leading to the destruction, loss, alteration or unauthorized disclosure of or access to personal data, the operators of the systems being developed would be obliged to notify the competent national data protection

authority as well as the data subjects: this could have important consequences on the reputation of companies using the IT2Rail systems.

Finally, Recital 78 expresses the need that:

> *"When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations. The principles of data protection by design and by default should also be taken into consideration in the context of public tenders".*

Article 25 details the obligations of data protection by design and by default by indicating that:

> *1. "Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.*
> *2. The controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons".*

2.2 MOBILITY AS A SERVICE (MAAS)

While the definition of MaaS could be used for any service that provides access for the user to a transportation service that implies the pay per use (in contraposition to the ownership of the private vehicle), the terms has been created aiming to create an offer of different transport services by a single umbrella, simplifying access and payment for the user. The most interesting cases involve several transport modes, including both public and private (but not owned by the user) transport. There are 4 levels of integration of MaaS services, identifying the different maturity of the services. The higher levels of integration (particularly when involving integrated bills/tickets (level 3)) highlight the importance of the EPS as well as of solutions similar to the IF adopted in IT2Rail.

Additional discussions on the implications of the MaaS for future projects in Shift2Rail could be seen as an instrument used by MaaS operators (at local and/or at European level) to further enhance and promote a more comprehensive offer of services.

2.3 POTENTIAL ETHICAL CHALLENGES

Right to be left alone

Principles such as the "right to be left alone" are also of special interest for travellers. European citizens can use two channels to remove personal information. First, they can reach out to the specific company asking its data protection officer to remove the data. Second, they can reach out to the national data protection officer to pursue erasure. How often do people use them? For some organizations quite frequently.

The national Data Protection Officers do not publish lists of requests. However, some companies do. One well-known company is Google. Google publishes statistics on removal requests, in the form of a Transparency Report[23]. From May 2014 through November 13, 2017 Google has removed 839,556 URLs – about 43% of those requested – from search results, and declined to remove 1,104,867 – nearly 57%. The reasons for not removing a URL include the information may be strongly in the public interest, the information may reside in a government document, or the information may come from a reputable journalistic source.

Just like Google is prepared to attend to such requests, it is also recommended that any player willing to join the Shift2Rail IP4 "Web of Transportation" ecosystem is also prepared for such requests as described in the General Data Protection Regulation (GDPR).

[23] https://transparencyreport.google.com/eu-privacy/overview

Non-discrimination

The EU's commitment to the principle of non-discrimination was reaffirmed in December 2000 in the Charter of fundamental Rights. Since the entry into force of the Lisbon treaty in December 2009, the Charter has the same binding legal value as the Treaties. In addition, the racial Equality directive requires Member States to prohibit discrimination on the ground of racial or ethnic origin in different areas, including access to services. Considering his framework, the IF may again, provide technical opportunities to ensure the non-discrimination according to personal features.