International Rail Transport Committee
Comité international des transports ferroviaires
Internationales Eisenbahntransportkomitee

General Secretariat
Secrétariat général
Generalsekretariat

Weltpoststrasse 20
CH-3015 Bern
T. +41 (0)31 350 01 90
F. +41 (0)31 350 01 99
info(at)cit-rail.org
www.cit-rail.org

- [X] Minutes / Protocole / Protokoll
- [ ] Resolutions / Protocole décisions / Beschlussprotokoll
- [ ] File note / Notice / Aktenvermerk
- [ ] Report / Rapport / Rapport

Original EN

Place, Date, Time of meeting / Lieu, date, heure / Ort, Datum, Zeit	Approved / Visa / Visum SDO	Date of this document / Etabli le / Erstellt am
Bern, 17 and 18 June 2020	Ref. F41a0	2020-06-18

Participants / Participants /Teilnehmer	
CFL	Charpentier Amandine
Eurostar	Marler Francesca
	Naylor Stephanie
LDZ	Klintaja Jana
LTG Link	Gintalas Andrius
MÁV-Start	Csenge Bujdoso
	Istvan Koos
NS	Kruize Gonnie
ÖBB	Leiter Martin
PKP Intercity	Beta Andrzej
	Klubiński Andrzej
Renfe	De Lucas De Rose Fernando
SNCB	Jonas Bianca
	Collard Ysaline
SNCF	Babaud Bettina
	Kalfoun Eliott
	Lebeze Noor
SJ	Carlsson Stefan
SZ	Hribernik Ana
	Kontarček Lucija
	Uršič Marjetka
Thalys	Goossens Gaëtan
	Lambert Anne
Trenitalia	De Girolamo Isabella
	Tiglie Laura
UZ	Biloshytskyi Sergii
	Morozov Vladlen
CIT	Dobler Sandra (minutes)
Sent apologies:	

Circulation / Distributeur / Verteiler

Participants

Trapazzo Enrico, Trenitalia (Chair of the CIV Committee)
Saintilan Isabelle, SNCF (Vice-Chair of the CIV Committee)

Other members of the CIV Committee

Members of the Group of PRR Experts

Vittorio Carta, DB (UIC PSG)
Luca Mariorenzi, Trenitalia, (UIC PES)
Olivier Roy, SNCF (UIC PATRIC)
David Hiscock, Eurostar/RMC (UIC RCF1)
Jabroer Petra, GIE Eurail
Hagdorn Adriaan, NS (Chair of the CUI Committee)
Marc Guigon, UIC

Subject / Thème / Thema

1st Data Protection Expert Meeting

Narrative / Texte / Text	Action by / Traité par / Bearbeitet durch
Working documents	
The Working Documents and the Appendices were sent on 3 June 2020.	These documents are available on the CIT website.
Participants confirmed that they took note and accepted the CIT Competition Law Guidelines, during their whole attendance at the CIT.	
ITEM 1 Implementation of the GDPR	
1.2 COVID-19 and GDPR In Italy, they had to take several measures due to COVID-19, which were stemming from decisions of the State:	

- the use of thermo-scanners to measure the temperature of the passengers
- the check of passengers, done by Trenitalia, under decision of the authorities
- the reimbursement through bonus
- the creation of name tickets

In Italy, they don't record the temperature, they just check it. If an employee is sick, he informs Trenitalia and the authority; the authority then tracks the person and sees with whom the employee had contacts.

In France, SNCF had to verify that passengers were allowed to travel (there were indeed peak hours, where passengers could travel only with an authorisation). If the passenger was not allowed, SNCF could disembark him. In Italy, it is the police that could disembark a passenger.

In the Netherlands, they need to wear a face mask in the train. NS launched a pilot to ask for the names but also destination of each passenger, but they don't have name tickets. Regarding employees, the Dutch authority said that companies are prohibited to measure the temperature of employees, but the latter can measure by themselves their temperature and then inform the company doctor. If an employee is sick, in the Netherlands, it is not possible to indicate the reason of the illness to the employer, just to the company doctor.

In Belgium, the authorities have the same position as in the Netherlands. People also have to wear a mask in public transport and respect social distancing. For the control on the train, the train controller does not need to compost the ticket anymore (it is not mandatory anymore). SNCB is not aware of what would happen if a passenger is not wearing a mask; he might be disembarked. For body temperature, the Belgium authority is quite strict about the possibility to store the data, stating that there needs to be a legal basis to do so normally (in principle, those data should not be stored, or just in case of positive results). The problem is more about the recording and not the collecting. In Belgium, there is no obligation to take the temperature, but the companies do it for employees.

In Latvia, LDZ does not take care of checking the passengers and does not measure their temperature; LDZ has only to inform passengers to be careful and responsible (by going to the doctor, respecting social distance). For now, there is no international traffic in Latvia. If an employee is ill, he must go to the doctor and he has to inform his employer. In Latvia, they have a mobile application about COVID-19.

In Austria, the employers are informed by the authorities, if an employee is sick. And then the employers need to take all the appropriate measures (like informing other employees if necessary, for example). ÖBB is then storing those data for proof reasons. For temperature, ÖBB does not check temperature of customers or employees.

As regards the proposal of guidelines of the CIT GS on the impact of COVID-19 in relation to data protection, the Experts made the following remarks:

- Under point 1.1, It was asked to indicate that in some countries health related data have to be provided by employees to the company doctor and not the employer.
- Under point 1.2, Trenitalia checked the content and made some modifications in it.
- The Experts shared the opinion that it was not necessary to speak about location data in the guidelines.

It was decided that the CIT GS would make those modifications and send the modified version to the participants of the meeting before sending it to all CIT members' representatives. The CIT GS received feedback from the participants. The final version of the guidelines is enclosed (**Appendix 1**). It will now be sent to all the members of the CIT.

1.3 Courts' judgments and authorities' decisions based on GDPR

1.3.1 Facebook Ireland and Schrems, CJUE C-311/18

NB: On 16 July 2020, the ECJ rendered its judgment in the Schrems Case II. It stated that the GDPR was applicable "*to the transfer of personal data for commercial purposes by an economic operator established in a Member State to another economic operator established in a third country, irrespective of whether, at the time of that transfer or thereafter, that data is liable to be processed by the authorities of the third country in question for the purposes of public security, defence and State security*".

"*Article 46(1) and Article 46(2)(c) of Regulation 2016/679 must be interpreted as meaning that the appropriate safeguards, enforceable rights and effective legal remedies required by those provisions must ensure that data subjects whose personal data are transferred to a third country pursuant to standard data protection clauses are afforded a level of protection essentially equivalent to that guaranteed within the European Union by that regulation, read in the light of the Charter of Fundamental Rights of the European Union. To that end, the assessment of the level of protection afforded in the context of such a transfer must, in particular, take into consideration both the contractual clauses agreed between the controller or processor established in the European Union and the recipient of the transfer established in the third country concerned and, as regards any access by the public authorities of that third country to the personal data transferred, the relevant aspects of the legal system of that third country, in particular those set out, in a non-exhaustive manner, in Article 45(2) of that regulation. Article 58(2)(f) and (j) of Regulation 2016/679 must be interpreted as meaning that, unless there is a valid European Commission adequacy decision, the competent supervisory authority is required to suspend or prohibit a transfer of data to a third country pursuant to standard data protection clauses adopted by the Commission, if, in the view of that supervisory authority and in the light of all the circumstances of that transfer, those clauses are not or cannot be complied with in that third country and the protection of the data transferred that is required by EU law, in particular by Articles 45 and 46 of that regulation and by the Charter of Fundamental Rights, cannot be ensured by other means, where the controller or a processor has not itself suspended or put an end to the transfer*".

It declared that: "*Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield is invalid*". Indeed, it considered that the limitations on the protection of personal data arising from the US domestic law on the access and use by US public authorities was not circumscribed to what is strictly necessary. Moreover, those provisions did not grant data subjects actionable rights before the Courts against the US authorities. Even if the Decision foresaw an Ombudsperson mechanism, the latter did not provide data subjects with any cause of action before a body which offers guarantees substantially equivalent to those required by EU law, such as to ensure both the independence of the Ombudsperson provided for by that mechanism and the existence of rules empowering the Ombudsperson to adopt decisions that are binding on the US intelligence services.

Now that the US do not benefit from an adequacy decision anymore, companies will have to rely on alternative data transfer mechanism to process personal data with that country.

1.3.2 SNCF Mobilités – Legitimate Interest

SNCF Mobilités has a product called "TGV Max" that allows passengers to take the TGV on an almost unlimited basis. After the strikes of 2018 in France, a passenger complained that he was unable to take the TGV according to his wishes because of the strike and asked for a financial compensation. However, when looking closer at the TGVs the passenger said he could not board, SNCF discovered that most of the TGVs the passenger allegedly wanted to use were a priori excluded from the TGV Max (according to the special Terms and Conditions of the product). Therefore, the strike itself did not prevent him from using the trains but the terms and conditions of TGV Max did.

SNCF Mobilités produced as proof the listing of the reservations of the passenger during the period of the strike. The passenger claimed that this was a violation of GDPR, as he did not consent to such use of his data.

The French Tribunal d'instance considered that there was a legitimate interest for SNCF Mobilités to produce this proof before the Court.

There is no appeal possible against this judgement (only a pourvoi en cassation).

1.4 Questions from members

1.4.1 CFL – Storage time of CCTV footages

CFL asked, which national law to apply for the storage of CCTV footages, in case of trains travelling in different countries.

In Austria, CCTV footages can be stored during only 72 to 120 hours. But for security reasons, it might be necessary to store them for several days. ÖBB stated that for carriers having trains travelling in different countries, this makes the situation complicated.

Thalys has the same issue as CFL. It applies the law of the data controller; since Thalys processes the data in Belgium, it applies Belgium law, under the principle of the one-stop-shop, because it would be the Belgium data protection authority competent for Thalys.

ÖBB shared the same opinion as Thalys, but this logic might not be followed in all countries (like in Germany and in Hungary).

For SNCB, it is the location law as first indicator, which should be applicable.

CFL mentioned that the data for CCTV in the trains is stored on the train. There is no backup of the images, the CCTV images are only stored in the train. When a train travels in several countries, it needs to comply with the rules of the country where it is.

The Data Protection Experts came therefore to the conclusion that CFL should apply the rule of the country where the train is and obey by the rules of that country.

LDZ asked how the information about the filming was provided to the passenger. CFL has a pictogram for that in the train and there is also a notice on the CFL website. For clients, when they buy a ticket, there is also a specific notice in the ticket office.

ÖBB mentioned that some guidelines exist on the information to provide to the passengers in relation to CCTV. Those guidelines can be found under (links in German):

https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/OHVideoueberwachungInOEPNV.html

https://www.datenschutz.rlp.de/de/themenfelder-themen/videoueberwachung/videoueberwachung-in-oeffentlichen-verkehrsmitteln/

Under the second link, on the right side, some examples of pictograms used in Germany are displayed.

1.4.2 CFL – Storage time of psychological records

CFL asked for how long other companies were storing psychological records of candidates and former employers.

CFL keeps it indeed for several years, especially in cases of employees candidating several times.

In the Netherlands, the law states that companies can store information of candidates only for four weeks (after the application period has ended), except if the candidate has given consent for the information to be kept longer. But this rule does not apply to the doctor, who makes the test; the doctor can keep the data for a longer period.

In Belgium, they have no law on that aspect. Therefore, they store all the data for the period during which the candidate can open action against SNCB. SNCB raised the issue if such data can still be considered as valid after several years.

In Latvia, they keep those data only for one year; for longer periods, people need to provide their consent.

1.4.3 LG – Use of biometrics (face recognition) of employees for sobriety tests at work

LDZ uses fingerprints data to enter the office building; this is based on an agreement between employees and employers.

For biometrics, ÖBB explained that consent is not the right legal basis. Tests of sobriety are allowed in Austria, but not on all employees but just for the ones for security reasons.

NS said that face recognition permits to verify that it is the right person taking the test. In the Netherlands, they don't use face recognition for sobriety. The law only permits them to test the sobriety of drivers.

LDZ asked about alcohol tests of employees, because by law, LDZ has to test them every day. In the Netherlands, there is no obligation by law to test everyday, only if there is a suspicion and on a regular basis not every day.

1.4.4 Eurostar – Transfer of personal data to UK (post-Brexit)

Eurostar was initially very concerned by Brexit and the potential impact to EU data flows; however, for the most part these fears have been alleviated.

They hope to see an adequacy decision granted to the UK swiftly, but overall Eurostar does not think that Brexit will have a consequence on data flows. As Eurostar for the most part is a data controller, they don't foresee any major issues with restricted transfers although some renegotiation of terms to include SCCs has been necessary.

Indeed, the UK will certainly continue to comply with GDPR, which is written into the EU withdrawal bill. In any case as international company, Eurostar will still need to apply the GDPR, since GDPR applies to EU citizens and this makes up a significant portion of Eurostar's passenger base.

Concerning the role of supervisory authority, post Brexit Eurostar shall be governed by the ICO for UK activities and the CNIL for Europe.

Thalys said that there might not be too much doubt for UK to get an adequacy decision.

ITEM 2 Convention 108+

2.3 Relation with GDPR

The CIT GS explained the content of the Convention 108+ and the fact that its aim was to better take into account new technologies, considering that the situation evolved since 1981 when the Convention 108 was concluded.

This raises issues for third countries, which are not part of that Convention.

ITEM 3 E-Privacy Regulation

3.1 Content

The CIT GS mentioned that this proposal concerns all data transferred via electronic means.

It explained that one of the problematic points of discussions at Council level was the numerous obligations concerning the information to be supplied to users for web browsers and other electronic communications software suppliers.

ITEM 4 PNR Directive and API Council Directive

4.1 PNR Directive (EU) 2016/681

The CIT GS mentioned that the aim of the PNR Directive is to fight against terrorism.

The Data Protection Experts discussed the Belgian Royal Decree, whose aim is to introduce PNR for buses and trains. This decree contains some rules about conformity checks. Eurostar had concerns about the liability for conformity checks, with those thresholds after 48 hours, 24 hours, etc. where the carriers have to send the data relating

to their passengers to the Passenger Information Unit (PIU, in charge of the database set up for the collection of PNR data). In Belgium though, there is still no government in place. Therefore, as long as there won't be a government, this Royal Decree will not be applicable. Things will certainly not move before a year. Eurostar launched a pilot project to see how to implement this Royal decree in the railway sector, but for now, there is no push to move this project forward. Projects are on stand-by as long as there is no certainty on when this Decree will be applicable. Eurostar had discussions with the Belgian PIU. The British government is also following closely this proposal of Royal Decree. With the United Kingdom leaving the EU, Eurostar will be directly impacted by this new regulation. SNCB will report if there are any development regarding the application of the Royal Decree.	SNCB
4.4 ECJ Case and compliance with ECHR and Charter of Fundamental Rights of the European Union 4.4.1 Belgium Case on the compatibility of PNR and API Directive to the right to privacy and the protection of personal data SNCB will report on the outcome of that case, when a judgment will be rendered.	SNCB
ITEM 5 California Consumer Privacy Act	
5.3 Possible impact on the railway sector Eurostar has data from American citizens, so before 1 January 2020, Eurostar did its best to comply with the CCPA. GDPR is stricter than CCPA for Eurostar. CCPA is for Eurostar dealing with financial aspects of sales of personal data. Eurostar changed its data protection policy to be in line with the CCPA. Under the 'Sharing your data' section of its privacy policy, it simply added "*We do not sell your personal data to anyone*": https://www.eurostar.com/uk-en/privacy-policy	
ITEM 6 Revision of the Manual on Data Protection	
6.1 New Commentaries of Articles The Data Protection Experts agreed on the modifications proposed. They also agreed that the CIT GS would integrate the guidelines on the impact of COVID-19 in relation to data protection in the body of the MDP, in the commented part. The final draft of the revised MDP (**Appendix 2**) has now been sent to translation in French and German. On 25 September 2020, it will be presented to the CIV Committee for adoption. If adopted, it should be published on the CIT website on 13 December 2020.	CIV Committee, CIT GS
6.2 Balance of legitimate interests' procedure The Data Protection Experts agreed that this would be a useful topic to add in the MDP. The Dutch authority published some guidelines on the way to interpret legitimate interest. Since those guidelines are only in Dutch, NS will make a summary of them in English. The Data Protection Experts are asked to provide to the CIT GS **until 5 September 2020** feedback on the way they interpret the notion of "legitimate interest" and if they are aware of guidelines published by their national authorities on that aspect. The CIT GS will then draft a proposal of text for the next revision of the MDP. It will base its work also on the guidelines published by the EDPB and the Art29 WG on that aspect: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf	NS Data Protection Experts

6.3 Transfer to third countries of data – Possible standardised solution The CIT GS explained that several CIT members were confronted to the problematic of transfer of personal data to third countries. Therefore, the CIT GS shared the opinion that the CIT should develop a common solution for its members. It had three possibilities in mind: - Standard contractual clauses: This would nevertheless not guarantee that the authorities in the third country would take into account those clauses. - Certification: The CIT would need an accreditation for that. - Code of conduct: The CIT GS shared the opinion that this would be the best option. The Data Protection Experts agreed that the Code of conduct would be the best solution. The redaction of a Code of conduct would nevertheless imply an important work. The CIT GS proposed therefore to build a special Task Force with some Data Protection Experts. The CIT GS explained that it would help if the Task Force could have an example of code of conduct, to start its work. The Data Protection Experts are therefore asked to inform the CIT GS **until 5 September 2020** if they wish to join this specific Task force. Moreover, they are also asked to provide to the CIT GS **until 5 September 2020** any information or examples they could have on drafting a Code of conduct.	Data Protection Experts
6.4 Data Protection and new technologies? The Data Protection Experts agreed that there was no need to develop a specific Chapter in the MDP on new technologies. Further information on that topic will simply be integrated in the respective chapters of the MDP. NS will also send to the CIT GS a list of their current projects in relation to new technologies.	NS
6.5 Next steps of the revision 6.5.1 Age of consent of children (art. 8 GDPR) The Data Protection Experts agreed on having a list with the age of consent of children in relation to information society services in the different countries. The Experts already provided some information on that: - In the Netherlands, children need to be 16 years old - In Belgium, 13 years old - In Italy, 14 years old - In the United Kingdom, 13 years old - In Latvia, 13 years old - In France, 15 years old SNCB sent a link to the website of the European Union Agency for Fundamental Rights, which published a list of those different ages: https://fra.europa.eu/en/publication/2017/mapping-minimum-age-requirements/use-consent#:~:text=According%20to%20Article%208%20of,age%2C%20not%20below%2013%20years. The CIT GS will base its work on that and integrate such a list in the MDP under Art. 8 GDPR. 6.5.2 Fining policy related to GDPR (art. 83 GDPR) The Data Protection Experts shared the opinion that it was unpredictable, to have guidelines on the fining, which might be imposed by the authorities, since this differs from one country to the other. SNCB mentioned the following website, where it is possible to see all the fines that have been imposed in the different countries: https://www.enforcementtracker.com/ ÖBB sent also a link to the German "Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder", which published guidelines for setting fines (link in German): https://www.datenschutzkonferenz-online.de/media/ah/20191016_bu%C3%9Fgeldkonzept.pdf Such information might be added in the MDP, but the CIT GS won't develop by itself guidelines on that respect, but just include reference to what is being done in the different countries.	

ITEM 7 Next meeting and Data Protection Workshop

7.1 Data Protection Experts meeting

The next Data Protection Experts meeting will take place on 24 March 2021 from 10.00 AM to 6.00 PM in Warsaw, at the kind invitation of PKP Intercity.

The CIT GS mentioned that for now, the Data Protection Experts Group did not have an official Chair. The role of the Chair is to approve the invitation, the working documents and the minutes before they are sent to all the members. The Chair also presides the meetings. He is also the one who has a certain right of review over the subjects to be discussed in the plenum and can propose particular subjects.

All representatives interested in holding the position of Chair of the Data Protection Experts Group are asked to send their CV and a motivation letter **until 5 September 2020**.

Data Protection Experts

7.2 Data Protection Conference

The Data Protection Experts agreed to organise a Conference next year on data protection. It will take place on 25 March 2021 from 9.00 AM to 5.00 PM in Warsaw, at the kind invitation of PKP Intercity.

The subject of the Conference will be "*Transport of passengers from a data protection perspective*".

This provides much liberty for the potential speakers to choose the subject they would like to tackle during the Conference.

The Data Protection Experts are kindly asked to liaise with the CIT GS **until 5 September 2020** if they wish to hold a presentation during the conference and if this should be the case, to mention on what thematic they would like to hold this presentation.

Data Protection Experts

The CIT GS will then prepare the programme of the conference accordingly.

ITEM 8 Calendar 2020-2021

15 September	UIC Door-to-Door Group	Brussels
16-17 September	UIC Air-Rail Group	Brussels
17 September	CER PWG	Brussels
18 September	CER CLG	Brussels
24September	Claims Department Conference	Bern
25 September	CIV Committee	Bern
15 October	UIC Air-Rail Group	Paris
21-22 October	CIV/SMPS Meeting	Bern
17-18 November	50th CIV Working Group	Bern
19 November	CIT General Assembly	Bern
23-24 February	51st CIV Working Group	Bern
24 March	**2nd Data Protection Experts Meeting**	**Warsaw**
25 March	**Data Protection Conference**	**Warsaw**
25-26 May	52nd CIV Working Group	Prague
22 September	Claims Department Conference	n/a
23 September	CIV Committee	n/a
18-19 November	53rd CIV Working Group	Bern
20 November	CIT General Assembly	Bern