Transport of passengers from a **data protection perspective**

Thursday
25 March 2021
Online meeting

The International Rail Transport Committee (CIT) has great pleasure in inviting the staff of CIT members, dealing with or interested in data protection issues, to the CIT Conference on data protection to be held online on Thursday, 25 March 2021.

Limited to CIT members

Invitation

The International Rail Transport Committee (CIT) has great pleasure in inviting the staff of CIT members, dealing with or interested in data protection issues, to the CIT Conference "Transport of passengers from a data protection perspective", to be held online on Thursday,25 March 2021.

Challenges Relating to Data Protection

Protection of personal data is of great importance in the day-to-day business of railway undertakings in their domestic activities and in international traffic. Personal data are everywhere: in the information provided when buying tickets, when handling claims or when someone signs a contract of carriage of goods.

Data protection falls within the scope of fundamental rights and freedoms, namely, the right to privacy of individuals with respect to the processing (collecting, saving or transferring) of personal data. The EU Regulation 1371/2007 on rail passengers' rights and obligations refers in Article 10(5) to the obligation of railway undertakings and ticket vendors not to disclose personal information on individual bookings to other railway undertakings and/or ticket vendors.

The execution of the transport contract encompasses thus the processing of different personal data from the passengers.

For this reason, the CIT General Secretariat developed a Manual on Data Protection for Transport Undertakings, which contains the CIT Guidelines on Data Protection to provide guidance to CIT members with respect to data protection requirements according to the GDPR, the CIT Model Data Processing Contract to assist its members in drafting their data processing contracts with data processors, commented articles and examples of clauses.

Overview and goals of the Conference

The aim of this Conference is to discuss data protection in relation to transport of passengers based on practical cases faced by railway undertakings and the solutions they provided to them.

During the morning sessions, participants will be given an overview on how railway undertakings managed data protection issues during the pandemic of COVID-19. They will then discuss some practical cases related to the use of data of passengers.

The afternoon sessions will focus on other regulations related to data protection than the GDPR. The Conference will end up with a presentation of new technological solutions used in the railway industry, before discussing the activities of CIT related to data protection.

The participants will be provided the possibility to ask questions to the participants after each presentation.

Target Audience

Employees of the CIT members, working or interested in the field of data protection in the passenger traffic but also in the freight traffic.

The participation to this Conference is free of charge and a certificate of attendance can be provided, upon request, to participants.

CIT Data Protection Conference

Programme

Time	Topic	Speaker
8.50-9.00	**Registration**	
9.00-9.10	Introductory remarks	Isabelle Saintilan, Chair of the CIV Committee
Session 1: Transport of passengers in time of COVID-19		
9.10-9.40	Vaccination and check of health data Q&A Session	CIT, Sandra Dobler
9.40-10.10	Tracking and tracing of passengers Q&A Session	Thalys, Gaëtan Goossens
10.10-10.40	Check of identity of passengers Q&A Session	Trenitalia, Isabella De Girolamo/Laura Tiglie
10.40-11.00	**Coffee break**	
Session 2: Data of passengers		
11.00-11.30	Access and use of reservation data of passengers Q&A Session	SNCF, Eliott Kalfoun
11.30-12.00	Video surveillance in passenger traffic Q&A Session	ÖBB, Martin Leiter
12.00-12.30	Transfer of personal data to third countries Q&A Session	SJ, Stefan Carlsson
12.30 – 13.30	**Lunch break**	

Session 3: What about other regulations than GDPR?		
13.30-14.00	E-Privacy Regulation Q&A Session	Affluo, Johan Vandendriessche
14.00-14.30	Digital Services Act package Q&A Session	Walder Wyss AG, Caroline Gaul
14.30-15.00	PNR and API Directive Q&A Session	SNCB, Bianca Jonas
15.00-15.10	**Coffee break**	
Session 4: New technologies and their impact on transport		
15.10-15.40	Renfe App and Mobility-as-a-Service (MaaS) Q&A Session	Renfe, Fernando De Lucas De Rose
15.40-16.10	CIT activities on GDPR Q&A Session	CIT, Sandra Dobler
16.10-16.40	Protection of the digital integrity Q&A Session	ethix, Johan Rochel
16.40-17.00	Closing remarks	Isabelle Saintilan, Chair of the CIV Committee

Speakers

CARLSSON Stefan
DPO, Information SecurityStrategist, SJ

DE GIROLAMO Isabella
Direzione Affari Legali e Societari, Trenitalia

DE LUCAS Fernando
Legal Advisory Manager, RENFE

DOBLER Sandra
Senior Legal Adviser, CIT

GAUL Caroline
Senior Associate, Walder Wyss

GOOSSENS Gaëtan
Data Privacy Officer, Thalys

JONAS Bianca
Data Protection Officer, SNCB

KALFOUN Eliott
Legal Counsel, SNCF

LEITER Martin
Data Protection Officer, ÖBB

ROCHEL Johan
Co-Founder, ethix

SAINTILAN Isabelle
Chair of the CIV Comittee, Legal Counsel for PassengerMatters, SNCF

TIGLIE Laura
Referente Data Protection,Trenitalia

VANDENDRIESSCHE Johan
Attorney at Law, Affluo, Belgium

General Information

Languages

The Conference will be held in English. We will try to accommodate questions in French and German.

Registration

Registration must be made until **17 March 2021**
Email: loic.gioria@cit-rail.org

The conference is limited to representatives of CIT members only. Participation is free-of-charge.

Location of the event

The Conference will be held online, on MS Teams.

The link to the Conference will be sent on 22 March 2021.

Contact

The General Secretariat of the CIT will be pleased to provide you with further information:
Tel. +41 31 350 01 90
Email: loic.gioria@cit-rail.org

International Rail Transport Committee
Comité international des transports ferroviaires
Internationales Eisenbahntransportkomitee

Vaccination and check of health data

CIT Data Protection Conference

25 March 2021

Sandra Dobler
Senior Legal Adviser

SUMMARY

- Personal data and their processing
- Sensitive data and their processing
- Check of health data
- Certificate of vaccination

WHAT ARE PERSONAL DATA?

https://grafimedia.eu/blog/data-protection-regulation-gdpr-guide/

WHAT ARE PERSONAL DATA (article 4 GDPR)?

any information relating to an identified or identifiable natural person directly or indirectly, e.g.: 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

LEGAL BASIS TO PROCESS PERSONAL DATA (article 6 GDPR)

- **Consent**
- **Necessary for the performance of a contract**
- **Necessity for compliance with a legal obligation;**
  Necessity in order to protect the vital interests of the data subject or of another natural person;
- **Necessity for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;**
- **Necessity for the purposes of the legitimate interests pursued by the controller or by a third party**

WHAT ARE SENSITIVE DATA (article 9 GDPR)?

personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, **data concerning health** or data concerning a natural person's sex life or sexual orientation

LEGAL BASIS TO PROCESS SENSITIVE DATA (article 9 GDPR)

- **Explicit consent**
- **Necessity in the field of employment and social security and social protection law**
- **Necessity to protect the vital interests of the data subject or of another natural person**
- **(…) (…) (…)**
- **Necessity for substantial public interest**
- **Necessity for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services**
- **Necessity for reasons of public interest in the area of public health**
- **(…)**

DATA PROTECTION AND COVID-19 - PASSENGERS

Body temperature screening in the train

https://www.iom.int/news/covid-19-forces-huge-numbers-ukrainians-home-face-fraught-future

Check of health data at the station

https://www.teleischia.com/212992/covid-19-rientri-7-maggio-7-positivi-al-test-rapido-e-nessuno-positivo-a-tampone-su-2310-viaggiatori/

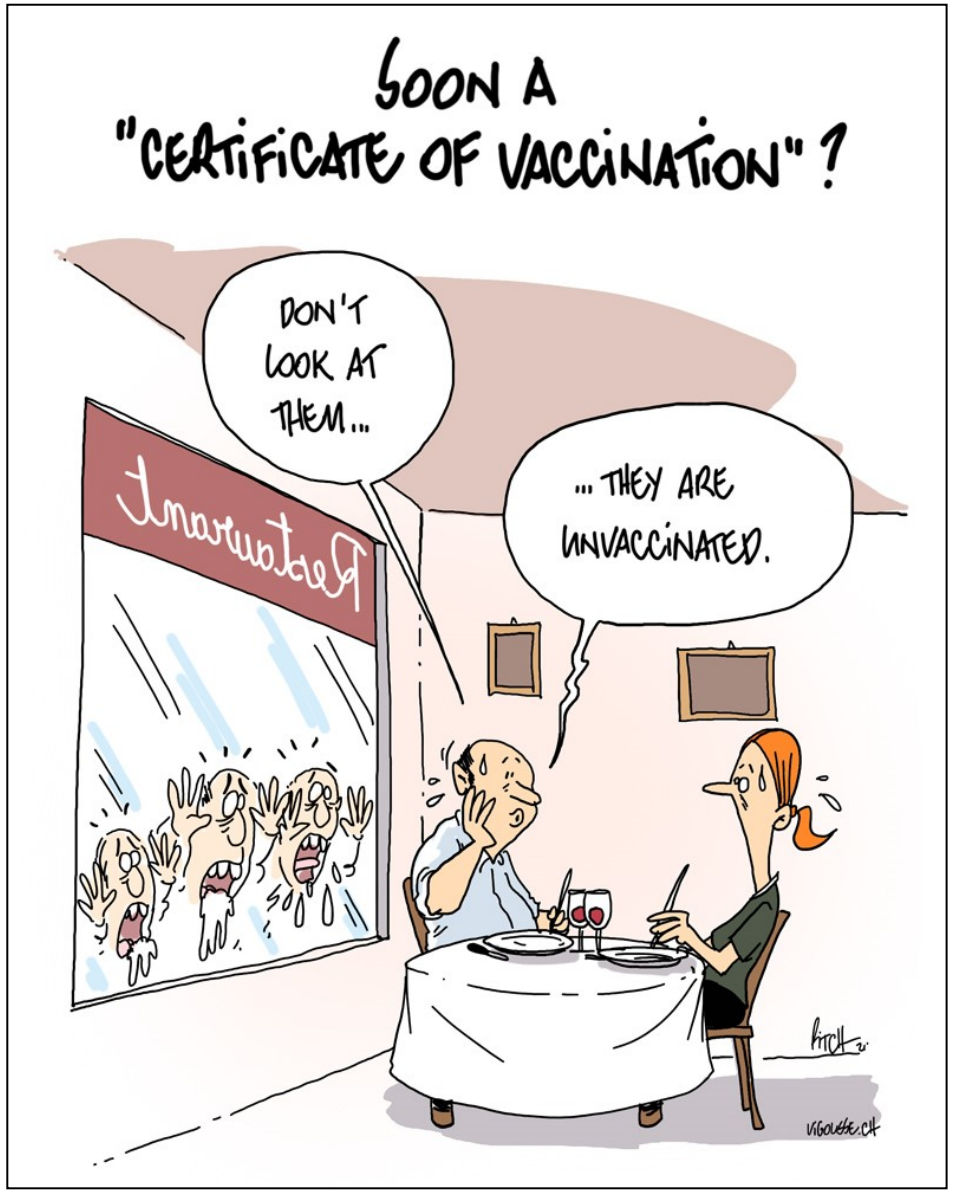
CERTIFICATE OF VACCINATION

Cinema?

Theatre?

Concert?

Travel?



LEGAL/PRACTICAL ISSUES BEFORE IMPLEMENTATION

Freedom of people to refuse to get vaccinated

Mandatory vaccination

Potential discrimination

LEGAL/ PRACTICAL ISSUES IN THE IMPLEMENTATION

- National or international certificate of vaccination?
- Which vaccines are recognized?
- What about the centers of vaccination?
- Which information to mention on the certificate (name, brand of vaccine, date of vaccination, date of expiration)?
- Only for vaccination? Or also for negative PCR Test? Or people with antibodies against COVID-19?
- Who can access the information?
- How to fight frauds (fake certificates, fake identity)?

SOLUTIONS IN PLACE/UNDER DEVELOPMENT

Israeli Green Pass

EU Digital Green Pass

IATA Lab App and Travel Pass App

Etc.

DATA PROTECTION AND COVID-19 – KEY POINTS

- **Don’t process personal data (including sensitive data)** if not necessary (non-existence of a ground to do so)
- If necessary, process (collect, store, use, disclose, etc.) **only the minimum amount** of personal data (including sensitive data)
- Comply in principle with the **rights of your passengers** as regards data protection (right to be informed, right to object, right of access, right to portability, right to be forgotten, right to rectification)
- Ensure that you have **measures in place to keep personal data** (including sensitive data) secure (e.g. no data breach possible, etc.)

Thank you
for your attention!

Questions?

Sandra Dobler
Senior Legal Adviser
Tel. : +41 31 350 04 80
E-mail : sandra.dobler@cit-rail.org

www.cit-rail.org

Tracking and Tracing Passengers

Railway companies' new obligations due to the Covid-19 health crisis

25/03/2021

Gaëtan Goossens
Data Protection Officer
gagoos@thalys.com
Data.protection@thalys.com

THALYS

Tracking and tracing passengers: an international railway company struggle

I. New obligations

II. Issues faced

III. Conclusion

THALYS

I. New obligations

The role of the railway company in the fight against Covid-19

A. Passenger location form

- First new obligation, from Germany
- Health data processing issue
  - Collection in sealed envelopes
  - Transfer without opening
- Negotiation with authorities
  - Better not to collect data
  - Simple announcement
- Blank forms available as a courtesy to passengers
- Replaced by a digital location form

B. Authorities' requests

- Collaborating
- Legal basis not always clear
  - Which authorities are competent?
- Lack of official documents
  - Simple emails
  - Unsigned documents
- Fewer requests (tracking apps)

C. Negative PCR tests

- Active role required by Dutch authorities
  - Visual check of the paper
  - Denial to board
  - No data retention
- Passive role required by France
  - Announcement
  - Covid test of Thalys staff ?
- No role required by Belgium
  - Announcement as a courtesy to passenger

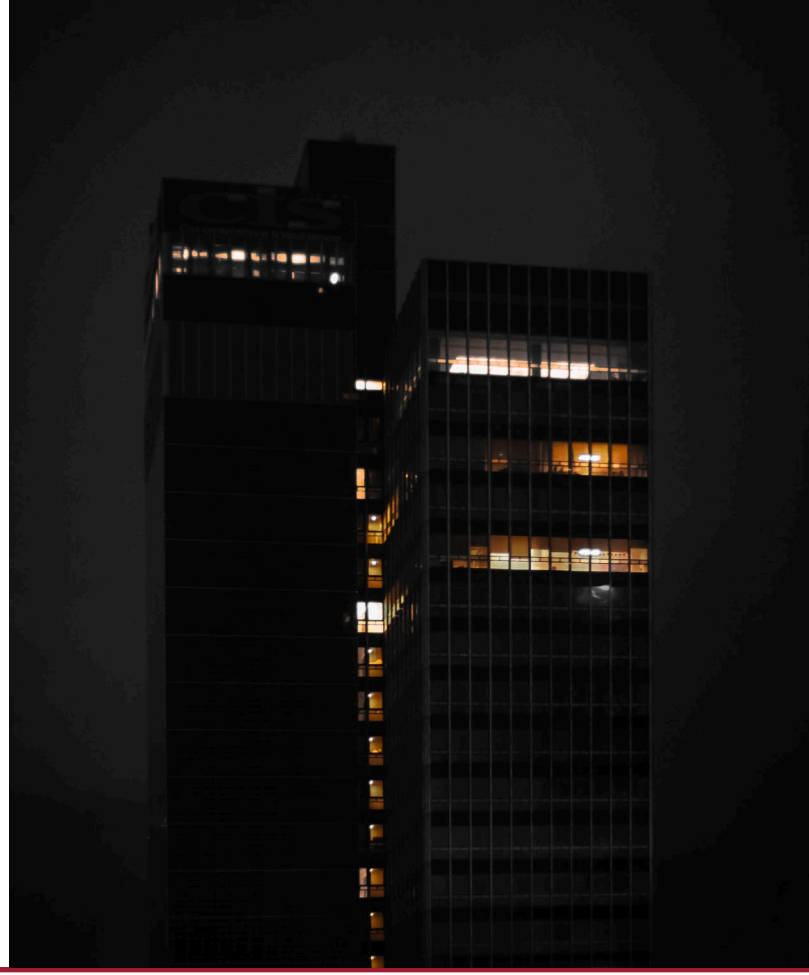
II. Issues

With new obligations comes change

THALYS

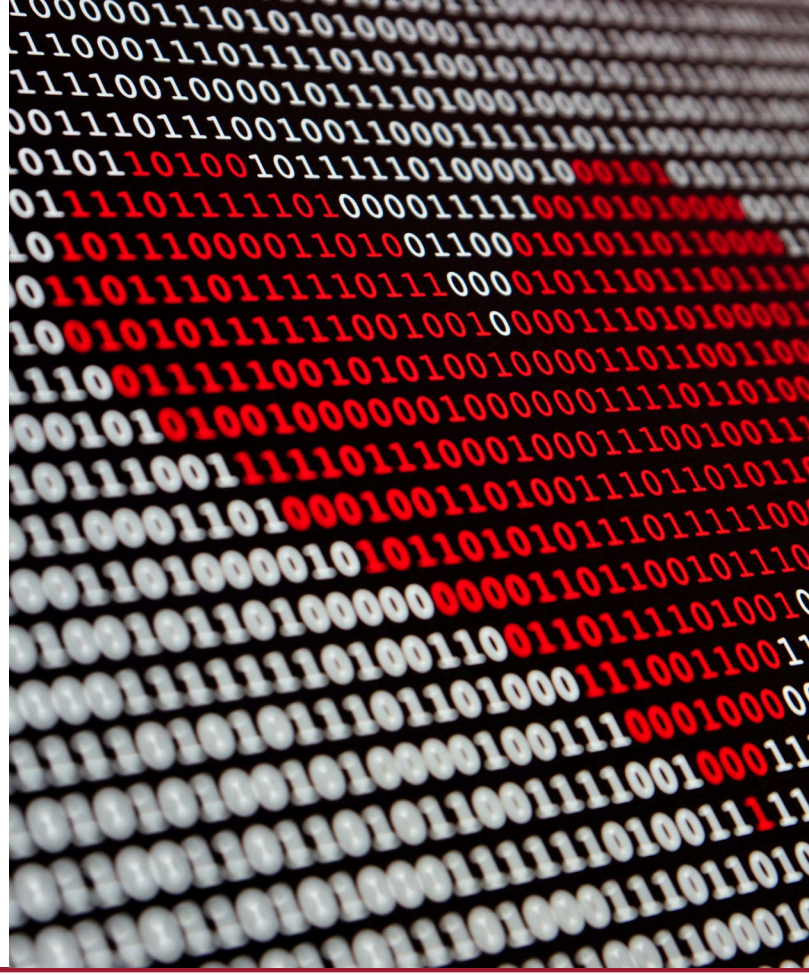
A. Decisions often applicable overnight

- Decisions taken in the evening
- Crisis meetings are necessary
- Hard to make decisions without legal texts
- Legal texts are often written quickly so they cannot go in depth



B. Data retention

- Not required to track passenger
- No data retention
- Information on booking servers can track passengers if needed
- Is public health a sufficient legal basis for processing health data?
- Could a train company be fined for someone getting sick because of a gap in tracing ?



C. Staff training

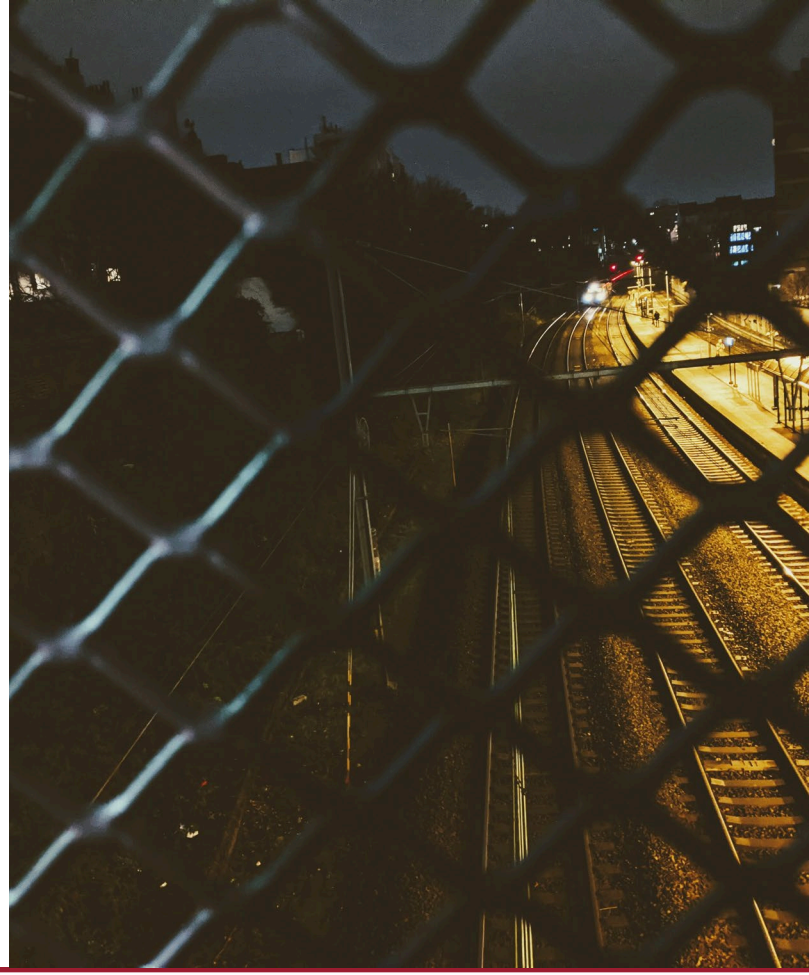
- Our staff are implementing the measures
- Not trained for that
- Training takes time
- Responsibility if our staff forgets to check passengers?

III. Conclusion

What to take from all this?

Conclusion

- Create costs to companies that are already struggling
- Sector has not been involved in decisions making process
- Creates difficulties for our staff
- Checks are harder to set up than for planes or boats because of access to trains
- Our responsibility is currently limited, but this could change



Thank you!

Gaëtan Goossens: gagoos@thalys.com

DPO: data.protection@thalys.com

Trenitalia nominative travel tickets

TRENITALIA
GRUPPO FERROVIE DELLO STATO ITALIANE

Summary

1. Trenitalia nominative travel tickets

2. The Nominative travel tickets on high-speed trains
   - Project history
   - How it works
   - Managing COVID-19 positive cases
   - On site ticket control
   - Purposes and retention of personal data
   - Focus on combating fraud from second contacts, secondary ticketing and IT
   - Focus on combating fraud from second contacts, secondary ticketing and IT - The case of event ticketing

1 Trenitalia nominative travel tickets

1. Trenitalia nominative travel tickets

In Trenitalia the following travel tickets are nominative:

- Regional season tickets;
- High-speed train season tickets;
- Night trains;
- Single travel tickets for regional trains purchased online;
- Travel tickets at a discounted rate (e.g. voter tickets);
- Travel tickets for High Speed trains since May 2020.

2 The Nominative travel tickets on high-speed trains

2. The Nominative tickets on high-speed trains – project history

Trenitalia has been evaluating the introduction of nominative tickets on high-speed trains since a few years.

2019: Trenitalia launched a study on the use of nominative tickets. Several internal departments were involved.

2020: As a result of the COVID-19 pandemic, the decree of the President of the Council of Ministers dated 26 April 2020 explicitly requested the use of the nominative tickets on high speed trains to:

(1) identify passengers and

(2) manage any suspected or confirmed case of COVID-19 on board.

2. The Nominative ticket on high-speed trains - how it works

Since May 2020, high-speed train tickets changed from a non-nominative to a "nominative" travel document.

Upon purchasing a travel ticket from any Trenitalia sales channel (i.e. ticket offices, self-service devices, travel agencies and online travel agencies, such as web portal and mobile channels), customers must provide the following identification data:

Identification data

- ✓ Name and surname
- ✓ Email address (mandatory only for tickets purchased online)
- ✓ Mobile telephone number (optional for all sales channels)

2. The Nominative ticket - managing COVID-19 positive cases

Trenitalia
- Does not carry out contact tracing and
- Does not receive communication of the name and surname of a COVID-19 positive customer.

Trenitalia
- Receives directly from the health authority notification of positive cases that was on board of train X;
- Communicates to the competent authority names of all the customers who have travelled on the same carriage of the positive case

➡ No further communication is given from the competent authority to Trenitalia on the specific case and no further controls are requested

2. The Nominative ticket- on site ticket control

The customers show up at the station and before entering the platform, show their ticket. It is a quick visual inspection of the travel document
The check is carried out by the staff of RFI (a company of Ferrovie dello Stato Italiane Group) present at the gates.

During the lockdown, customers also had to be in possession of a self-certification to certify the reasons for their move.
This document was subject to control by the Police.

2. The Nominative ticket on high-speed trains - purposes and retention of personal data (1/3)

Purposes of the processing are:	Nature of the provision	Legal basis
Issue of the travel document	Mandatory	Contractual
Sending any service communications related to the purchased trip using the contact details provided by the data subject (optionally, e-mail and/or text message)	Optional	Consent
Check the validity of the travel document	Mandatory	Contractual
Invoice issue	Mandatory	Legal obligation
Fight fraud from second contacts, secondary ticketing and computer fraud;	Mandatory	Legitimate interest
Protection of assets and personnel and management of emergency procedures	Mandatory	Legitimate interest
Containment of the contagion from COVID-19	Mandatory	DPCM (Prime Minister's decree) 14.07.2020

The Retention of personal data: The trip data is kept for 10 years starting from the date of the trip or the expiration date of the season ticket.

2. The Nominative ticket on high-speed trains - purposes and retention of personal data (2/3)

Containment of the contagion from COVID-19:

As per DPCM of 14th July 2020, in order to contain the contagion from COVID-19, a specific declaration is required from each traveler to certify:

I. He/she is not affected by COVID-19 or not been subject to a mandatory quarantine

II. He/she does not to have symptoms attributable to COVID-19 (e.g. body temperature above 37.5 °C, cough, cold) and has not been in contact with a person affected by COVID-19 in the last 14 days;

III. Commit to renounce the trip and to inform the competent health authority if any of the aforementioned symptoms emerge before the trip or occur within 8 days from the arrival

2. The Nominative ticket on high-speed trains - purposes and retention of personal data (3/3)

<u>Containment of the contagion from COVID-19</u> - Doctors and nurses COVID-19 initiative

- The initiative offers free travel to doctors and nurses recruited by the Civil Protection for the establishment of specialist medical unit to combat COVID-19, in support of Regional health entities

- For this type of travel ticket, the personal registration number is required (Register of doctors)


6. The Nominative ticket: focus on combating fraud from second contacts, secondary ticketing and computer fraud

Advantages of nominative tickets

“Not nominative” tickets make it easier to carry out common frauds as:

- ticket data (PNR and CP) can be easily stolen from unsuspecting customers by subjects dedicated to this type of activity, particularly at the self service machines;
- knowing the PNR and CP of the travel tickets allows you to modify the trip without the knowledge of the real buyer or to obtain a refund of the ticket, if it was paid in cash, in favor of the scammer.

The operations described above can be carried out on the nominative tickets only by the actual holder. Ticket stealing will no longer be effective as nominative tickets cannot be reusable or refundable without the conformity between the document shown at the ticket office and the document indicated in the refund phase. Furthermore, the nominative tickets allow customers, who have requested to use the service and voluntarily provided their telephone number/e-mail, to be notified in the event of further transactions on their securities (this service is similar to the SMS sent by a bank for each transaction on a specific bank account and it will concern, for example, changes on travel document).

7. The Nominative ticket: focus on combating fraud from second contacts, secondary ticketing and computer fraud - The case of event ticketing (1/3)

As part of the fight against the phenomenon of the so-called secondary ticketing, the 2019 Italian budget law provided that, starting from 1 July 2019:

- tickets for access to events in venues with a capacity of more than 5,000 spectators must be nominative

- access to the show area is subject to personal recognition, through effective controls and mechanisms for verifying the identity of the participants, including minors.

7. The Nominative ticket: focus on combating fraud from second contacts, secondary ticketing and computer fraud - The case of event ticketing (2/3)

A report submitted to the Italian Privacy Authority complained that Budget Law:

- failed to consult the Authority on the law, provided for by the EU Regulation;
- failed to comply with the principle of proportionality and data minimization.

In giving his opinion, the Privacy Authority, while noting the lack of consultation by the legislator, considers the processing of personal data provided for by the new provisions to be proportionate with:

- the fight against avoidance and “tax evasion”;
- consumer protection;
- the guarantee of public order.

In fact, the regulatory provision limits the need for nominative tickets and the consequent verification of the users identity only to certain types of shows for venues over 5000 spectators, postponing the detailed identification of the technical rules to the implementation phase.

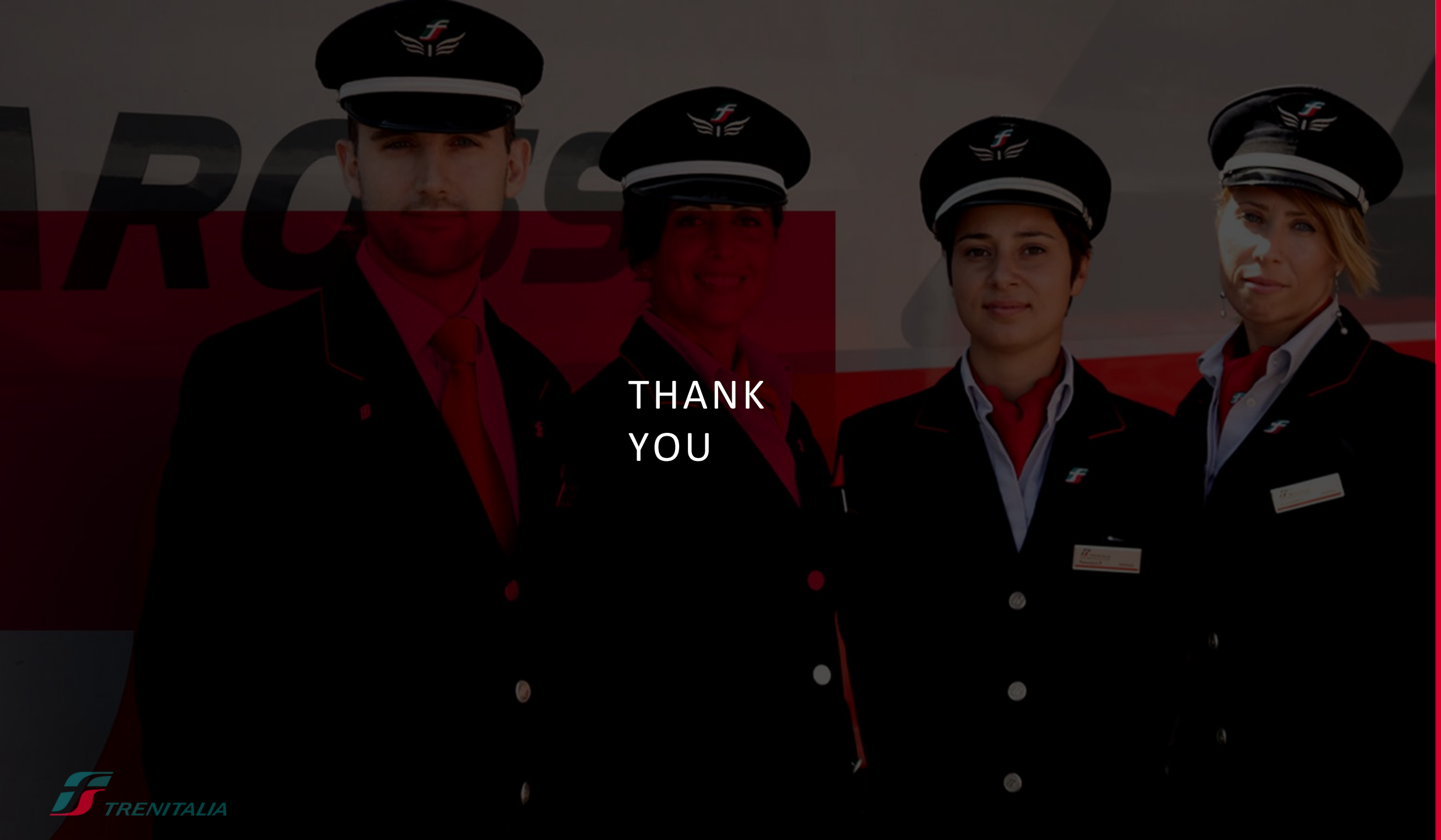
7. The Nominative ticket: focus on combating fraud from second contacts, secondary ticketing and computer fraud - The case of event ticketing (3/3)

In the discussions with the Privacy Authority Office, the Italian Revenue Agency gave account of all the guarantees introduced, in particular:

- the principle of minimization was respected by providing that the buyer's data are collected only in case of online purchases (first name, surname and a mobile telephone number) in order to certify the identity and prevent multiple purchases;
- no identification is required in case of traditional purchase at authorized box offices.

Regarding the data of those attending an event:

- only first name and surname must be printed on the admission ticket;
- the identity will be verified at the moment of the entry, showing the personal identity card.



THANK YOU

“TGV MAX” CLIENT AGAINST SNCF :

AN EXEMPLE OF THE APPLICATION OF GDPR IN LITIGATIONS THAT SEEM TO BE FAR FROM DATA PROTECTION

THE FACTS

A client applied to the St Denis district court in February 2019 in order to obtain the reimbursement of her TGV Max subscription, the paid tickets or transport costs and damages for the moral prejudice suffered as a result of a strike movement followed from April 2018.

In defense, SNCF produced in court a listing of the client's trips over the period considered, those she made and those she was able to book but that she cancelled.

At the hearing, the client's lawyer argued that SNCF had violated the provisions of the GDPR, French national rules on data protection and the freedom to come and go of its client.

SNCF Voyageurs was authorized to respond to this point within 15 days via a "note under advisement".

ARGUMENTS RAISED BY THE CLIENT'S LAWYER IN ORDER TO DEFEND AN INFRINGMENT OF THE GDPR

→SNCF VOYAGEURS provides all of the client's travels

→SNCF VOYAGEURS has to provide a proof of the lawfulness of the data processing

→The client has not been informed about the data processing

→This data processing is not necessary for the execution of the transport contract

ARGUMENTS RAISED BY SNCF VOYAGEURS

→ Effective Date of GDPR Vs Date of subscription of TGV MAX by the Client

→Legal Ground for Data Processing : Execution of the Contract/Legitimate Interest

→Information of the Client made by the General Conditions of Sale

→Preservation of data as evidence and proportionality of data retention periods

JUDGMENT

→ Article 7 of French Data Law which applied before GDPR mentioned the execution of the contract as a legal ground for data protection

→ SNCF Voyageurs made a declaration to the “CIL” (Correspondants Informatique et Libertés) before GDPR and produced that declaration in the litigation

→The customer's legal action constitutes a legitimate interest of SNCF Voyageurs in order to provide the means of proof in support of its means of defense.

→ A decision in line with other European decisions

POINTS OF ATTENTION ARISING FROM THIS COURT DECISION

→ Updating the Treatment Records

→ Ensure the proportionality of the data communicated in the litigation

→ Be more transparent when drafting general conditions of sales or confidentiality charter

→Document the legitimate interest internally in order to be able to produce that kind of document in justice if needed.

Thank you!

CIT Workshop
Transport of passengers from a data protection perspective
March 25 2021

Video surveillance in passenger traffic

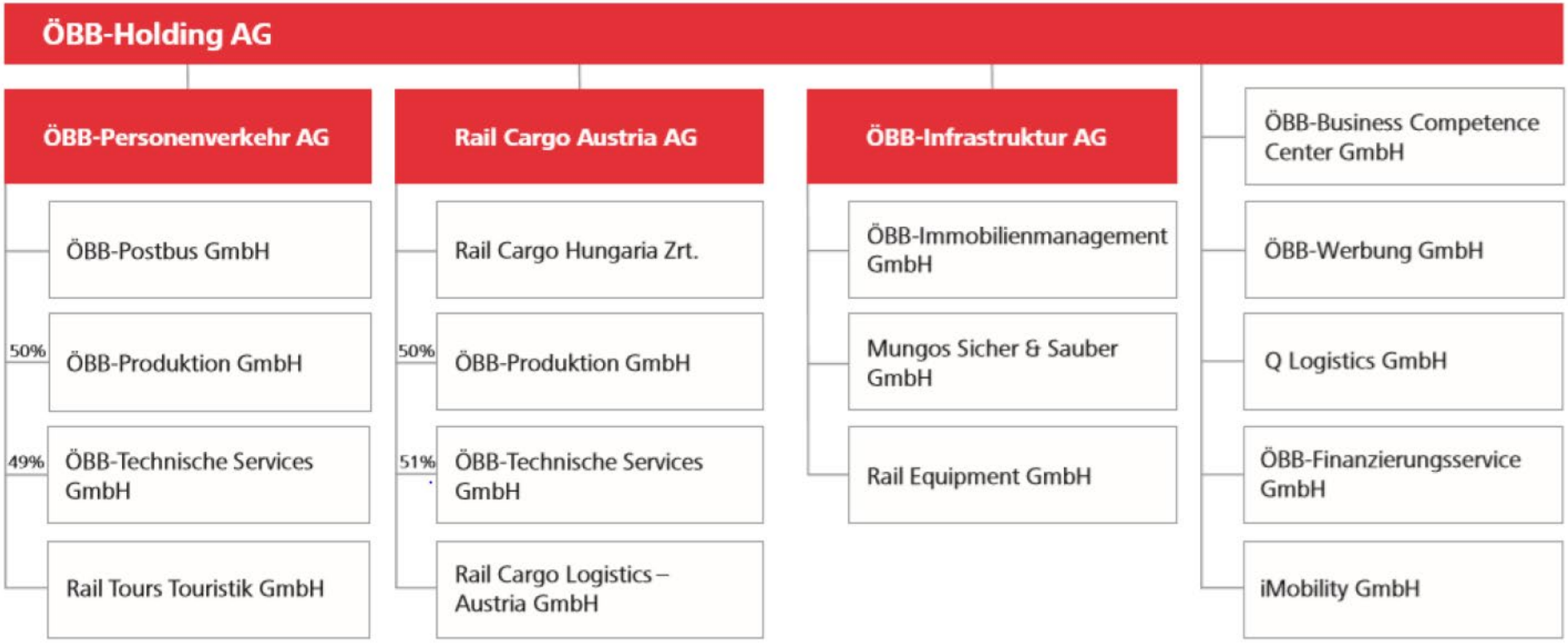
Martin Leiter
ÖBB Group Data Protection Officer

hite / weiß

Agenda

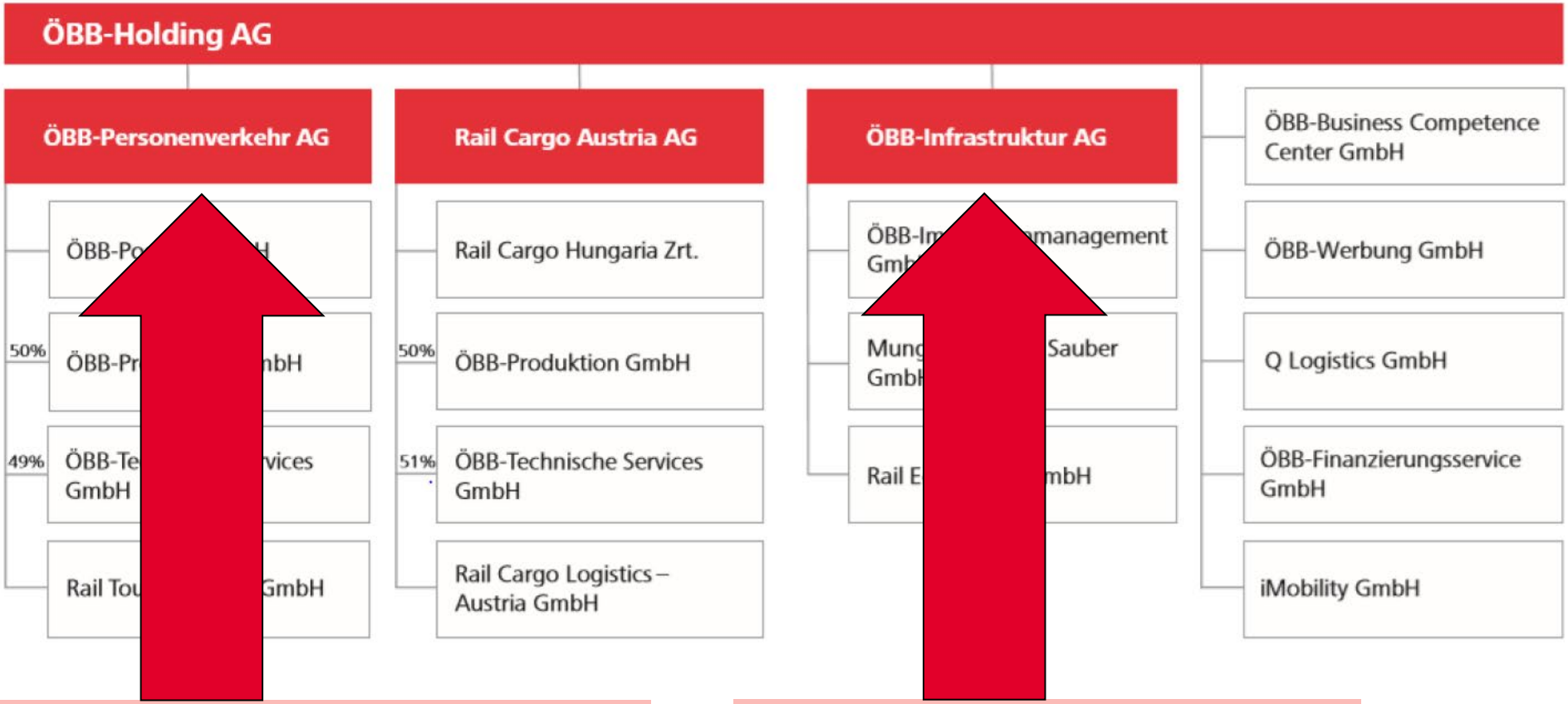
- ÖBB Group
- Legal basis of video surveillance
- Video surveillance of passengers
- Cross border topics
- Information obligation
- Cooperation with the security authorities

ÖBB Group



- + further subsidiaries in 18 European countries

ÖBB Group


ÖBB-Holding AG
ÖBB-Personenverkehr AG
Rail Cargo Austria AG
ÖBB-Infrastruktur AG
ÖBB-Business Competence Center GmbH
ÖBB-Werbung GmbH
Q Logistics GmbH
ÖBB-Finanzierungsservice GmbH
iMobility GmbH
Rail Cargo Hungaria Zrt.
50%
ÖBB-Produktion GmbH
51%
ÖBB-Technische Services GmbH
Rail Cargo Logistics – Austria GmbH
50%
49%
Rail passengers
People at railway stations

legal basis for video surveillance

- Art 6 (1) lit f GDPR
  - Legitimate interest in ensuring the safety of passengers and employees and the protection of property
- Austrian Data Protection Act:
  - Art 50a ff DSG 2000 („video surveillance“) in force until 24.5.2018
  - Art 12, 13 DSG („image processing“) in force since 25.5.2018

legal basis for video surveillance

- Art 6 (1) lit f GDPR
  - Legitimate interest in ensuring the safety of passengers and employees and the protection of property
- Austrian Data Protection Act:
  - Art 50a ff DSG 2000 [illegible] force until 24.5.2018
  - Art 12, 13 [illegible] („image processing“) in force since [illegible] 2018

- Austrian Federal Administrative Court („BVwG“)
  - there is no opening clause for video surveillance, Austrian Law therefore is unapplicable (25.11 2019)
  - Preliminary Ruling of the ECJ ist not required, since there is no doubt about it (2.3.2020)
  - Similar: German Federal Administrative Court (BVerwG 27.3.2019)

- → ONLY legal basis is the GDPR

Video surveillance of passengers

- Railway stations:
  - Controller = ÖBB Infrastruktur AG
  - Publicly accessible areas in railway stations (about 7.000 cameras all over the country)
  - Body cams worn by security personnel (service provided by a subsidiary company)

- In the trains:
  - Controller = ÖBB Personenverkehr AG
  - Cameras on the trains (local transport only)
  - Bodycams worn by ticket inspectors

Video surveillance of passengers

- All those processing activites where registered by the Austrian Data Protection Authority (DPA) (before 25.5.2018) by a „prior checking“ („Vorabkontrolle“)
- Therefore no Data Protection Impact Assessment (DPIA) required
  - Austrian law provides exeptions from the obligation to adopt a DPIA for processings registered by the DPA before 2018
- Storage duration 120 hours
  - Austrian law allowed 72 hours as a rule, exeptions had to be separately authorized by the the DPA
- Works council agreements existing for Body Cams and the video surveillance in the trains

Cross border topics

- ÖBB Personenverkehr AG operates local trains across the border in every neighbouring country (Germany, Czech Republic, Slovakia, Hungary, Slovenia, Italy, Switzerland and Liechtenstein)
- Switching off the surveillance when crossing the border is technically not possible
- 2015: legal opinion of a law firm about special requirements in those countries
  - Four countries: Austrian law is applicable → therefore no further legal requirements
  - Four countries: local law is applicable
    - in two of these countries, a registration was required
      - In one of those countries, information has to be provided in the local language (both in the trains and on the homepage)

Information obligation

- Since § 13 DSG (Austrian Data Protection Act) is unapplicable, information has to be given according to Art 13 GDPR
- In the trains
  - → pictogram (see next pages)
  - → General data privacy statement on the homepage (in German and English)
  - → CCTV data privacy statement on the homepage (six languages)
- In the stations
  - → pictogram (see next pages)
  - → Handouts
  - → data privacy statement on the homepage (in German and English)
- Body cams
  - Is worn visibly on the chest / the shoulder
  - Can only be manually activated
  - Flashing red light is indicating the recording

Pictogram


Video
VERANTWORTLICHER / CONTROLLER
ÖBB-Personenverkehr AG, FN 248742 y
A-1100 Wien (Vienna), Am Hauptbahnhof 2
+43 1 93000 0; datenschutz.personenverkehr@pv.oebb.at
RECHTSGRUNDLAGE & ZWECK / LEGAL BASIS & PURPOSE
Art. 6 (1) (f) DSGVO (GDPR)
Schutz des Eigentums & Vandalismusprävention /
Protection of property & prevention of vandalism
SPEICHERDAUER / RETENTION PERIOD
120 Stunden maximal / 120 hours maximum
DATENSCHUTZERKLÄRUNG / PRIVACY STATEMENT
Abrufbar / available: www.oebb.at
IF 000

Pictogram

ÖBB-Infrastruktur AG
FN 71396 w
Praterstern 3
A-1020 Wien (Vienna)
T: +43 1 93000 0

Visibility of body cams

Cooperation with the security Authorities

- If there was an (criminal) incident in the recording area of the video surveillance, the data is only transmitted
  1. directly to police autorities (State offices for criminal investigations in each Austrian State (LKA) and the Federal office for criminal investigations (BKA))
  2. in case of a specific complaint
  3. based on a specific request concerning place and time
  4. in a technically safe way (encypted server to server transmission)
- There is neither a „general access“ for the authorities nor a „live-stream“ (or similar solution for live access)
- Live watching is possible for the police (e.g. in case of high-risk football games)
  - but only on ÖBB equipment in ÖBB premises
  - Only by prior appointment

Contact information

Mag. Martin Leiter
ÖBB-Holding AG
Group Data Protection Officer

Am Hauptbahnhof 2
A-1100 Wien
Tel. +43 1 93000 9744290
mobile +43 664 2866931

martin.leiter@oebb.at

Thank you for your attention!


SJ

”- A presentation of our work with third country transfers, how we plan and carry out our work with elements of both challenges and opportunities.”

SJ Group Information & IT Security:

Data Protection Officer Information Strategist

Stefan Carlsson

Agenda:

- Short presentation SJ
- GDPR at SJ
- SJ's work on third country transfers
- Dialogue – Questions

We bring people closer together, every day.

- SJ is a Swedish travel partner that offers sustainable train travel, both independently and in collaboration with others
- The Group has 4,600 employees and sales of approximately SEK 7.9 billion (1€= 10 SEK)
- As the market-leading train operating company, SJ connects Sweden and is the gateway to Scandinavia's capitals
- Operate services from Narvik in the north to Copenhagen in the south, and from Stockholm in the east to Oslo in the west
- Every day, 140,000 people choose to travel on one of SJ's 1,200 departures from 284 stations

GDPR at SJ.

- SJ observed early that there were to be new requirements and expectations on all controllers as of May 25th 2018.
- Our project started in January 2017
- A hand over to the organisation on May 25th 2018.
- A support organisation / project helped the organisation with guidance until December 2018.
- Since both Norway and Denmark follow GDPR we can complement and develop our GDPR work and compliance together.

3rd country transfers.

“The goal to combine the need for a free flow of personal data with effective protection of the individual's integrity runs like a common thread through the years and has been constantly evolving.”

3rd country transfers the Directive 95/46

1995 Directive 95/46 on the protection of individuals with regard to the processing of personal data.

“The increasing scientific and technical cooperation demands and facilitates flow of personal data which benefits the need for progress and development. At the same time with an common level of protection for personal data.”

3rd country transfers, Safe Harbour 1998.

7 principles for self-certification to prevent organizations within EU or US from disclosing or losing personal information.

Notice – inform individuals

Choice – possibility to opt out

Onward Transfer – data to third parties

Security – prevent loss of information

Data Integrity – relevant and reliable

Access – correct or delete inaccurate

Enforcement – effective means

3rd country transfers, Schrems I.

In 2013 a complaint against Facebook Ltd Ireland was filed by Max Schrems. In short the complaint was aimed to prohibit Facebook to further transfer data from Ireland to the US.

It was due to alleged mass surveillance programs in the US which wasn't in accordance with the EU protection law unless an organization can guarantee adequate protection.

In 2015 The Safe Harbour framework was ruled invalid by the Court of Justice of the European Union.

3rd country transfers Privacy Shield 2016.

In 2016 the final version of the EU – U.S Privacy Shield was approved by EU member states representatives.

After that the EU commission adopted the framework and it went to effect in July 2016 and Privacy Shield replaced Safe Harbour.

3rd country transfers GDPR from the 25 th of may 2018.

General Data Protection Regulation is our regulation in the European Union and the European Economic Area on the protection of individuals regarding personal data and on the free movement of such data.

Repealing The Data Protection Directive 95/46/EC.

GDPR is tightly related the EU Charter title II:
- article 7 Respect for private and family life
- article 8 Protection of personal data

3rd country transfers - Schrems II, 2020.

Max Schrems argued that Facebook was obliged under US law to make transferred personal data available to US authorities and then used in various monitoring programs in a way that is incompatible with the fundamental rights of EU.

In July 2020 The Privacy Shield framework was ruled invalid for transferring personal data to the US by the Court of Justice of the European Union.

Milestones in summary

1995
Directive 95/46
on the protection of individuals with regard to the processing of personal data.

1998
Safe Harbour 1998
7 principles to prevent organizations within EU or US from disclosing or losing personal information.

2013
Schrems I
In 2013 a complaint against Facebook Ltd Ireland was filed. The complaint was aimed to prohibit Facebook to further transfer data from Ireland to the US.

2016
Privacy Shield
In 2016 the final version of the EU – U.S Privacy Shield was approved.
It went to effect in July 2016 and replaced Safe Harbour.

2018
GDPR
the protection of individuals regarding personal data and on the free movement of such data.
Repealing The Data Protection Directive 95/46/EC.

2020
Schrems II
Facebook was obliged under US law to make data available to US authorities. The EU-court ruled that Privacy Shield no longer were sufficient protection.

SJ's work with 3rd country transfers.

- Extended focus came naturally with the EU-court ruling "Schrems II" in mid July.
- Initially we addressed US transfers and that Privacy Shield no longer gave sufficient protection.
- Rather quickly we adjusted the scoop to all 3rd country transfers.
- We started an internal information campaign addressing strategic level as well as both tactical and operational levels.
- …and the discussion on how to approach this challenge..

SJ's work with 3rd country transfers – how did we start?

Much is of course inspired of and led according to the EDPB-guidelines. They helped us to form an approach based on the following five steps/areas.

- Inventory and documentation.
- Contacting the relevant suppliers/partners.
- Analysing mitigating possibilities.
- Collaboration internally and externally.
- Identify ongoing or planned projects.

Inventory and document.

- Identify all transfers to 3rd countries and the transfer tools used.
- Check if all sub-contractors used in the transfers have contracts addressing GDPR responsibility.
- Make reconciliations and updates to the register of personal data processing's.

Contact relevant Suppliers and Partners.

- Request information about sub contractors.
- Check sub-assistants in 3rd countries
- Challenge the Suppliers proactively. What analyzes and findings that they have done that can benefit our common compliance.
- Perform a risk assessment and analysis of actions for agreements based on the Privacy Shield.

Start analysing mitigating possibilities.

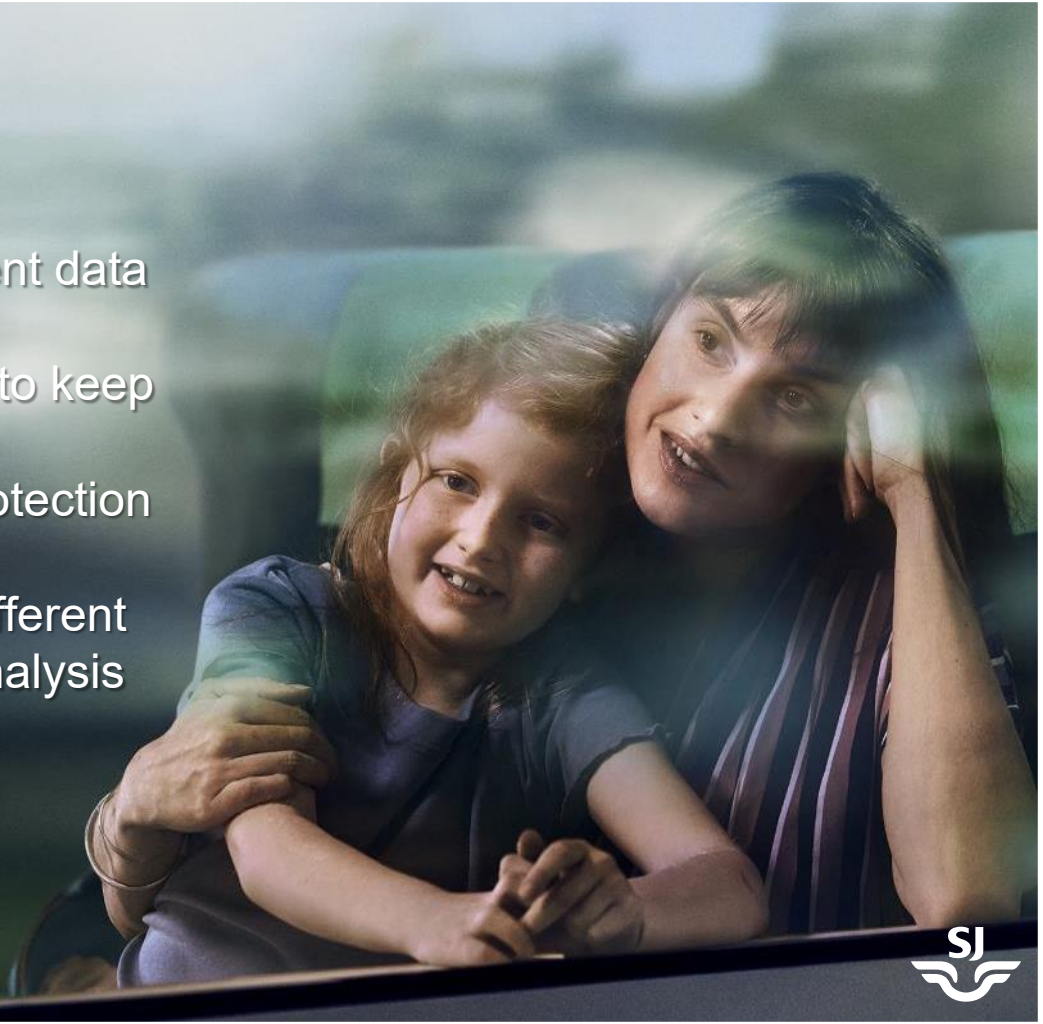
- Solutions established within the EU, without access from 3rd country?
- Encryption and pseudonymization?
- Other Means of mitigating measures?

Collaboration internally and externally.

- Create processes where all affected units are involved in the work.
- Build a common experience and knowledge base.
- Benchmarking – how do others do?
- Keep in touch and correspondence with trade associations.
- Don’t forget planned and ongoing projects, they might otherwise add to the challenge.

Some Challenges.

- How to keep continuity in sufficient data protection.
- External law and practice – how to keep up over time.
- Defining an adequate level of protection over time.
- Managing activities that are in different phases, all from identification, analysis to realization and test.



Some possibilities.

- Team up your organization’s GDPR skills.
- Align with already existing processes routines and administration.
- It is people who need to help and support each other regardless of whether you are a supplier or a customer.
- If the great leaps of progress not always occur, focus on step by step improvements.
- Use guidelines by EDPB and your DPA and use their support.

Summary

Through this work, we are confident that we comply with the GDPR regulation including the 3rd country transfers.

Thank you very much for this opportunity!

AFLUO,

A status update on the draft ePrivacy Regulation

AFLUO

Introduction

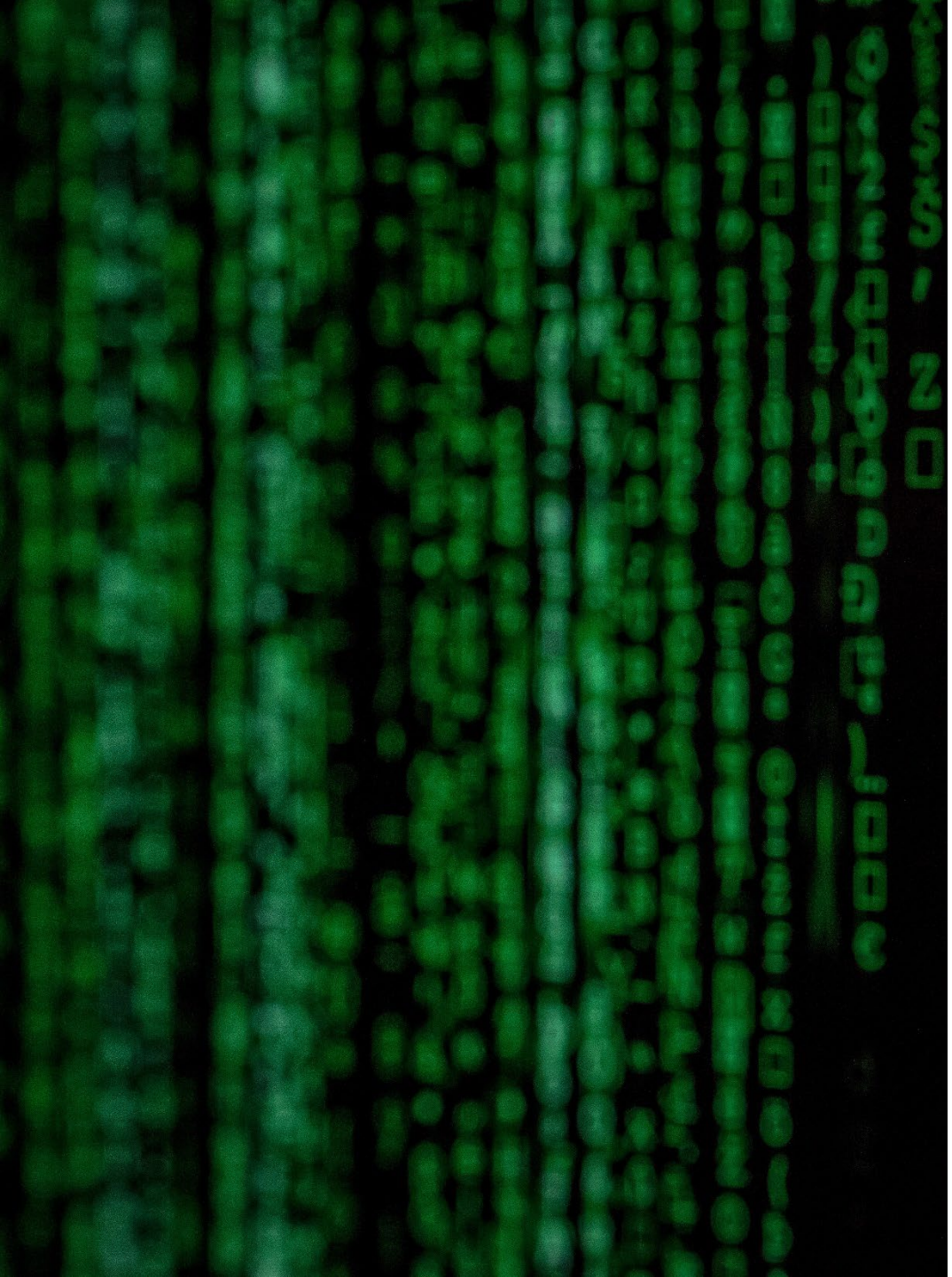
Status update

Why is ePrivacy important for railway transport?

Photo by José Martín Ramírez C on Unsplash

Draft ePrivacy Regulation

- Reform of data protection law incomplete
  - GDPR
  - Directive 2002/58/EC still in force
  - Article 95 GDPR: difficult interplay between GDPR and Directive
- Current status
  - Initial proposal: 10 January 2017
  - Trilogue ongoing since 10 February 2021
- Why is ePrivacy Regulation relevant?
  - Improved customer experience and customer retention
  - Customer tracking (marketing, security, service optimisation, …)
  - Direct marketing
  - IoT



Developments in the legislative process

What has changed and what has remained since the original draft text?

Photo by Markus Spiske on Unsplash

Developments in the legislative process

- Scope
  - Processing of electronic communications data (content and metadata)
  - Processing after receipt by end-user no longer covered
- Use of electronic communications data
  - Confidentiality
  - Prohibition of use (during transit)
  - Use during transit restricted to providers of electronic networks and services

Developments in the legislative process

- Cookies
  - Scope is larger than merely cookies:
    - Use of processing and storage capabilities of terminal equipment
    - Collection of information from end-users' terminal equipment
  - General prohibition, with exceptions
    - End-user consent (alignment with GDPR definition)
    - Strictly necessary for providing a service specifically requested by the end-user
    - Audience measuring (service provider or third party, separate or joint controller)
    - Necessary to maintain or restore security of information society service or terminal equipment, prevent fraud or prevent or detect technical faults

Developments in the legislative process

- Cookies
  - General prohibition with exceptions
    - Necessary for software update
      - Necessary for security reasons, does not change the privacy settings
      - End-user is informed in advance
      - End-user is given possibility to postpone or turn off automatic installation of updates
    - Further processing, if compatible
      - Information erased or anonymised if no longer needed
      - Limited to pseudonymised information
      - Not used for profiling of end-user
      - Restriction on data sharing

Developments in the legislative process

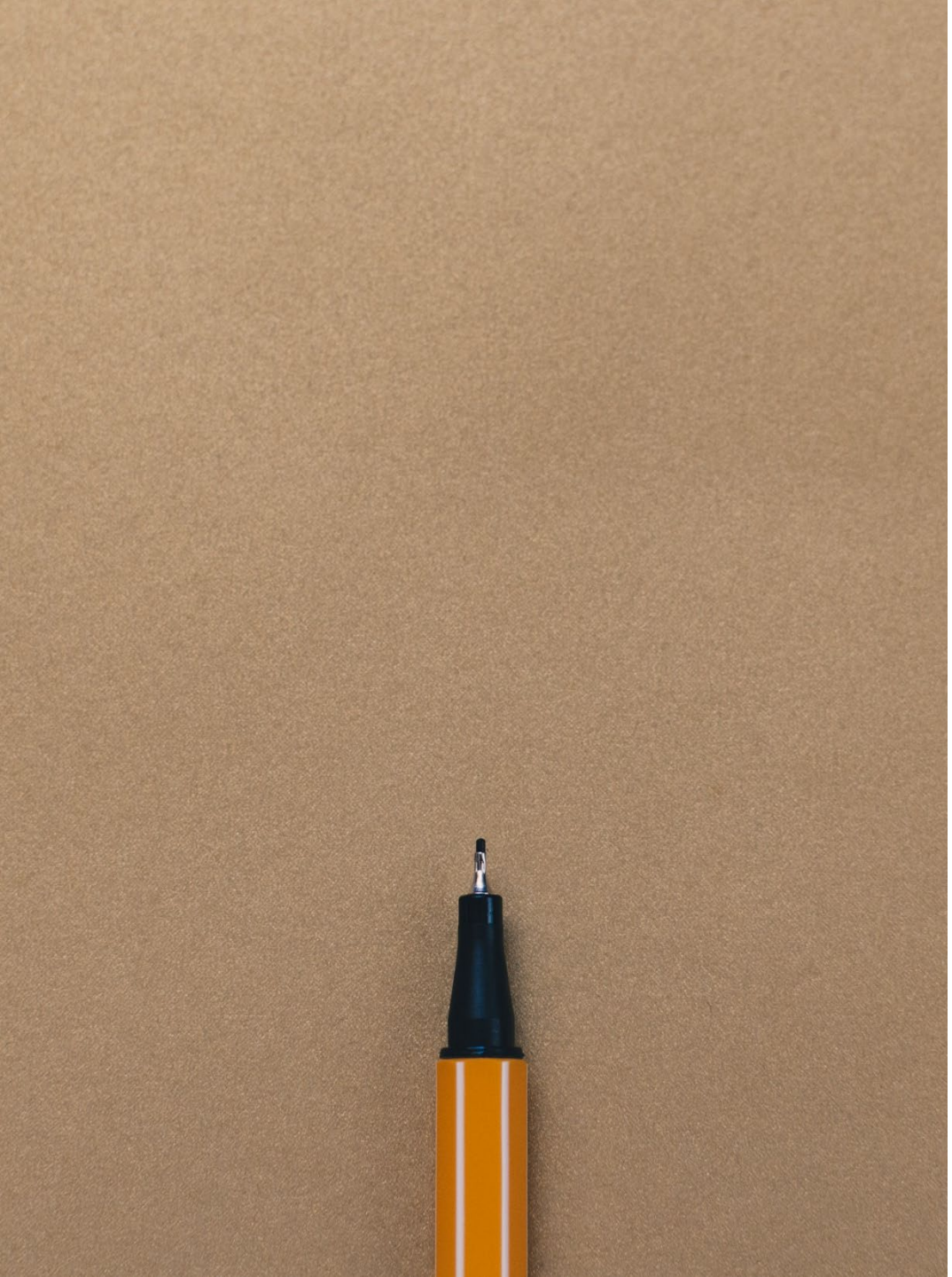
- Protection of end-user equipment: collection of information emitted by terminal equipment
  - Prohibition with exceptions
    - Necessary for creating and maintaining a connection
    - End-user consent (aligned with GDPR definition)
    - Necessary for statistical purposes
      - Limited in time and space to the extent necessary
      - Data is made anonymous or erased as soon as no longer necessary
  - Prominent notice is required for two last exceptions

Developments in the legislative process

- Direct marketing communications
  - Direct marketing or advertising?
  - Natural persons: soft opt-in
    - Consent
    - Existing client
      - Conditional opt-out
      - Possibility for time restrictions
  - Legal persons
    - National law must secure legitimate interests of legal persons

Developments in the legislative process

- Direct marketing calls
  - Calling line identification
  - Optional direct marketing code or prefix (member state law)
  - Reveal identity and use effective return addresses or numbers
  - Inform end-users
    - Nature of the call
    - Identity
    - Contact details
  - Natural persons
    - Opt-out
    - Provide natural persons information and opportunity to opt-out
  - Legal persons
    - National law must secure legitimate interests of legal persons



General conclusion

Photo by Kelly Sikkema on Unsplash

General conclusion

- Clarification of scope of ePrivacy Regulation
  - Distinction between communications services providers and others
- Alignment with GDPR
  - Consent definition
  - Enforcement and penalties
- Latest text version allows more processing (conditional)
  - Measuring technologies and analytics cookies
  - Device fingerprinting
  - Further compatible use
- Direct marketing essentially unchanged

Affluo Brussel
Greenhouse Brussels
Berkenlaan 8A+8B
B-1831 Diegem

Affluo Antwerpen
Van Immerseelstraat 66
2018 Antwerpen

info@affluo.be
www.affluo.be

Johan Vandendriessche
Partner | Affluo
Professor ICT Law | UGent
Lecturer Information Security Law | Solvay Brussels School
j.vandendriessche@affluo.be
+32 486 36 62 34

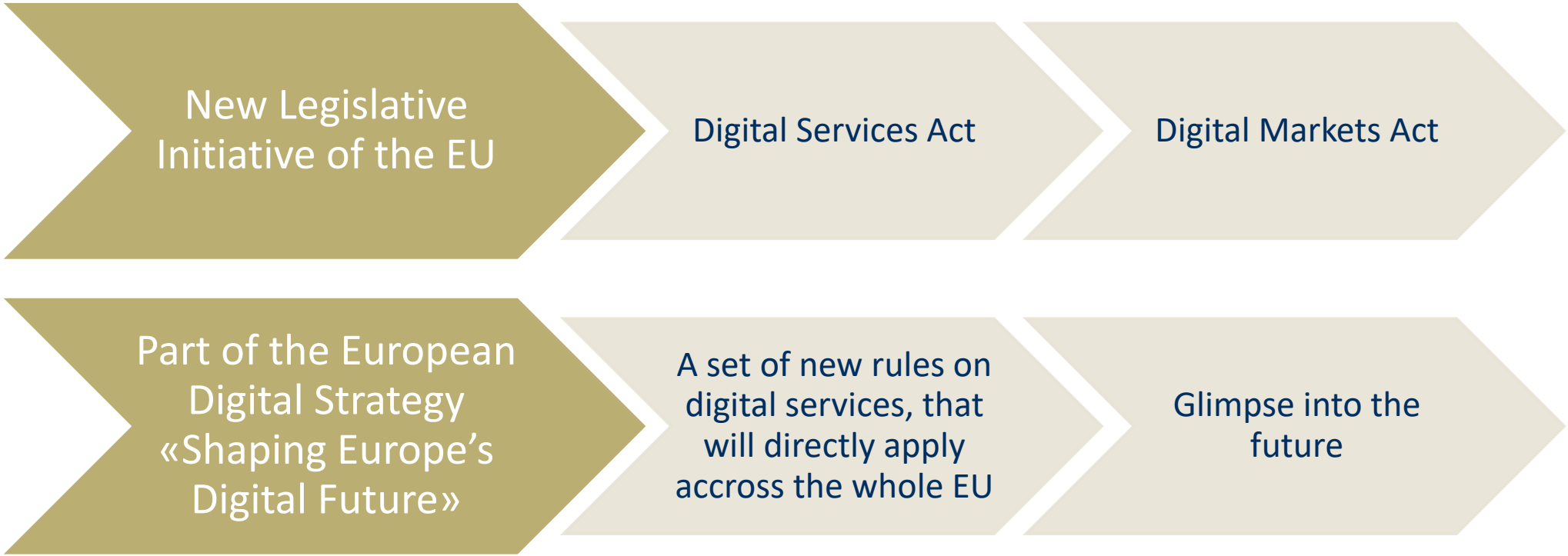
AFFLUO,

Digital Services Act Package

CIT Data Protection Conference

Caroline Gaul

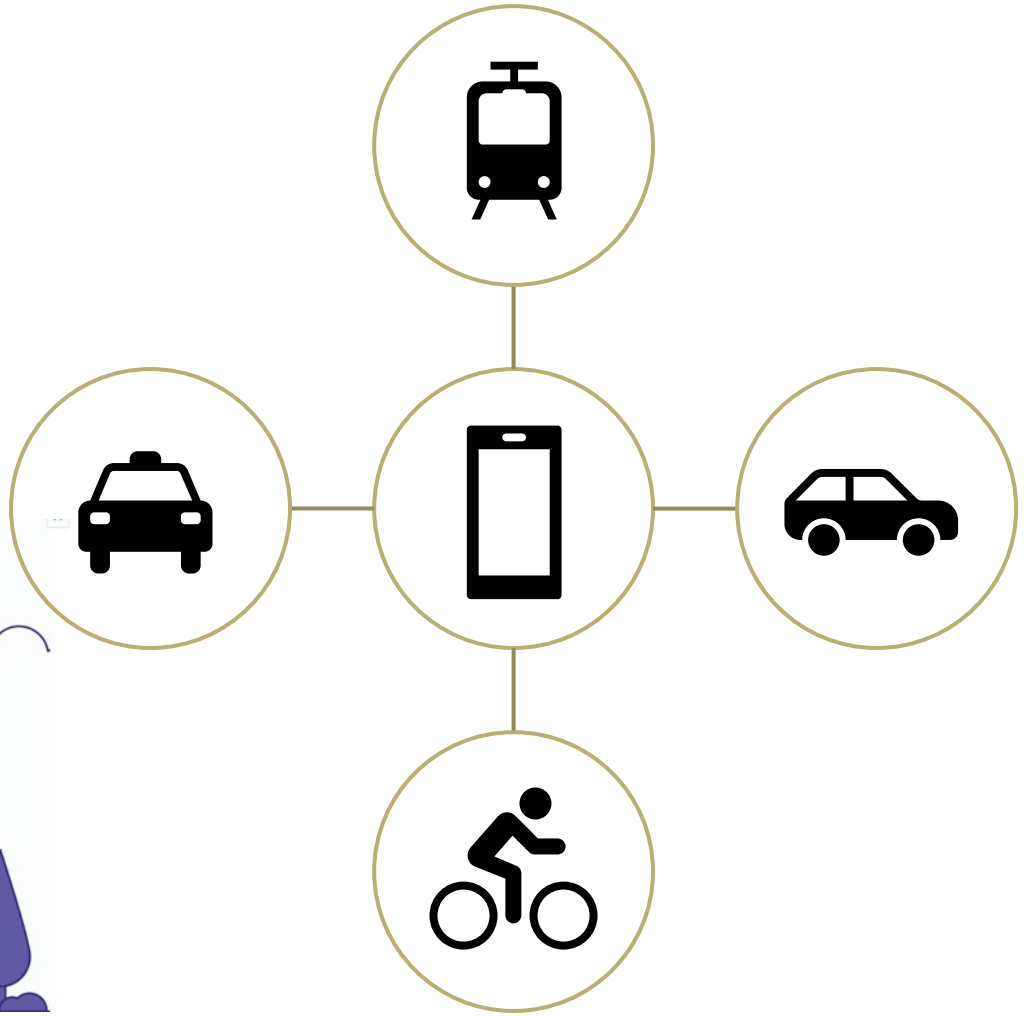
Digital Services Act Package



Online Platforms

Mobility as a Service (MaaS)

One platform for unlimited mobility. Public transport, e-bikes, car sharing and more…



Risks and Challenges

May be misused for the trade and exchange of **illegal goods**

May be misused to spread **fake news**

Their algorithms may amplify the spread of **disinformation**

So large and powerful that they become **gatekeepers**, able to act as private rule-makers, imposing **unfair conditions** on their business partners

Less choice or customers

Goals of the Digital Services Act Package

Create a safer digital space

- Customer Protection
- Transparency
- Accountability

Establish a level playing field for business users to foster

- Innovation
- Growth
- Competitiveness

Digital Services Act: Liability

Liability

In General: No liability of the provider of the intermediary services unless it plays an «active role» by having knowledge of or control over the information provided

New

Online platforms can be held liable under consumer protection law, if reasonably well-informed consumer would believe that the product or service provided on the platform is provided by the online platform itself

Digital Services Act: Obligations

Many new obligations…

- Establish a **single point of contact** for the electronic communication
- Designate a **legal respresentative** and notify such person to the Digital Services Coordinator
- **Further requirements for GTCs**: include information on restrictions regarding the use of the services, e.g. content moderation
- Introduce a **notice and action mechanism**
- Far reaching transparency **reporting obligations** (not applying to **micro or small enterprises**: enterprises which employ fewer than 50 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 10 million)

Digital Services Act: Obligations

Online Platforms (not applying to micro and small enterprises)

- Introduce a **complaint and redress mechanism** and **out of court dispute settlement**
- **"trusted flaggers"**
- Measures against misuse
- **Report serious criminal offences** to law enforcement or judicial authorities
- **KYBC "Know Your Business Customer"**
- **Design and organise the online interface** in a way that enables traders to comply with their obligations regarding pre-contractual information and product safety information under applicable Union law
- Introduce user-facing **transparency of online advertising**

Digital Services Act: Obligations

Very large online platforms: Provide services to ≥ 45 million users in the EU

- **Risk assessment:** illegal content, negative effects to the fundamental rights of their users, intentional manipulation, e.g. related to electoral processes
- **External risk auditing**
- **Further requirements for GTCs:** set out the main parameters used in their recommender system
- **Share data** with authorities to monitor and assess compliance with the DSA and to vetted researchers conducting research to identify and understand systemic risks stemming from the use of the platform
- Appoint a **compliance officer**

Digital Services Act: Enforcement

Digital Services Coordinators have large enforcement powers, e.g.:

- Order cessation of infringements
- Impose fines
- Adopt interim measures to avoid the risk of serious harm

The EU Commission may impose fines on very large online platforms

- up to 6% of its total turnover in the preceding financial year or
- periodic penalty payments of up to 6% of the average daily turnover in the preceding financial year per day

Digital Markets Act

Very Large Online Platforms

Systemic role in the market

Gatekeepers

Digital Markets Act: Obligations

Some of the new obligations

- Refrain from combining personal data sourced from core platform services with personal data from other services offered by the gatekeeper
- Refrain from using, in competition with business users, any data not publicly available, which is generated through activities by those business users
- Provide access to the data generated by business users as well as effective portability of data generated through the activity of a business user or end user
- Allow business user to offer the same products or services at different prices through other channels

Digital Markets Act: Obligations

Some of the new obligations

- Provide companies advertising on their platform with the tools and information necessary for advertisers and publishers to carry out their own independent verification of their advertisements hosted by the gatekeeper
- Refrain from treating its own products and services more favorably in rankings than those of third parties
- Provide access to app stores on fair and non-discriminatory general conditions
- Refrain from preventing users form un-installing any pre-installed software or app if they whish so

Digital Markets Act: Enforcement

Periodic penalty payments of up to 5% of the average daily turnover

Additional remedies may be imposed, if necessary and as a last resort option, non-financial remedies including behavioral and structural remedies, e.g. the divestiture of (parts of) a business.

Fines of up to 10% of the gatekeepers worldwide turnover

Thank you for your attention

Caroline Gaul

Senior Associate

Direct phone: + 41 58 658 51 35
caroline.gaul@walderwyss.com

Walder Wyss Ltd.
Seefeldstrasse 123
P.O. Box
8034 Zurich
Switzerland

walderwyss attorneys at law

nmbs

CIT Data Protection Conference

25th March 2021

PNR & API

Bianca Jonas, SNCB

Agenda

1. PNR & API in general
2. PNR & API in Belgium
3. Q&A

PNR & API in general

API

Directive 2004/82/CE of 29 April 2004

Definition

API: Advance Passenger data

All information usually contained in travel documents like passeports and identity cards collected by air carriers during check-in and transmitted after check-in closure to border control or other authorities of a country.

Application

- Transport by air carriers*
- All flights into the territory of the Member states

Purpose

Improving **border controls** and combatting **illegal immigration.**

DATA PROTECTION AND PRIVACY

* Member states can create stronger rules to extend application.

PNR

Directive of 27 April 2016

Definition

Personal name record: Record of each passenger's travel requirements

- information necessary to enable reservations to be processed and controlled by the booking and participating air carriers
- for each journey booked by or on behalf of any person,
- whether it is contained in reservation systems, departure control systems used to check passengers onto flights, or equivalent systems providing the same functionalities.

Application

- Transport by air carriers*
- All extra-EU flights*

Purpose

Preventing, detecting, investigating and prosecuting **terrorist offences or serious crime.**

* Member states can create stronger rules to extend application.

DATA PROTECTION AND PRIVACY

PNR data

Consequences for Member States:

- Designate a **PIU (** Passenger Information Unit) in charge of processing PNR
  - » Assessment of passengers against pre-determined criteria and update or creating new criteria therefore
  - » Provide PNR data in specific cases (case-by-case study)
  - » transfer to competent authorities, other PIU and Europol

- **Transfer** PNR data:
  - » 24h and 48h before departure
  - » Immediately after flight closure

- **Adopt and notify a list** with competent authorities to request and receive PNR data

- Lay down rules on **penalties** to infringements

- Provide a **national supervisory authority**

DATA PROTECTION AND PRIVACY


sncb
PNR & API in Belgium

PNR Data and international transport in Belgium

"It doesn't make any sense to apply these measures to planes and to leave acces to international busses and trains completely open" **Jan Jambon, former** Minister of Interior and Security.

PRN data wil be given to PIU, a service at SPF Interior

Competent authorities:

- the federal police,
- the State Security,
- the Military Enquiry Service
- Customs duties work together.

" The purpose is not only to process this information but also to get to know the movements of certain criminals." **Jan Jambon**.

DATA PROTECTION AND PRIVACY

PNR data in Belgium - Theory

Law of 25 December 2016 – about processing passengers data &
Royal Decree of 3 February 2017.

Who?

- Carriers **and travel operators**
  - » No indication about successive carriers but SNCB could be considered as a carrier and foreign transport companies would have to respect this legislation

What?

- For all extra- and **intra-EU travels**, even with private jet,
  - » With destination to,
  - » Coming from or
  - » Transiting Belgium
- Also travels with **HST (ONLY)** (e.g. Thalys, Eurostar, TGV and ICE) not HSL (oral explication of government not yet confirmed)

DATA PROTECTION AND PRIVACY

PNR data in Belgium - Theory

Law of 25 December 2016 – about processing passengers data + Royal Decree of 3 February 2017.

Obligations

- No ID-control but a verification
  - » Data will be passed to authorities (details about how are not known yet)
- Send available information of customers/passengers to the PIU of FOD BiZ at 4 moments:
  - » 48 hours before departure
  - » 24 hours before departure
  - » Boarding
  - » **For HST also at arrival if changements**

Financial consequences

- Fine 50.000 € max (75.000 € recidivism within two years).
- Budget: gates, controls
- Clients: waiting lines

DATA PROTECTION AND PRIVACY

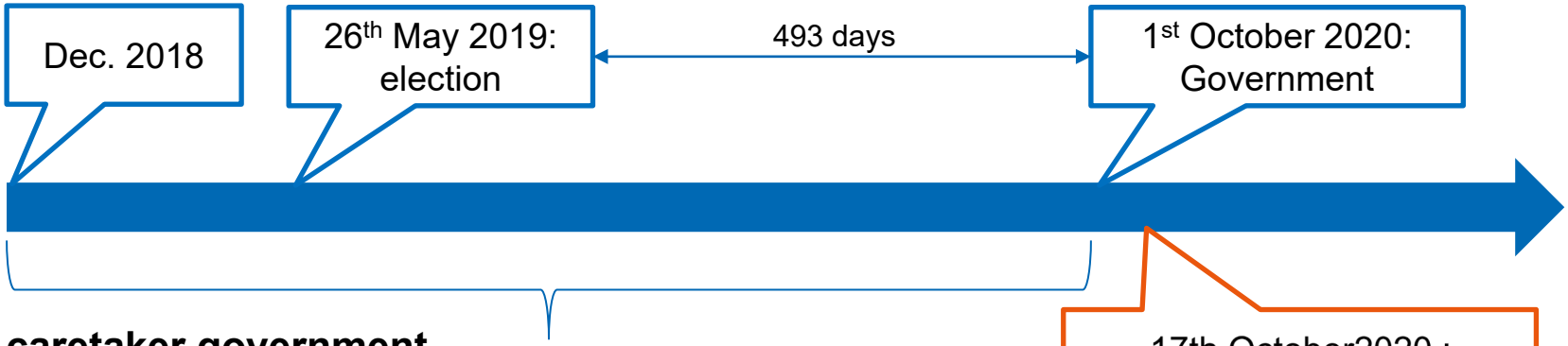
PRN & API data in Belgium – In practice

1. Test of datatransfer with Eurostar (Brussels – London) but suspended because of Brexit
2. Running tests between BiZa/SPF Interieur (ministery for Interior) and bus sector for Flixbus (who has an electronic database like Uber)
3. **Jurisdictional procedure** of a human right organization
4. Technical work method not yet defined
5. No data aggregation planned until now, risk that the same data will be sent several times (travel operator and distributor).

DATA PROTECTION AND PRIVACY

PNR & API data in Belgium – In Practice

Obligation to fullfill as soon as the Ministery of Interior and Security, as well as the Ministery of Mobility sent ***two notification letters*** with ***all implementation directive*** guidelines. These letters will determine the start date and hopefully answer above mentionned open points.



caretaker government
(limited powers to all decisions which are strictly necessary to guarantee an uninterrupted function of public service.)

17th October2020 : decision of const. Court (10 questions to CJCE)

DATA PROTECTION AND PRIVACY

* Presentation has been established on 15 May 2019.

Case law

The Human Rights League went to the constitutional court to ask annulation of the law of 25th December 2016 (Belgian PRN law).

Motivation:

- The law is against privacy and data protection because PNR is large and the collection is too general;
- This law is against the principles of free mouvement of goods and people.

Decision of the court = no decision but:

1. 10 questions adressed to the CJCE*
2. Compatibiity of the Belgian Law with privacy and data protection
3. Asking for interpretation of some notions
4. Asking the validity of the PNR Directive with regards to the principle of free mouvement of goods and people

DATA PROTECTION AND PRIVACY

Other news

The Commission's Report "COM(2020) 305 final" on the revision of the PNR Directive published in summer 2020 puts off the table the question of a possible extension of the scope of the Directive to rail for the time being, because of the significant legal, practical and operational questions and makes it subject to a comprehensive impact assessment.

The Council conclusions 14746/19 on widening the scope of PNR data to transport modes other than air, adopted by the Justice and Home Affairs Council on 2-3 December 2019 recommend that the Commission carries out a study to explore the need for and feasibility of the collection, storage and processing of PNR data for cross-border transport services other than air traffic.

Q&A

Contact

Privacy : dpo@b-rail.be

DATA PROTECTION AND PRIVACY

Thank you!

RENFE APPS AND MAAS

Data Protection conference - CIT
25th March 2021
Fernando de Lucas de Rose

Renfe Cercanías

Renfe ticket

Play Renfe

Club + Renfe

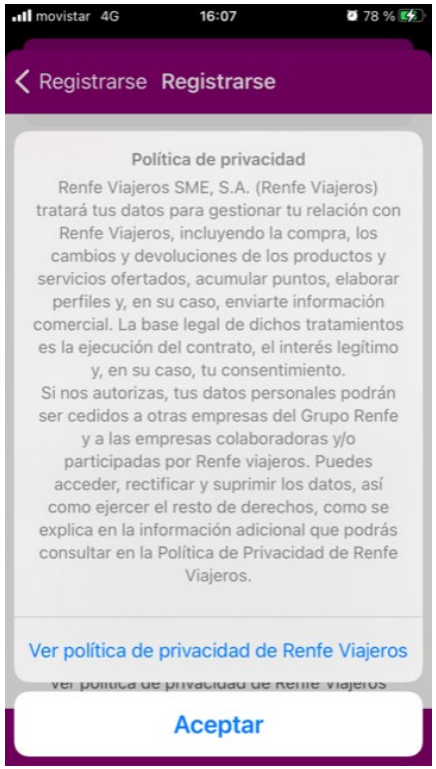
Renfe Horarios

Renfe Atendo

App	Service	Choices
Renfe Cercanías	Commuter trains	Ticket sale Customer claim Schedules
Renfe ticket	Medium distance Regional High Speed	Ticket sale Loyalty program Hotels / leisure
Renfe horarios	All	Schedules
Atendo	All	PMR assistance
Club + Renfe	All	On board magazine
Play Renfe	All	On board wifi and entertainment

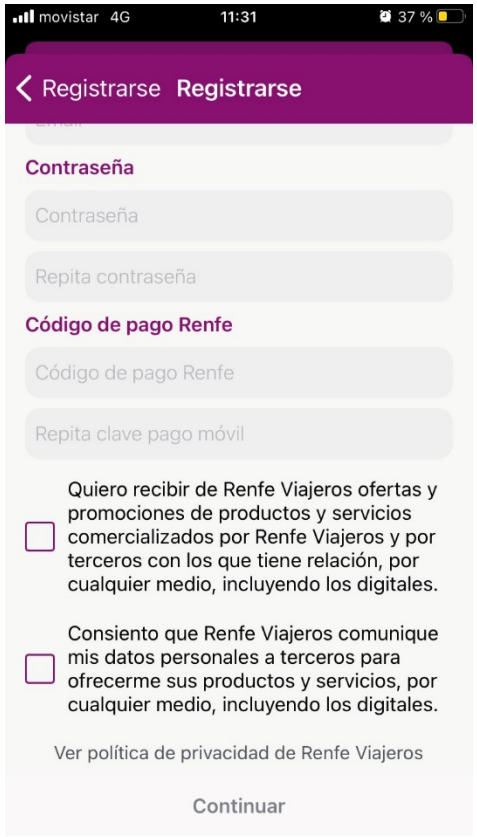
Renfe ticket

- **Registration required. Provision of personal data.**
- **Compliance with information according to GDPR.**



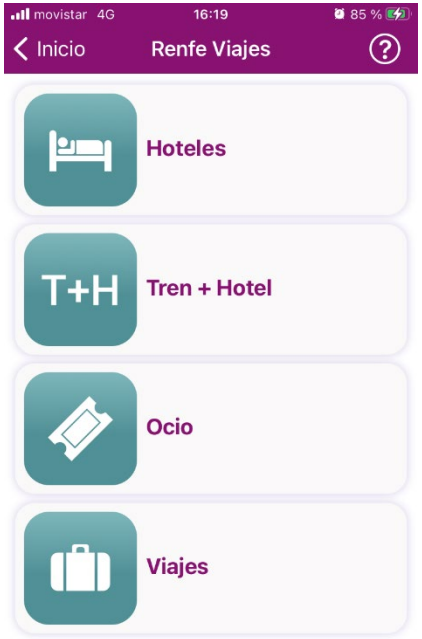
- **Information provided according to art. 13 GDPR.**
- **Information provided for layers in accordance with AEPD (Spain´s DP Authority).**
- **Further information on website.**
- **Positive action of acceptance required.**

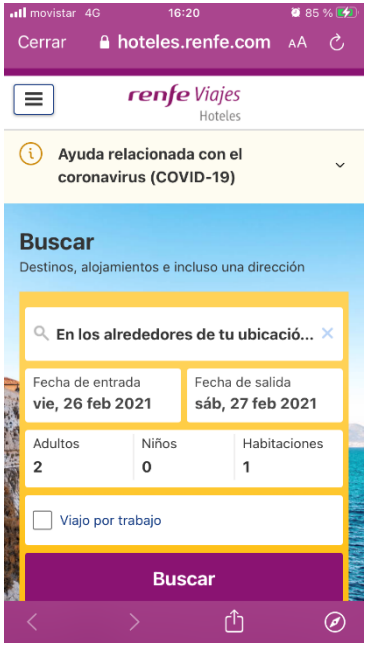
Renfe ticket



- **Advertising and promotional communications subject to previous authorisation.**
- **Further information on website.**
- **Positive action of acceptance required.**
- **Boxes not previously marked.**

Renfe ticket





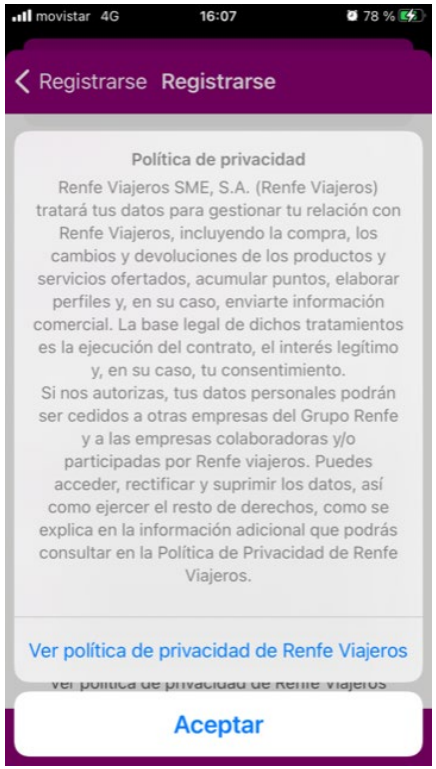
Provision of personal data

Booking Data Controller

Privacy policy of Booking.com

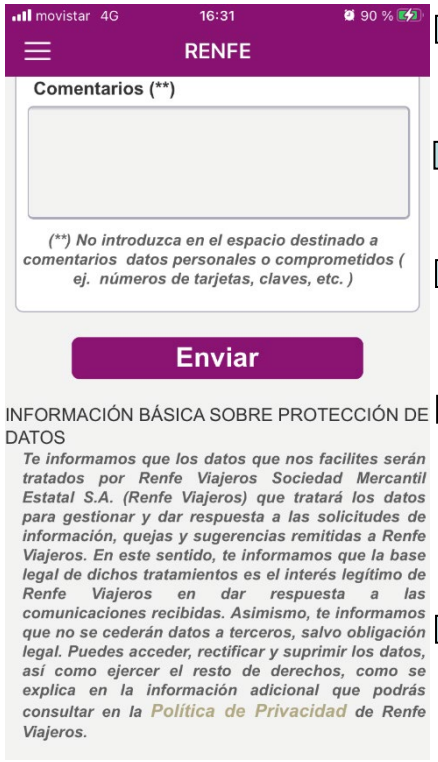
Renfe Cercanías

- **Registration required. Provision of personal data.**
- **Compliance with information according to GDPR.**



- **Information provided according to art. 13 GDPR.**
- **Information provided for layers in accordance with AEPD (Spain´s DP Authority).**
- **Further information on website.**
- **Positive action of acceptance required.**

Renfe Cercanías



- **Information request/Claims/Suggestions.**
- **For registered users.**
- **Compliance with art. 13 GDPR in case new data are provided.**
- **Information provided for layers in accordance with AEPD (Spain´s DP Authority).**
- **Positive action of acceptance required.**

MaaS: Mobility as a Service → RaaS (Renfe as a Service)

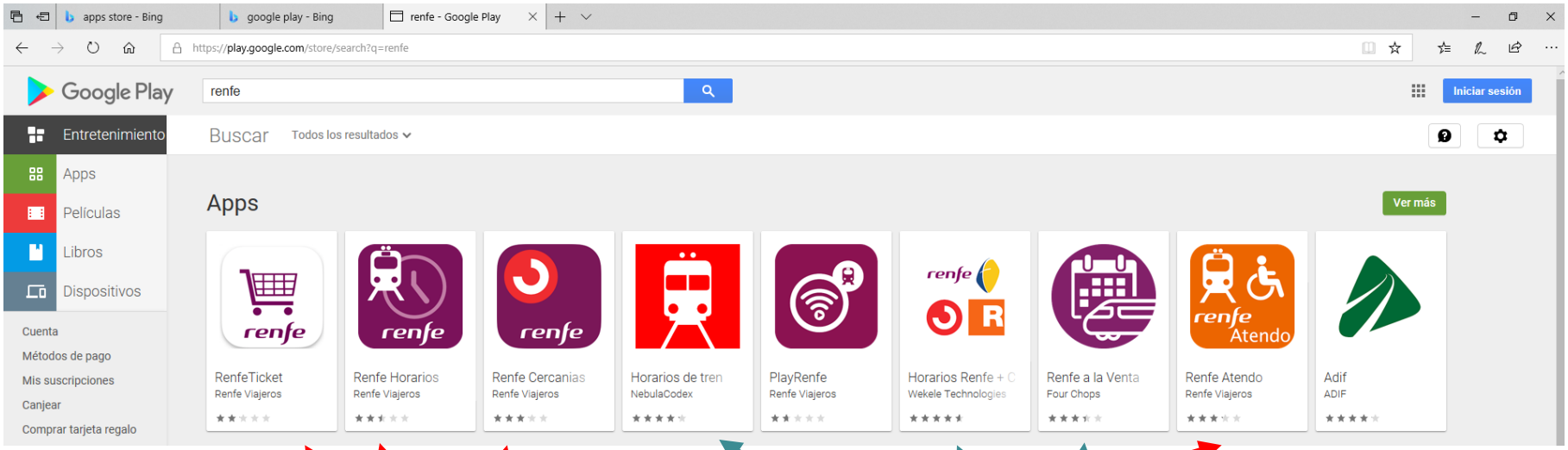
- **Currently, under development.**
- **Transition from several Apps into a single platform.**
- **Integration of several means of transport into a single platform.**
- **From first mile until the last mile.**
- **Railway, bus, cars, parkings, bicycles, additional services, among others.**
- **Public or private operators.**
- **Data Protection is a cornerstone.**

Data Protection issues to be taken into account according to GDPR:

- **The Key: Privacy by design.**
- **Correct detection of personal data flows as data are provided by different sources.**
- **Correct identification of data controller. Joint controllers?**
- **Compliance with information when data are collected.**
- **Impact Assesment, valuation of risks and measures to be implemented.**

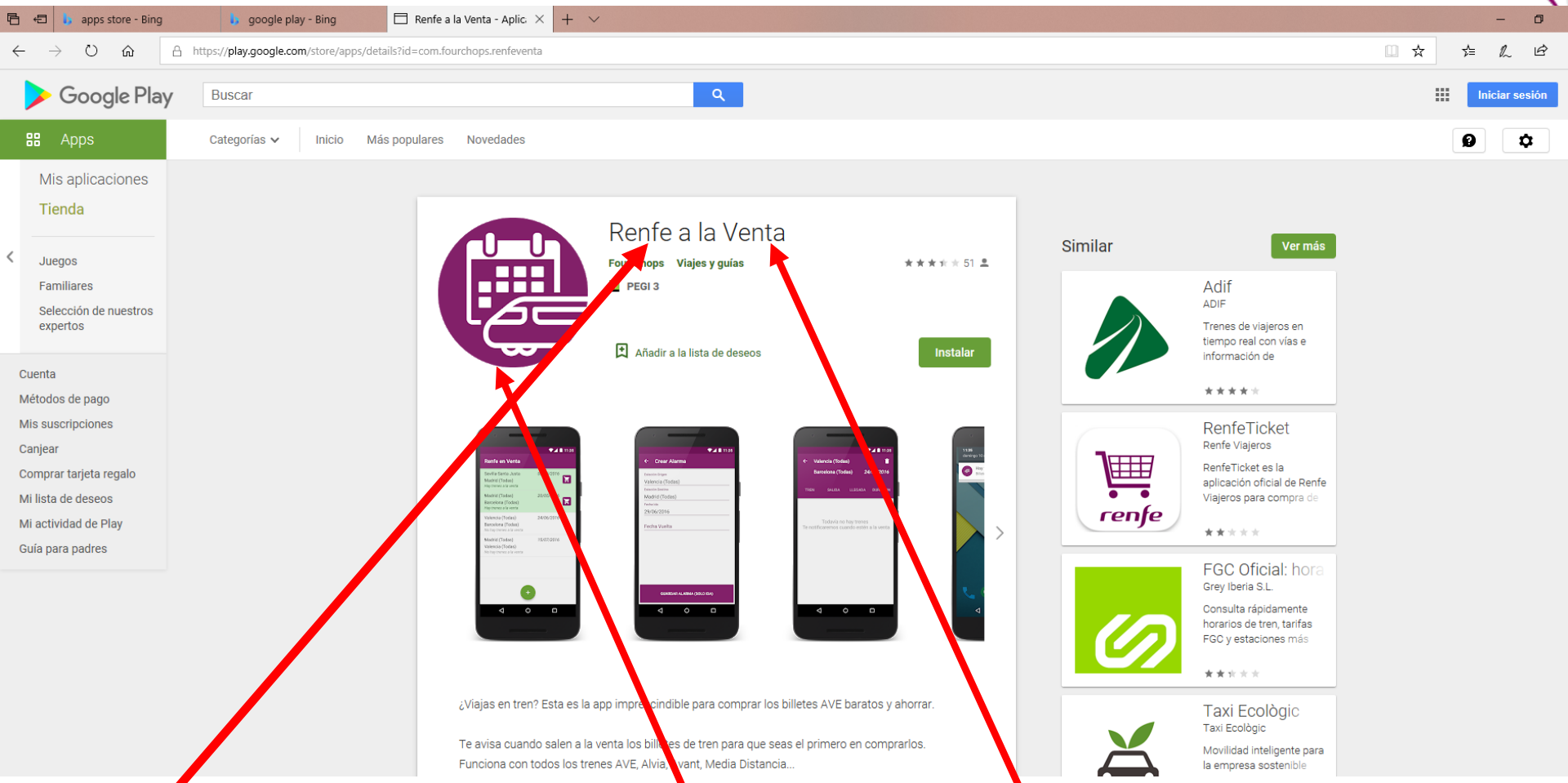
Other legal issues with Apps

- **Breach of trademarks rights.**
- **Non official Apps and impersonation.**
- **Non accurate or misleading information / consumers claims.**



Official Apps

Non official Apps

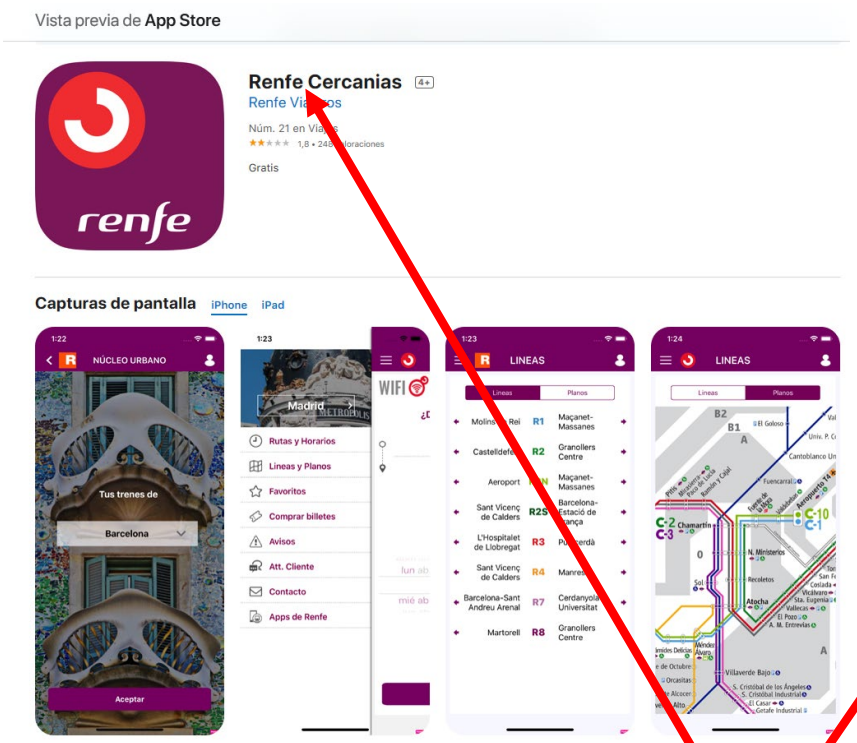


Non-authorized trademark use

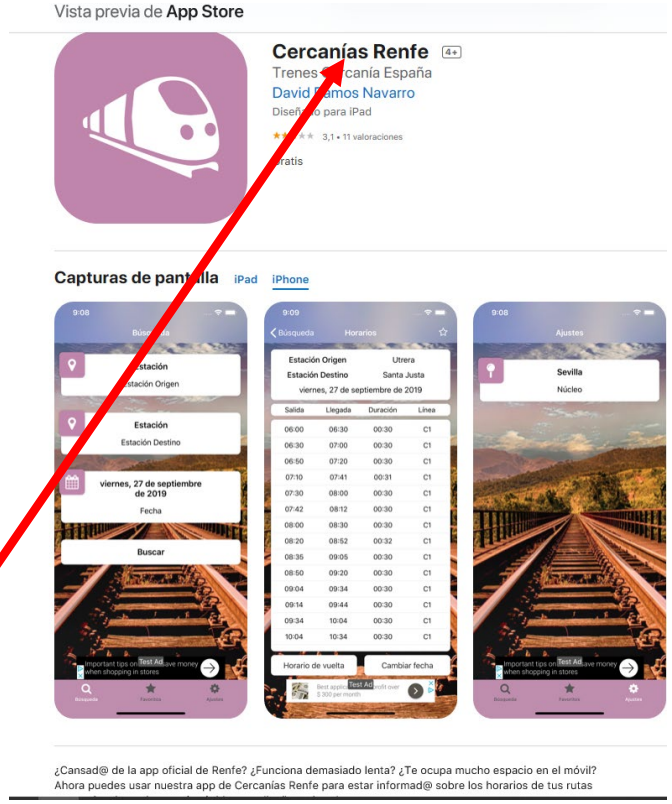
Same corporate colours

Misleading name. It is not an app for ticket sales

Official App



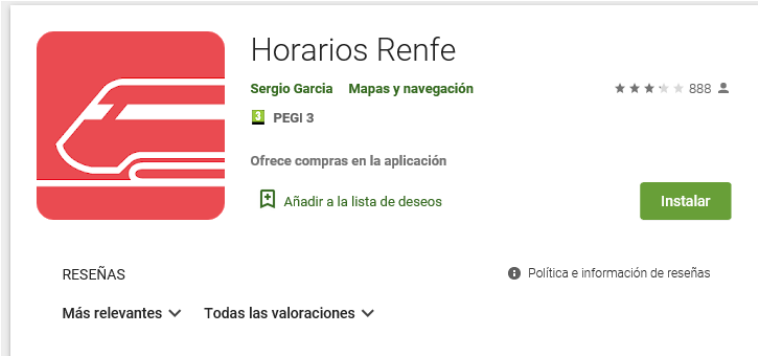
Non official App



Trademark use

Non accurate information on non official Apps may derive on customer claims.

Example:



"Wrong schedules, low level app, idleness of Renfe…"

What can we do?

Never give up.

Frequent review and surveillance on app stores to detect potential breaches.

As soon as an app disapears, a new one comes up.

Faster and better results when claiming against the app owner instead of claiming through app stores customer services.

renfe

Thank you very much

International Rail Transport Committee
Comité international des transports ferroviaires
Internationales Eisenbahntransportkomitee

CIT activities on GDPR

CIT Data Protection Conference

25 March 2021

Sandra Dobler
Senior Legal Adviser

SUMMARY

- Manual on Data Protection for transport undertakings (MDP)
- Development of a code of conduct
- CIT Data Protection Experts' Group
- Next CIT Data Protection Conference

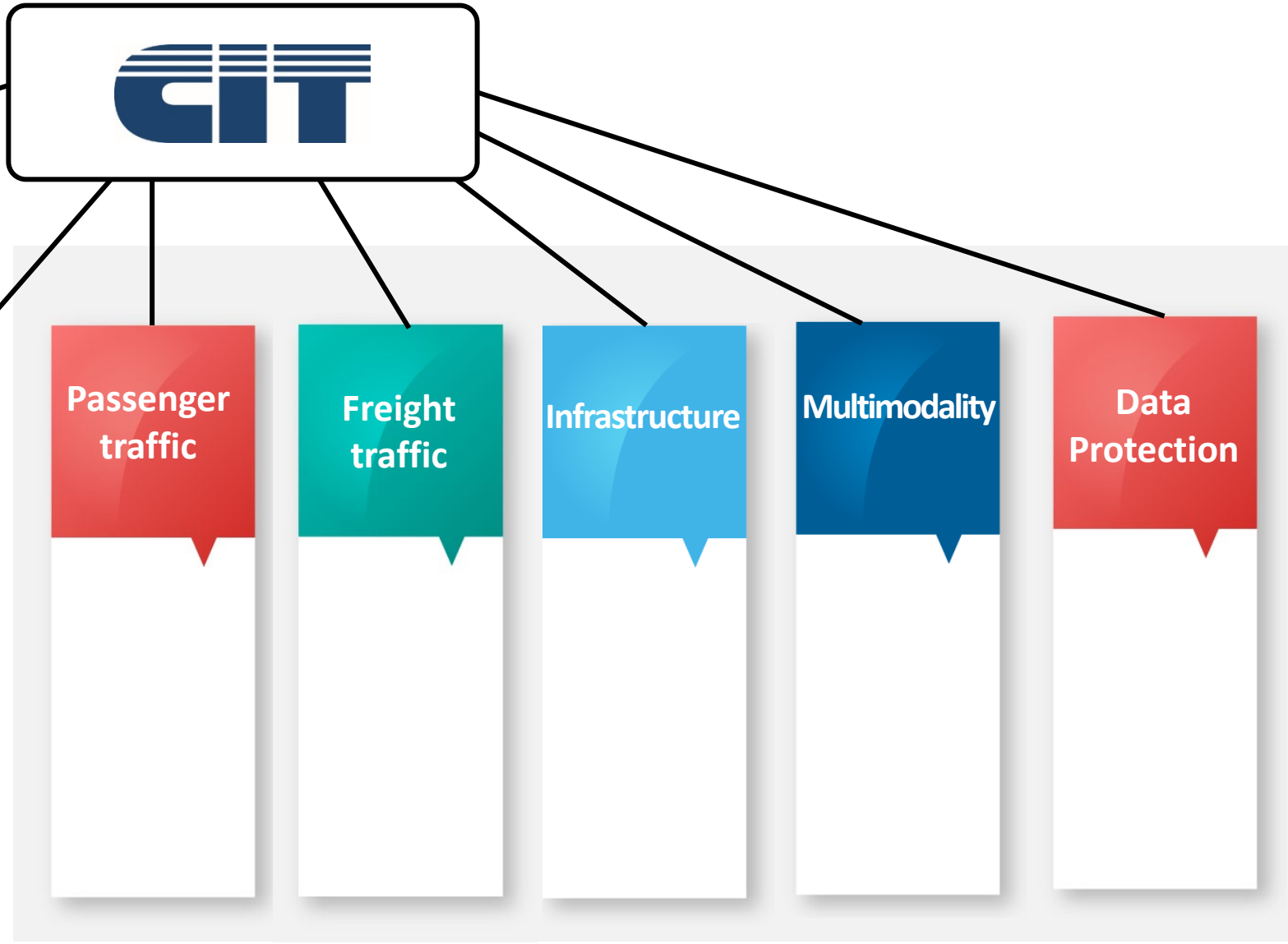
WHO WE ARE

Members

200 railway + maritime companies from all around the world

Aim

- Implementation of international and EU transport law
- Standardisation of the contractual relationships



CIT PRODUCTS IN PASSENGER TRAFFIC

Railway Undertakings
B2B

Passengers
B2C

Multimodality
R2P

CIT Products in Passenger Traffic

Opt in | Opt out

Railway undertakings
B2B

Glossary
Glossary on the technical terms used in the CIT documents with translations in EN-FR-DE.
Fact sheet

Leaflet on COTIF-CIV-PRR-SMPS
Leaflet describing the various COTIF/CIV-PRR – SMPS liability regimes which are used in international passenger traffic.
Fact sheet

MIRT Manual on ticketing
Manual on the standards for issuing international paper and electronic tickets.
Manual Opt out

AIV Agreement concerning the handling of claims
Agreement governing the relationships between transport undertakings on the roles and responsibilities for claim procedures.
Agreement Opt out

MCOOP Manual on cooperation between railway
Manual containing a boilerplate contract and general terms and conditions as well as commentaries to them for the international cooperation of railway undertakings to provide carriage of passengers.
Manual Opt in

AJC Agreement on journey continuation
Agreement governing the relationships between railway undertakings to support international passengers in the event of disruption to their journey.
Agreement Opt in

MDP Manual on data protection
Manual containing commentaries and guidelines concerning the data protection rules, as well as good practice examples and boilerplate contracts on data processing.
Manual Opt in

Passengers
B2C

RID Notice
Notice for the attention of passengers concerning the restrictions on the carriage of dangerous goods as hand luggage or registered luggage, or in or on board vehicles (car on train) or registered luggage, or in or on board vehicles.
Terms and Conditions Opt in

GCC-CIV/PRR General conditions of carriage
General conditions of carriage applicable in the contractual relationship between passengers and carriers for domestic and/or international journeys.
Terms and Conditions Opt in

RID Info-table
Info-Table on the Dangerous goods permitted to be carried as hand or registered luggage, or in or on board vehicles (car on train).
Fact sheet

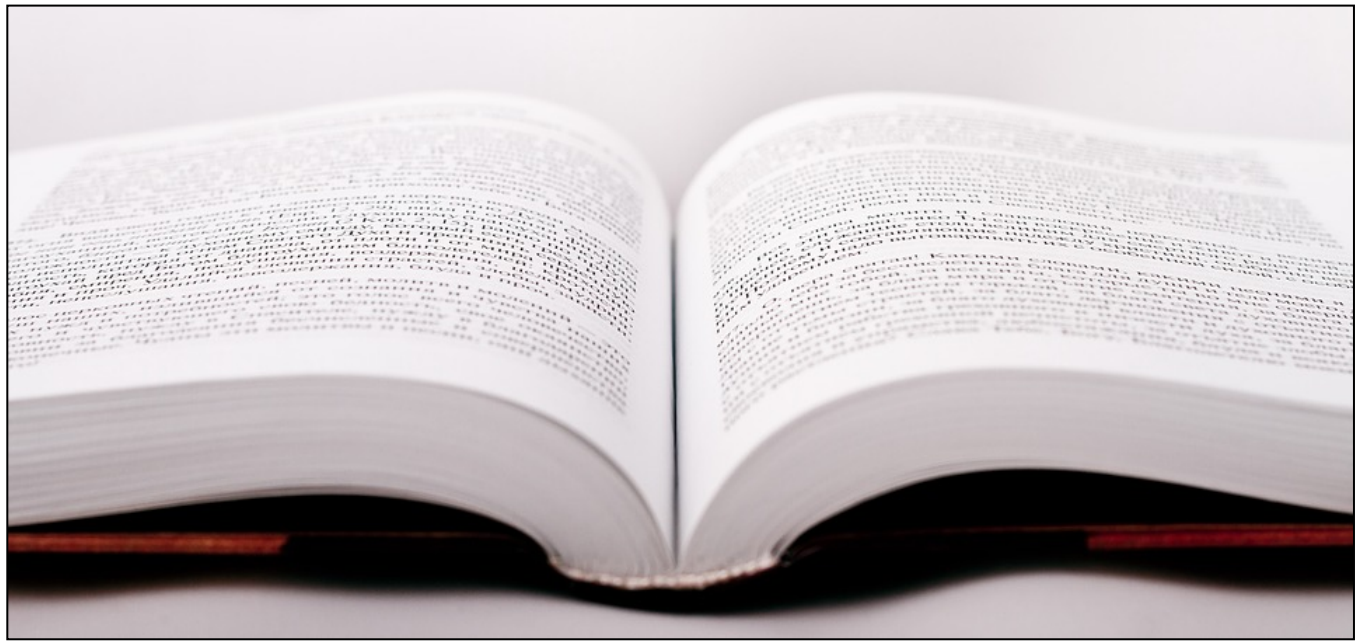
Multimodality
R2P

Air-rail boilerplate contract
Boilerplate contract with commentaries for the cooperation between railway undertakings and airline companies.
Agreement Opt in

Air-rail comparative table
Comparative analysis on the international legal framework for air and rail passenger traffic.
Fact sheet

MANUAL ON DATA PROTECTION FOR TRANSPORT UNDERTAKINGS (MDP) 1/2

Guidelines

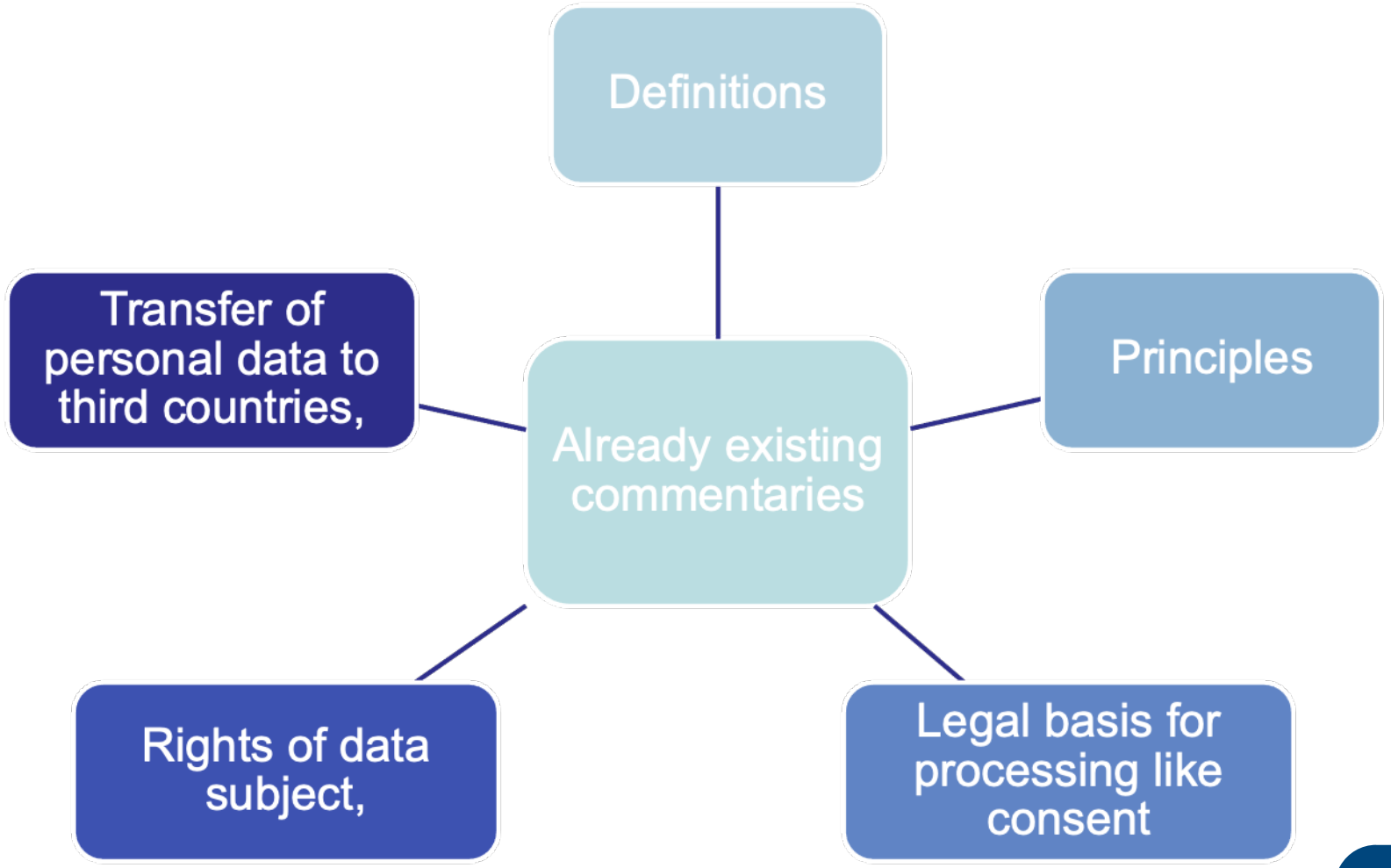


Commentaries

Boilerplate contracts on data processing

Examples of clauses

MANUAL ON DATA PROTECTION FOR TRANSPORT UNDERTAKINGS (MDP) 2/2 - COMMENTARIES



MANUAL ON DATA PROTECTION FOR TRANSPORT UNDERTAKINGS (MDP) 2/2 - COMMENTARIES

New cases and legal opinions

Data processing impact assessment (DPIA)

- Explanations and templates on how to do a DPIA

Balance of legitimate interests

- Explanations on how to do it

Age of consent of children

- Information on age for information society services

Fining policy

- Information on fines in the different Member States

DEVELOPMENT OF A CODE OF CONDUCT

Issue

- Transfer of personal data to third countries

Solution

- Development of a code of conduct

What is it?

- Codes of Conduct, under the GDPR, are voluntary sets of rules that assist members of that Code with data protection compliance and accountability in specific sectors or relating to particular processing operations.

Steps

- Development within a Dedicated Data Protection Experts in the coming months

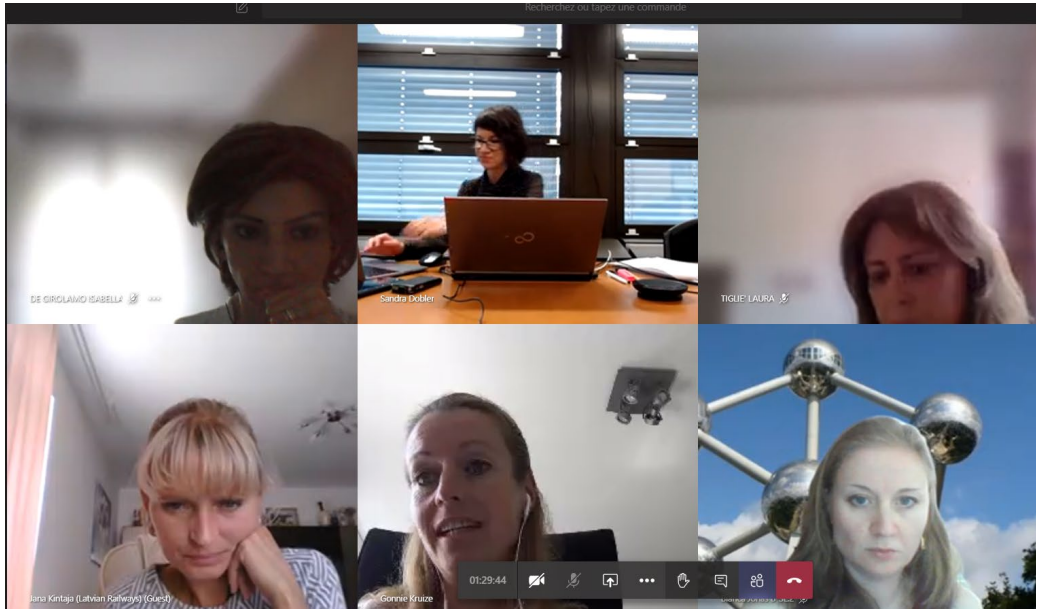
CIT DATA PROTECTION EXPERTS' GROUP

Who?

Data Protection Officers and Experts

What?

Annual meetings
E-mail exchanges
Platform of discussion



New members always welcome to join!

NEXT CIT DATA PROTECTION CONFERENCE

Thank you
for your attention!

Questions?

Sandra Dobler
Senior Legal Adviser
Tel. : +41 31 350 04 80
E-mail : sandra.dobler@cit-rail.org

www.cit-rail.org

Lab for Innovation Ethics
Lab d’éthique de l’innovation
Laboratorio per l’etica dell’innovazione
Lab für Innovationsethik

Digital Integrity
A new human right?

CIT, 25th March 2021

Dr. Johan Rochel

Digital Integrity

Digital Integrity

Objectives

- Understand what is digital integrity
- Explore its role as a human right
- Discussion potential cases of application

Digital Integrity

Definition

A right to protect individuals using digital technologies

a) Protect their capacity to use digital technologies

b) Protect their essential interests when using these digital technologies (person as user)

c) Protect their essential interests when being monitored/surveilled by digital technologies (person as object)

⇒ Interesting “glasses” to identify new threats made possible by digital technologies

Digital Integrity

a) Their capacity to use digital technologies

It is about making sure that individuals have the capacity to access and use digital technologies.

⇒ Access to internet as key example

⇒ Resources to use digital technologies (”digital divide”)

Digital Integrity

b) Protect their essential interests when using these digital technologies (person as user)

It is about protecting individuals from being:

⇒ monitored, tracked and measured when using digital technologies

⇒ threatened and hurt when using digital technologies (eg. Cyber-bullying ; cyber-stalking ; misuse of personal data)

⇒ taken away their person's identity and capacity to act

Digital Integrity

c) Protect their essential interests when being monitored by digital technologies (person as object)

It is about protecting individuals from being:

⇒ monitored, tracked and measured by digital technologies (eg. CCTV, “smart city”)

⇒ controlled by digital technologies/on the basis of information made available by digital technologies

Digital Integrity

What digital integrity is NOT

- It is not the protection of one's digital avatar ("second life") – it is the protection of a person acting trough digital technologies or being the object of these technologies
- It is not the protection of a person in the "cyberspace" – geographical/spatial metaphors are misleading. Focus should be put on a person using digital technologies.
- It is not the creation of a digital dimension of human beings – digital integrity is useful in expressing specific threats to someone's mental and physical integrity. Mind and body are key.


Circle K

The role of digital integrity

The role of digital integrity is to provide **consistency** between several norms/rights.

It is a concretization of the protection of human dignity with respect to the potential threats that digital technologies pose.

It serves to promote a substantial definition of what freedom should be about and how this freedom relates to the protection of privacy in informational matters.

Dignity

DIGITAL INTEGRITY

Individual freedom

Informational self-determination ; privacy ; data protection

The role of digital integrity

Digital integrity requires…

⇒ To have a clear view on what individual freedom means in a context of digital technologies

⇒ To determine which essential interests should be protected in this context

Digital integrity is the norm to answer the key question: **what does that imply to be a free person using digital technologies ?**

Potential cases of application

Person as user

⇒ Having the resources to use digital technologies (access, knowledge, financial resources) – eg. Exclusion of workers on gig-economy platform like Uber

⇒ Protecting personality rights – digital technologies make new threats possible, eg. Children bullying using communication tools

⇒ Respect of one's capacity to use digital technologies anonymously – searching for information, connecting, shopping => same standards as in offline activities ?

Potential cases of application

Person as object

Numerous surveillance/monitoring mechanisms used by private companies, group of individuals, state actors

Person as object

Human surveillance vs. advanced digital technologies surveillance

Both scenario affect potentially individual freedom – but only smart camera scenario affects digital integrity => further threats: database, automatized treatment of information, matching of information, small-scale surveillance

Discussion

Many thanks

www.ethix.ch

rochel@ethix.ch

SAVE THE DATE

- Preliminary date for the next Data Protection Conference has been set to Thursday 23 March 2023.
- Please give us your feedback on the conference by filling out the survey.

www.cit-rail.org