International Rail Transport Committee
Comité international des transports ferroviaires
Internationales Eisenbahntransportkomitee

Ref. F41a03
2020-06-03

Original: EN

# 1st meeting of the Data Protection Experts Videoconference, 17-18 June 2020

# Working document

**Agenda:**

1 Implementation of the GDPR ..... 2
2 Convention 108+ ..... 5
3 E-Privacy Regulation ..... 7
4 PNR Directive and API Council Directive ..... 8
5 California Consumer Privacy Act ..... 11
6 Revision of the Manual on Data Protection ..... 13
7 Next meeting and Data Protection Workshop ..... 15
8 Calendar 2020 ..... 16

**Appendices to the working document are available here.**

**ITEM 1**

**Implementation of the GDPR**

# 1 Implementation of the GDPR

## 1.1 Two years application of GDPR

It makes two years now that the GDPR is applicable.

The EU Commission will now review this year the implementation of the GDPR.

The European Commission already issued a report on that aspect last year. In this report, it underlined the success of the GDPR in harmonising data protection rules at EU level. It mentioned though that some countries were adopting diverging regulations, what might be detrimental to a uniform application of the GDPR (for example Germany's stricter requirements for data protection officers) or some had not yet adopted a national legislation based on GDPR (Greece, Portugal and Slovenia). It also pointed out the need for a better cooperation between supervisory authorities and a better alignment with the work of the European Data Protection Board (EDPB). The EU Commission also pointed out the greater awareness in the public of their privacy rights under the GDPR and a willingness to exercise them. It welcomed the fact that non-EU countries are also developing data protection regulations, which echo the content of the GPDR (Brazil and India for example).

The EDPB also published this year a contribution to the evaluation of the GDPR. It took a positive view of the implementation of the GDPR in its contributions and is of the opinion that it is premature to revise the legislative text at this point in time. It underlined though that supervisory authorities need more resources to carry out their duties under the GDPR. The EDPB is in favour of intensifying the efforts to adopt the ePrivacy Regulation.

The Data Protection Experts are asked to provide feedback **during the meeting** on issues they might have faced while implementing the GDPR and the possible areas where CIT could support them in their work.

## 1.2 COVID-19 and GDPR

COVID-19 raised different issues in relation to data protection, since in many countries, to fight against COVID-19, many personal data (health data, location data, etc.) have been processed.

The EDPB released therefore a Statement on the processing of personal data in the context of the COVID-19 outbreak.

It mentions in this document some statements about the lawfulness of processing (in particular health data and location data), also in relation with employees.

The national data protection authorities of different countries have also published guidance and information on that matter: https://globalprivacyassembly.org/covid19/

For its part, the CIT GS was asked to make a presentation on data protection and COVID-19 during the UIC Task Force meeting on COVID-19 (see **Appendix 1** enclosed). The CIT GS treated the question of the processing of personal and sensitive data (concerning health data in particular) by railway undertakings. It came to the conclusion that this was authorised, if justified by a legal obligation or by public interest for health, but that it should be limited to what was strictly necessary.

The CIT GS suggests publishing guidelines on that matter, regarding the number of questions this issue raised. A first draft of such guidelines is enclosed to the Working Document (see **Appendix 2**). The Experts are asked to provide their feedback on this draft **during the meeting**.

If the Data Protection Experts agree with the content of those guidelines, the CIT GS suggests to first send them as a circular letter to the CIT members and second to integrate their content in the revised MDP. The Data Protection Experts are asked for their opinion on that proceeding.

## 1.3 Courts' judgments and authorities' decisions based on GDPR

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

This case follows the judgment Schrems I, where the ECJ declared that the safe harbour decision was invalid. Mr Schrems had indeed complained because Facebook Ireland was sending personal data of its users to Facebook Inc. in the USA. Mr Schrems shared the opinion that the United States did not offer sufficient protection against surveillance, by the public authorities, of the data transferred to that country.

This second Schrems case is about the validity of Commission Decision 2010/87 of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council.

For now, only the conclusions of the Advocate General have been released. He stated that this decision was valid, in particular, "*the fact that that decision and the standard contractual clauses which it sets out are not binding on the authorities of the third country of destination and therefore do not prevent them from imposing obligations that are contrary to the requirements of those clauses on the importer does not in itself render that decision invalid. The compatibility of Decision 2010/87 with the Charter depends on whether there are sufficiently sound mechanisms to ensure that transfers based on the standard contractual clauses are suspended or prohibited where those clauses are breached or impossible to honour. In his view, that is the case in so far as there is an obligation — placed on the data controllers and, where the latter fail to act, on the supervisory authorities — to suspend or prohibit a transfer when, because of a conflict between the obligations arising under the standard clauses and those imposed by the law of the third country of destination, those clauses cannot be complied with*". He also analysed the validity of the Privacy Shield and questioned it in the light of the right to respect for private life and the right to an effective remedy.

It is now necessary to wait for the judgment of the ECJ.

## 1.4 Questions from members

### 1.4.1 CFL – Storage time of CCTV footages

For video surveillance in trains, the Luxembourger supervisory authority imposes a retention period of 30 days maximum. However, Luxembourg being a border country, CFL trains travel to Germany, Belgium and France.

The conservation rules in these countries differ from the ones in Luxembourg, namely that in Belgium the images can be kept for up to three months while in France, companies cannot go beyond 30 days and in Germany, the judges tolerate a delay of 10 days maximum.

The question that arises is what rules apply for trains traveling in Germany. Can CFL apply "its" rules, namely to keep the images for a period of 30 days for example or does CFL have to respect the retention periods imposed by Germany?

### 1.4.2 CFL – Storage time of psychological records

CFL asked the CIT GS what are the periods of conservation of psychological files of candidates and former employees. There are no regulations in Luxembourg or in neighbouring countries which imposes retention periods for psychological files that are held on candidates or former employees.

Similarly, CFL is not aware in Luxembourg and in neighbouring countries, of recommendations as to these time limits.

CFL wanted therefore to know if other companies were also facing such issues and how they solved it.

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

When carrying out a data protection impact assessment, LG faced the problem that they did not have any valid legal ground for such processing at work when biometric data is processed for security purposes (for e.g., performing sobriety tests for those working with dangerous machines. Those people work night shifts and on weekends and there might not be a person to check on employee sobriety every time).

In general, such processing of biometric data is prohibited, unless one of the derogations provided for under Article 9 of the GDPR or the national law implementing the GDPR applies.

There are two derogations that could be applicable to LG to legitimize the processing of biometric data: (1) explicit consent (Article 9(2)(a) of the GDPR) and (2) the necessity of the processing for carrying out the obligations of the controller or in the field of employment and social security and social protection law in so far as it is authorised by Union or national law or a collective agreement.

In LG's opinion, consent is not valid because generally consents of employees are not considered as "freely given".

As for the second basis, neither EU, nor Lithuanian national law does introduce any national exception on the basis of Article 9(2)(b) for processing biometric data. Therefore, LG decided to initiate changes of collective agreements providing for appropriate safeguards for the fundamental rights and the interests of employees.

LG would like to know the opinion of the other experts on that matter.

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

The UK decided to leave the European Union, by a public vote which took place in June 2016.

This decision raised many issues as regards the regulation, which would then be applied post-Brexit.

Negotiations are still ongoing in that respect between the EU and the UK.

One of the questions, which was risen, is the transfer of personal data to UK in the post-Brexit time.

Eurostar will explain during the meeting its approach to Brexit, on that aspect.

Other railway undertakings are welcome to explain if they are impacted by Brexit and how they will deal with transfer of personal data to UK.

1.4.5 UIC – Health data and other personal data collection in time of COVID-19

During the UIC Task Force on COVID-19, the CIT GS was led to discuss the processing of health data and other personal data collection.

This concerns the measurement of the temperature of employees and passengers, but also the obligation for the carrier to check in some countries the right to travel of the passengers.

The CIT GS would be interested to know what are the practices in place by the different railway undertakings.

**Proposed resolutions**:

The Experts Group:

- takes note of the report;
- as regards Point 1.1, the Experts share the opinion that the CIT GS should work on:
- regarding Point 1.2, the Experts provide the following feedback on the draft of guidelines related to COVID-19:
- concerning Point 1.4, the Experts advise to:
- …

**ITEM 2**

**Convention 108+**

## 2 Convention 108+

### 2.1 Background

The Protocol (CETS No. 223) amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) was adopted on 18 May 2018.

It is open for signature since 25 June 2018.

The aim of the reform was to better address challenges resulting from the use of new information and communication technologies, and on the other hand to strengthen the implementation of Convention 108.

### 2.2 Content

The main modifications arising from this modernisation concern the following points:

- Definitions: The concept of “file” is not used anymore. The Convention speaks now of “data controller”, “processor” and “recipient”.
- Scope: It applies to automated and non-automated processing of personal data in the private and public sectors. It does not apply anymore to data processing carried out by a natural person for the exercise of purely personal or household activities. Parties have no longer the possibility to make declarations to exclude the application of the Convention to certain types of data processing.
- Duties of parties: They have to adopt in their domestic law the measures necessary to give effect to the provisions of the Convention and have to accept that the Convention Committee checks that. International organisations (like the EU) can access the Convention.
- Proportionality and legal basis: The principle of proportionality is clarified to apply throughout the entire processing and is reinforced by the principle of data minimisation. The legal basis to process personal data are also clarified.
- Sensitive data: It includes now also genetic and biometric data, as well as data processed for the information they reveal relating to trade-union membership or ethnic origin.
- Data security: An obligation to notify without delay any security breaches is introduced, limited though to cases which may seriously interfere with the rights and fundamental freedoms of data subjects, which should be notified, at least, to the supervisory authorities.
- Transparency of processing: The data controllers have to provide a required set of information to that purpose, except if the processing is expressly prescribed by law or if it is impossible or involves disproportionate efforts.
- Rights of the data subject: The data subject is entitled to obtain knowledge of the reasoning underlying the data processing. Another new right is the right not to be subject to a decision which affects the data subject which is based solely on an automated processing, without the data subject having his views taken into consideration. Data subjects have the right to object at any time to their personal data being processed, unless the controller demonstrates compelling legitimate grounds for the processing which override their interests or rights and fundamental freedoms.
- Additional obligations: Accountability gains in importance, with the obligation for the controllers to be able to demonstrate compliance with the data protection rules. Controllers should take all appropriate measures (including when the processing is outsourced) to ensure that the right to data protection is ensured (privacy by design, privacy impact assessment, privacy by defaults).
- Exceptions and restrictions: The rights laid down in the Convention can be limited through new grounds, essential objectives of public interest and a reference to the right

to freedom of expression. The list of provisions of the Convention that can be restricted has been slightly extended.

- Supervisory authorities: The authorities also have now a duty to raise awareness, provide information and educate all players involved (data subjects, controllers, processors, etc). They can also take decisions and impose sanctions.
- Forms of cooperation: The supervisory authorities have to coordinate their investigations, to conduct joint actions and to provide to each other information and documentation on their law and administrative practices relating to data protection. The information exchanged between the supervisory authorities will include personal data only where such data are essential for cooperation or where the data subject has given the specific, free and informed consent. The supervisory authorities also have to form a network in order to organise their cooperation and to perform their duties.
- Convention Committee: It has not only a consultative role anymore, but also has assessment and monitoring powers.

### 2.3 Relation with GDPR

The Convention contains a new disposition, whose aim is to facilitate, where applicable, the free flow of information regardless of frontiers, while ensuring an appropriate protection for individuals with regard to the processing of personal data.

Data flows between Parties cannot be prohibited or subject to special authorisation as all of them, having subscribed to the common core of data protection provisions set out in the Convention offer a level of protection considered appropriate, except if there is a real and serious risk that such transfer would lead to circumventing the provisions of the Convention.

One other exception is the existence of harmonised rules of protection shared by States belonging to a regional international organisation and governing data flows like this is the case in the European Union with the GDPR.

In the procedure for providing an adequacy decision, it will be taken into account if the country in question is part of the Convention 108+.

The Data Protection Experts are asked for their opinion on the significance of this modernisation of Convention 108+.

### 2.4 Impact on non-EU countries

Regarding transborder flows of data to a recipient that is not subject to the jurisdiction of a Party, an appropriate level of protection in the recipient State or organisation is to be guaranteed. To ensure that, the Convention establishes two main means, either by law or by ad hoc or approved standardised safeguards that are legally binding and enforceable (notably contractual clauses or binding corporate rules) and implemented.

**Proposed resolutions**:

The Experts Group:

- takes note of the report;
- as regards Point 2.3, the Experts consider:
- …

**ITEM 3**

**E-Privacy Regulation**

# 3 E-Privacy Regulation

## 3.1 Content

The European Commission has proposed a Regulation on Privacy and Electronic Communications, which should in particular impose new obligations when using cookies on web sites. This will therefore have an impact for carriers' websites. The proposed Regulation focuses on ensuring the privacy and security of all data transferred via electronic means. The subject matter of the Regulation is thus much wider than GDPR. It will govern all 'electronic communications data' which encompasses any information concerning the content transmitted and information exchanged for the purpose of transmitting, distributing or enabling the exchange of electronic communications content, including geographical location data and electronic communications metadata.

What is particularly of concern to the Member States is the fact that the proposal imposes numerous obligations concerning the information to be supplied to users for web browsers and other electronic communications software suppliers. Numerous discussions have also taken place on the question of conditional access to website content and the need to put an end to commercial models, such as online services financed by advertising, while respecting the relevant provisions of GDPR. Another point of disagreement concerned the co-operation of national regulators and the role of the European Data Protection Board.

## 3.2 Progress in its adoption

The e-Privacy regulation should replace the Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). Initially, it should have been applicable at the same time than the GDPR. The first draft was adopted by the EU Parliament in October 2017.

On 22 November 2019, the representatives of the Council rejected the Finnish Presidency on the ePrivacy Regulation.

The Croatian Presidency has proposed a new version of the text, which still need to be discussed. The latest Council Presidency text introduces the possibility to invoke the legal basis of "legitimate interests", similar to those in the GDPR, in storing or processing the users' data. However, strict conditions are attached to it, including the obligation to carry out a prior data protection impact assessment, to implement appropriate security measures and to inform the user in advance - who may at any time object. Moreover, the legal basis of "legitimate interests" may in no way be used in certain cases: when the user is a child, for profiling, and when sensitive data are involved.

The CT GS is not aware of a decision taken on that text by the Council. The Data Protection Experts are asked to inform the CIT GS **during the meeting**, if they have updates on that matter.

**Proposed resolutions**:

The Experts Group:

- takes note of the report;
- as regards Point 3.2, the Experts provide the following feedback:
- …

**ITEM 4**

**PNR Directive and API Council Directive**

# 4 PNR Directive and API Council Directive

## 4.1 PNR Directive (EU) 2016/681

The Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 concerns the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. In a Passenger Name Record (PNR), all data and processes relating to a flight booking (personal data, including the date of birth, the names of accompanying persons, the means of payment used to purchase the flight ticket and an unspecified text field which the airline fills in independently) are recorded electronically and stored for a certain period of time even after the end of the flight in the respective computer reservation systems.

So far, this directive is only applicable in air transport. However, EU Member States are free to adopt national legislation that is stricter than EU law, for example:

- In Belgium, a Royal Decree has been prepared to introduce compulsory PNR for buses and trains. A case is already pending though before the Belgian Constitutional Court, where the latter, by judgment of 17 October 2019, has asked several questions to the ECJ on the compatibility of this Belgian PNR legislation with European law (in particular regarding the right to privacy and the protection of personal data), see Item 4.5.1;
- Italy already has existing national rules on cooperation between the Italian authorities and the Italian air carriers.

Other countries are also discussing similar legal acts.

Under the Finnish Presidency, the first talks on the possible extension of the PNR Directive to other modes of transport, including railways, took place last Summer.

## 4.2 API Council Directive 2004/82/EC

The Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data is being evaluated by the Commission.

The aim of this Directive is to improve border controls and combating illegal immigration by the transmission of advance passenger data by carriers to the competent national authorities. It is limited to air traffic though but the evaluation study is also analysing the possibility to expand the Directive to other transport modes. The public consultation ended at the end of last year.

## 4.3 Possible extension to rail traffic

The sector is lobbying to show that such an extension of the PNR and API Directives to the railway sector would be detrimental to the latter. Indeed, the railway sector, unlike the airline sector, is completely open and based on the idea of turn-up-and-go. The aviation is a point-to-point service, whereas the railway service serves several stations. All the measures and the security processes needed to implement the PNR and API Directives would also lead to an increase of the costs and the price of the services.

The CIT GS is following the discussions on that matter and supporting the CER in its lobbying.

The Data Protection Experts are asked to provide feedback on those matters, if they have some.

## 4.4 ECJ Case and compliance with ECHR and Charter of Fundamental Rights of the European Union

### 4.5.1 Belgium Case on the compatibility of PNR and API Directive to the right to privacy and the protection of personal data

This case was brought by the NGO League of Human Right (LDH) in an appeal before the Belgium's Constitutional Court.

The LDH asked for the annulation of the Belgium law, the Passenger Name Record Act (PNR). The LDH is concerned about the fact that the law concerns every passenger, irrespective of any objective proof of any individual being likely to pose a risk to public safety.

As a reminder, this Law was adopted on 25 December 2016 and concerns the treatment of passenger information. A Royal Decree was then also published on 3 February 2017. It establishes an obligation for carriers and travel operators to communicate passenger information. This law mainly aims to transpose the PNR Directive into Belgian legislation.

The collected PNR data are transferred to a Passenger Information Unit (PIU), which is in charge of the database set up for that purpose. The PNR system is applicable in Belgium to air carriers (as determined by the PNR Directive). It was extended to bus and train carriers. The contested Act also transposes the API Directive, which requires air carriers to transfer certain data, inter alia, to combat illegal immigration and to improve border control.

For the railway sector this Decree only relates to high speed trains (HST). It applies to carriers and distributors of HST tickets. They must send to the PIU, the data relating to their passengers, 48 hours and 24 hours before their departure time, and immediately upon closing of the train, and also at the time of the arrival of the train at its final destination, if the data have been modified in the intervening period. If the data are the same at these different times, the operator or the distributor can confine itself to confirming that the data are identical; otherwise, it may simply send the updated data. In the light of specific and real terrorist threats or specific and real threats of serious crime, the unit can ask to receive data at other times too. In addition, carriers must check the identity of the passenger when they get on the train; distributors must perform this check at the time of the sale of the travel document.

This Decree does however present a number of grey areas: the definition of a high speed train, the carrier responsible for carrying out the checks, how the data are transferred to the authorities, etc.

The letter of notification indicating the effective date of application of this Decree has not been released yet. Therefore, this Decree is not yet applicable.

The Belgium Constitutional Court has asked ten prejudicial questions to the ECJ on the following topics:

- Compatibility of the system of the PNR Directive with the right to respect for private life and the protection of personal data, in particular on the following points, the extremely broad and non-exhaustive character of the PNR data, the general and untargeted character of the PNR system, which concerns all passengers without distinction, the systematic prior assessment of the PNR data of all passengers;
- Possibility to process PNR data in the framework of monitoring the activities pursued by intelligence and security services;
- Designation of the PIU as authority that decides on granting access to PNR data in the framework of targeted searches, after a period of six months;
- General retention period of the data of five years, without making a distinction between passengers that could pose a risk for public safety and other passengers;
- Application of Article 23 of the General Data Protection Regulation (GDPR) to the contested law;
- Applicability of the obligations to the API Directive to flights within the European Union, which could indirectly implicate the reintroduction of internal border controls;
- Transitional period of applicability of the contested law, if it is declared that it violates European law.

The case is still pending.

#### 4.5.2 German Case on the compatibility of PNR Directive to the right to the protection of personal data and the right to respect for private and family life

On 20 January 2020, the District Court of Cologne, Germany, submitted to the ECJ the question whether the European Passenger Name Record (PNR) Directive violates fundamental rights.

The case was brought before the District Court of Cologne by the GFF, the German Society for Civil Rights, which have been fighting the PNR Directive.

GFF considered the PNR Directive to violate the right to the protection of personal data and the right to respect for private and family life. The aim was to bring down the PNR Directive by submitting the case to the highest European court. GFF is supporting several individuals that

have filled complaints against the airline Deutsche Lufthansa AG for transferring passenger data to the German Federal Criminal Police Office.

The case is still pending.

4.5.3 PNR Agreement between the EU and Canada, Opinion 1/15 of 26 July 2017 from ECJ

Even if those two abovementioned cases are still pending, the Opinion rendered by the ECJ in 2017 might show in which direction the judgments will go.

In this case, the ECJ had indeed to rule on the compatibility of a draft international agreement with the Charter of Fundamental Rights of the European Union, and, in particular, with provisions relating to respect for private life and the protection of personal data.

The envisaged agreement permitted the systematic and continuous transfer of PNR data of all air passengers to a Canadian authority with a view to those data being used and retained, and possibly transferred subsequently to other authorities and to other non-member countries, for the purpose of combating terrorism and serious transnational crime. To that end, the envisaged agreement, amongst other things, provided for a data storage period of five years and laid down particular requirements in relation to PNR data security and integrity, such as immediate masking of sensitive data, whilst also providing for rights of access to and correction and erasure of data, and for the possibility of administrative and judicial redress.

The PNR data covered by the envisaged agreement included, in particular, besides the name(s) of the air passenger(s) and contact information: information necessary to the reservation, such as the dates of intended travel and the travel itinerary, information relating to tickets, groups of persons checked-in under the same reservation numbers, information relating to the means of payment or billing, information concerning baggage and general remarks regarding the passengers.

The ECJ considered that the PNR agreement could not be concluded in its current form because several of its provisions were incompatible with the fundamental rights recognised by the European Union: the transfer of PNR data constituted interferences with the right guaranteed in Article 7 of the Charter and the fundamental right to the protection of personal data guaranteed in Article 8 of the Charter; the PNR data, taken as a whole, may reveal a complete travel itinerary, travel habits, relationships existing between air passengers and the financial situation of air passengers, their dietary habits or state of health, and may even provide sensitive information about those passengers (information that reveals racial or ethnic origin, political opinions, religious beliefs, etc.); moreover, several provisions of the agreement were not limited to what is strictly necessary and did not lay down clear and precise rules; there was no precise and solid justification for the transfer of sensitive data to Canada; furthermore, the continued storage of the PNR data of all air passengers after their departure from Canada, which the envisaged agreement permits, was not limited to what is strictly necessary (for example for air passengers in respect of whom no risk has been identified as regards terrorism or serious transnational crime on their arrival in Canada and up to their departure from that country);

**Proposed resolutions**:

The Experts Group:

- takes note of the report;
- as regards Point 4.3, the Experts provide the following feedback:
- …

**ITEM 5**

**California Consumer Privacy Act**

## 5 California Consumer Privacy Act

### 5.1 Content

The California Consumer Privacy Act (CCPA) was enacted in 2018 and took effect on 1 January 2020.

It protects Californian residents.

It applies to any business, including any for-profit entity that collects, shares or sells consumers' personal data, which does business in California, and satisfies at least one of the following thresholds:

- Has gross annual revenues in excess of $ 25 millions;
- Buys, receives, or sells the personal information of 50'000 or more consumers, households, or devices;
- Derives 50 percent or more of annual revenues from selling consumers' personal information.

The business does not need to have a physical presence in California (or in the United States) to fall under the CCPA. The latter does not cover health providers, insurers, banks and financial companies, credit reporting agencies (which already have rules in place in their sector).

It grants different rights to Californian residents:

- Right to know what personal information is collected, used, shared or sold: This encompasses also the right to get a full list of all the third parties with whom those data is shared with. This law has a retroactive effect, in the sense that a consumer can request all data collected on him from the previous 12 months from the applicability of the regulation;
- Right to delete personal information held by a business and by extension, a business's service provider;
- Right to opt-out of sale of personal information. The consumers are able to stop a business to sell their information. For children under 13 years old, they must consent with a parent or a guardian and for children under 16 years old, they must provide opt in consent;
- Right to non-discrimination in terms of price or service when a consumer exercises a privacy right under CCPA.

It encompasses also new obligations for the business:

- Provide notice to consumers at or before data collection;
- Create procedures to respond to requests from consumers: For requests to opt-out, businesses must provide a "Do Not Sell My Info" link on their website or mobile app;
- Respond to requests from consumers within specific timeframes;
- Verify the identity of consumers who make requests to know and to delete: If it is unable to verify a request, the business may deny it but must comply to the greatest extent it can;
- Disclose financial incentives offered in exchange for the retention or sale of consumer's personal information and explain how they calculate the value of the personal information. The business must also explain how the incentive is permitted under the CCPA;
- Maintain records of requests and how they were responded for 24 months in order to demonstrate compliance.

The fines in case of infringement can go up to $7'500 per violation and in civil damages to $750 per affected consumer.

## 5.2 Relation with GDPR

There are similarities between CCPA and GDPR, therefore CCPA being sometimes called the Californian GDPR.

But while CCPA is similar to GDPR on many levels, it is narrower in some respects. For example, CCPA does not specifically provide consumers the right to correct inaccurate personal data, restrict processing, or object to processing — and it provides somewhat more limited rights for consumers to access and delete personal data. Some rules like having to notify a data breach within 72 hours does not exist in the CCPA.

Both regulations foresee to have a data inventory and mapping of data flows, processes and/or systems to respond to individual requests, data privacy practices in a privacy policy, written contracts with the service providers, but the requirements are sometimes different between the two regulations. Therefore, it is important to refer to each regulation to be sure to be compliant with it.

Moreover, the definitions in the CCPA and in the GDPR differ.

For example, the CCPA defines the sale of personal information as selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration.

Personal information is defined in the CCPA as *« information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household ».* Personal information under the CCPA includes direct identifiers (such as real name, alias, postal address, social security numbers), unique identifiers (such as cookies, IP addresses and account names), biometric data (such as face and voice recordings), geolocation data (such as location history), internet activity (such as browsing history, search history, data on interaction with a webpage or app), sensitive information (such as health data, personal characteristics, behavior, religious or political convictions, sexual preferences, employment and education data, financial and medical information). Personal information also includes data that by inference can lead to the identification of an individual or a household. Aggregate and anonymous data is exempt from the CCPA, unless it is in any way re-identifiable.

To get a good comparison of those two regulations, it can be referred to the following comparative.

## 5.3 Possible impact on the railway sector

This regulation will impact directly any railway undertaking, which would have an activity, leading to handle personal information of Californian residents. In a broader scope, this will impact all big companies doing business online.

It's the first Law in the United States to set up such rules on consumer data, and coming from one of the biggest State of the country, this might influence also other States or the entire country to focus more on privacy. Since the US Privacy Shield is put into question by some (like the International Safe Harbor Privacy Principles at its time), a national regulation would certainly facilitate the transfer of personal data to the US.

The Data Protection Experts are asked to provide their feedback **during the meeting**, if the CCPA had an impact on their business and if yes, how they solved it.

**Proposed resolutions**:

The Experts Group:

- takes note of the report;
- concerning Point 5.3, the Experts provide the following feedback:
- …

**ITEM 6**

**Revision of the Manual on Data Protection**

# 6 Revision of the Manual on Data Protection

## 6.1 New Commentaries of Articles

The CIT GS continued the commentaries to the different articles of the GDPR (see **Appendix 3**).

It added under some Articles new cases and legal opinions (see Points 3.1.4.1.2, 3.2.2.2, 3.2.5.4.2, 3.3.2.1, 3.4.3.1).

It also commented some Articles, which had no commentaries until now (see Point 3.2.1 on Article 5 GDPR, Point 3.2.2.1 on Article 6(1)(b) GDPR, Point 3.4 on Chapter IV GDPR and Point 3.4.12 on Article 35 GDPR).

Concerning Article 35 GDPR on the Data Processing Impact Assessment (DPIA), the CIT GS considered at first to have a separate Chapter in the MDP on that matter. While writing this Chapter, it noticed that it would make more sense to have it directly under the commentaries, since this Chapter represents also a commentary of the law. Moreover, it decided under that point to present two templates on how to proceed with a DPIA. The CIT GS would like to know if the Data Protection Experts consider those templates as necessary and relevant and if they should be mentioned under Article 35 GDPR or in a new Chapter.

Those modifications will be discussed more in details during the meeting.

The Data Protection Experts are asked for their opinion on that proposal.

If the Experts agree on those modifications, the text will then be sent to be checked from a linguistic point of view. The next step will be to translate the revised MDP into French and German. The three linguistic versions will be presented for adoption to the CIV Committee in September 2020. The publication should then take place on 13 December 2020.

## 6.2 Balance of legitimate interests' procedure

This is a further point the CIT GS would like to work on, this means explaining the criteria to take into account when having to assess the existence of a legitimate interest.

Before doing so, the CIT GS would like to hear the practices the Experts might have put in place on that aspect.

## 6.3 Transfer to third countries of data – Possible standardised solution?

One of the important topics tackled during the last Data Protection Workshop was the transfer of personal data to third countries.

The CIT GS would like to hear the point of view of the Data Protection Experts, if there is a need for the CIT GS to work on standardizing a solution to permit such transfer.

## 6.4 Data Protection and new technologies?

During the last Data Protection Workshop, an interesting presentation took place about the use of new technologies and their impact on data protection (e.g Artificial intelligence, Internet of things, social networks, etc).

The CIT GS would like to know if the Data Protection Experts see a need to develop also in that direction the MDP, by adding for example a special chapter on that matter or by tackling it under the commentaries of articles.

## 6.5 Next steps of the revision

### 6.5.1 Age of consent of children (art. 8 GDPR)

Art. 8 GDPR states that for the age of consent, national law can foresee a lower threshold than 16 years old (but not below 13 years old).

The CIT GS would be interested in knowing what are the age limits applicable in their countries. The CIT GS reflects on adding a list with those different national age limits in the MDP. The Experts are asked to provide their opinion on that **during the meeting**.

6.5.2 Fining policy related to GDPR (art. 83 GDPR)

The GDPR imposes maximum administrative fines (of 2 or 4% depending on the obligation violated). To fix the concrete amount of the fine though, it is only indicated that the administrative fine should be effective, proportionate and dissuasive.

Therefore, some authorities, like the Dutch Data Protection Authority, decided to release a GDPR fining policy. It encompasses four categories of violations, with examples depending on company size and maximum fine:

- Category I: €0 to €200,000
- Category II: €120,000 to €500,000
- Category III: €300,000 to €750,000
- Category IV: €450,000 to €1 million

To categorize the violation, the authority will take into account criteria such as the duration of the infringement, the number of data subjects affected, the rapidity of reaction of the company, the type of personal data involved.

The CIT GS would like to know if other national authorities have issued such kind of policies.

If this should be the case, the CIT GS suggests analysing them and take them as reference in the MDP. The CIT GS would like to hear the opinion of the Data Protection Experts on that idea.

6.5.3 Other points

The CIT GS would like to know if the Data Protection Experts consider that other topics should be handled in the MDP.

If this should be the case, they are asked to communicate them **during the meeting**.

**Proposed resolutions**:

The Working Group:

- takes note of the report;
- as regards Point 6.1, the Experts provide the following feedback:
- concerning Point 6.2, the Experts share the opinion that:
- ad Point 6.3, the Experts are in favor of:
- regarding Point 6.4, the Experts suggests to:
- concerning Point 6.5, the Experts think that:
- …

**ITEM 7**

**Next meeting and Data Protection Workshop**

## 7 Next meeting and Data Protection Workshop

Almost sixty people took part in the Data Protection Workshop on 18 June 2019, from thirty different undertakings. Initial feedback received had been very positive and encouraging for the prospect of running a workshop every year.

The CIT GS decided therefore to organise a yearly meeting of the Data Protection Experts. Moreover, every two years, a Workshop such as the one of 2019 will take place.

The next Workshop should take place in 2021.

The CIT GS suggests having a one-day Workshop like in 2019. Regarding the theme of this Workshop, the CIT GS would suggest having one central topic, which would be discussed from different perspectives. One idea could be to have as topic the “transport of passengers from a data protection perspective”, which could give to the speakers enough leeway to tackle it in different manners (e.g. transport of children, transport of passengers in times of pandemic like COVID-19, assistance to PRM, etc.).

The CIT GS also suggests holding a Data Protection Experts meeting the day before the Workshop.

Regarding the date, the CIT GS would hold the Data Protection Experts Meeting on 24 March 2021 and the Data Protection Experts Workshop on 25 March 2021, both in Warsaw, at the kind invitation of PKP Intercity.

The Experts are asked to provide feedback on the organisation of such meetings and the topics to be handled **until 31 July 2020**.

**Proposed resolutions**:

The Experts Group:

- takes note of the report;
- concerning the organisation of a meeting and a Workshop on 24-25 March 2021, the Data Protection Experts are asked to provide feedback until 31 July 2020;
- …

**ITEM 8**

**Calendar 2020**

## 8 Calendar 2020

| | | |
|---|---|---|
| 12 June | UIC Innovation Workshop | Videoconference |
| 17-18 June | Data Protection Experts Meeting | Videoconference |
| 23 June | CER PWG | Videoconference |
| 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 |
| 24 September | Claims Department Conference | Rome |
| 25 September | CIV Committee | Rome |
| 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 |
| 25 November | UIC Passenger Services Group | Luxembourg |
| 26 November | UIC Innovation Workshop | Paris |

**Proposed resolutions:**

The Experts Group:

- takes note of the report;
- …