International Rail Transport Committee
Comité international des transports ferroviaires
Internationales Eisenbahntransportkomitee

1st Meeting of the Data Protection Experts, 17-18 June 2020, Video Conference

Appendix 3 to the Working document

Edition of 13~~15~~ December ~~2019~~2020

Manual on Data Protection for Transport Undertakings (MDP)

Applicable with effect from 13~~15~~ December ~~2019~~2020

This document is restricted to CIT members

In accordance with point 2.6 a) of the CIT Statutes, this document is a recommendation and only binds members to the extent that members adopt it (opting-in principle).

Amendment No	Amended items	Applicable with effect from

Earlier versions are available here: https://www.cit-rail.org/en/passenger-traffic/cit-documentation/

Contents

1 Preamble

1.1 Content and purpose of the manual

The Manual on Data Protection for Transport Undertakings (MDP) provides CIT members with an introduction to the general principles of data protection, as well as more detailed explanations on specific points of interest for transport undertakings.

1.2 Scope

This Manual applies to all CIT members which deal with personal data from citizens of the European Union (EU), irrespective of whether they are themselves based in the EU or not.

It has a non-binding effect for the CIT members, who may choose to refer to it.

It is intended solely for the internal use of the CIT members.

1.3 Legal basis

The Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR) has been applicable since 25 May 2018.

This new Regulation is applicable in all fields and for all kinds of services, including railway transport services.

1.4 Structure

This Manual contains several parts:

- This preamble is followed by the GDP CIT that summarise the main obligations stemming from the GDPR for railway undertakings.
- The second part is dedicated to the commentary of the different articles of the GDPR. The commentaries are based on the guidelines published by the European Data Protection Board (EDPB, previously the Article 29 Working Party [Art. 29 WP]). This second part also includes the questions raised by the CIT members on data protection as well as the answers provided by the CIT, but also Courts' and authorities' decisions in so far as they are known.
- The third part of this Manual contains examples of clauses. These may be considered as good practices for informing or requesting the consent of customers.
- The last part of this Manual contains the boilerplate contracts on data processing.

Whilst every care has been taken to ensure the accuracy of the information provided in this Manual at the time of publication, this information is intended as guidance only. It should not be considered as legal advice.

2 CIT Guidelines on Protection of Privacy and Processing of Personal Data used in International Passenger Traffic by Rail

The present Guidelines are of recommendatory non-binding nature and are primarily designed for the CIT Members established in the European Union (EU) or offering services to natural persons in the EU. The Guidelines present an overview of the main notions and principles applicable to personal data protection and privacy in the EU as established by the Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

The CIT Members process personal data on daily basis, among others in relation to ticketing, after-sales services, as well as marketing. They can act both as data controllers and data processors for the purposes of these Guidelines. It is recommended for the CIT Members to use the present document as guidance when preparing internal and public privacy policies, as well as various customer forms both on paper and electronically.

2.1 Definitions

Data Controller	A natural or legal person, or a public authority, that determines the purposes and means of the processing of personal data (e.g. a carrier, which requires a name and a date of birth to be indicated on the ticket, or defines the categories of personal information necessary to become a registered user of an railway undertaking's app or web-page).
Data Processor	A natural or legal person that processes personal data on behalf of the controller. The data processor can be among others a railway undertaking, a distributor, or a third party entrusted with processing (e.g. storage of personal data). The data controller can also fulfil functions of the data processor.
Data Subject	A natural person, whose personal data is subject to processing by the data processor as determined by the data controller (e.g. a passenger).
Personal Data	Any information relating to identified or identifiable natural person ('data subject'). A natural person is identifiable by reference to an identifier such as a name, an identification number, location data, and online identifier or to factor(s) specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. A dynamic IP address registered by a railway undertaking when a person accesses the web-page constitutes personal data, only if the railway undertaking has legal means which enable it to identify the data subject with additional data which the internet service provider has about that person. Anonymous information, i.e. personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable, does not constitute personal data covered by the Regulation 2016/679 or these Guidelines.
Processing	Processing of personal data entails any operation on personal data, including but not limited to collection, recording, organisation, structuring, storage, adaptation, disclosure by transmission, erasure, performed wholly or partly by automated means and other than by automated means.

2.2 Scope

2.2.1 These Guidelines relate to any processing of personal data under the control of a CIT Member established in the EU or offering services to the data subjects in the EU.

2.2.2 Nothing in these Guidelines is meant to prevent CIT Members from applying more stringent or additional measures or derogations contained in applicable national laws for the protection of data subject's privacy.

2.3 Basic principles of processing personal data

2.3.1 Personal data undergoing processing under the control of a CIT Member must be:

2.3.1.1 processed lawfully, fairly and in an transparent manner in relation to the data subject (i.e. is based on consent of the data subject, or necessary for the performance of the contract or for the compliance with a legal obligation according to the EU or the national law to which the controller is subject, or necessary for the purpose of the legitimate interests pursued by the controller or by a third party, unless such interests are overridden by the interests, fundamental rights and freedoms of the data subject which require protection of personal data);

2.3.1.2 processed for specified, explicit and legitimate purpose (e.g. for issuing nominative tickets only name and surname are to be collected, but not the place of residence, which will be then used for marketing purposes);

2.3.1.3 collected only to the extent that it is adequate, relevant and necessary for the set legitimate purpose (e.g. for the purpose of claims handling, the carrier has to collect only the necessary information to be able to assess the claim);

2.3.1.4 accurate and, where necessary kept up to date;

2.3.1.5 stored only for as long as it might be necessary for the purpose of data processing (e.g. only for the period of limitation of actions under the CIV Uniform Rules);

2.3.1.6 processed in accordance with the principles of privacy by design and privacy by default, as detailed in point 2.7 below;

2.3.1.7 processed with appropriate security safeguards, as detailed in point 2.8 below, among others to protect personal data from unauthorised or unlawful processing, accidental loss, destruction or damage.

2.3.2 If processing is based on the consent of a data subject, this consent has to be free, specific, informed and unambiguous. If the data subject, who declines to provide consent faces legal consequences, such consent does not qualify as free. In this situation, the data controller can process information on another ground of lawfulness, e.g. if he is required to do so by the EU or national law. The CIT Member shall be able to demonstrate that the data subject has consented to the specific processing of his or her personal data. The data subject has the right to withdraw his or her consent. Special stricter conditions apply if the data controller seeks consent for the processing from a child.

2.3.3 Each CIT Member shall maintain a record of processing activities under its responsibility, including information about the contact details of the controller and its data protection officer, the purposes of processing, description of the categories of data subjects and the categories of personal data, whether the personal data has been transferred or disclosed.

2.4 Special categories of data

2.4.1 The processing of sensitive data, including data concerning health, such as data related to data subject's reduced mobility is generally prohibited.

2.4.2 Despite the general prohibition, the processing of special categories of data can be permitted if:

2.4.2.1 the data subject gave his explicit consent to processing (e.g. when requesting the necessary PRM assistance in line with the PRR or other laws), except when prohibited by national law, or

2.4.2.2 processing is necessary to fulfil obligations and to exercise specific rights of the data subject or the controller in the field of employment, social security and social protection law (e.g. special fare discounts for PRMs), or

2.4.2.3 processing is necessary to protect the vital interest of the data subject or of another person, where the data subject is physically or legally incapable of giving consent (e.g. information necessary for the fulfilment of advance payments according to the PRR), or

2.4.2.4 processing relates to personal data which are manifestly made public by the data subject.

2.5 Information obligation towards passengers as data subjects

2.5.1 The CIT Member acting as a data controller shall take appropriate measures to provide information to the data subject in a concise transparent, intelligible and easily accessible form, using clear and plain language.

2.5.2 The following information has to be provided to the data subject at the time when his/her personal data is obtained:

2.5.2.1 the identity and contact details of the controller and/or controller's representative;

2.5.2.2 the contact details of the data protection officer;

2.5.2.3 the legal basis and the purpose(s) of processing;

2.5.2.4 recipients or categories of recipients of the personal data;

2.5.2.5 where applicable, the intended transfer of personal data to a third country and the related risks (e.g. absence of adequacy decision by the European Commission, lack of appropriate safeguards etc.);

2.5.2.6 the period for which the personal data will be stored or criteria that are used to determine this period;

2.5.2.7 the right of the data subject to access, rectify or erase his/her personal data and to data portability;

2.5.2.8 the right of the data subject to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

2.5.2.9 the right to lodge a complaint with a supervisory authority;

2.5.2.10 if the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, and if the data subject is obliged to provide his/her personal data – information about possible consequences of failure to provide such data;

2.5.2.11 the existence of automated decision-making, including profiling, the logics behind it, significance and the envisaged consequences of such processing for the data subject.

2.5.3 If the CIT Member acting as a data controller intends to process the personal data of the data subject for other than initial purpose, he is obliged to provide all the respective information, as required under point 2.5.2 above.

2.5.4 The CIT Member acting as the data controller shall provide on request of the data subject a confirmation of processing of his personal data, a copy of the personal data being processed and additional information according to point 2.5.2 and information about the source of data, if personal data was not received from the data subject. The CIT Member may charge a reasonable fee based on administrative costs for further additional copies of personal data provided.

2.6 Access to data by passengers as data subjects

2.6.1 The CIT Member acting as a data controller shall establish procedures for:

2.6.1.1 disclosing to the data subject whether his personal data are being processed;

2.6.1.2 ensuring access of the data subject to a personal data file and providing a copy of the processed personal data upon request of the data subject, also in electronic form;

2.6.1.3 ensuring the data subject's right to object to automated processing and profiling of his personal data, unless it is required for legitimate purposes overriding the data subject's interests. Where the data subject objects to processing for direct marketing purposes, the processing and profiling for these purposes should be stopped;

2.6.1.4 allowing the data subject to exercise the right to rectify inaccurate personal data or to delete data processed in violation of the applicable principles and rules on data protection, including where personal data is no longer necessary for the purposes for which it was collected or if the data subject has withdrawn its consent for processing of the personal data, or the processing was initially unlawful. The CIT Member shall notify the data subject about the rectification and erasure of the personal data according to his request.

2.7 Data protection by design and by default

2.7.1 The CIT Member acting as a data controller shall implement appropriate technical and organisational measures, both when designing the processing and conducting the processing, taking into account the state of the art, the cost of implementation, the nature, scope, context and purposes of processing as well as the potential risks for rights and freedoms of the data subjects. Such measures may include, but are not limited to pseudonymisation in light of data minimisation requirement.

2.7.2 The CIT Member acting as a data controller shall implement appropriate technical and organisational measures to ensure that by default only personal data which is necessary for each specific purpose of the processing are processed. This obligation applies to the amount of personal data collected, the extent of processing, the period of their storage and their accessibility. Thus, if data is collected for handling of passengers' complaints, only the personal data necessary for this purpose shall be collected, and shall not be stored for longer than the duration of the limitation of action for claims related to that complaint or as required by the national law.

2.8 Security of data processing and transmission

2.8.1 Appropriate technical and organisational measures shall be taken for the protection of personal data against accidental loss and unauthorized access, alteration or dissemination, in particular where the processing involves the transmission of data over a network.

2.8.2 Technical and organisational measures to ensure security of data processing include, but are not limited to: pseudonymisation and encryption of personal data, ongoing measures to ensure confidentiality, integrity, availability and resilience of processing systems and services, measures to deal with physical or technical incidents in a timely measure, regular testing and assessing of the effectiveness of the measures in place.

2.8.3 Where the CIT Member acting as a data controller uses new data processing technologies or there is otherwise a likelihood that the processing may result in a high risk to the rights and freedoms of natural persons, the CIT Member shall perform an impact assessment prior to the processing.[1]

2.8.4 The CIT Member acting as a data controller can demonstrate compliance with its obligations by adhering to the approved codes of conduct or approved certification mechanisms, if they are in place.

2.9 Obligation to designate a data protection officer[2]

2.9.1 The CIT Members shall designate a data protection officer if they engage in regular and systematic monitoring of data subjects on a large scale (e.g. through location tracking or loyalty programs) or may do so voluntarily. The contact details of the data protection officer shall be published, communicated to the supervisory authority and communicated to the data subjects, where necessary.

2.9.2 The data protection officer may be a staff member or fulfil his tasks based on a service contract. He shall always be in a position to perform his duties and tasks in an independent manner.

[1] For the criteria of "high risk" see: Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purses of Regulation 2016/679, WP 248.
[2] For further details on obligations related to the Data Protection Officers, see: Article 29 Data Protection Working Party, Guidelines on Data Protection Officers ("DPOs"), adopted 5 April 2017, WP 243 rev. 01.

2.10 Obligation to notify the supervisory authority

2.10.1 In the case of personal data breach, the CIT Member acting as a data controller shall without undue delay, if feasible within 72 hours after having become aware of it, notify the breach to the competent supervisory authority, unless the data breach is unlikely to result in a risk to the rights and freedoms of natural persons. The CIT Member acting as a data controller shall comply with any additional requirements according to the national law regarding the content and format of such notification.

2.10.2 Where the personal data processing is likely to result in a high risk to the data subject according to the impact assessment, and no measures to mitigate that risk are or can be taken by the CIT Member acting as a data controller, the CIT Member shall consult the supervisory authority prior to the processing.

2.11 Relations between the data controller and the data processor

2.11.1 Where the processing is to be carried out on behalf of the CIT Member acting as a data controller, it shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures.

2.11.2 Processing by a processor shall be governed by a contract or another binding legal act under the national law that sets out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.

2.11.3 The contract shall stipulate that the processor among other shall:

2.11.3.1 Process personal data only on written instructions from the CIT Member acting as the data controller, including cases where processing required the transfer of personal data to a third country, unless required by the EU law or the national law of the EU Member States;

2.11.3.2 Ensure that persons authorised to process the personal data committed to confidentiality obligation;

2.11.3.3 Take all necessary measures to ensure security of processing;

2.11.3.4 Request authorisation of the CIT Member acting as a data controller before subcontracting another processor or transferring the personal data to a third country;

2.11.3.5 Assist the CIT Member acting as a data controller to respond to requests by the data subject, including with respect to access to the personal data, erasure and rectification of this data;

2.11.3.6 Upon request of the CIT Member acting as a data controller, delete and/or return all the personal data to this CIT Member after the end of processing, unless the EU or the EU Members State law requires storage of the personal data by the processor for a certain period of time;

2.11.3.7 Make available to the CIT Member acting as a data controller all information necessary to demonstrate compliance with its obligations (inspections, audits etc.).

2.12 Transfer of data to third countries

2.12.1 The CIT Member acting as a data controller can transfer personal data of the data subject within the EU without any additional reservations, upon due information provided to the data subject about the recipient of the data and the purpose of transfer, and if necessary subject to data subject's consent.

2.12.2 Before transferring the personal data to a third country, the CIT Member has to check whether the country of destination is covered by an adequacy decision from the European Commission. If it is not the case, the CIT Member may make use of the appropriate safeguards according to Article 46 of the Regulation 2016/679, including a legally binding and enforceable instrument between public authorities (e.g. EU – U.S. Privacy Shield), binding corporate rules, standard data protection clauses adopted by the European Commission, approved codes of conduct or approved certification mechanisms.

2.12.3 In case of absence of the adequacy decision and appropriate safeguards, the CIT Member may only transfer the data subject's personal data to third countries, if the data subject explicitly consented to the transfer after having been informed of the possible risks, or the transfer is necessary for the conclusion or performance of the contract with the data subject or with a third person in the interest of the data subject, or the transfer is necessary to pursue legal claims or for important reasons of public interest. If none of these derogations apply, the CIT Member may only transfer data subject's personal data to third countries, if the conditions under the last sub-paragraph of paragraph 1 of Article 49 of the Regulation 2016/679 are met.

2.13 CIT Group of Experts on Data Protection

2.13.1 Given the rapidly changing digital environment and new business models in the railway sector, complex questions related to personal data protection in international passenger traffic by rail may arise. The CIT Members may request support from the CIT General Secretariat which will in turn consult the CIT Group of Experts on Data Protection.

2.13.2 The CIT Members are to report to the CIT General Secretariat any personnel changes that need to be reflected in the Group of Experts' contact list available on the CIT web-page: www.cit-rail.org.

3 Commentary to the Articles of the GDPR[3]

3.1 General provisions (Chapter I GDPR)

3.1.1 Subject-matter and objectives (Art. 1 GDPR)

[To be drafted ~~by June 2020~~]

3.1.2 Material scope (Art. 2 GDPR)

[To be drafted ~~by June 2020~~]

3.1.3 Territorial scope (Art. 3 GDPR)

[To be drafted ~~by June 2020~~]

3.1.4 Definitions (Art. 4 GDPR)

3.1.4.1 Courts' and authorities' decisions

3.1.4.1.1 Notion of "personal data" – IP Address, ECJ C-582/14

In the case Breyer v. Bundesrepublik Deutschland (C-582/14), the dynamic IP address registered by an online media services provider when a person accesses a website that the provider makes accessible to the public constitutes personal data, where this provider has the legal means (e.g. in the event of a cyber-attack) to identify the data subject with additional data, which the internet service provider has about that person. The ECJ considered that the storage of this personal data is only possible with the person's consent.

For railway undertakings, this would mean that if they save the IP addresses of their clients, the question arises as to whether they have the legal means to obtain additional information from the internet provider about the identity of the person behind the IP address. Nevertheless, in all the cases clients will have to be informed whether their IP address is being saved.

3.1.4.1.2 Notion of "personal data" – E-mail address, Question for written answer E-007174/17 to the Commission (Richard Sulik, ECR, 22 November 2017) and Answer given by Ms Jourova on behalf of the Commission (21 February 2018)

Using direct identifiers of an individual (this means for example his name) is a personal data falling under GDPR. For e-mail addresses not using direct identifiers, they may also constitute personal data when combined with other data (like an address or date of birth).

The same goes for profesionnal e-mail addresses of employees, which would also fall under GDPR, but not an e-mail address of a legal person (like info@company.com).

Therefore, the processing of an e-mail address such as flower1234@gmail.com, which can with other data in its possession be related to a natural person falls under GDPR.

3.1.4.1.~~2~~3 Notion of "personal data" – Information, ECJ C-434/16

In the case Peter Nowak v. Data Protection Commissioner (C-434/16), the ECJ stated that it is not disputed that a candidate at a professional examination is a natural person who can be identified, either directly, through his name, or indirectly, through an identification number, these being placed either on the examination script itself or on its cover sheet.

In this context, it is of no relevance whether the examiner can or cannot identify the candidate at the time when he/she is correcting and marking the examination script. For information to be treated as 'personal data' within the meaning of Article 2(a) of Directive 95/46, there is no requirement that all the information enabling the identification of the data subject must be in the hands of one person. It is also undisputed that, in the event that the examiner does not

[3] The drafting of this Chapter takes place in two steps. The first part was adopted during the CIV Committee in June 2019. The second part will be drafted and adopted for the CIV Committee in 2020.

know the identity of the candidate when he/she is marking the answers submitted by that candidate in an examination, the body that set the examination, in this case the CAI, does, however, have available to it the information needed to enable it easily and infallibly to identify that candidate through his identification number, placed on the examination script or its cover sheet, and thereby to ascribe the answers to that candidate.

The ECJ went even further by stating that information relating to a candidate contained in his or her answers submitted at a professional examination and in the comments made by the examiner with respect to those answers also constitutes personal data. It interpreted very broadly the notion of "personal data" as encompassing all kinds of information, not only objective, but also subjective, in the form of opinions and assessments, provided that it 'relates' to the data subject. As regards the latter condition, this is satisfied if the information, by reason of its content, purpose or effect, is linked to a particular person.

This case is of significance for railway undertakings, because according to this judgement, the file number they might use for passengers or for their own employees, and the information they might collect on their customers or employees (such as notes, etc.) would fall under the definition of personal data.

3.1.4.1.~~43~~ Notion of "legitimate interests" – ECJ C-13/16

In the case Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v. Rīgas pašvaldības SIA 'Rīgas satiksme' (C-13/16), the ECJ had a chance to interpret the concept of 'necessity for the realisation of the legitimate interests of a third party'. In this regard it laid down three cumulative conditions so that the processing of personal data is lawful:

1. **the pursuit of a legitimate interest by the data controller or by the third party or parties to whom the data are disclosed**: in the case at hand the interest of a third party in obtaining the personal information of a person who damaged their property in order to sue that person for damages was qualified as a legitimate interest.
2. **the need to process personal data for the purposes of the legitimate interests pursued**: the ECJ noted that the personal data has to meet the standard of being "strictly necessary" (e.g. to bring a legal action against a person, the name and surname are not enough, and the address and ID number would also be required); and
3. **the fundamental rights and freedoms of the person concerned by the data protection do not take precedence**: the analysis under the third condition would depend on the specific circumstances of each case.

3.1.4.2 Questions from members[4]

3.1.4.2.1 Links to personal data as personal data

One of the CIT members asked if a reference/link to personal data constitutes personal data.

Academic literature suggests that links to personal data can be considered as personal data and are therefore subject to the requirements of the GDPR[5]. Moreover, Article 17(2) of the GDPR suggests that links to personal data are subject to the right to erasure ('right to be forgotten'). Given the broad definition of 'personal data' in Article 4 of the GDPR, it is reasonable to assume that links to personal data will be considered as personal data by the national and EU courts.

3.1.4.2.2 Notion of "data controller and "data processor"

When a passenger makes a booking through a retailer, the personal data of that passenger (since the tickets of that CIT member are nominative) are being transferred through the retailer's system, the distributor's system (if a distributor is involved) and the system of the railway undertaking's provider before they reach the railway undertaking's passenger system. Which of these various actors is a data controller and which is a data processor?

Several undertakings mentioned that in this situation, they consider that their distributors are data controllers for the passengers' personal data, which they collect. The railway undertaking will also be a data controller, but only for the part of the personal data that the distributor will

[4] Answers provided by the CIT GS.
[5] See e.g. Paul Bernal, 'The EU, the US and Right to be Forgotten', in Serge Gutwirth, Ronald Leenes, Paul de Hert (eds), *Reloading Data Protection. Multidisciplinary Insights and Contemporary Challenges* (Springer, 2014), at 67-68.

transfer to it. The distinction is really important, because of the different obligations and responsibilities towards the data subject and the obligation to have a data processing agreement between the data controller and the data processor.

However, some members were of the view that the criterion for distinguishing the data processor and the data controller in the distribution process should be to determine who decides to collect the personal data in question.

3.2 Principles (Chapter II GDPR)

3.2.1 Principles relating to processing of personal data (Art. 5 GDPR)

When processing personal data, the data controllers need to respect those principles, regardless of what is the legal basis used to process the data.

3.2.1.1 Notion of fairness and lawfulness (Art. 5(1)(a) GDPR)

It includes the reasonable expectations of the data subjects; the data subject should not be surprised of the way how his personal data will be processed[6]. It should here also be taken into account the possible adverse consequences processing may have on him and also the potential effects of imbalance between the parties[7].

Concerning lawfulness, it is necessary that the processing is valid under the applicable law. In case of processing based on the performance of a contract for example, this would mean that the processing shall be valid under the applicable contract law and also consumer protection law[8].

3.2.1.2 Notion of purpose limitation principle (Art. 5(1)(b) GDPR)

It means that the personal data must be collected for specified, explicit and legitimate purposes, and not further processed in an incompatible way with those purposes[9].

3.2.1.3 Notion of data minimisation principle (Art. 5(1)(c) GDPR)

As little data as possible shall be processed in order to achieve the purpose[10].

3.2.1.4 Notion of "without delay" (Art. 5(1)(d) GDPR)~~[To be drafted by June 2020]~~

It needs a case-by-case analysis.

In a case in another law field, the European Court of justice stated that without undue delay did not mean several weeks of even several months[11].

[6] European Data Protection Board, Guidelines 2/2019 on the processing of personal data under Article 6(2)(b) GDPR in the context of the provision of online services to data subjects Version 2.0, Adopted on 8 October 2019, p. 6§12, in: https://edpb.europa.eu/our-work-tools/our-documents/smernice/guidelines-22019-processing-personal-data-under-article-61b_en.

[7] European Data Protection Board, Guidelines 2/2019 on the processing of personal data under Article 6(2)(b) GDPR in the context of the provision of online services to data subjects Version 2.0, Adopted on 8 October 2019, p. 6§12, in: https://edpb.europa.eu/our-work-tools/our-documents/smernice/guidelines-22019-processing-personal-data-under-article-61b_en.

[8] European Data Protection Board, Guidelines 2/2019 on the processing of personal data under Article 6(2)(b) GDPR in the context of the provision of online services to data subjects Version 2.0, Adopted on 8 October 2019, p. 6§13, in: https://edpb.europa.eu/our-work-tools/our-documents/smernice/guidelines-22019-processing-personal-data-under-article-61b_en.

[9] European Data Protection Board, Guidelines 2/2019 on the processing of personal data under Article 6(2)(b) GDPR in the context of the provision of online services to data subjects Version 2.0, Adopted on 8 October 2019, p. 6§14, in: https://edpb.europa.eu/our-work-tools/our-documents/smernice/guidelines-22019-processing-personal-data-under-article-61b_en.

[10] European Data Protection Board, Guidelines 2/2019 on the processing of personal data under Article 6(2)(b) GDPR in the context of the provision of online services to data subjects Version 2.0, Adopted on 8 October 2019, p. 6§15, in: https://edpb.europa.eu/our-work-tools/our-documents/smernice/guidelines-22019-processing-personal-data-under-article-61b_en.

[11] ECJ, C-443/18 - Commission / Italy (Bactérie Xylella fastidiosa), Recital 38, in: http://curia.europa.eu/juris/liste.jsf?language=fr&jur=C%2CT%2CF&num=c-443/18&parties=&dates=error&docnodecision=docnodecision&allcommjo=allcommjo&affint=affint&affclose=affclose&alldocrec=alldocrec&docdecision=docdecision&docor=docor&docav=docav&docsom=docsom&docinf=docinf&alldocnorec=alldocnorec&docnoor=docnoor&docppoag=docppoag&radtypeord=on&newform=newform&docj=docj&docop=docop&docnoj=docnoj&typeord=ALL&domaine=&mots=&resmax=100&Submit=Rechercher

The European Data Protection Board defines it as meaning: “as soon as possible »[12].

3.2.2 Lawfulness of processing (Art. 6 GDPR)[13]

Before processing personal data, the data controller needs to have a lawful ground for doing so. Without this lawful ground, it cannot process data. There are six alternative legal grounds which permit personal data to be processed:

- consent;
- performance of a contract;
- legal obligation;
- vital interests;
- performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- legitimate interests.

It is important to analyse which is the appropriate ground to use in each situation before processing the personal data. This is in line with the principles of fairness and purpose limitation but requires to identify the purposes of processing[14].

Consent might be a false friend. On the one hand it is certainly the easiest legal ground to use, in terms of proof: if there is a dispute with the data subject regarding the processing of his data, it will be easy to prove that the data subject gave his consent (through the application he filled in, or the box he ticked, etc.); in contrast, it would often be much more difficult to demonstrate that there is, for example, a legitimate interest or a public interest in processing the data. On the other hand, even if consent has been given, if the conditions that make it valid are not met, then this consent will not have any validity.

When processing their customers’ data, several railway undertakings therefore refer to other lawful grounds, such as the performance of a contract, public interest and legitimate interests. The CIT GS advises analysing first whether any other lawful grounds are applicable and only to consider using consent as justification as a second step, but in this case, to ensure that all the conditions which make consent valid are met.

Even after having obtained the consent of the data subject, this does not give the data controller carte blanche to do as he wishes with the personal data. He still has to observe the data processing principles contained in the GDPR (cf. Art. 5 GDPR) and he cannot collect more data than necessary.

3.2.2.1 Performance of a contract (Art. 6(1)(b) GDPR)[15]

This article applies when the processing is objectively necessary for the performance of a contract with a data subject or in order to take pre-contractual steps at the request of a data subject.

3.2.2.1.1 Notion of “necessity”

If there are realistic, less intrusive alternatives, the processing is not necessary and it is therefore not possible to base itself on Article 6(1)(b) GDPR[16].

[12] European Data Protection Board, Guidelines on Personal data breach notification under Regulation 2016/679 (wp250rev.01), As last Revised and Adopted on 6 February 2018, p. 20, in: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052.
[13] From: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.
[14] European Data Protection Board, Guidelines 2/2019 on the processing of personal data under Article 6(2)(b) GDPR in the context of the provision of online services to data subjects Version 2.0, Adopted on 8 October 2019, p. 7§18, in: https://edpb.europa.eu/our-work-tools/our-documents/smernice/guidelines-22019-processing-personal-data-under-article-61b_en.
[15] From : https://edpb.europa.eu/our-work-tools/our-documents/smernice/guidelines-22019-processing-personal-data-under-article-61b_en.
[16] European Data Protection Board, Guidelines 2/2019 on the processing of personal data under Article 6(2)(b) GDPR in the context of the provision of online services to data subjects Version 2.0, Adopted on 8 October 2019, p. 8§25, in: https://edpb.europa.eu/our-work-tools/our-documents/smernice/guidelines-22019-processing-personal-data-under-article-61b_en.

The processing must be genuinely necessary for the performance of a contract and not unilaterally imposed on the data subject by the data controller. The fact that the processing activities are mentioned in the contract does not make it by itself necessary for the performance of the contract[17].

It is therefore important to analyse the aim, the purpose and the objective of the service falling under the contract. The processing needs to be objectively necessary for a purpose in relation to the delivery of the contractual service to the data subject. The data controller should be able to prove that it won't be able to perform the contract without processing those personal data[18]. The expectations of the parties should also be taken into account, to assess if the data subject could expect such processing[19].

3.2.2.1.2 "Necessity for the performance of a contract"

Three conditions need to be fulfilled, in order to rely on this legal basis[20]:

1. Existence of a contract
2. Contract is valid pursuant to applicable national contract laws
3. The processing is objectively necessary for the performance of the contract

If the processing is not necessary for the performance of the contract or goes beyond what is necessary, the data controller can still try to analyse if the processing would be justified by another legal basis.

E.g.: Purchase of a good on Internet by credit card with home delivery, the retailer will need to perform the contract, the data subject's credit card information and billing address for payment purposes and the data subject's home address for delivery. If the retailer wants to build profils about the tastes of its customers, this would not be necessary for the performance of the contract and would not be justified by this legal basis[21].

If the contract consists of several separate services or elements of a service that can be performed independently of one another, the applicability of this legal basis should be assessed separately for each service[22].

Under performance of the contract, the EDPB shares the opinion that "*certain actions can be reasonably foreseen and necessary within a normal contractual relationship, such as sending formal reminders about outstanding payments or correcting errors or delays in the performance of the contract*"[23].

The EDPB considers that processing personal data for service improvement cannot be justified under the performance of the contract, even if such a clause is included in the contractual terms. The same goes for processing for fraud prevention, which goes, for the EDPB, beyond

[17] European Data Protection Board, Guidelines 2/2019 on the processing of personal data under Article 6(2)(b) GDPR in the context of the provision of online services to data subjects Version 2.0, Adopted on 8 October 2019, p. 9§28, in: https://edpb.europa.eu/our-work-tools/our-documents/smernice/guidelines-22019-processing-personal-data-under-article-61b_en.
[18] European Data Protection Board, Guidelines 2/2019 on the processing of personal data under Article 6(2)(b) GDPR in the context of the provision of online services to data subjects Version 2.0, Adopted on 8 October 2019, p. 9-10§30, in: https://edpb.europa.eu/our-work-tools/our-documents/smernice/guidelines-22019-processing-personal-data-under-article-61b_en.
[19] European Data Protection Board, Guidelines 2/2019 on the processing of personal data under Article 6(2)(b) GDPR in the context of the provision of online services to data subjects Version 2.0, Adopted on 8 October 2019, p. 10§32-33, in: https://edpb.europa.eu/our-work-tools/our-documents/smernice/guidelines-22019-processing-personal-data-under-article-61b_en.
[20] European Data Protection Board, Guidelines 2/2019 on the processing of personal data under Article 6(2)(b) GDPR in the context of the provision of online services to data subjects Version 2.0, Adopted on 8 October 2019, p. 9§26, in: https://edpb.europa.eu/our-work-tools/our-documents/smernice/guidelines-22019-processing-personal-data-under-article-61b_en.
[21] European Data Protection Board, Guidelines 2/2019 on the processing of personal data under Article 6(2)(b) GDPR in the context of the provision of online services to data subjects Version 2.0, Adopted on 8 October 2019, p. 10-11§35, in: https://edpb.europa.eu/our-work-tools/our-documents/smernice/guidelines-22019-processing-personal-data-under-article-61b_en.
[22] European Data Protection Board, Guidelines 2/2019 on the processing of personal data under Article 6(2)(b) GDPR in the context of the provision of online services to data subjects Version 2.0, Adopted on 8 October 2019, p. 11§37, in: https://edpb.europa.eu/our-work-tools/our-documents/smernice/guidelines-22019-processing-personal-data-under-article-61b_en.
[23] European Data Protection Board, Guidelines 2/2019 on the processing of personal data under Article 6(2)(b) GDPR in the context of the provision of online services to data subjects Version 2.0, Adopted on 8 October 2019, p. 12§38, in: https://edpb.europa.eu/our-work-tools/our-documents/smernice/guidelines-22019-processing-personal-data-under-article-61b_en.

what is necessary for the performance of the contract. Processing for online behavioural advertising cannot be justified by the performance of the contract either. For those processing, other legal basis might be used, like the consent or the legitimate interest[24].

For processing for personalisation of content, the performance of the contract may justify it, according to the EDPB, but only if it is an intrinsic aspect of the service (which will depend on the nature of the service, the expectations of the average data subject and if the service can be provided without personalisation)[25].

3.2.2.1.3 Termination of the contract[26]

When the contract terminates, in principle, the processing of the data is no longer necessary for the performance of the contract and the controller will need to stop processing.

If the termination necessitates some administration, such as returning goods or payment, they can be processed under the legal basis of the performance of the contract.

This would mean that the data controller shall also erase the data, since they are no longer necessary, except if the processing is still necessary for specific purposes like complying with a legal obligation or the establishment, exercise or defence of legal claims, then the legal basis won't be the performance of the contract but other legal bases mentioned under Art. 6 GDPR.

3.2.2.1.4 Necessary for taking steps prior to entering into a contract[27]

Some preliminary processing of personal data may be necessary before entering into a contract, so that to facilitate the actual entering into that contract. It should be the data subject making the request in the context of potentially entering into a contract. This provision does not cover unsolicited marketing or other processing carried out solely on the initiative of the data controller or at the request of a third party.

E.g: A data subject contacts a data controller to inquire about its services and to respond to this enquiry, the data controller might need to process some personal data of the data subjects.

3.2.2.2 Court's decisions

3.2.2.2.1 Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV v. Planet49 GmbH, ECJ C-673/17

Planet49, an online gaming company, transferred the personal data of participants in a promotional lottery organised by that company to the company's sponsors and partners. The internet users where asked to provide their postcode, names and addresses. There was a checkbox to tick for that information to be transferred to "certain sponsors and cooperation partners" to receive offers from their "respective commercial sectors". Further information was provided on a link. There was also a second checkbox already ticked where by accepting to take part in the lottery, the internet users also agreed for a web analytics service to set cookies that would analyse their surfing and use behaviour on websites, which would enable to set advertising based on their interests. The internet users could participate in the lottery, only if at least the first checkbox was ticked.

The question was if the consent was validly given.

The ECJ stated that "*the consent referred to in those provisions is not validly constituted if, in the form of cookies, the storage of information or access to information already stored in a*

[24] European Data Protection Board, Guidelines 2/2019 on the processing of personal data under Article 6(2)(b) GDPR in the context of the provision of online services to data subjects Version 2.0, Adopted on 8 October 2019, p. 14-15§48-56, in: https://edpb.europa.eu/our-work-tools/our-documents/smernice/guidelines-22019-processing-personal-data-under-article-61b_en.

[25] European Data Protection Board, Guidelines 2/2019 on the processing of personal data under Article 6(2)(b) GDPR in the context of the provision of online services to data subjects Version 2.0, Adopted on 8 October 2019, p. 15-16§57, in: https://edpb.europa.eu/our-work-tools/our-documents/smernice/guidelines-22019-processing-personal-data-under-article-61b_en.

[26] European Data Protection Board, Guidelines 2/2019 on the processing of personal data under Article 6(2)(b) GDPR in the context of the provision of online services to data subjects Version 2.0, Adopted on 8 October 2019, p. 12-13§40-44, in: https://edpb.europa.eu/our-work-tools/our-documents/smernice/guidelines-22019-processing-personal-data-under-article-61b_en.

[27] European Data Protection Board, Guidelines 2/2019 on the processing of personal data under Article 6(2)(b) GDPR in the context of the provision of online services to data subjects Version 2.0, Adopted on 8 October 2019, p. 13§45-47, in: https://edpb.europa.eu/our-work-tools/our-documents/smernice/guidelines-22019-processing-personal-data-under-article-61b_en.

website user's terminal equipment is permitted by way of a pre-checked checkbox which the user must deselect to refuse his or her consent". Moreover, the information that the service provider must give to a website user includes the duration of the operation of cookies and whether or not third parties may have access to those cookies.

3.2.2.~~3~~1 Questions from members[28]

3.2.2.~~3~~1.1 Notion of "public interest"

Does the notion of "public interest" of Article 6 GDPR also cover the railway business?

"Public interest" could be used for a general economic interest activity provided by a transport company, but not for commercial railway lines. In the first case the contracting entity actually has functions of a public service nature. From a practical point of view though, this could raise some issues if a train is passing from a railway line operated through a public service commitment to a commercial line. Therefore, public interest would not be sufficient to justify the processing of personal data.

The fact that the railway undertaking operating the line is a public or private entity should not matter in any case. This interpretation also emanates from the GDPR, which says in Recital 45: "Where processing is carried out in accordance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, the processing should have a basis in Union or Member State law. This Regulation does not require a specific law for each individual processing. A law as a basis for several processing operations based on a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority may be sufficient. It should also be for Union or Member State law to determine the purpose of processing. Furthermore, that law could specify the general conditions of this Regulation governing the lawfulness of personal data processing, establish specifications for determining the controller, the type of personal data which are subject to the processing, the data subjects concerned, the entities to which the personal data may be disclosed, the purpose limitations, the storage period and other measures to ensure lawful and fair processing. It should also be for Union or Member State law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public authority or another natural or legal person governed by public law, or, **where it is in the public interest to do so**, including for health purposes such as public health and social protection and the management of health care services, **by private law**, such as a professional association" (Recital 45). Recital 128 also states that "The rules on the lead supervisory authority and the one-stop-shop mechanism should not apply where the processing is carried out by public authorities or private bodies in the public interest" (Recital 128).

In some countries, the authorities considered that railway business is in the public interest, even for private train operators.

3.2.3 Conditions for consent (Art. 7 GDPR)[29]

3.2.3.1 Elements of valid consent

A valid consent is (Art. 4(1) GDPR):

1. freely given
2. specific
3. informed and
4. contains no ambiguous indication of the data subject's wishes to consent

3.2.3.1.1. Free/freely given consent

This means a real choice and control for the data subject.

[28] Answers provided by the CIT GS.

[29] For now, only the chapter on consent has been developed completely. This does not mean that consent is a more important legal basis compared to the other legal grounds. The latter will be commented on during the second phase of the revision of the MDP next year.

In the following situations, the consent is in principle not valid:

- No real choice
- The data subject feels compelled to consent
- The data subject will suffer negative consequences if he does not consent
- Consent is a non-negotiable part of terms and conditions
- The data subject is not able to refuse or withdraw his consent without detriment

E.g.: To use a mobile app for photo editing, it is necessary to provide the GPS location; moreover, the app informs the user that the data collected will be used for behavioural advertising purposes. Neither geo-localisation nor online behavioural advertising are necessary for the provision of the photo editing service, but since users cannot use the app without consenting to these purposes, the consent cannot be considered as freely given.

3.2.3.1.2. Specific consent

In the case where a service involves multiple processing operations for several purposes, consent is presumed not to have been freely given if it is not possible for the data subjects to give separate consent for those different processing operations, by consenting for some and not for others. The same applies if there are several purposes and the data subject does not have the possibility to give consent for each of them, i.e. consent needs to be specific.

The consent must be specific in order to ensure a degree of user control and transparency for the data subject.

This means that before asking for consent, it is necessary to:

- Determine a specific, explicit and legitimate purpose for the intended processing activity: Otherwise, it may result in unanticipated use of personal data by the data controller or by third parties and in loss of data subject control. The specific consent can cover different operations if they serve the same purpose. If a controller later on wishes to process the data for a purpose other than the one for which the data subject consented, the data controller will need to seek additional consent for this other purpose. Improving users' experience, marketing purposes, IT security purposes and future research are examples of purposes that are too vague or too general.
- For different purposes, the data controller should provide a separate opt-in for each purpose, to allow users to give specific consent for specific purposes.
- Specific information about the data that are processed for each purpose has to be provided for each separate consent request, so that the data subjects are aware of the impact of the different choices they have.

Example: a retailer uses the same consent request to ask a customer to consent to have his personal data used to send marketing by e-mail as well as to share them with other companies. This is not valid, because there is no separate consent for the two separate purposes. With regard to sending contact details to commercial partners, the data controller will not need to ask for specific consent for each partner if, for all of them, the details are being sent for marketing reasons, but he should provide the identity of each commercial partner at the moment when consent is requested

3.2.3.1.3. Informed consent

It is essential to provide information to the data subject prior to obtaining his consent, otherwise the consent will not be valid. For consent to be informed and therefore valid, the data subject must be provided with the following information:

- **Data controller's identity**: if there are several data controllers that will process the data, they should all be named. On the other hand, the data processors' identities do not need to be given for the consent to be valid, but their identities must be provided in

order to comply with other obligations of the GDPR (Art. 13 and 14 GDPR), which require data controllers to provide a full list of recipients or categories of recipients, including data processors. Therefore, the consent might be valid even if not all the information referred to in Art. 13 and 14 GDPR is mentioned in the process of obtaining consent (but these points will have to be mentioned in other places, such as the company's privacy notice).

- **Purpose of each of the processing operations for which consent is sought**
- **What data will be collected and used**
- **Existence of the right to withdraw consent**
- **Information about the use of the data for automated decision-making**
- **Possible risks of data transfers due to absence of an adequacy decision and of appropriate safeguards**
- **Other information depending on the case**

There is no requirement in the GDPR on the form in which the information has to be provided, e.g. written, oral, audio or video, but the following elements are necessary:

- **Use of clear and plain language:** So the message should be easily understandable to the average person and not only to lawyers;
- **Request for consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form;**
- **No long privacy policies that are difficult to understand or statements full of legal jargon;**
- **Information relevant for making informed consent may not be hidden in general terms and conditions:** e.g.: the declaration of consent must be named as such; wording such as "I know that…" is not sufficient;
- **Information needs to allow the data subjects to easily identify who the data controller is and to understand what they are agreeing to;**
- **Clear description of the purpose for data processing for which consent is requested;**
- **Adapt the way to provide information to the targeted audience:** the data controller cannot use the same language if its targeted audience includes minors;
- **For consent by electronic means, the request must be clear and concise;**
- **If consent is requested as part of a contract, the request for consent should be clearly distinguishable from the other matters, in a way that clearly stands out or in a separate document. It cannot simply be a paragraph with terms and conditions.**

Example: an undertaking could organise a panel test to determine if the information sheet it wants to provide is understandable. If the result of the panel test is positive, the report of that test should be kept as a reference.

Example: if the identity of the controller or the purpose of the processing is not apparent from the first information layer of the layered privacy notice and is located in further sub-layers, it will be complicated for the data controller to demonstrate that the data subject has given informed consent, unless the data controller can show that the data subject in question accessed that information prior to giving consent.

3.2.3.1.4. Unambiguous indication of wishes, in particular in the digital context

Consent requires an active motion or declaration; it can be a written (many different shapes and sizes) or (recorded) oral statement (if national contract law admits it and if due note is taken of the information available to the data subject prior to the indication of consent), including by electronic means.

The use of pre-ticked opt-in boxes or opt-out constructions is invalid as consent, as well as silence or inactivity or the fact that the data subject is merely proceeding with a service. Blanket acceptance of general terms and conditions cannot be seen as a clear affirmative action to consent.

Data controllers should design consent mechanisms in ways that are clear to data subjects. Data controllers must avoid ambiguity and must ensure that the action by which consent is given can be distinguished from other actions. Therefore, merely continuing the ordinary use of a website is not conduct from which one can infer an indication of wishes by the data subject to signify his or her agreement to a proposed processing operation.

On the other hand, and for the CIT GS quite unclear, is the affirmation in the GDPR stating that when consent is to be given following a request by electronic means, the request for consent should not be unnecessarily disruptive to the use of the service for which the consent is provided. The EDPB specified though that an active affirmative motion by which the data subject indicates consent can be necessary when a less infringing or disturbing modus would result in ambiguity; thus it may be necessary that a consent request interrupts the use experience to some extent to make that request effective.

Example: message on the screen saying that if “you swipe this bar to the left, you agree to the use of information X for purpose Y. Repeat the motion to confirm” would be a way to get consent; or waving in front of a smart camera, turning a smartphone around clockwise or in a figure eight motion, as long as the data controller is able to demonstrate that consent was obtained this way and data subjects must be able to withdraw consent as easily as it was given.

Example: Scrolling down or swiping through a website will not satisfy the requirement of a clear and affirmative action, because such an action is not sufficiently unambiguous.

Consent should be given prior to the processing activity. In principle, it may be sufficient to ask for consent once, but if the purposes for data processing change or if an additional purpose is envisaged, then a new and specific consent needs to be obtained.

3.2.3.1.5 Additional conditions for obtaining valid consent

There are also additional conditions to obtain valid consent:

- **Demonstrate consent:** the burden of proof is on the data controller. As long as a data processing activity lasts, the obligation to demonstrate consent exists. After the data processing activity ends, the proof of consent should be kept no longer then strictly necessary for compliance with a legal obligation or for the establishment, exercise or defence of legal claims [Art. 17(3)(b) and (e) GDPR]. There is no time limit in the GDPR for how long consent will last, but it will depend on each case. The best option would be to refresh the consent at appropriate intervals by providing all the information again, to ensure the data subject remains well informed.
- **Withdrawal of consent:** The data controller must ensure that consent can be withdrawn by the data subject as easily as giving consent and at any given time. Giving and withdrawing consent does not need to take place through the same action, but if consent was given in an easy way, withdrawing consent should not be more complicated. For example, if consent was obtained through the use of a service-specific user interface, such as a website, an app or by e-mail, the data subject must be able to withdraw consent via the same electronic interface, because if he needs to use another interface just for withdrawal, this would require undue effort. If consent is withdrawn, all data processing operations which were based on consent and took place before the withdrawal of consent remain lawful. However, the data controller must stop the processing actions concerned; if there is no other lawful basis justifying the processing (e.g. further storage) of the data, they should be deleted by the data controller. Data controllers have to delete

data that were processed on the basis of consent once that consent is withdrawn, assuming that there is no other purpose justifying the continued retention. A data subject may also request erasure of other data concerning him that is processed on another lawful basis. Data controllers are also obliged to assess automatically whether continuing to process the data in question is appropriate, even in the absence of an erasure request by the data subject. If the data subject withdraws his consent and the controller wishes to continue to process the personal data on another lawful basis, he cannot silently migrate from consent which is withdrawn to this other lawful basis - he needs to notify the data subject in accordance with the information requirements in Art. 13 and 14 GDPR and under the general principle of transparency.

- **No coercion:** If the data subject refuses or withdraws his consent, he should not face, for example, any costs, deception, intimidation, coercion or significant negative consequences. Otherwise, the consent is not freely given and there is no genuine choice.
    - Example: a lifestyle mobile app asks for consent to access the phone's accelerometer. This is not necessary for the app to work, but it is useful for the data controller to know the movements and activity levels of its users. If the user revokes his consent and because of that, the app works only to a limited extent, then the consent was not validly obtained, because the withdrawal was linked to detrimental effects. Therefore, the data controller will have to delete all personal data on the users' movements collected this way.
    - Example: A data subject subscribes to a fashion retailer's newsletter with general discounts. The retailer asks for consent to collect more data on shopping preferences, so as to send personalised fashion discounts. When the data subject revokes his consent, he will receive non-personalised fashion discounts again. Here, there is no detrimental effect on the data subject, so the consent was valid.

Withdrawal has to be possible without detrimental effect, i.e. free of charge or without lowering service levels. Example: a music festival sells tickets through an online ticket agent and when buying a ticket, consent is requested to use contact details for marketing purposes. To indicate consent, it is just necessary for the customer to select yes or no. But to withdraw consent, the customer needs to contact a call centre which is open only during working hours free of charge; this is not compliant with GDPR, because this is more burdensome than a mouse click 24/7.

3.2.3.1.6 Data subject's rights

In case of consent, data subjects have the right to data portability. But they do not have the right to object to the data processing, even if the right to withdraw will provide a similar outcome.

Data subjects also have the right to erasure when consent has been withdrawn and the right to restriction, rectification and access.

3.2.3.2 Consent in specific situations

3.2.3.2.1 Consent and electronic communications[30]

The procedure for the adoption of a Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications, also called ePrivacy Regulation) is still ongoing (as at 15 December 2019): Originally, the ePrivacy Regulation should have been in force at the same time as the GDPR. This deadline could not be met.

There is an important interconnection between the GDPR and the ePrivacy Regulation. The ePrivacy Regulation will be a lex specialis in the field of publicly available electronic communications services in public communication networks.

Nevertheless, on some topics, the ePrivacy Regulation will refer to the GDPR, for example regarding the requirements for consent. Therefore, the GDPR conditions for obtaining valid

[30] From: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.

consent are applicable in situations falling within the scope of the current e-Privacy Directive (Directive 2002/58/EC) and the future ePrivacy Regulation.

As stated by the EDPB, under the future ePrivacy Regulation, consent will also play an important role: “Organisations are likely to need consent under the ePrivacy instrument for most online marketing messages or marketing calls, and online tracking methods including by the use of cookies or apps or other software”[31].

3.2.3.2.2 Consent and employment

In the field of labour, it is problematic to use consent for the processing of personal data.

The employee is certainly in a dependent relationship with his employer. Therefore, he will not take the risk of denying his consent to data processing, because he might fear detrimental effects. For example, an employee might be afraid to refuse to consent to the activation of monitoring systems, such as camera observation in a workplace or to fill out assessment forms.

In some situations though, consent might be used, but only in exceptional circumstances, when it will have no adverse consequences at all, whether or not the employee gives his consent. For example, a film crew is filming in the company and the employer asks his employees to give their consent to be filmed; they can refuse and change the filming location.

Imbalances of power can also occur in other situations, not only in the field of employment, as soon as there is a risk of deception, intimidation, coercion or significant negative consequences, such as substantial extra costs. If there are elements of compulsion, pressure or inability to exercise free will, then consent has not been freely given.

3.2.3.2.3 Consent and (transport) contract

Consent is presumed not to be freely given if it is tied to the acceptance of terms or conditions or to the provision of a contract or a service, even though the personal data requested are not necessary for the performance of that contract or service. The processing of personal data for which consent is sought cannot as a matter of fact become the counter-performance of a contract, whether directly or indirectly. It is not therefore possible to blur the two lawful grounds for processing personal data: contract and consent.

As stated by the EDPB, “If a controller seeks to process personal data that are in fact necessary for the performance of a contract, then consent is not the appropriate lawful basis”[32]. The appropriate lawful basis in this case could be the performance of the contract.

It is important to determine the scope of the contract and what personal data would be necessary to perform it. The term “necessary for the performance of a contract” needs to be interpreted strictly; there needs to be a direct and objective link between the processing of the data and the purpose of the execution of the contract. For example: for a sales agreement, the address and credit card details of the data subject to deliver goods purchased online; for a contract of employment, bank account details to pay the salary to the employee.

The data controller therefore needs to be especially careful when a contract (which could include the provision of a service) has a request for consent to process personal data tied to it.

If a data controller chooses to rely on consent for any part of the processing, he must be prepared to respect that choice and stop that part of the processing if an individual withdraws consent. It would not be fair to an individual to send out the message that data will be processed on the basis of consent if other lawful bases are relied on. So a data controller cannot change from consent to other lawful bases as it wishes. For example, it would not be allowed to use another legal basis retrospectively, such as the legitimate interest basis, in order to justify processing, where problems have been encountered with the validity of consent. Because of the requirement to disclose the lawful basis which the controller is relying upon at the time of collection of personal data, data controllers must have decided prior to collection what the applicable lawful basis is.

[31] Article 29 Working Party, Guidelines on consent under Regulation 2016/679 Adopted on 28 November 2017, as last Revised and Adopted on 10 April 2018, p. 4, in: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.
[32] Article 29 Working Party, Guidelines on consent under Regulation 2016/679 Adopted on 28 November 2017, as last Revised and Adopted on 10 April 2018, p. 8, in: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.

In the railway sector[33], railway undertakings regularly process personal data of their customers. This raises issues regarding the lawful basis to process such data. Special attention should therefore be paid to the reason why those personal data are processed. There may be various purposes:

- For the transport of the passenger
- For the handling of passenger claims, or passenger requests for information or reimbursement
- For marketing purposes

The passengers and the railway undertakings are bound by a transport contract. The main obligations of the parties in this contract are the carriage and the payment of the price. As mentioned above, the scope of the contract will determine whether the data processed have to be considered necessary for the performance of a contract. Regarding the purposes mentioned above, we have to ask:

1) Do they fall under the scope of the transport contract?
2) If so, which personal data are necessary for the performance of this contract?

For the transport of the passenger:
The information needed depends on different factors:

- For Rail Pass Ticket: The performance of the contract would justify the processing of the following data: first name and last name of the passenger will be necessary, a copy of the ID card and the passenger's country of residence. With regard to payment of the price, it will be necessary to pay by credit card for online booking (therefore the credit card number will have to be provided) and the address will also need to be given to send the documents.
- For Non (integrated) Reservation Ticket: it should be possible to buy such a ticket completely anonymously, e.g. if a passenger buys it at the ticket office by paying cash. Nevertheless, if the passenger buys it online, at the time of payment he will have to provide personal data (name, surname, credit card number; or if he pays per invoice, his address and e-mail address so that the e-ticket can be sent); regarding e-tickets, for some technical and security reasons, the name and surname have to be given when buying the ticket, so that the controller on board can check that the ticket has not been used several times.
- For integrated Reservation Ticket: In some countries, the reservation is linked to the name of the passenger. Here also the same remarks as for NRT apply[34].
- Date of birth? the processing of the above-mentioned information would fall under the scope of the performance of the contract, so no consent would be necessary. Railway undertakings also often request the date of birth; it is doubtful if this information can be requested, except to verify whether the passenger is old enough for his personal data to be processed or to enter into a contractual relationship.
- What about facilities on board? the above-mentioned personal data are collected for the railway undertaking to be able to carry the passenger. Nevertheless, passengers often have some online facilities on board, such as WiFi or the possibility of ordering online from the mini-bar. These are facilities which do not fall under the scope of the transport contract. Therefore, the transport contract cannot be used to justify the processing of

[33] The following considerations are not from the EDPB Guidelines, but are reflexions of the CIT GS. Like the rest of this manual, they are only of a recommendatory nature. This should not be considered as legal advice either, but only as guidance.
[34] See also on this matter the Code of Conduct for Booked Public Passenger Transport Journeys in Sweden established by Samtrafiken, a company owned by transport companies.

personal data for such facilities on board. The processing can be justified through the service contract, which in this case will be contracted out.

For the handling of passenger claims or passenger requests for information or reimbursement:
This is a grey zone; the opinions of railway undertakings differ. Some consider these to be aspects that fall under the scope of the transport contract, others do not. For the CIT GS, it is possible to consider that these are all aspects that result from improper performance of the contract. Therefore, they would fall under the scope of the contract and would not necessitate further justification in addition to performance of the contract. It would also be possible to use the legitimate interest of the data controller as justification for the processing of such information; otherwise, it will not be able to handle the request. Consent might not be a suitable justification in this case, since it would not be freely given consent; indeed, if the passenger wants to be reimbursed or receive compensation, he will have no other choice than to provide personal data. Nevertheless, several railway undertakings still share the opinion that consent would be the most secure option (because it would be easier to prove) and some national authorities also consider that for online sales and claims handling, consent is necessary. In all cases, it is important to inform the customer about the processing, the personal data that will be processed and the purpose of the processing. The personal data to provide would be:

- For handling of claims or reimbursement: if the passenger requests compensation or reimbursement, he will have to provide his name, surname and certainly his bank account. If he just wants to complain without asking for compensation, he should be able to do so anonymously.
- For information: if a passenger requests information, he should be able to provide as little information as possible, e.g. just an e-mail address to get an answer.

For marketing purposes:
This is completely unrelated to the performance of the transport contract. Therefore, to process personal data for marketing purposes, the CIT GS advises requesting the passenger's consent before doing so. This is corroborated by the EDPB, which, while referring to the future ePrivacy Regulation, stated that: "Organisations are likely to need consent under the ePrivacy instrument for most online marketing messages or marketing calls, and online tracking methods including by the use of cookies or apps or other software" [35].

Furthermore, companies quite often refer to a long list of purposes for which the personal data will be used; this is nevertheless not a proper way to act, since it is important that the passenger is informed specifically and clearly about the different purposes and operations and he should also have the opportunity to say which purpose he agrees to and which he does not agree to, as described later on in this manual.

Some railway undertakings refer in practice to other legal grounds to justify the processing of personal data as regards marketing, such as the legitimate interest for processing personal data for general travel-based marketing; for advanced personalised marketing, these railway undertakings use the performance of contracts as a lawful ground, since they offer loyalty programmes, for which membership conditions apply.

3.2.3.2.4 Consent given prior to the applicability of the GDPR

Consent obtained before the entry into force of the GDPR continues to be valid if it is in line with the conditions laid down in the GDPR. For example, the GDPR requires that a data controller must be able to demonstrate that valid consent was obtained, so all presumed consents of which no references are kept will automatically be below the consent standard of the GDPR and will need to be renewed. For example, all presumed consents that were based on a more implied form of action by the data subject (such as a pre-ticked opt-in box) will also not meet the GDPR standard of consent. If the consent previously obtained under the old legislation does not meet the standard of GDPR consent, then the data controllers must undertake action to comply with these standards, for example by refreshing consent in a GDPR-compliant way.

[35] Article 29 Working Party, Guidelines on consent under Regulation 2016/679 Adopted on 28 November 2017, as last Revised and Adopted on 10 April 2018, p. 4, in: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.

Under the GDPR, it is not possible to switch between one lawful basis and another. If a data controller is unable to renew consent in a compliant way and is also unable – as a one-off situation – to make the transition to be GDPR compliant by basing data processing on a different lawful basis while ensuring that continued processing is fair and accounted for, the processing activities must be stopped. In any event the data controller needs to observe the principles of lawful, fair and transparent processing.

3.2.3.3 Court's and authorities' decisions

[To be drafted]

3.2.3.~~3~~4 Questions from members[36]

3.2.3.~~4~~3.1 Inquiry about satisfaction on the handling of complaints

CIT members asked whether, in the case where a customer does not give his consent to use his personal data for commercial purposes, but only for handling of complaints, the railway undertaking is still allowed to contact this customer to inquire if he was satisfied about the handling of his claim or if the consent statement should include an explicit reference to quality management.

There is no consensus on that matter among the CIT members. Some consider that this would fall under the carrier's responsibility to handle claims to the customer's entire satisfaction, so the carrier would have a legitimate interest to process the personal data. This solution makes sense if the carrier justifies the handling of claims under a legal basis other than consent [see the legitimate interest of Art. 6 §1(f) GDPR]. If the carrier uses consent as a legal basis, then it would make sense, as seen under Point 3.2.3 Conditions of consent, also to specify that one of the purposes of processing will also be to find out whether customer is satisfied.

3.2.3.~~4~~3.2 Consent and cookies

A customer buys tickets online on a website and enters his e-mail address for that purpose. He returns to that website a second time to check fares and timetables anonymously (without logging in this time) and does not book anything. However, he later receives an e-mail with marketing information about the trains and destinations he just checked. The question is whether this is in line with the GDPR.

This raises issues regarding GDPR. The customer must be informed when visiting the website and when booking that such targeting methods are being used on the website. He needs to give prior consent to the distribution of such e-mails and for such marketing activities.

This also raises questions relating to cookies. A lot of websites already have notifications about the use of cookies. Such notifications must include information about the use of cookies.

The Dutch Data Protection Agency spoke critically on this matter[37]. It mentioned that it had received many complaints from internet users who had their access to websites blocked after refusing to accept tracking cookies. It published guidance on this issue. It made it clear that "internet visitors must be asked for permission in advance for any tracking software to be placed – such as third-party tracking cookies; tracking pixels; and browser fingerprinting tech – and that that permission must be freely obtained. Ergo, a free choice must be offered". It shared the opinion that cookie walls do not comply with the principles of consent of the GDPR. This would mean that if internet users cannot navigate on a website without accepting all the cookies used on that website (not only site-functional cookies, but also advertising cookies), there is no free choice and the consent given would not be valid. On the other hand, some would say that the website owner is free to limit access to its website to users who are prepared to accept all the cookies. With regard to this issue, it will also be important to wait for the entry into force of the e-Privacy Regulation, to see if it provides clearer rules.

3.2.3.~~4~~3.3 Transfer of information with personal data from the allocator to the train controller, for the checking of tickets on the train

A CIT member inquired whether the allocator needs to inform the customer that his personal data (or parts of it) has been transferred to the TCO of the train in question for ticket control (in some cases the TCO can be a completely external partner or another railway undertaking,

[36] Answers provided by the CIT GS.
[37] See: http://snip.ly/wu63c3#https://techcrunch.com/2019/03/08/cookie-walls-dont-comply-with-gdpr-says-dutch-dpa/.

not the railway undertaking being the allocator), and whether that allocator must keep track of such personal data transfers.

This is a question on which there is no consensus among the CIT members, since some use consent in the different situations relating to the transport contract and others use the legal basis of the fulfilment of the contract as justification, or other legal obligations. Here also, it is in all the cases important that the allocator/issuer informs the customer that personal data may be transferred to third parties, including other carriers involved.

3.2.3.~~4~~3.4 Consent for night trains

A CIT member has created a form where the night train passenger agrees, through his signature, that he will give the rail pass + night train supplements to the on-board staff for ticket control at night. In this case it is therefore not only the name, the passport number and the date of birth, but also the ticket itself, which are collected by the sleeper/couchette attendant on the night train (not always being the same staff controlling the tickets on the night train) and these sleeper/couchette attendants are not employed by the railway undertaking. The tickets are kept for the night in the locked compartment of the sleeper/couchette attendant and given back to the passenger in the morning. If the passenger does not agree to hand over his rail pass ticket and reservations, he will be awakened at night when the night train crosses into another country.

The CIT GS responded that as long as the passenger may choose freely whether or not to hand over his rail pass, there are no concerns with this solution, because it is merely a service. Oral information would have been enough, and consent is already proved by the action of the passenger's giving the ticket to the staff.

3.2.4 Conditions applicable to child's consent in relation to information society services (Art. 8 GDPR) [38]

This concerns in particular (but not only, e.g. collection of children's personal data also falls under the scope of this Article) the purposes of marketing and creating personality or user profiles for children.

Article 8 GDPR applies only if:

1. The processing is related to the offer of information society services directly to a child:
    a. "Information society service": "Information society services" cover contracts and other services that are concluded or transmitted online. Where a service has two economically independent components, one being the online component such as the offer and the acceptance of an offer in the context of the conclusion of a contract or the information relating to products or services, including marketing activities, this component is defined as an information society service. The other component, being the physical delivery or distribution of goods, is not covered by the notion of an information society service. It includes the online delivery of a service. An information society service forming an integral part of an overall service whose main component is not an information society service (e.g. a transport service) must not be qualified as an information society service.
    b. "Offered directly to a child": For example, if an information society service provider makes it clear to potential users that it is only offering its service to persons aged 18 or over, and this is not undermined by other evidence (such as the content of the site or marketing plans) then the service will not be considered to be "offered directly to a child" and Article 8 GDPR will not apply.
2. The processing is based on consent

When consent applies, there are different age limits applicable regarding the child:

- Child ≥ 16 years old → processing is lawful

[38] From: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.

- Child between 13-16 years old → it depends on national law. The data controller must be aware of those national laws. It is important for him to take into account the public targeted by its services. If the data controller provides a cross-border service, it cannot always rely on complying only with the law of the Member State in which it has its main establishment, but may also need to comply with the respective national laws of each Member State in which it offers the information society service(s). This depends on whether a Member State chooses to use the main place of establishment of the data controller as a point of reference in its national law, or the residence of the data subject.
- Child < 13 years old → processing is unlawful, except if the holder of parental responsibility gives or authorises consent.

When providing information society services to children on the basis of consent, data controllers will be expected to make reasonable efforts to verify that the user is over the age of digital consent, and these measures should be proportionate to the nature and risks of the processing activities. If the users state that they are over the age of digital consent then the data controller can carry out appropriate checks to verify that this statement is true, because if the child is not old enough to provide valid consent on his own behalf, then this will render the processing of data unlawful. If the child states that he is below the age of digital consent then the data controller can accept this statement without further checks but he will need to go on to obtain parental authorisation and verify that the person providing that consent is a holder of parental responsibility.

In some low-risk situations, it may be appropriate to require a new subscriber to a service to disclose his year of birth or to fill out a form stating that he is (not) a minor. If doubts arise, the controller should review its age verification mechanisms in a given case and consider whether alternative checks are required.

The information to provide in order to obtain valid consent must be understandable to the audience addressed by the data controller, paying particular attention to the position of children. In order to obtain informed consent from a child, the data controller must explain in language that is clear and plain for children how it intends to process the data it collects. If it is the parent that is supposed to consent, then a set of information may be required that allows adults to make an informed decision.

What is reasonable, both in terms of verifying that a user is old enough to provide his own consent, and in terms of verifying that a person providing consent on behalf of a child is a holder of parental responsibility, may depend upon the risks inherent in the processing as well as the available technology. In low-risk cases, verification of parental responsibility via email may be sufficient. Conversely, in high-risk cases, it may be appropriate to ask for more proof, so that the controller is able to verify and retain the information. For example, an online gaming platform wants to make sure underage customers only subscribe to its services with the consent of their parents or guardians. The controller follows these steps: Step 1: Ask the user to state whether he is under or over the age of 16 (or alternative age of digital consent). If the user states that he is under the age of digital consent: Step 2: The service informs the child that a parent or guardian needs to consent or authorise the processing before the service is provided to the child. The user is requested to disclose the email address of a parent or guardian. Step 3: The service contacts the parent or guardian and obtains his consent via email for processing those personal data and takes reasonable steps to confirm that the adult has parental responsibility. Step 4: In case of complaints, the platform takes additional steps to verify the age of the subscriber. As a general rule, data controllers should avoid verification solutions which themselves involve excessive collection of personal data.

When the child comes of age, consent by a holder of parental responsibility or authorised by a holder of parental responsibility for the processing of personal data of children can be confirmed, modified or withdrawn, once the data subject reaches the age of digital consent. So if the child does not take any action, the consent will remain a valid ground for processing. But the data controller needs to inform the child about the possibility of withdrawing consent himself.

The GDPR does not deal with the question of whether it is lawful for a minor to conclude online contracts though; this is a matter that concerns national law.

3.2.5 Processing of special categories of personal data (Art. 9 GDPR) [39]

3.2.5.1 Definition of "special categories of personal data"

Special categories of personal data, so called "sensitive data", are defined in the GDPR as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as 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.

3.2.5.2 Lawful grounds for processing sensitive data

Different lawful grounds can be used to justify the processing of sensitive data.

3.2.5.2.1 Explicit consent

Explicit consent is needed in cases where serious data protection risks emerge, which means:

- Sensitive data
- Data transfers to third countries or international organisations in the absence of adequate safeguards
- Automated individual decision-making including profiling

Express statement of consent means:

- e.g. written statement,
- filling in an electronic form,
- sending an e-mail,
- uploading a scanned document carrying the signature of the data subject,
- using an electronic signature,
- Oral statement would be difficult to prove as express statement. But an organisation may also obtain explicit consent through a telephone conversation, provided that the information about the choice is fair, intelligible and clear, and the organisation asks for specific confirmation from the data subject (e.g. pressing a button or providing oral confirmation).
- For example, a data controller may also obtain explicit consent from a visitor to its website by offering an explicit consent screen that contains "Yes and No check boxes", provided that the text clearly indicated the consent, for instance: "I hereby consent to the processing of my data" and not for instance "It is clear to me that my data will be processed".
- Two stage verification of consent can also be an option, e.g. a data subject receives an e-mail notifying him of the controller's intent to process a record containing medical data. The data controller explains in the e-mail that he is requesting consent for the use of a specific set of information for a specific purpose. If the data subject agrees to the use of this data, the data controller asks him for an e-mail reply containing the statement "I agree". After the reply is sent, the data subject receives a verification link that must be clicked, or an SMS message with a verification code, to confirm agreement.

The performance of a contract is not an exception that permits the processing of sensitive data. Therefore, in such a situation, the data controller should first analyse the other conditions of Article 9 GDPR and if none of them apply, then he should analyse the explicit consent.

For example, travel from Brussels to Paris by rail of a person with reduced mobility. The railway company offers an assisted travelling service for passengers that cannot travel unassisted. To be able to arrange the appropriate services for the passenger, the undertaking requires him to

[39] From: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.

provide information on his state of health. The railway undertaking asks for explicit consent to process the health data for the purpose of arranging the requested travel assistance. The data processed on the basis of consent should be necessary for the requested service. Moreover, the travel should remain available without travel assistance.

3.2.5.3 Courts' and authorities' decisions

3.2.5.3.1 Swedish Government Official Reports (SOU 2003:87) on processing of sensitive data based on "public interest"

The Swedish Government analysed different questions in anticipation of proposed Swedish legislation. One of them was related to a transport company that coordinates taxi and assistance services.

The Swedish Government considered that "public interest" was a lawful ground to process sensitive data, if the aim of this processing was to provide assistance to a passenger. Indeed, it considered that there was a public interest for travellers not to be discriminated against based on disabilities.

3.2.5.4 Questions from members[40]

3.2.5.4.1 Social protection law and sensitive data of disabled persons and persons with reduced mobility

Can the "social protection law" mentioned in Article 9 let. b GDPR justify the processing of sensitive data (such as health data of persons with reduced mobility in the booking assistance)?

For the purpose of carrying passengers with disabilities or passengers with impaired mobility and orientation, it might be possible to apply Article 9(2)(b) of the GDPR (social protection law) as justification for the processing of sensitive data of disabled persons and persons with reduced mobility, because the term "social protection" can also include, in a wider context, the legal obligation of carriers to ensure non-discriminatory rules for transport of this group of people.

Nevertheless, it might be easier to use another legal basis.

3.2.5.4.2 Sensitive data and COVID-19

With the pandemic of COVID-19, many sensitive data had to be processed by railway undertakings about their passengers but also about their employees. How is it in line with GDPR?

Processing of personal data concerning health shall be prohibited. BUT except for the reasons mentioned under Art. 9 GDPR.

The EDPB released a statement on that matter[41].

According to the EDPB, "*In the employment context, the processing of personal data may be necessary for compliance with a legal obligation to which the employer is subject such as obligations relating to health and safety at the workplace, or to the public interest, such as the control of diseases and other threats to health. The GDPR also foresees derogations to the prohibition of processing of certain special categories of personal data, such as health data, where it is necessary for reasons of substantial public interest in the area of public health (Art. 9.2.i), on the basis of Union or national law, or where there is the need to protect the vital interests of the data subject (Art. 9.2.), as recital 46 explicitly refers to the control of an epidemic*".

Recital 46 GDPR states indeed that: "*The processing of personal data should also be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis. Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and*

[40] Answers provided by the CIT GS.

[41] European Data Protection Body, Statement on the processing of personal data in the context of the COVID-19 outbreak, Adopted on 19 March 2020, in: https://edpb.europa.eu/our-work-tools/our-documents/other/statement-processing-personal-data-context-covid-19-outbreak_en.

their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters ».

3.2.6 Processing of personal data relating to criminal convictions and offences (Art. 10 GDPR)

[To be drafted ~~by June 2020~~]

3.2.7 Processing which does not require identification (Art. 11 GDPR)

[To be drafted ~~by June 2020~~]

3.3 Rights of the data subject (Chapter III GDPR)

3.3.1 Transparency and modalities: Transparent information, communication and modalities for the exercise of the rights of the data subject (Art. 12 GDPR)

[To be drafted ~~by June 2020~~]

3.3.2 Information and access to personal data: Information to be provided where personal data are collected from the data subject (Art. 13 GDPR)

~~3.3.2.1 Courts' and authorities' decisions[To be drafted by June 2020]~~

3.3.2.1.1 Videosurveillance of employees, ECHR-Grand Chamber, Case Lopez Ribalda and Others v. Spain (Applications nos. 1874/13 and 8567/13)

An employer in a Spanish supermarket discovered inconsistencies between his store's inventory level and sales figures. Having suspicions of theft, he decided to install surveillance cameras. While some were visible and oriented towards the entrances and exits of the store, others were hidden and directed towards the cash registers. Beforehand, the employer informed the Spanish Data Protection Agency of his intention to set up surveillance cameras. It also installed a sign announcing the existence of such video surveillance.

Hidden cameras allowed the employer to discover that several employees were actually robbing money. Those employees were immediately fired, unable to view the recordings.

The ECHR analysed the case in the light of Article 8 Convention for the Protection of Human Rights and Fundamental Freedoms.

It considered different elements: if the employee had been informed beforehand of the possibility of such monitoring and of its implementation, the extent and degree of intrusion into the privacy of surveillance, if the surveillance was justified on legitimate grounds, if there were other less intrusive measures to achieve the same goal, what were the consequences of surveillance for the employee and if the employee did have adequate guarantees.

Regarding the degree of intrusion of video surveillance, the ECHR stressed that it is necessary to distinguish the different places in which it is carried out. While intrusion is very serious in intimate places like in toilets and changing rooms, it is only serious in closed work spaces like offices and the intrusion is reduced in places visible or accessible to people, colleagues or a large audience. In this case, it was carried out in a place open to the public. The intrusion was therefore not significant. Furthermore, although the employer had not previously fixed the duration of the surveillance, the surveillance lasted only ten days. It was also based on legitimate grounds, namely suspicion of theft.

Then the Court spoke about the right of information and stated: "*Given the importance of the right to information in such cases, the Court finds that only an overriding requirement relating to the protection of significant public or private interests could justify the lack of prior information*" (Judgment, Recital 133).

The EHCR mentioned that the Spanish Courts did not take into account the absence of information given to employees by the employer. The Grand Chamber nevertheless put this failure into perspective due to the margin of appreciation available to the national authorities and the particular circumstances of the case. In fact, the employer had reasonable suspicion, which arose from the concerted action of several employees. The national courts could therefore

consider that the invasion of the employees' privacy caused by the secret video surveillance was proportionate.

In addition, the EHCR noted that the employees had other guarantees. They could therefore appeal to the Data Protection Agency, which could sanction the employer. They could also sue the employer for compensation for the alleged breach of the data protection law.

The Court therefore concluded that the national authorities had not failed in their obligations under art. 8 of the Convention so as to exceed their margin of appreciation.

3.3.3 Information and access to personal data: Information to be provided where personal data have not been obtained from the data subject (Art. 14 GDPR)

[To be drafted ~~by June 2020~~]

3.3.4 Information and access to personal data: Right of access by the data subject (Art. 15 GDPR)

[To be drafted ~~by June 2020~~]

3.3.5 Rectification and erasure: Right to rectification (Art. 16 GDPR)

3.3.5.1 Questions from members[42]

3.3.5.1.1 Change of personal data on request by the passenger

A CIT member inquired whether a railway undertaking can ask for payment for the “service” of changing a passenger’s personal data (e.g. a change of name due to marriage).

This is different from a situation where the passenger asks the seller to reissue a ticket under the name of another person, which is considered to be a refund of the old ticket and the issuance of a new ticket.

According to Article 12(5) of the GDPR, in the first case, such personal information has to be corrected free of charge. A reasonable fee relating to administrative costs can be charged only if requests for data rectification/update are manifestly unfounded or excessive, in particular if such requests are repetitive.

3.3.6 Rectification and erasure: Right to erasure (“right to be forgotten”) (Art. 17 GDPR)

[To be drafted ~~by June 2020~~]

3.3.7 Rectification and erasure: Right to restriction of processing (Art. 18 GDPR)

[To be drafted ~~by June 2020~~]

3.3.8 Rectification and erasure: Notification obligation regarding rectification or erasure of personal data or restriction of processing (Art. 19 GDPR)

[To be drafted ~~by June 2020~~]

3.3.9 Rectification and erasure: Right to data portability (Art. 20 GDPR)

[To be drafted ~~by June 2020~~]

3.3.10 Right to object and automated individual decision-making: Right to object (Art. 21 GDPR)

[To be drafted ~~by June 2020~~]

3.3.11 Right to object and automated individual decision-making: Automated individual decision-making, including profiling (Art. 22 GDPR)

[To be drafted ~~by June 2020~~]

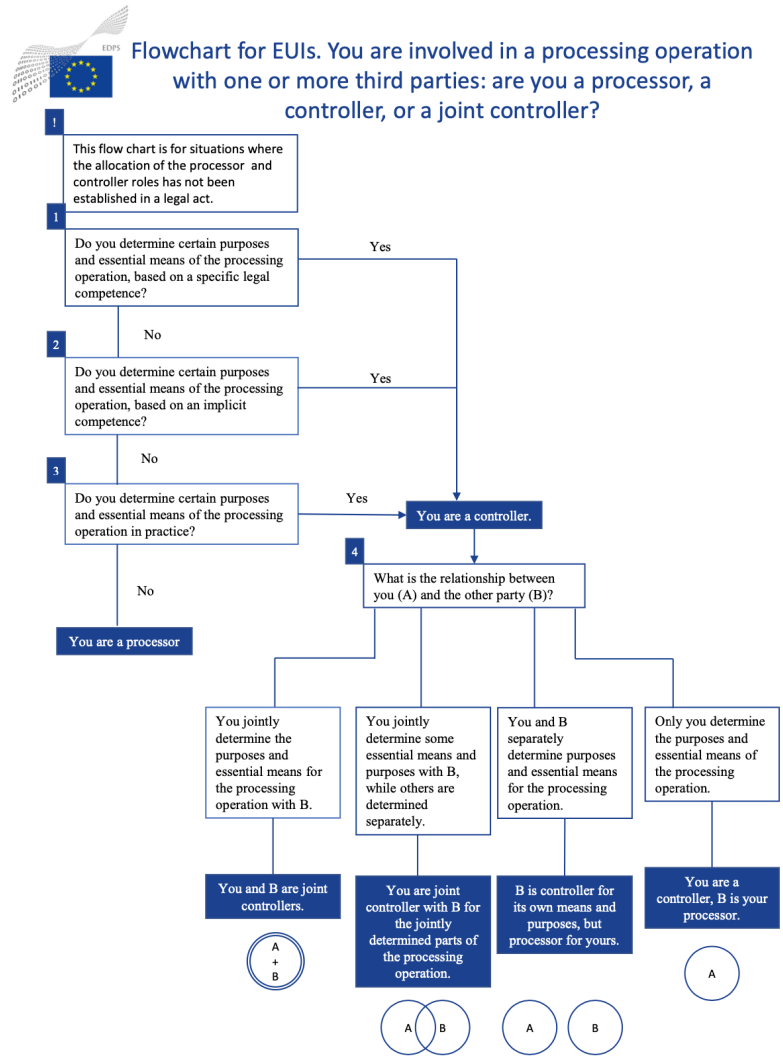
3.3.12 Restrictions: Restrictions (Art. 23 GDPR)

[To be drafted ~~by June 2020~~]

[42] Answers provided by the CIT GS.

3.4 Controller and processor (Chapter IV GDPR)

This flowchart published by the European Data Protection Supervisor describes how to distinguish data controller, data processor and joint controller[43]: ~~[To be drafted by June 2020]~~



Note: The aim of this flowchart is to clarify the initial qualification as controller or processor, rather than setting out what happens when a processor exceeds its mandate/role by becoming involved in determining essential means of the processing.

3.4.1 General obligations: Responsibility of the controller (Art. 24 GDPR)

3.4.2 General obligations: Data protection by design and by default (Art. 25 GDPR)

3.4.3 General obligations: Joint controllers (Art. 26 GDPR)

3.4.3.1 Courts' and authorities' decisions

3.4.3.1.1 Notion of joint controller, ECJ C-40/17

In the case Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV, the ECJ had to define the notion of joint controller and the question of consent in relation to social networks.

Fashion ID was an online fashion clothing business. It placed the Facebook "Like" button on its website. Thanks to the insertion of this button, Facebook received from Fashion ID personal data of each visitor of this company's site, without them being informed and regardless of whether they were registered on Facebook or clicked on the "like" button.

[43] European Data Protection Supervisor, Flowchart for EUIs, in : https://edps.europa.eu/sites/edp/files/publication/19-11-19_flowchart_controllership_en.pdf.

The Verbraucherzentrale NRW, an association of public utility defending the interests of consumers, criticized Fashion ID for having transmitted to Facebook personal data belonging to visitors of its website, on the one hand, without their consent and, on the other hand, in violation of the information obligation provided for by the provisions relating to the protection of personal data.

The Oberlandesgericht of Düsseldorf, competent to settle this dispute, seized the ECJ so that it determines in particular (i) if the manager of an Internet site which inserts the button "like "of Facebook must be considered as co-responsible for the processing and (ii) if, if necessary, this manager must first obtain the consent of the site visitor as well as inform him of his rights.

The ECJ reminded that under Directive 95/46/EC, the notion of data controller is defined "broadly as the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data (see, to that effect, judgment of 5 June 2018, Wirtschaftsakademie Schleswig-Holstein, C-210/16, EU:C:2018:388, paragraphs 26 and 27)" (ECJ C-40/17 Recital 65).

The ECJ clearly stated that: "*it appears that a natural or legal person may be a controller, within the meaning of Article 2(d) of Directive 95/46, jointly with others only in respect of operations involving the processing of personal data for which it determines jointly the purposes and means. By contrast, and without prejudice to any civil liability provided for in national law in this respect, that natural or legal person cannot be considered to be a controller, within the meaning of that provision, in the context of operations that precede or are subsequent in the overall chain of processing for which that person does not determine either the purposes or the means*" (ECJ C-40/17 Recital 74).

It concluded that: "*Fashion ID appears to have embedded on its website the Facebook 'Like' button made available to website operators by Facebook Ireland while fully aware of the fact that it serves as a tool for the collection and disclosure by transmission of the personal data of visitors to that website, regardless of whether or not the visitors are members of the social network Facebook. Moreover, by embedding that social plugin on its website, Fashion ID exerts a decisive influence over the collection and transmission of the personal data of visitors to that website to the provider of that plugin, Facebook Ireland, which would not have occurred without that plugin. In these circumstances, and subject to the investigations that it is for the referring court to carry out in this respect, it must be concluded that Facebook Ireland and Fashion ID determine jointly the means at the origin of the operations involving the collection and disclosure by transmission of the personal data of visitors to Fashion ID's website*" (ECJ C-40/17 Recitals 77-79), equal if Fashion ID does not itself have access to the personal data collected and transmitted to the provider of the social plugin with which it determines jointly the means and purposes of the processing of personal data. But the ECJ considered that for the subsequent operations involving the processing of personal data carried out by Facebook Ireland after their transmission to the latter, Fashion ID cannot be considered to be a controller and therefore liable since it was impossible for it to determine the purposes or means of those operations.

It also pointed out regarding consent, "*that such consent must be given prior to the collection and disclosure by transmission of the data subject's data. In such circumstances, it is for the operator of the website, rather than for the provider of the social plugin, to obtain that consent, since it is the fact that the visitor consults that website that triggers the processing of the personal data. As the Advocate General noted in point 132 of his Opinion, it would not be in line with efficient and timely protection of the data subject's rights if the consent were given only to the joint controller that is involved later, namely the provider of that plugin. However, the consent that must be given to the operator relates only to the operation or set of operations involving the processing of personal data in respect of which the operator actually determines the purposes and means*" (ECJ C-40/17 Recital 102). The same goes for the duty to inform.

3.4.4 General obligations: Representatives of controllers or processors not established in the Union (Art. 27 GDPR)

3.4.5 General obligations: Processor (Art. 28 GDPR)

3.4.6 General obligations: Processing under the authority of the controller or processor (Art. 29 GDPR)

3.4.7 General obligations: Records of processing activities (Art. 30 GDPR)

3.4.8 General obligations: Cooperation with the supervisory authority (Art. 31 GDPR)

3.4.9 Security of personal data: Security of processing (Art. 32 GDPR)

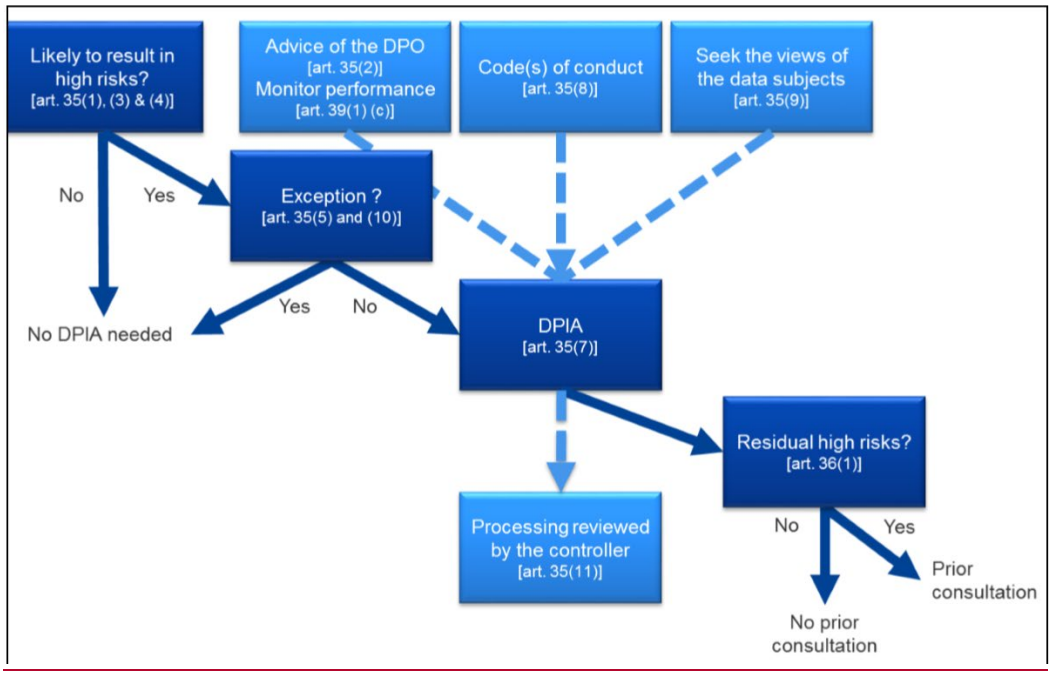
3.4.10 Security of personal data: Notification of a personal data breach to the supervisory authority (Art. 33 GDPR)

3.4.11 Security of personal data: Communication of a personal data breach to the data subject (Art. 34 GDPR)

3.4.12 Data protection impact assessment and prior consultation: Data protection impact assessment (Art. 35 GDPR)[44]

A Data protection impact assessment (DPIA) is a "process for building and demonstrating compliance"[45] with the GDPR.

A DPIA is only required when the processing is "likely to result in a high risk to the rights and freedoms of natural persons". This means[46]:



Rights and freedoms of individuals should be understood as the rights to data protection and privacy, but may also involve other fundamental rights such as freedom of speech, frededom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion[47].

[44] Based on : https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.
[45] From: Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 Adopted on 4 April 2017, as last Revised and Adopted on 4 October 2017, p. 4, in https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.
[46] From: Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 Adopted on 4 April 2017, as last Revised and Adopted on 4 October 2017, p. 7, in https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.
[47] From: Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 Adopted on 4 April 2017, as last Revised and Adopted on 4 October 2017, p. 6, in https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

A DPIA can be used to assess a single data processing operation or multiple processing operations, which are similar (nature, scope, context, purpose, risks). Eg.: A single DPIA by a railway undertaking before installing video surveillance in all its train stations.

For joint data controllers, they need to define, who is responsible of what (e.g.: measures to treat risks and to protect the rights and freedoms of the data subjects).

3.4.12.1 When should a DPIA be done?

The GDPR mentions examples when a DPIA is required: for new data processing technologies, for systematic and extensive evaluation of personal aspects relating to natural persons based on profiling those data or following the processing of special categories of personal data, for biometric data or data on criminal convictions and offences or related security measures and for monitoring publicly accessible areas on a large scale (Recitals 89 and 91 GDPR).

Art. 35§3 GDPR gives also examples when a DPIA is required: systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effect concerning the natural person or similarly significantly affect the natural person (in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or morevemnts, in order to create or use personal profiles (Recital 71 GDPR), processing on a large scale of special categories of 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 or of personal data relating to criminal convictions and offences, systematic monitoring of a publicly accessible area on a large scale.

The GDPR also mentions cases when a DPIA is not required: processing of personal data from patients or clients by an individual physician, other health care professional or lawyer (Recital 91 GDPR).

In case of doubt, a DPIA should be done.

The EDPB developed criteria to determine when a DPIA is necessary[48]:

1. **Evaluation or scoring**: Including profiling and predicting. Eg.: Fraud database, company building behavioural or marketing profiles based on usage or navigation on its website.
2. **Automated decision making with legal or similar significant effect**: Eg.: Processing may lead to the exclusion or discrimination against individuals.
3. **Systematic monitoring**: Processing used to observe, monitor or control data subjects, including data collected through networks or a systematic monitoring of a publicly accessible area.
4. **Sensitive data or data of a highly personal nature**: 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 and personal data relating to criminal convictions and offences. This includes also personal data linked to household and private activities (such as electronic communications), personal data which impact the exercise of a fundamental right (such as location data, whose collection can go against the freedom of movement), personal data whose violation clearly involves serious impacts in the data subject's daily life (e.g. financial data, which might be used for payment fraud). It is

[48] From: Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 Adopted on 4 April 2017, as last Revised and Adopted on 4 October 2017, p. 9-11, in https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

important to distinguish if those personal data have been made already publicly available in the assessment.

5. **Data processed on a large scale**: For the EDPB, large scale means:
    a. Number of data subjects concerned
    b. Volume of data and/or the range of different data items being processed
    c. Duration or permanence of the data processing activity
    d. Georgraphical extent of the processing activity
6. **Matching or combining datasets**: Datasets coming from different data processing operations performed for different purposes and/or different data controllers in a way that would exceed the reasonable exprectations of the data subject.
7. **Data concerning vulnerable data subjects**: Eg.: Children, employees, more vulnerable segments of the population requiring special protection (mentally ill persons, asylum seekers, elderly, patients, etc.), cases where an imbalance in the relationship between the position of the data subject and the data controller can be identified.
8. **Innovative use or applying new technological or organisational solutions**: The impact of the use of new technologies on individuals' rights and freedoms may be unknown. E.g. Internet of things.
9. **Processing in itself prevents data subjects from exercising a right or using a service or a contract**: Eg.: Processing operations that aim at allowing, modifying or refusing data subjects' access to a service or entry into a contract. Eg.: Bank screens its customers against a credit reference database in order to decide whether to offer them a loan.

In some cases, just meeting one of these criteria is enough to require a DPIA.

Examples where a DPIA would be necessary: The use of a camera system to monitor driving behaviour on highways, where the data controller envisages to use an intelligent video analysis system to single out cars and automatically recognize license plates → it is 3) a systematic monitoring and 8) an innovative use or applying technological or organisational solutions; A company systematically monitoring its employees' activities, including the monitoring of the employees' work station, internet activity, etc. → 3) systematic monitoring, 7) data concerning vulnerable data subjects; The gathering of public social media data for generating profiles → 1) Evaluation or scoring, 5) Data processed on a large scale, 6) Matching or combining datasets, 4) Sensitive data or data of a highly personal nature.

Examples where a DPIA would not be necessary: An online magazine using a mailng list to send a generic daily digest to its subscribers → 5) Data processed on a large scale; An e-commerce website displaying adverts for vintage car parts involving limited profiling based on items viewed or purchased on its own website → 1) Evaluation or scoring.

3.4.12.2 Procedure to carry out a DPIA

The procedure to carry out a DPIA is the following:

- **When?** Prior to the processing, if possible, during the design of the processing, even if some processing operations are unknown. The DPIA might need to be updated in the development of the processing operations. "*Carrying out a DPIA is a continual process, not a one-time exercise*"[49]. Once a DPIA has been done, it might be useful to redo it since things might evolve over time. Therefore, it would be wrong to think that doing a DPIA once is sufficient. A regular review might be needed.

[49] From: Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 Adopted on 4 April 2017, as last Revised and Adopted on 4 October 2017, p. 14, in https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

- **Who?** The data controller is responsible, but the DPIA can be carried out by someone else (even a third-party). Should be also included in the DPIA:
    - **+ Advice of Data Protection Officer:** The data controller must also seek the advice of the Data Protection Officer, if there is one, who should monitor the DPIA. This should be documented in the DPIA, as well as the decision taken.
    - **+ Assistance of Data Processor:** The data processor should also assist the data controller and provide information. Its role and responsibility must be contractually defined.
    - **+ Views of the data subjects or their representatives:** If appropriate, those views should be sought (e.g. through a survey, generic study, questions, etc.) and the data controller should document if its final decision differes from the views of the data subjects. If the data controller considers not appropriate to seek the views of data subjects, it should also document why (e.g. in case of risk for the confidentiality of the business plans or if this would be disproportionate or impracticable).
    - Involve if necessary the different business units, experts (lawyers, IT experts, security experts, sociologists, ethics, etc.) and the Chief Information Security Officer (CISO)
- **What to mention in the DPIA?** It should be mentioned:
    a. Description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the data controller;
    b. Assessment of the necessity and proportionality of the processing operations in relation to the purposes;
    c. Assessment of the risks to the rights and freedoms of data subjects;
    d. Measures envisaged to address the risks and demonstrate compliance with GDPR.
    e. Compliance with a Code of conduct or with certifications, seals and marks or Binding corporate rules should be mentioned and taken into account.
- **Need to publish the DPIA?** No, but possible to publish the DPIA or parts of the DPIA (e.g. a summary or a conclusion). But if the DPIA shows that the processing would result in a high risk to the rights and freedoms of natural person, then the data controller will have to consult the supervisory authority and provide the DPIA.
- **Consultation of the supervisory authority?** Only if the processing would result in a high risk. According to the EDPB, based on Art. 35§7 and Recitals 84 and 94, the "residual risks" need to be taken into account, that means that in order to have to contact the supervisory authority, the risks need to stay high, even if the data controller has foreseen appropriate measures to mitigate it. Therefore, if the data controller cannot find sufficient appropriate measures to reduce the risks to an acceptable level (residual risks must no be high anymore), the supervisory authority needs to be consulted. Appropriate measures depend on the situation. Member State law may also require that controllers consult with, and obtain prior authorisation from, the supervisory authority in relation to processing by a data controller for the performance of a task carried out by the data controller in the public interest, including processing in relation to social protection and public health (art. 36§7 GDPR).

3.4.12.3 Checklist for a DPIA[50]

[50] From: Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 Adopted on 4 April 2017, as last Revised and Adopted on 4 October 2017, p. 22, in https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

The EDPB advises to take into account following criteria to assess if the DPIA is compliant with the GDPR:

- a systematic description of the processing is provided (Article 35(7)(a) GDPR):
    - nature, scope, context and purposes of the processing are taken into account;
    - personal data, recipients and period for which the personal data will be stored are recorded;
    - a functional description of the processing operation is provided;
    - the assets on which personal data rely (hardware, software, networks, people, paper or paper transmission channels) are identified;
    - compliance with approved codes of conduct is taken into account (Article 35(8) GDPR);
- necessity and proportionality are assessed
    - measures envisaged to comply with the Regulation are determined, taking into account:
        - measures contributing to the proportionality and the necessity of the processing on the basis of:
            - specified, explicit and legitimate purpose(s;
            - lawfulness of processing
            - adequate, relevant and limited to what is necessary
            - limited storage duration
        - measures contributing to the rights of the data subjects:
            - information provided to the data subject (Articles 12, 13 and 14 GDPR);
            - right of access and to data portability (Articles 15 and 20 GDPR);
            - right to rectification and to erasure (Articles 16, 17 and 19 GDPR);
            - right to object and to restriction of processing (Article 18, 19 and 21 GDPR);
            - relationships with processors (Article 28 GDPR);
            - safeguards surrounding international transfer(s) (Chapter V GDPR);
            - prior consultation (Article 36 GDPR)
- risks to the rights and freedoms of data subjects are managed
    - origin, nature, particularity and severity of the risks are appreciated (cf. recital 84) or, more specifically, for each risk (illegitimate access, undesired modification, and disappearance of data), from the perspective of the data subjects:
        - risks sources are taken into account (recital 90 GDPR);

- potential impacts to the rights and freedoms of data subjects are identified in case of events including illegitimate access, undesired modification and disappearance of data;
- threats that could lead to illegitimate access, undesired modification and disappearance of data are identified;
- likelihood and severity are estimated (recital 90 GDPR);

- measures envisaged to treat those risks are determined (Article 35(7)(d) and recital 90 GDPR);

- interested parties are involved:
  - the advice of the DPO is sought (Article 35(2) GDPR);
  - the views of data subjects or their representatives are sought, where appropriate (Article 35(9) GDPR).

3.4.12.4 Templates for a DPIA[51]

It exists different templates for the carryout out of a DPIA. The CIT decided to refer to two of them here.

3.4.12.4.1 ICO Data Protection Template[52]

The following template comes from the Information Commisserion's Office (ICO), a British independent authority, encompasses following points:

- **Step 1: Identify the need for a DPIA**
  - Explication of the project : The project should be explained, as well as the aim to achieve and what type of processing are involved. It is possible here to refer or to link to other documents.
- **Step 2 : Describe the processing**
  - Description of the nature of the processing : How will the data be collected, stored, deleted ? What is the source of the data ? Will the data be shared with someone ? A flow diagram might be useful here. What types of processing involved present likely high risks ?
  - Description of the scope of the processing : What is the nature of the data, does it include special category of data or criminal offence data ? How much data will be collected and used ? How often ? How long will they be kept ? How many individuals are affected ? What is the geographical area it covers ?
  - Description of the context of the processing : What is the nature of the relation between the data controller and the individuals ? How much control will the individuals have on the processing ? Would they expect that their data are used in the projected way ? Do those individuals include children or other vulnerable groups ? Are there prior concerns over this type of processing or security flaws ? Is it novel in any way ? What is the current state of technology in this area ? Are there any current issues of public concern that should be factored in ? Has the data controller signed up to any approved code of conduct or certification scheme ?
  - Description of the purposes of the processing : What is the goal ? What is the intended effect on individuals ? What are the benefits of the processing ?

[51] From : Information Commissioner's Office, Sample DPIA template v0.3, in : https://ico.org.uk/media/about-the-ico/consultations/2258461/dpia-template-v04-post-comms-review-20180308.pdf
[52] [52] From : Information Commissioner's Office, Sample DPIA template v0.3, in : https://ico.org.uk/media/about-the-ico/consultations/2258461/dpia-template-v04-post-comms-review-20180308.pdf.

- **Step 3 : Consultation process**
  - Consultation with relevant stakeholders : Here it should be considered how to consult with relevant stakeholders. It should be described when and how individuals' views will be seeked or if it is not appropriate to do so. It should also be mentioned if other persons from the organisation need to be involved, if the data processors also need to asssist, if security experts or other experts need to be consulted.
- **Step 4 : Assess necessity and proportionality**
  - Description of the compliance and proportionality measures, in particular : What is the lawful basis for processing ? Does the processing actually achieve the purpose ? Is there another way to achieve the same outcome ? How will function creep be prevented ? How will data quality and data minimisation be ensured ? What information will be provided to the individuals ? How will the data controller help to support their rights ? What measures will be taken to ensure that data processors comply ? How will any international transfers be safeguarded ?
- **Step 5 : Identify and assess risks**
  - Description of the source of risk and nature of the potential impact on individuals : It includes associated compliance and corporate risks as necessary. Here a table should be realised mentioning in a first colonne the different source of risks and then three columns about « Likelihood of harm » and the choice between : Remote, possible or probable, « Severity of harm » and the choice between : Minimal, significant or severe and « Overall risk » with the choice between : Low, medium or high.
- **Step 6 : Identify measures to reduce risk :**
  - For risk identified as medium or high under step 5, additional measures should be found to reduce or eliminate them. Here again, a table should be done, with a first colonne on « Risk », a second colonne on « Options to reduce or eliminate risk », a third colonne on « Effect on risk » with the choice between : Eliminated, reduced and accepted, a fourth colonne on « Residual risk » and the choice between : Low, medium and high. A last colonne with « Measure approved » and the choice between : Yes/No.
- **Step 7 : Sign off and record outcomes**
  - Here again, a table should be realised, like this :

Item	Name/Date	Notes
Measures approved by	[Name/Date]	Integrate actions back into project plan, with data and responsibility for completion
Residual risks approved by :	[Name/Date]	If accepting any residual high risk, consult the supervisory authority before going ahead
DPO advice provided by :	[Name/Date]	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice	[Name/Date]	
DPO advice accepted or overruled by :	[Name/Date]	If overruled, the data controller must explain his reasons

Comments :	[Name/Date]	
Consultation responses reviewed by :	[Name/Date]	If the data controller's decision departs from individuals' views, he must explain his reasons
Comments :	[Name/Date]	
This DPIA will be kept under review by :	[Name/Date]	The DPO should also review ongoing compliance with DPIAs

3.4.12.4.2 CNIL Template[53]

The Commission nationale de l'informatique et des libertés (CNIL) is an independent French administrative regulatory body, whose mission is to ensure the application of the data privacy law. It published the following template:

- **Step 1 : Study of the context**
  - Overview of the processing
    - Description of the processing under consideration

Description of the processing	[Description]
Processing purposes	[enumerate]
Processing stakes	[enumerate]
Data controller	[Name]
Data processor	[Name]

    - Sector-specific standard applicable to the processing

Standards applicable to the processing	**Consideration**
[enumerate]	[enumerate]
[enumerate]	[enumerate]

  - Data, processes and supporting assets
    - Data description, recipients and storage duration

Data types	**Recipients**	**Storage Duration**
[enumerate]	[enumerate]	[enumerate]
[enumerate]	[enumerate]	[enumerate]

    - Description of the processes and supporting assets [insert a diagram of data flows and a detailed description of the processes carried out]

Processes	**Detailed description of the process**	**Data supporting assets**
[enumerate]	[enumerate]	[enumerate]

[53] From : Commission nationale informatique & libertés, Privacy Impact Assessment (PIA) : Methodlogy, February 2018 Edition, in : https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-2-en-templates.pdf

[enumerate]	[enumerate]	[enumerate]

- **Step 2 : Study of the fundamental principles**
  - Assessment of the controls guaranteeing the proportionality and necessity of the processing
    - Explanation and justification of purposes

Purposes	**Legitimacy**
[enumerate]	[enumerate]
[enumerate]	[enumerate]

    - Explanation and justification of lawfulness

Lawfulness criteria	**Applicable**	**Justification**
The data subject has given consent to the processing of his or her personal data for one or more specific purposes	[Yes/No]	[Justification]
Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract	[Yes/No]	[Justification]
Processing is necessary for compliance with a legal obilgation to which the data controller is subject	[Yes/No]	[Justification]
Processing is necessary in order to protect the vital interests of the data subject or of another natural person	[Yes/No]	[Justification]
Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller	[Yes/No]	[Justification]
Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are	[Yes/No]	[Justification]

overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child		

- Explanation and justification of data minimization

Details about the data processed	**Data categories**	**Justification of the need and relevance of the data**	**Minimization controls**
[details]	[enumerate]	[Justification]	[enumerate]
[details]	[enumerate]	[Justification]	[enumerate]

- Explanation and justification of data quality

Data quality controls	**Justification**
[enumerate]	[Justification]
[enumerate]	[Justification]

- Explanation and justification of storage durations

Data types	**Storage duration**	**Justification of the storage duration**	**Erasure mechanism at the end of the storage duration**
Common data	[enumerate]	[Justification]	[enumerate]
Archived data	[enumerate]	[Justification]	[enumerate]
Functional traces	[enumerate]	[Justification]	[enumerate]
Technical logs	[enumerate]	[Justification]	[enumerate]

- Assessment of the controls

Controls guaranteeing the proportionality and necessity of the processing	**Acceptable/can be improved on ?**	**Corrective controls**
Purposes : specified, explicit and legitimate	[enumerate]	[enumerate]
Basis : lawfulness of processing, prohibition of misuse	[enumerate]	[enumerate]
Data minimization : adequate, relevant and limited	[enumerate]	[enumerate]

Data quality : accurate and kept up-to-date	[enumerate]	[enumerate]
Storage durations : limited	[enumerate]	[enumerate]

- Assessment of controls protecting data subjects' rights

  - Determination and description of the controls for information for the data subjects

Exemption from having to inform the data subjects (if the processing benefits from an exemption from the right to information, art. 12-14 GDPR)	**Justification**
[enumerate]	[Justification]
[enumerate]	[Justification]

Otherwise :

Controls for the right to information	**Implementation**	**Implementation justification or justification why not**
Presentation of the terms & conditions for use/confidentiality	[enumerate]	[Justification]
Possibility of accessing the terms & conditions for use/confidentiality	[enumerate]	[Justification]
Legible and easy-to-understand terms	[enumerate]	[Justification]
Existence of clauses specific to the device	[enumerate]	[Justification]
Detailed presentation of the data processing purposes (specified objectives, data matching where applicable, etc.)	[enumerate]	[Justification]
Detailed presentation of the personal data collected	[enumerate]	[Justification]
Presentation of any access to the identifiers of the device, the smartphone/tablet or computer, by specifying whether these identifiers are communicated to third parties	[enumerate]	[Justification]

Presentation of the user's rights (consent withdrawal, data erasure, etc.)	[enumerate]	[Justification]
Information on the secure data storage method, particularly in the event of sourcing	[enumerate]	[Justification]
Arrangements for contacting the company (identity and contact details) about confidentiality issues	[enumerate]	[Justification]
Where applicable, information for the user on any change concerning the data collected, the purposes and confidentiality clauses	[enumerate]	[Justification]
Regarding transfer of data to third parties : detailed presentation of the purposes of transmission to third parties	[enumerate]	[Justification]
Regarding transfer of data to third parties : detailed presentation of the personal data transmitted	[enumerate]	[Justification]
Regarding transfer of data to third parties : indication of the identity of third-party bodies	[enumerate]	[Justification]

- Determination and description of the controls for obtaining consent (where processing lawfulness is based on consent)

Controls for obtaining consent	**Implementation**	**Implementation justification or justification why not**
Express consent during registration	[enumerate]	[Justification]
Consent segmented per data category or processing type	[enumerate]	[Justification]
Express consent prior to sharing data with other users	[enumerate]	[Justification]
Consent presented in an intelligible and easily accessible form,	[enumerate]	[Justification]

using clear and plain language adapted to the target user (particularly for children)		
Obtaining parents' consent for minors under 13 years of age	[enumerate]	[Justification]
For a new user, consent must once again be obtained	[enumerate]	[Justification]
After a long period without use, the user must be asked to confirm his/her consent	[enumerate]	[Justification]
Where the user has consented to the processing of special data (e.g. his/her location) the interface clearly indicates that said processing takes place (icon, light)	[enumerate]	[Justification]
Where the user changes device, smartphone or computer, reinstalls the mobile app or deletes his/her cookies, the settings associated with his/her consent are maintained	[enumerate]	[Justification]

- Determination and description of the controls for the rights of access and to data portability

Exemption from the right of access (if the processing benefits from an exemption from the right of access, Art. 15 GDPR)	**Justification**	**Arrangements for responding to the data subjects**
[enumerate]	[Justification]	[enumerate]
[enumerate]	[Justification]	[enumerate]

Otherwise :

Controls for the right of access	**Internal data**	**External data**	**Justification**
Possibility of accessing all of the user's personal data, via the common interfaces	[enumerate]	[enumerate]	[Justification]

Possibility of securely consulting the traces of use associated with the user	[enumerate]	[enumerate]	[Justification]
Possibility of downloading an archive of all the personal data associated with the user	[enumerate]	[enumerate]	[Justification]

Lastly, where the right to data portability applies to processing according to Art. 20 GDPR :

Controls for the right to data portability	**Internal data**	**External data**	**Justification**
Possibility of retrieving, in an easily reusable format, personal data provided by the user, so as to transfer them to another service	[enumerate]	[enumerate]	[Justification]

- Determination and description of the controls for the rights to rectification and erasure :

Exemptions from the rights to rectification and erasure (if the processing benefits from an exemption from the right to rectification and erasure, Art. 17 GDPR)	**Justification**	**Arrangements for responding to the data subjects**
[enumerate]	[Justification]	[enumerate]
[enumerate]	[Justification]	[enumerate]

Otherwise :

Controls for the rights to rectification and erasure	**Internal data**	**External data**	**Justification**
Possibility of rectifying personal data	[enumerate]	[enumerate]	[Justification]

Possibility of erasing personal data	[enumerate]	[enumerate]	[Justification]
Indication of the personal data that will nevertheless be stored (technical requirements, legal obligations, etc.)	[enumerate]	[enumerate]	[Justification]
Implementing the right to be forgotten for minors	[enumerate]	[enumerate]	[Justification]
Clear indications and simple steps for erasing data before scrapping the device	[enumerate]	[enumerate]	[Justification]
Advice given about resetting the device before selling it	[enumerate]	[enumerate]	[Justification]
Possibility of erasing the data in the event the device is stolen	[enumerate]	[enumerate]	[Justification]

- Determination and description of the controls for the rights to restriction of processing and to object

Exemptions from the rights to restriction and to object (if the processing benefits from an exemption from the right to restriction and to object, Art. 21 GDPR)	**Justification**	**Arrangements for responding to the data subjects**
[enumerate]	[Justification]	[enumerate]
[enumerate]	[Justification]	[enumerate]

Otherwise :

Controls for the rights to restriction and erasure	**Internal data**	**External data**	**Justification**

Existence of « Privacy » settings	[enumerate]	[enumerate]	[Justification]
Invitation to change the default settings	[enumerate]	[enumerate]	[Justification]
« Privacy » settings accessible during registration	[enumerate]	[enumerate]	[Justification]
« Privacy » settings accessible after registration	[enumerate]	[enumerate]	[Justification]
Existence of a parental control system for children under 13 years of age	[enumerate]	[enumerate]	[Justification]
Compliance in terms of tracking (cookies, advertising, etc.)	[enumerate]	[enumerate]	[Justification]
Exclusion of children under 13 years of age from automated profiling	[enumerate]	[enumerate]	[Justification]
Effective exclusion of processing the user's data in the event consent is withdrawn	[enumerate]	[enumerate]	[Justification]

- Determination and description of the controls applicable to processors

Processor's name	**Purpose**	**Scope**	**Contract reference**	**Compliance with Art. 28**
[Name]	[enumerate]	[enumerate]	[reference]	[enumerate]
[Name]	[enumerate]	[enumerate]	[reference]	[enumerate]

- Determination and descirption of the controls on transfer of data outside the European Union

Data sets and storage location	Member State	EU	Country recognized as providing adequate	Other country	Justification and supervision (standard contractual clauses,

			protection by the EU		internal corporate regulation)
[enumerate]	[enumerate]	[enumerate]	[enumerate]	[enumerate]	[enumerate]
[enumerate]	[enumerate]	[enumerate]	[enumerate]	[enumerate]	[enumerate]

➢ Assessment of the controls

Controls to protect the rights of data subjects	**Acceptable/can be improved on**	**Corrective controls**
Information for the data subjects (fair and transparent processing)	[enumerate]	[enumerate]
Obtaining consent	[enumerate]	[enumerate]
Exercising the rights of access and to data portability	[enumerate]	[enumerate]
Exercising the rights to rectification and erasure	[enumerate]	[enumerate]
Exercising the rights to restriction of processing and to object	[enumerate]	[enumerate]
Data Processors : identified and governed by a contract	[enumerate]	[enumerate]
Transfers : compliance with the obligations bearing on transfer of data outside the European Union	[enumerate]	[enumerate]

- **Step 3 : Study of data security risks**
  - Assessment of security controls

➢ Description and assessment of controls implemented for treating the risks related to data security

Controls bearing specifically on the data being processed	**Implementation or justification why not**	**Acceptable/can be improved on ?**	**Corrective controls**
Encryption	[Describe here the means implemented for ensuring the confidentiality of	[enumerate]	[enumerate]

	data stored (in the database, in flat files, back-ups, etc.), as well as the procedure for managing encryption keys (creation, storage, change in the event of suspected cases of data compromise, etc.). Describe the encryption means employed for data flows (VPN, TLS, etc.) implemented in the processing]		
Anonymization	[Indicate here whether anonymization mechanisms are implemented, which ones and for what purpose]	[enumerate]	[enumerate]
Data partitioning (in relation to the rest of the information system)	[Indicate here if processing partitioning is planned, and how this is carried out]	[enumerate]	[enumerate]
Logical access control	[Indicate here whether the users' profiles are defined and attributed. Specify the authentication means implemented. Where applicable, specify the rules applicable to passwords (minimum length, required characters, validity duration, number of failed attempts before access to account is locked, etc.)]	[enumerate]	[enumerate]

Traceability (logging)	[Indicate here whether events are logged and how long these traces are stored for]	[enumerate]	[enumerate]
Integrity monitoring	[Indicate here whether mechanisms are implemented for integrity monitoring of stored data, which ones and for what purpose. Specify which integrity control mechanisms are implemented on data flows]	[enumerate]	[enumerate]
Archiving	[Describe here the processes of archive management (delivery, storage, consultation, etc.) under your responsibility. Specify the archiving roles (offices of origin, transferring agencies, etc.) and the archiving policy. State if data may fall within the scope of public archives]	[enumerate]	[enumerate]

- Description and assessment of general security controls

General security controls regarding the system in which the processing is carried out	**Implementation or justification why not**	**Acceptable/can be improved on ?**	**Corrective controls**
Operating security	[Describe here how the software updates (operating systems, applications, etc.) and applications of security corrective controls are carried out]	[enumerate]	[enumerate]

Clamping down on malicious software	[State here whether an antivirus software is installed and updated at regular intervals on the workstations]	[enumerate]	[enumerate]
Managing workstations	[Describe here the controls implemented on workstations (automatic locking, firewall, etc.)]	[enumerate]	[enumerate]
Website security	[Indicate here whether ANSSI's « recommendations for securing websites » have been implemented]	[enumerate]	[enumerate]
Backups	[Indicate here how backups are managed. Clarify whether they are stored in a safe place]	[enumerate]	[enumerate]
Maintenance	[Describe here how physical maintenance of hardware is managed, and state whether this is contracted out. Indicate whether the remote maintenance of apps is authorized, and according to what arrangements. Specify whether defective equipment is managed in a specific manner]	[enumerate]	[enumerate]
Security of computer channels (networks)	[Indicate here the type of network on which the processing is carried out (isolated, private or Internet). Specify which firewall system, intrusion detection systems or other active or passive devices are in charge of ensuring network security.]	[enumerate]	[enumerate]
Monitoring	[Indicate here whether real-time monitoring of local network is implemented and with	[enumerate]	[enumerate]

	what means. Indicate whether monitoring of hardware and software configurations is carried out and by what means.]		
Physical access control	[Indicate here how physical access control is carried out regarding the premises accomodating the processing (zoning, escorting of visitors, wearing of passes, locked doors and so on). Indicate whether there are warning procedures in place in the event of a break-in.]	[enumerate]	[enumerate]
Hardware security	[Indicate here the controls bearing on the physical security of servers and workstations belonging to customers (secure storage, security cables, confidentiality filters, secure erasure prior to scrapping, etc.).]	[enumerate]	[enumerate]
Avoiding sources of risk	[Indicate here whether the implantation area is subject to environmental disasters (flood zone, proximity to chemical industries, earthquake or volcanic zone, etc.). Specify if dangerous products are stored in the same area.]	[enumerate]	[enumerate]
Protecting against non-human sources of risks	[Describe here the means of fire prevention, detection and fighting. Where applicable, indicate the means of preventing water damage. Also specify the means of power supply monitoring and relief.]	[enumerate]	[enumerate]

- Description and assessment of organisational controls (governance)

Organisational controls (governance)	**Implementation or justification why not**	**Acceptable/can be improved on ?**	**Corrective controls**
Organisation	[Indicate if the roles and responsiblities for data protection are defined. Specify whether a person is responsible for the enforcement of privay laws and regulations. Specify whether there is a monitoring committee (or equivalent) responsible for the guidance and follow-up of actions concerning the protection of privacy.]	[enumerate]	[enumerate]
Policy (management of rules)	[Indicate whether there is an IT charter (or equivalent) on data protection and the correct use of IT ressources]	[enumerate]	[enumerate]
Risk management	[Indicate here whether the privacy risks posed by new treatments on data subjects are assessed, whether or not it is systematic and, if applicable, according to which method. Specify whether an organization-level mapping of privacy risks is established.]	[enumerate]	[enumerate]
Project management	[Indicate here whether device tests are performed on non-real/anonymous data.]	[enumerate]	[enumerate]
Management of incidients and data breaches	[Indicate here whether IT incidents are subject to a documented	[enumerate]	[enumerate]

	and tested management procedure.		
Personal management	[Indicate here what awareness-raising controls are carried out with regard to a new recruit. Indicate what controls are carried out when persons who have been accessing data leave their job.]	[enumerate]	[enumerate]
Relations with third parties	[Indicate here, for processors requiring access to data, the security controls and arrangements carried out as regards such access.]	[enumerate]	[enumerate]
Supervision	[Indicate here whether the effectiveness and adequacy of privacy controls are monitored.]	[enumerate]	[enumerate]

- Risk assessment : potential pricacy breaches
  - Analysis and assessment of risks

Risk	**Main risks sources**	**Main threats**	**Mai n potential impacts**	**Main controls reducing the severity and likelihood**	**Severity**	**Likelihood**
Illegitimate access to data	[enumerate]	[enumerate]	[enumerate]	[enumerate]	[enumerate]	[enumerate]
Unwanted change of data	[enumerate]	[enumerate]	[enumerate]	[enumerate]	[enumerate]	[enumerate]
Disappearance of data	[enumerate]	[enumerate]	[enumerate]	[enumerate]	[enumerate]	[enumerate]

  - Assessment of the risks :

Risks	Applicable/can be improved on ?	Corrective controls	Residual severity	Residual likelihood
Illegitimate access to data	[The assessor must determine whether the existing or planned controls (already undertaken) sufficiently reduce this risk for it to be deemed acceptable.]	[Where applicable, he shall indicate here any additional controls that would prove necessary.]	[enumerate]	[enumerate]
Unwanted change of data	[The assessor must determine whether the existing or planned controls (already undertaken) sufficiently reduce this risk for it to be deemed acceptable.]	[Where applicable, he shall indicate here any additional controls that would prove necessary.]	[enumerate]	[enumerate]
Disappearance of data	[The assessor must determine whether the existing or planned controls (already undertaken) sufficiently reduce this risk for it to be deemed acceptable.]	[Where applicable, he shall indicate here any additional controls that would prove necessary.]	[enumerate]	[enumerate]

- **Step 4 : Validation of the DPIA**
  - Preparation of the material required for validation
    - Synthesis of the compliance of the controls selected to ensure compliance with the fundamental principles :

Controls selected to ensure compliance with the fundamental principles	Assessment [choose between : Non applicable, Unsatisfactory, Planned improvement, Acceptable]
Controls guaranteeing the proportionality and necessity of the processing :	
Purpose(s) : specified, explicit and legitimate	

Bais : lawfulness of processing, prohibition of misuse	
Data minimization : adequate, relevant and limited	
Quality of data : accurate and kept up-to-date	
Storage durations : limited	
Controls to protect the personal rights of data subjects :	
Information for the data subjects (fair and transparent processing)	
Obtaining consent	
Exercising the right of access and right to data portability	
Exercising the rights to rectification and erasure	
Exercising the right to restriction of processing and right to object	
Processors : identified and governed by a contract	
Transfers : compliance with the obligations bearing on transfer of data outside the European Union	

- Synthesis of the compliance with good security practices of controls implemented for treating the risks related to data security :

Controls implemented for treating the risks related to data security	**Assessment [choose between : Non applicable, Unsatisfactory, Planned improvement, Acceptable]**
Controls bearing specifically on the data being processed :	
Encryption	
Anonymisation	
Data partitioning (in relation to the rest of the information system)	
Logical access control	
Traceability (logging)	
Integrity monitoring	
Archiving	
Paper document security	
General security controls regarding the system in which the processing is carried out :	
Operating security	
Clamping down on malicious software	
Managing workstations	

Website security	
Backups	
Maintenance	
Security of computer channels (networks)	
Monitoring	
Physical access control	
Hardware security	
Avoiding sources of risk	
Protecting against non-human sources of risks	
Organisational controls (governance) :	
Organisation	
Policy (management of rules)	
Risk management	
Project management	
Management of incidents and data breaches	
Personnel management	
Relations with third parties	
Supervision	

- Elaboration of action plan

Additional controls requested	**Manager**	**Frequency**	**Difficulty**	**Cost**	**Progress**
[enumerate]	[enumerate]	[enumerate]	[enumerate]	[enumerate]	[enumerate]
[enumerate]	[enumerate]	[enumerate]	[enumerate]	[enumerate]	[enumerate]

- Documentation of the advice of the person in charge of « Data Protection » aspects :

  On dd/mm/yyyy, the Data Protection Officer of the company X issued the following opinion concerning the compliance of the processing and DPIA studies carried out. [Signature]

- Documentation of the view of data subjects or their representatives

  The data subjects [were/were not] consulted [and expressed the following view on the compliance of the processing in light of the study perfomed] :

  Justification of the data controller's decision :

- Formal validation of the DPIA

  - Documentation of the validation :

On dd/mm/yyyy, the Managing Director of the company X validates the DPIA for the processing of [describe the object of the processing], in light of the study carried out, in his capacity as data controller.

The purposes of the processing are to [describe the purpose of the processing]

This is because the controls planned for complying with the fundamental principles underpinning privacy protection and for addressing the risks to the privacy of data subjects have been deemed acceptable in light of these stakes. The implementation of additional controls will neverthess have to be demonstrated, as will continuous improvement of the DPIA. [Signature]

3.4.13 Data protection impact assessment and prior consultation: Prior consultation (Art. 36 GDPR)

3.4.14 Data protection officer: Designation of the data protection officer (Art. 37 GDPR)

3.4.15 Data protection officer: Position of the data protection officer (Art. 38 GDPR)

3.4.16 Data protection officer: Tasks of the data protection officer (Art. 39 GDPR)

3.4.17 Codes of conduct and certification: Codes of conduct (Art. 40 GDPR)

3.4.18 Codes of conduct and certification: Monitoring of approved codes of conduct (Art. 41 GDPR)

3.4.19 Codes of conduct and certification: Certification (Art. 42 GDPR)

3.4.20 Codes of conduct and certification: Certification bodies (Art. 43 GDPR)

3.5 Transfers of personal data to third countries or international organisations (Chapter V GDPR)

The novelty of the GDPR was its extraterritorial impact. It is applicable not only within the European Union, but also outside the EU.

Chapter V of the GDPR concerns the transfer of personal data to third countries or international organisations. It contains several clauses for derogations, which allow personal data to be transferred to third countries or international organisations. There is a hierarchy that has to be observed between these different clauses for derogations. This means that a data controller cannot choose freely which of these derogations he would like to apply.

Before transferring personal data to a third country or an international organisation, the data controller must start by analysing whether an adequacy decision exists about that country or organisation, as defined in Article 45 GDPR.

3.5.1 General principle for transfers (Art. 44 GDPR)

The conditions laid down in Chapter V need to be complied with in order for the transfer of personal data to a third country or to an international organisation to take place.

There is a hierarchy between the different criteria mentioned under Chapter V, as will be described below.

3.5.2 Transfers on the basis of an adequacy decision (Art. 45 GDPR)[54]

3.5.2.1 Definition of adequacy decision

An “adequacy decision” is a decision rendered by the European Commission about a third country or an international organisation, where the European Commission confirms formally that the level of data protection in this third country or in this international organisation is essentially equivalent to the level of data protection in the EU.

[54] Based on: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

3.5.2.2 Concept of adequacy

"Adequacy" means that the level of protection in the third country must essentially be equivalent to that guaranteed in the EU. However, the means used for this might differ from those employed within the EU.

The European Commission will regularly review whether the conditions that led to this adequacy decision are still met or not. National data protection authorities may institute legal proceedings if they find that a claim by a person against an adequacy decision is well founded.

3.5.2.3 Effect of an adequacy decision

If the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection, it will render an adequacy decision.

This adequacy decision has binding effects on EU Members States.

Thanks to this, the transfer of personal data to that third country, territory or specified sector(s) within that third country, or to that international organisation will not require any specific authorisation.

3.5.2.4 Countries benefiting from an adequacy decision (as at 15 December 2019)[55]

The European Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the United States of America (limited to the Privacy Shield framework) as providing adequate protection.

Discussions are ongoing concerning South Korea.

3.5.3 Transfers subject to appropriate safeguards (Art. 46 GDPR)

[To be drafted ~~by June 2020~~]

3.5.4 Binding corporate rules (Art. 47 GDPR)

[To be drafted ~~by June 2020~~]

3.5.5 Transfers or disclosures not authorised by Union law (Art. 48 GDPR)

[To be drafted ~~by June 2020~~]

3.5.6 Derogations for specific situations (Art. 49 GDPR)[56]

3.5.6.1 Conditions to fulfil before applying Article 49 GDPR

It is important to note that Article 49 GDPR is not applicable if there exists an adequacy decision for the third country in question or for the international organisation or if there are appropriate safeguards for that transfer: This means that if Article 45 GDPR or Article 46 GDPR are applicable, Article 49 GDPR does not apply.

Article 49 GDPR contains different derogations for specific situations:

- Explicit consent
- Performance of a contract between the data subject and the data controller
- Performance of a contract between a data controller and a third party
- Important reasons of public interest
- Legal claims

[55] From: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en.
[56] Based on: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_en.

- Vital interests
- Register
- Compelling legitimate interest

Even when applying Article 49 GDPR, it is important to comply with the other requirements arising from the GDPR.

3.5.6.2 General conditions applicable to all paragraphs of Article 49 GDPR

There are some general conditions that are applicable cumulatively to all derogations mentioned in Article 49 GDPR. So before applying one of these derogations, it is important not to forget to comply with these general conditions as well:

1. **Occasional and not repetitive transfer**: a transfer to third countries or international organisations should not happen on a regular basis, only under random, unknown circumstances and within arbitrary time intervals. Data transfer that occurs regularly within a stable relationship between the data controller and a certain data processor can basically be deemed as systematic and repeated, and therefore not occasional or non-repetitive. This condition is mentioned for "contract" and "legal claims" derogations. Nevertheless, for the other derogations, they should also be applied only exceptionally.
2. **Necessary test**: the data transfer has to be "necessary" for a certain purpose. It requires an evaluation by the data controller in the EU of whether the transfer of personal data can be considered necessary for the specific purpose.
3. **Decisions from third countries' authorities~~, courts~~ or tribunals are not in themselves legitimate grounds for data transfers to third countries**: Therefore, a transfer in response to a decision from third countries to authorities is only lawful if it is in line with the conditions set out in Chapter V. For example, if there is an international agreement between two countries, EU companies should generally refuse direct requests from authorities and refer the requesting third country authority to an existing mutual legal assistance treaty or agreement.

3.5.6.3 Interpretation of the different provisions of Article 49 GDPR

3.5.6.3.1 Explicit consent (Art. 49(1) (a) GDPR)

The cumulative conditions to apply Art. 49 (1) (a) GDPR are:

1. **General conditions of Article 4(11) and 7 GDPR** (see Point 3.2.3 on consent)
    a. Freely given consent,
    b. Specific consent,
    c. Informed consent and
    d. Unambiguous consent
2. **Explicit consent**: this is stricter than the definition of consent given in Article 4 GDPR (for definition see Point 3.2.3 on consent)
3. **Specific consent**: this needs to be specifically given for the particular data transfer or set of transfers. The data exporter must make sure to obtain specific consent before the transfer is put in place, even if this occurs after the data have been collected.
4. **Informed consent**: Information must be provided on:
    a. Data controller's identity;
    b. Purpose of the transfer;
    c. Type of data;

d. Existence of the right to withdraw consent;

e. Identity or categories of all recipients;

f. All countries to which the personal data are transferred;

g. Specific risks resulting from the fact that:

   i. the data will be transferred to a country that does not provide for an adequate level of data protection based on a European Commission decision,

   ii. this country does not provide for adequate protection and,

   iii. no adequate safeguards aimed at providing protection for the data are being implemented.

h. Consent is the lawful ground for the transfer.

Such notice, which could be standardised, should also include, for example, information that in the third country there might not be a supervisory authority and/or data processing principles and/or that data subject rights might not be provided for in the third country. See Example of Information Clause under Point 4.2.

5. **Transparency**: the general transparency requirements of Articles 13 and 14 GDPR should also be complied with.

3.5.6.3.2 Performance of a contract between the data subject and the data controller (Art. 49(1)(b) GDPR)

The cumulative conditions to apply Art. 49 (1) (b) GDPR are:

1. **Necessity of the data transfer**:

   - Example where derogation is not applicable: for business purposes, a corporate group has centralised its payment and human resources management functions for all its staff in a third country; here there is no direct and objective link between the performance of the employment contract and such transfer; in this case, standard contractual clauses or binding corporate rules may be suitable for this particular transfer.

   - Example where derogation is applicable: the transfer by travel agents of personal data concerning their individual clients to hotels or to other commercial partners that would be used to organise these clients' stay abroad, since, in this case, there is a sufficient close and substantial connection between the data transfer and the purposes of the contract (organisation of clients' travel).

2. **Occasional transfers**: it has to be determined on a case by case basis. Data transfer regularly occurring within a stable relationship would be deemed as systematic and repeated, hence not merely of an "occasional" character.

   - Examples where derogation is applicable: personal data of a sales manager travelling for his job to clients in third countries are to be sent to those clients to arrange meetings; personal data from a bank in the EU have to be transferred to a bank in a third county to execute a client's request to make a payment, if this transfer does not occur in the framework of a stable cooperation relationship between the two banks.

3.5.6.3.3 Performance of a contract between a data controller and a third party (Art. 49(1)(c) GDPR)

The cumulative conditions to apply Art. 49 (1) (c) GDPR are:

1. **Necessity of the data transfer and conclusion of the contract in the interest of the data subject**:

- Example where derogation is not applicable: for business purposes, an organisation has outsourced activities such as payroll management to service providers outside the EU. Here, there is no close and substantial link between the transfer and a contract concluded in the data subject's interest, even if the end purpose of the transfer is the management of staff; in this case, standard contractual clauses or binding corporate rules may be suitable for this transfer.

2. **Occasional transfers**: see Point 3.5.6.2 above (General conditions applicable to all paragraphs of Article 49 GDPR).

3.5.6.3.4 Important reasons of public interest (Art. 49(1)(d) GDPR)

The cumulative conditions to apply Art. 49 (1) (d) GDPR are:

1. **Only public interests recognised in Union law or in the law of the Member State to which the data controller is subject can lead to the application of this derogation**: the derogation only applies when it can also be deduced from EU law or the law of the Member State to which the data controller is subject that such data transfers are allowed for important public interest purposes, including in the spirit of reciprocity for international cooperation. The existence of an international agreement or convention which recognises a certain objective and provides for international cooperation to foster that objective can be an indicator when assessing the existence of a public interest, as long as the EU or the Member States are a party to that agreement or convention.

    - Example where derogation is not applicable: the data transfer is requested (for example by a third country authority) for an investigation which serves a public interest of a third country, such as combatting terrorism which, in an abstract sense, also exists in EU or Member State law.

2. **Restricted to specific situations**: the derogation should remain an exception and not become the rule.

3. **Strict necessity test**: See Point 3.5.6.2 above (General conditions applicable to all paragraphs of Article 49 GDPR).

This derogation can be used by public authorities as well as private entities, i.e. public, private or even international organisations. The essential requirement for the applicability of this derogation is that an important public interest is found, rather than the nature of the organisation. For example, international data exchange between competition authorities, tax or customs administrations, between financial supervisory authorities, between services competent for social security matters, or for public health in tracing contagious diseases or in order to reduce and/or eliminate doping in sport.

3.5.6.3.5 Legal claims (Art. 49(1)(e) GDPR)

The cumulative conditions to apply Art. 49 (1) (e) GDPR are:

1. **Establishment, exercise or defence of legal claims**: The relevant procedure has to have a basis in law, including a formal, legally defined process, but it is not necessarily limited to judicial or administrative procedures. The transfer needs to be made in a procedure, so a close link is necessary between a data transfer and a specific procedure regarding the situation in question; the abstract applicability of a certain type of procedure is not sufficient.

    - Examples where derogation is not applicable: transfer on the grounds of the mere possibility that legal proceedings or formal procedures may be brought in the future.

    - Examples where derogation is applicable: criminal or administrative investigation in a third country regarding anti-trust law, corruption, insider trading or similar situations, where the purpose of the transfer is to defend oneself or to obtain a

reduction or waiver of a fine legally foreseen; transfer for formal pre-trial discovery procedures in civil litigation; actions by the data exporter to institute procedures in a third country for commencing litigation or seeking approval for a merger.

2. **National law**: it may contain “blocking statutes”, prohibiting or restricting the transfer of personal data to foreign courts or possibly other foreign official bodies. Data controllers and data processors need to be aware of this.
3. **Necessity of the data transfer**: it requires a close and substantial connection between the data in question and the specific establishment, exercise or defence of the legal position. The mere interest of third country authorities or possible “good will” to be obtained from the third country authority as such is not sufficient. The principle of data minimisation is important; personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed, which means:
    a. There should be a careful assessment of whether anonymised data would be sufficient in the particular case,
    b. If this is not the case, then transfer of pseudonymised data could be considered,
    c. If it is necessary to send personal data to a third country, its relevance to the particular matter should be assessed before the transfer, so that only a set of personal data that is actually necessary is transferred and disclosed.
4. **Occasional transfer**: Each specific case must be carefully assessed.

3.5.6.3.6 Vital interests (Art. 49(1)(f) GDPR)

The cumulative conditions to apply Art. 49(1)(f) GDPR are:

1. **Vital interest of the data subject:** the law assumes that the imminent risk of serious harm to the data subject outweighs data protection concerns. The transfer must relate to the individual interest of the data subject or to that of another person’s and, when it bears on health data, it must be necessary for an essential diagnosis.
    - Examples where derogation is applicable**:** medical emergency and the transfer is directly necessary in order to give the medical care required; it can concern the physical but also mental integrity of the data subject; the data subject, whilst outside the EU, is unconscious and in need of urgent medical care and only his usual doctor, established in an EU Member State, is able to supply data; after the occurrence of natural disasters, the sharing of personal information with entities and persons for the purpose of rescue and retrieval operations can justify the transfer.
    - Example where derogation is not applicable**:** transfer of personal medical data outside the EU only for general medical research that will not yield results until sometime in the future.
2. **Data subject is not able to give his/her consent – physically or legally – to this transfer**: this derogation is not applicable if the data subject is able to make a valid decision. The ability to make a valid decision can depend on physical, mental and legal incapability (e.g. for minors). Legal incapability has to be proved, depending on the case, through a medical certificate or through a governmental document confirming the legal situation of the person.
    - Example where derogation is not applicable: the fact that personal data is required to prevent eviction from a property does not fall under the derogation, even if housing is considered as a vital interest, because the person concerned can provide his consent for the transfer of his data.

3.5.6.3.7 Register (Art. 49 (1)(g) GDPR)

A record is in principle an official list or record of names or items. It can be in written or in electronic format.

The cumulative conditions to apply Art. 49 (1)(g) GDPR are:

1. **Written or electronic register.**
2. **Register intended to provide information to the public**: private registers, which are in the responsibility of private bodies, are outside the scope of the derogation, e.g. private registers regarding credit-worthiness.
3. **Open to consultation either for the public in general or any person who can demonstrate a legitimate interest**: but the conditions for consultation set forth by Union or Member State law need to be fulfilled for the transfer to take place.
    - Examples where derogation is applicable: registers of companies, registers of associations, registers of criminal convictions, (land) title registers or public vehicle registers.
4. **Transfer cannot involve the entirety of the personal data or entire categories of the personal data contained in the register.**
5. **In some cases, transfer can only be done at the request of the person having a legitimate interest or if this person is the recipient of the information**: this condition applies only if the transfer is made from a register established by law and where it is to be consulted by persons having a legitimate interest.

3.5.6.3.8 Compelling legitimate interest (Art. 49(1)§2 GDPR)

This is the derogation of last resort, if no other derogation can be used.

The cumulative conditions to apply Art. 49 (1) §2 GDPR are:

1. **No other derogation applicable:** No adequacy decision, no appropriate safeguards, no binding corporates rules and no derogations for a specific situation stated in Article 49(1) (a-g) GDPR are applicable. If none of these other derogations is applicable, then it is possible to analyse whether Art. 49 (1) §2 GDPR is applicable.
2. **Compelling legitimate interests of the data controller**: only interests which are "compelling" are relevant, so not all "legitimate interests" would fall under the scope of this derogation. This legitimate interest will need to be essential for the data controller.
    - Example where derogation is applicable: data controller is compelled to transfer the personal data in order to protect its organisation or systems from serious immediate harm or from a severe penalty which would seriously affect its business.
3. **Necessity test**: See Point 3.5.6.2 above (General conditions applicable to all paragraphs of Article 49 GDPR).
4. **Not repetitive**: See Point 3.5.6.2 above (General conditions applicable to all paragraphs of Article 49 GDPR).
5. **Limited number of data subjects**: there is no absolute threshold; it will depend on the context, on a case by case basis. For example, if a data controller needs to transfer personal data to detect a unique and serious security incident in order to protect its organisation, it will have to analyse how many employees' data he will have to send.
6. **Balancing the "compelling legitimate interest of the controller" against the "interests or rights and freedoms of the data subject" on the basis of an assessment of all circumstances surrounding the data transfer and providing for suitable safeguards**: a balancing test needs to be performed. The data exporter has to assess all circumstances of the data transfer in question and, based on this assessment, pro-

vide “suitable safeguards” regarding the protection of the data transferred. When assessing the risks and what, under the given circumstances, might be considered as “suitable safeguards” for the rights and freedoms of the data subject, the data controller needs particularly to take into account:

a. Any possible damage (physical and material, but also non-material, e.g. relating to a loss of reputation);

b. The nature of the data;

c. The purpose of the processing;

d. The duration of the processing;

e. The situation in the country of origin;

f. The situation in the third country and, if any, the country of final destination of the transfer;

g. Application of additional measures as safeguards in order to minimise the identified risks caused by the data transfer for the data subject. In the absence of additional safeguards, the data controller’s interests in the transfer will in any case be overridden by the interests or rights and freedoms of the data subject. For example, safeguards might include measures aimed at ensuring deletion of the data as soon as possible after the transfer or limiting the purpose for which the data may be processed following the transfer; technical and organisational measures aimed at ensuring that the transferred data cannot be used for other purposes than those strictly foreseen by the data exporter should be examined.

7. **Information of the supervisory authority**: this does not mean that the transfer needs to be authorised by the supervisory authority, but it is an additional safeguard by enabling the supervisory authority to assess the data transfer. It is advised that the data exporter records all relevant aspects of the data transfer, e.g. the compelling legitimate interest pursued, the “competing” interests of the individual, the nature of the data transferred and the purpose of the transfer.

8. **Providing information on the transfer and the compelling legitimate interests pursued to the data subject**: the data controller must inform the data subject of the transfer and of the compelling legitimate interests pursued. This information must be provided in addition to that required to be provided under Articles 13 and 14 GDPR.

3.5.6.4 Questions from members[57]

3.5.6.4.1 Information to the passenger on transfer of personal data to third countries

A CIT member inquired about a situation where reservations (where personal data must be provided) have been made in trains by a booking system outside the EU. Does the issuer (in a EU country) need to inform the passenger every time a booking with personal data is made, i.e. when personal data has been delivered to a non-EU railway undertaking (and from that non-EU railway undertaking has possibly been passed on again to e.g. State authorities in that country?) Must the allocator keep trace of/store all such bookings in a particular way? Or is it enough that the issuer/seller of such tickets informs the customer “once” that “when the passenger asks to make reservations in a non-EU train, the issuer/seller will pass on personal data that are requested by the authorities in the country of the carrier? If the passenger does not agree to provide the necessary data and to allow its transfer, the issuer/seller is not able to sell a ticket for such trains.

[57] Answers provided by the CIT GS.

In a regular case not concerning third-countries or international organisations, general information to the passengers on the transfer of their personal information during the booking should be sufficient, if this is necessary to fulfil the contract of carriage. However, if the personal data are transferred to a third country, it would be necessary to inform the data subject about any risks and precautionary measures relating to the transfer of personal data to third countries for which there is no adequacy decision of the European Commission and no appropriate safeguards and to have a legal justification for such transfer.

3.5.7 International cooperation for the protection of personal data (Art. 50 GDPR)

[To be drafted ~~by June 2020~~]

3.6 Independent supervisory authorities (Chapter VI GDPR)

[To be drafted ~~by June 2020~~]

3.6.1 Independent status: Supervisory authority (Art. 51 GDPR)

3.6.2 Independent status: Independence (Art. 52 GDPR)

3.6.3 Independent status: General conditions for the members of the supervisory authority (Art. 53 GDPR)

3.6.4 Independent status: Rules on the establishment of the supervisory authority (Art. 54 GDPR)

3.6.5 Competence, tasks and powers: Competence (Art. 55 GDPR)

3.6.6 Competence, tasks and powers: Competence of the lead supervisory authority (Art. 56 GDPR)

3.6.7 Competence, tasks and powers: Tasks (Art. 57 GDPR)

3.6.8 Competence, tasks and powers: Powers (Art. 58 GDPR)

3.6.9 Competence, tasks and powers: Activity reports (Art. 59 GDPR)

3.7 Cooperation and consistency (Chapter VII GDPR)

[To be drafted ~~by June 2020~~]

3.7.1 Cooperation: Cooperation between the lead supervisory authority and the other supervisory authorities concerned (Art. 60 GDPR)

3.7.2 Cooperation: Mutual assistance (Art. 61 GDPR)

3.7.3 Cooperation: Joint operations of supervisory authorities (Art. 62 GDPR)

3.7.4 Consistency: Consistency mechanism (Art. 63 GDPR)

3.7.5 Consistency: Opinion of the Board (Art. 64 GDPR)

3.7.6 Consistency: Dispute resolution by the Board (Art. 65 GDPR)

3.7.7 Consistency: Urgency procedure (Art. 66 GDPR)

3.7.8 Consistency: Exchange of information (Art. 67 GDPR)

3.7.9 European data protection board: European Data Protection Board (Art. 68 GDPR)

3.7.10 European data protection board: Independence (Art. 69 GDPR)

3.7.11 European data protection board: Tasks of the Board (Art. 70 GDPR)

3.7.12 European data protection board: Report (Art. 71 GDPR)

3.7.13 European data protection board: Procedure (Art. 72 GDPR)

3.7.14 European data protection board: Chair (Art. 73 GDPR)

3.7.15 European data protection board: Tasks of the Chair (Art. 74 GDPR)

3.7.16 European data protection board: Secretariat (Art. 75 GDPR)

3.7.17 European data protection board: Confidentiality (Art. 76 GDPR)

3.8 Remedies, liability and penalties (Chapter VIII GDPR)

[To be drafted ~~by June 2020~~]

3.8.1 Right to lodge a complaint with a supervisory authority (Art. 77 GDPR)

3.8.2 Right to an effective judicial remedy against a supervisory authority (Art. 78 GDPR)

3.8.3 Right to an effective judicial remedy against a controller or processor (Art. 79 GDPR)

3.8.4 Representation of data subjects (Art. 80 GDPR)

3.8.5 Suspension of proceedings (Art. 81 GDPR)

3.8.6 Right to compensation and liability (Art. 82 GDPR)

3.8.7 General conditions for imposing administrative fines (Art. 83 GDPR)

3.8.8 Penalties (Art. 84 GDPR)

3.9 Provisions relating to specific processing situations (Chapter IX GDPR)

[To be drafted ~~by June 2020~~]

3.9.1 Processing and freedom of expression and information (Art. 85 GDPR)

3.9.2 Processing and public access to official documents (Art. 86 GDPR)

3.9.3 Processing of the national identification number (Art. 87 GDPR)

3.9.4 Processing in the context of employment (Art. 88 GDPR)

3.9.5 Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (Art. 89 GDPR)

3.9.6 Obligation of secrecy (Art. 90 GDPR)

3.9.7 Existing data protection rules of churches and religious associations (Art. 91 GDPR)

3.10 Delegated acts and implementing acts (Chapter X GDPR)

[To be drafted ~~by June 2020~~]

3.10.1 Exercise of the delegation (Art. 92 GDPR)

4 Examples of clauses

4.1. Consent clause

4.1.1 Reminder: elements to mention in the consent clause

As seen under Point 3.2.3 on consent, different elements need to be mentioned when asking for a person's consent, i.e.:

- Data controller's identity: if there are several data controllers, which of them will process the data,
- Purpose of each of the processing operations for which consent is sought,
- What data will be collected and used,
- Existence of the right to withdraw consent,
- Where applicable:
  - Information about the use of the data for automated decision-making,
  - Possible risks of data transfers to third parties due to absence of an adequacy decision and of appropriate safeguards.

Moreover, the processing of personal data has to be limited to what is necessary. Therefore, even if the consumer has given his consent, the data controller cannot do a "fishing expedition" and collect as much personal data as possible. National legislation can also require that some information is collected; therefore, it is always important to refer to applicable national law too.

There are different ways to formulate a clause of consent, from the shortest to the most detailed.

4.1.2 Example 1: short version of a consent clause

The shortest one consists of a reference with a link to a webpage, where the privacy policy of the company can be found:

"I agree that I have read and accept the Privacy Policy and that I am not under [AGE]"

This short version is not totally compliant with the GDPR, since all the essential elements mentioned under Point 4.1.1 should normally figure directly in the clause of consent and not in another webpage. We would therefore not advise such a short solution.

4.1.3 Example 2: intermediate version of a consent clause

The intermediate solution would be to mention all the essential elements of Point 4.1.1 and to provide more information through a reference to a webpage:

> "I agree to have my personal data [ENUMERATE THE DATA THAT WILL BE COLLECTED AND USED] processed for the purpose of [ENUMERATE THE PURPOSE] by [CONTACT DETAILS OF THE PERSONS HAVING ACCESS TO THE PERSONAL DATA, DATA CONTROLLER'S ALSO]. I can revoke my consent at any time. More information can be found under [WEBSITE]".[58]

An alternative would be:

> "I agree that [ENUMERATE THE DATA THAT WILL BE COLLECTED AND USED] may be used for [ENUMERATE THE PURPOSE] (please tick box if you agree). I can revoke my consent at any time by contacting [CONTACT DETAILS OF THE DATA CONTROLLER]".[59]

[58] Example based on: https://www.intercity.pl/en/dokumenty/formularze/formularz_en.pdf, in a slightly modified form.
[59] Example from: https://www.bahn.com/en/view/mdb/bahnintern/international/redaktion_bahn.com/pdf-datein/pdf_2018/mdb_281742_a4-fahrgastrechte_formular_2018_fgr-en-20181015.pdf, in a slightly modified form.

4.1.4 Example 3: long version of a consent clause

The last option would be the longest one. In this option, instead of referring to a website where the privacy policy can be found, all the information is directly provided in the consent clause. In this solution, the consent clause and the information clause are amalgamated in the same clause.

This solution has the advantage of being thorough, but it is not practical, especially in a non-digital world.

4.2. Information clause[60]

4.2.1 Reminder: elements to mention in the information clause

The information clause is linked to the consent clause. As mentioned before, this information clause can be directly added to the consent clause or it can instead be included in the undertaking's privacy policy website.

Such a clause must in all the cases contain the following information:

- the data controller's identity
- the contact details of the data protection officer, where applicable;
- the purposes of the processing as well as the legal basis for the processing;
- where the processing is based on legitimate interests, the legitimate interests pursued by the controller or by a third party;
- the recipients or categories of recipients of the personal data, if any;
- where applicable, the fact that the data controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or reference to the appropriate or suitable safeguards and the means by which a copy of them can be obtained or where they have been made available;
- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- the existence of the right to request from the data controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to the processing as well as the right to data portability;
- where the processing is based on consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- the right to lodge a complaint with a supervisory authority;
- whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

[60] The way to present such a clause may vary from one company to the other. Some undertakings chose to present it in the form of a list: https://www.sj.se/en/travel-terms/terms-and-conditions-of-data-protection.html##whenyouareamemberofsjpriocovered byacompanyagreementsjbizhaveansjannualpassoraloginaccount ; others to separate the different chapters in different tabs: https://en.oui.sncf/en/privacy; and others to separate the information in sections corresponding to every individual service of the company: https://www.cd.cz/en/info/cim-se-ridime/-31051/. There is no one right way to do it, but the most important thing is that the data subject understands the information provided.

- the existence of automated decision-making, including profiling, and, at least in these cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

4.2.2 Example 1: Long formal version of an information clause [61]

A detailed version containing all this information would be:

"**Privacy Policy**

This website is managed by [COMPANY + CONTACT DETAILS]. You are invited to familiarise yourself with the information below, which details the management of your personal data and the conditions of use of the website.

The protection of the personal data of the persons it is in contact with is very important to [COMPANY]. Hereinafter, we set out the principles we follow and for what purpose we collect and process personal data (this means information that determines your identity or allows us to identify you) via this website, and other means operated by [COMPANY].

We collect and process your personal data carefully, only for the purposes described in this Privacy Statement and only to the extent necessary as defined therein and within the scope of the applicable legal regulations. We only store your personal data to the extent and as long as it is required for the performance of our services or as we are legally obligated.

This confidentiality charter applies to all sites, mobile applications and services of [COMPANY].

Personal data collected:

At [COMPANY], we scrupulously follow the principle of "minimisation", meaning that we collect only the data that is strictly necessary to the purposes defined above, namely:

- identification data (name, email address, IP address): this data is essential for any orders, registration for a customer account or for the security of the sites and transactions of [COMPANY];
- banking data: this data is essential for any orders or reimbursements. Also, you can register your banking details (except the card security code) in your customer account to facilitate your future purchases;
- data related to your searches and your order [product purchased (destination, date, price,…)]: this data is essential to provide the ordered service and after-sales service;
- data related to your habits and centres of interest (favourite destinations, choice of additional services,…): this data is useful for making personalised offers;
- contact data (telephone No., email address, postal address): this data is useful to contact you if required (problem relating to your order or a purchased product, travel information) or to send you your train tickets, either to your home or electronically;
- technical data: during browsing, [COMPANY] collects information such as the version of your browser, operating system used or the model of terminal used. This data is necessary for optimal display and functioning of [COMPANY] sites and applications;
- geolocation: the [COMPANY] mobile application includes a geolocation function that can be activated exclusively through consent from you. This data lets us offer you personalised services (closest station/next departure from the nearby station);

[61] Example derived from different websites, in particular:
https://en.oui.sncf/en/privacy.
https://www.cp.pt/passageiros/en/privacy.
https://www.cit-rail.org/en/datenschutzerklarung-en/.

- browsing data (searches, number of visits, date of last visit,…): this data is useful for making commercial offers.

Consent:

The personal data transmitted by the data subject may require his/her express consent, in accordance with the intended purpose. In such cases, the data subject freely gives his/her consent in a specific, informed and explicit way, in each of the means of interaction with [COMPANY].

The data subject may always require the withdrawal of any of his/her consents for the corresponding processing. Consent can be withdrawn through the website, in the personal area, or by filling out a specific form to be delivered to our sales points upon unambiguous identification of the data subject. The consent withdrawal, regarding specific personal data processing, does not compromise the lawfulness of the processing already carried out based on such consent.

Purpose of the processing:

The personal data transmitted by the data subject through the different means of interaction with [COMPANY] is intended for one or several of the following purposes:

- processing your orders:
    - enabling carriers and travel partners to provide you with services ordered,
    - ensuring payment for the products that you have purchased,
    - monitoring and providing after sales service for products ordered (information, cancellations, reimbursements, exchange, complaints);
- managing your customer account: at [COMPANY], the customer account is not mandatory. However, it is very useful because it is an account that is entirely dedicated to you and makes it easy for you to:
    - easily place orders (automatic entry of your data: identification, subscription cards, bank details, travel preferences),
    - access your order data;
- communicate with you: for [COMPANY], maintaining contact with you is essential, but we only do so in a carefully controlled manner and we only send you electronic communications, via email, SMS or mobile notification, for the following reasons:
    - monitoring orders: sending confirmations of orders and any other messages relating to the service that you have ordered,
    - the management of your customer account: confirmation of creation or closure, modification of passwords,
    - making commercial offers: only in one of the following two cases:
        - if you are registered for the "Newsletter" service from [COMPANY];
        - if you have ordered products on the [COMPANY] site or the [COMPANY] mobile application;
        - In all cases, you may unsubscribe from our commercial newsletter service by clicking on the "unsubscribe" link at the bottom of the newsletters
- offering you personalised products and services: at [COMPANY], we are intent on constantly offering you products that are most likely to be suitable for you. At [COMPANY], we offer you personalised content:
    - in the commercial communications that we send to you,
    - when you browse the [COMPANY] sites,

- through certain services using geolocation (only on the [COMPANY] mobile application),
- via targeted and personalised advertising banners on other sites;

- fighting fraud: the security and proper functioning of our sites is a major issue. The data is analysed automatically by our subcontractor [NAME + CONTACT DETAILS] to determine a level of fraud risk associated with each order.
  - The analysis criteria include the browsing behaviour, the data relating to the terminal used and the bank details
  - According to the results of this risk analysis, and after a check by our anti-fraud teams, [COMPANY] may do one of the following:
    - validate your order;
    - request additional substantiating documentation;
    - refuse the order;
    - cancel the order and reimburse the funds.
  - In case of any confirmed problem with an order, or in the case of an outstanding debt, your data will be written to an alert file belonging to [COMPANY], which may, for future orders, make additional checks.
  - You can, at any time, make a complaint or request information by contacting [COMPANY] customer services.
- offer you games/competitions: in this context, [COMPANY] and/or its partners will use the data that you have agreed to communicate strictly for the purposes of implementing the game/competition and communication.

Recipients of the personal data collected:

Access to your personal data is strictly limited to our administrative personnel, our employees, the accounts department, and, as appropriate, to our subcontractors. The subcontractors in question are bound by an obligation of confidentiality and may only use your data in accordance with our contractual provisions, and the applicable legislation.

Other than the cases detailed above, we undertake not to give third parties access to your data without your prior consent, unless we are required to do so due to a legitimate reason (a legal obligation, measures against fraud or abuse, the exercise of rights of defence, etc.).

Your data may be sent abroad, so long as the destination State is deemed capable of guaranteeing an appropriate level of protection, or if this transfer operates in the context of an international treaty with this State. In default of this, you will be expressly informed of such a transfer, and you will be requested to give your consent in advance.

Protection and safety:

[COMPANY] undertakes to adopt administrative, technical, physical and organisational measures which ensure the safety, integrity and privacy of the data subject's personal data, appropriate to the risk of each processing and consistent with the practices established in the European Union. Such measures are applied to protect the personal data against its dissemination, improper use, non-authorised access or the loss, change or destruction, as well as any other form of unlawful processing.

Partners and subcontractors who have access to personal data shall be obliged to adopt the safety, organisational and technical protocols and measures required for the protection of such data.

The data used to make payments, particularly regarding credit/debit cards, are provided directly in the platforms of the corresponding service providers. [COMPANY] does not have access to such data.

The data subject ensures that the personal data he/she provides is true and accurate and undertakes to notify any change thereof. Any damage caused to [COMPANY] or to any third party due to the provision of incorrect, inaccurate or incomplete information in the registration forms, is the sole responsibility of the person who introduced or provided such information.

The data subject undertakes not to disclose his/her username and password. If he/she decides to share such data with someone, he/she shall be responsible for all activities performed in his/her personal area of [COMPANY].

Data subject's rights:

The legislation of data protection grants data subjects the right to information regarding the purposes and processing of their data, the right to access, correct, delete and restrict the processing, and the right to transfer their data and contest automated individual decisions.

To exercise the above-mentioned rights, the data subject shall contact the Data Protection Officer of [COMPANY] [NAME + CONTACT DETAILS].

The data subject may also submit a complaint to the competent national supervisory authority [CONTACT DETAILS].

Personal data storage period:

When there is no specific legal requirement, the personal data shall be stored for no longer than is absolutely necessary in order to comply with the purposes for which the data were collected. The period during which the data is stored depends on the purpose for which the information is processed.

Contacts:

The data subject may contact us for any questions regarding the application of the General Data Protection Regulation by [COMPANY], through the website page of Customer Information/Contacts, the e-mail [COMPANY] or by mail sent to the Data Protection Officer, [NAME + CONTACT DETAILS].

Privacy policy changes:

In order to ensure the adequacy of the document, [COMPANY] may at any time change this Privacy Policy, without prior notice and with immediate effect. Such changes shall be properly advertised on the website and at ticket offices and, if necessary, the data subject must confirm that he has taken note of the change and must give his consent to it.

This Privacy Policy was updated on [DATE]".

4.2.3 Example 2: Long, more casual version of an information clause [62]

"**Privacy Policy**

This website is managed by [COMPANY]. You are invited to familiarise yourself with the information below, which details the management of your personal data and the conditions of use of the website.

The protection of the personal data of the persons it is in contact with is very important to [COMPANY]. Hereinafter, we set out the principles we follow and for what purpose we collect and process personal data (this means information that determines your identity or allows us to identify you) via this website, and other means operated by [COMPANY].

We collect and process your personal data carefully, only for the purposes described in this privacy statement and only to the extent necessary as defined therein and within the scope of the applicable legal regulations. We only store your personal data to the extent and as long as it is required for the performance of our services or as we are legally obligated.

> This confidentiality charter applies to all sites, mobile applications and services of [COMPANY].

[62] Example derived from different websites, in particular:
https://en.oui.sncf/en/privacy.
https://www.cp.pt/passageiros/en/privacy.
https://www.cit-rail.org/en/datenschutzerklarung-en/.

Personal data collected:

At [COMPANY], we scrupulously follow the principle of "minimisation", meaning that we collect only the data that is strictly necessary for the purposes defined above, namely:

- identification data (name, email address, IP address): this data is essential for any orders, registration for a customer account or for the security of the sites and transactions of [COMPANY];
- banking data: this data is essential for any orders or reimbursements. Also, you can register your banking details (except the card security code) in your customer account to facilitate your future purchases;
- data related to your searches and your order (product purchased (destination, date, price,…)): this data is essential to provide the ordered service and after-sales service;
- data related to your habits and centres of interest (favourite destinations, choice of additional services,…): this data is useful for making personalised offers;
- contact data (telephone No., email address, postal address): this data is useful in order to contact you if required (problem relating to your order or a purchased product, travel information) or to send you your train tickets, either to your home or electronically;
- technical data: during browsing, [COMPANY] collects information such as the version of your browser, operating system used or the model of terminal used. This data is necessary for optimal display and functioning of […] sites and applications;
- geolocation: the [COMPANY] mobile application includes a geolocation function that can be activated exclusively through consent from you. This data lets us offer you personalised services (closest station/next departure from the nearby station);
- browsing data (searches, number of visits, date of last visit,…): this data is useful for making commercial offers.

The sources of data are:

- You:
    - when you complete forms on the [COMPANY] sites and applications,
    - when you browse [COMPANY] sites and applications (pages consulted, duration of consultation of pages),
    - when you specifically give your consent,
    - For each of them, you are informed of the data that is necessary and that which is optional, by asterisks on the entry forms.
- the technical information:
    - your IP address, the telecoms operator and the macroscopic location of the IP address,
    - the information provided by the browser on the operating system and the browser used,
    - cookies.

Purpose of the processing:

The personal data transmitted by the data subject through the different means of interaction with [COMPANY] is intended for one or several of the following purposes:

- processing your orders:
    - enabling carriers and travel partners to provide you with services ordered,
    - ensuring payment for the products that you have purchased,
    - monitoring and providing after sales service for products ordered (information, cancellations, reimbursements, exchange, complaints);
- managing your customer account: at [COMPANY], the customer account is not mandatory. However, it is very useful because it is an account that is entirely dedicated to you and makes it easy for you to:
    - easily give orders (automatic entry of your data: identification, subscription cards, bank details, travel preferences),
    - access your order data;
- communicate with you: for [COMPANY], maintaining contact with you is essential, but we only do so in a carefully controlled manner and we only send you electronic communications, via email, SMS or mobile notification, for the following reasons:
    - monitoring orders: sending confirmations of orders and any other messages relating to the service that you have ordered,
    - the management of your customer account: confirmation of creation or closure, modification of passwords,
    - making commercial offers: only in one of the following two cases:
        - if you are registered for the "Newsletter" service from [COMPANY];
        - if you have ordered products on the [COMPANY] site or the [COMPANY] mobile application;
        - In all cases, you may unsubscribe from our commercial newsletter service by clicking on the "unsubscribe" link at the bottom of the newsletters
- offering you personalised products and services: at [COMPANY], we are intent on constantly offering you products that are most likely to be suitable for you. At [COMPANY], we offer you personalised content:
    - in the commercial communications that we send to you,
    - when you browse the [COMPANY] sites,
    - through certain services using geolocation (only on the [COMPANY] mobile application),
    - via targeted and personalised advertising banners on other sites;
- fighting fraud: the security and proper functioning of our sites is a major issue. The data is analysed automatically by our subcontractor [name + contact details] to determine a level of fraud risk associated with each order.
    - The analysis criteria include the browsing behaviour, the data relating to the terminal used and the bank details
    - According to the results of this risk analysis, and after a check by our anti-fraud teams, [COMPANY] may do one of the following:
        - validate your order;

        - request additional substantiating documentation;
        - refuse the order;
        - cancel the order and reimburse the funds.
    - In case of any confirmed problem with an order, or in the case of an outstanding debt, your data will be written to an alert file belonging to [COMPANY], which may, for future orders, make additional checks.
    - You can, at any time, make a complaint or request information by contacting [COMPANY] customer services.
- offer you games/competitions: in this context, [COMPANY] and/or its partners will use the data that you have agreed to communicate strictly for the purposes of implementing the game/competition and communication.

Recipients of the personal data collected:

Access to your personal data is strictly limited to our administrative personnel, our employees, the accounts department, and, as appropriate, to our subcontractors. The subcontractors in question are bound by an obligation of confidentiality and can only use your data in accordance with our contractual provisions, and the applicable legislation.

Other than the cases detailed above, we undertake not to give third parties access to your data without your prior consent, unless we are required to do so due to a legitimate reason (a legal obligation, measures against fraud or abuse, the exercise of rights of defence, etc.).

Your data may be sent abroad, so long as the destination State is deemed capable of guaranteeing an appropriate level of protection, or if this transfer operates in the context of an international treaty with this State. In default of this, you will be expressly informed of such a transfer, and you will be requested to give your consent in advance.

Protection and safety:

[COMPANY] is particularly vigilant concerning the security of your data and devotes significant human and technical resources to protect it. A strict security policy is in place to define the processes, working methods and rules for technical protection to be used. The security measures used include, but are not limited to:

- automated systems for protection against cyber attacks are active;
- computer code on the [COMPANY] websites is subject to security reviews;
- automated tools periodically carry out security tests on the websites;
- the security of websites is audited by companies that are experts in the subject;
- personal data of customers is subject to strict access control;
- experts in cyber security can intervene at any time to handle security incidents.

Data subject's rights:

In accordance with the provisions of Regulation No 2016/679, known as the General Data Protection Regulation (GDPR), you have the following rights concerning your data and the right to make sure that [COMPANY] is complying with its commitments:

- Right of access: you may contact us to find out what data [COMPANY] has concerning you;
- Right to correction and deletion: you may correct data concerning you and request that it be deleted;
- Right of objection: you may object to [COMPANY] performing various processes;

- Right to portability: you may request that [COMPANY] sends you the data concerning you (identification and order data exclusively) in an electronic format (CSV file).

It is nevertheless reiterated that the exercise of these rights is not absolute and may be limited for reasons of legitimate interest (customer dispute) or for legal reasons.

How can I exercise my rights?

- Right of access, correction, deletion and portability:
  - If you have a customer account, you can undertake these operations directly, by connecting to your customer account.
  - If not, you may send your requests to [COMPANY] customer services using the following electronic form or by letter to the following address: [CONTACT DETAILS]
- Right of objection: you may exercise your right of objection as follows:
  - for commercial newsletters: by clicking the "unsubscribe" link mentioned in the newsletters that are sent to you by [COMPANY], which then undertakes not to send you any more commercial newsletters;
  - for personalisation and cookies: by using [see below under Cookies];
  - for all other requests: by sending your requests to [COMPANY] customer services using the following electronic form or by letter to the following address: [CONTACT DETAILS].

For all of these requests, and for security reasons, you will be asked to identify yourself and communicate a copy of your identity document to [COMPANY] customer services.

What should be done in case of a dispute?

If you are not satisfied with a response to one of these rights, or in case of a dispute on the use of your data, you may send your requests:

- To the [COMPANY] Personal Data Protection Officer [CONTACT DETAILS]
- To the supervisory authority [CONTACT DETAILS]

Personal data storage period:

The data is only kept for periods that are strictly necessary:

- for the implementation of orders;
- for legal and regulatory constraints, notably in matters of dispute management;
- for the provision of personalised services.

The general data retention policy used by [COMPANY] is as follows:

- identification data: three years from the last visit to the site or connection to the service;
- order data: three years from the date of the order;
- bank details: either a maximum of 13 months in order to manage the after-sales service (reimbursements), or for the period of validity of the bank card in case it is recorded on the customer account;
- prospect data: one year after the date of the last activity on [COMPANY] sites or the last opening of a newsletter;
- connection logs: one year from each connection;
- cookies: 13 months maximum from their being saved on your computer or terminal;
- geolocation data: only for the browsing session.

Contacts:

The data subject may contact us for any questions regarding the application of the General Data Protection Regulation by [COMPANY], through the website page of Customer Information/Contacts, the e-mail [COMPANY] or by mail sent to the Data Protection Officer, [NAME + CONTACT DETAILS].

Privacy policy changes:

In order to ensure the adequacy of the document, [COMPANY] may at any time change this privacy policy, without prior notice and with immediate effect. Such changes shall be properly advertised on the website and ticket offices and, if necessary, the data subject must confirm that he has taken note of the change and must give his consent to it.

This privacy policy was updated on [DATE]".

4.2.4 Example 3: Short version of an information clause[63]

The information clause can also be shorter. However, the risk is that some elements mentioned under Point 4.2.1 might be forgotten.

"The administrator of personal data provided in relation to [TYPE OF DOCUMENT PROVIDED, e.g. claim, refund application, complaint, information, suggestions] is [COMPANY], with its registered office in [ADDRESS]. If you have any questions relating to the processing of personal data, we recommend that you contact the Data Protection Officer appointed by the controller, [NAME + ADDRESS]. Your personal data is collected and processed in order to deal with your claim/request for compensation/request for information/suggestions. The scope of the data includes the data given in the [TYPE OF DOCUMENT PROVIDED, e.g. claim, refund application, complaint, information, suggestions]. The legal basis for processing is Art. [LEGAL BASIS, e.g. 6 § 1 letter a and letter c GDPR]. The period of personal data processing is [PERIOD OF TIME, e.g. 5 years; OR indicate that the data will be processed as long as it is necessary for the case]. You have the right to withdraw your consent, request access to personal data, rectify it, delete it, restrict its processing, transfer it or object to its processing. Persons who do not have full legal capacity are required to obtain the prior consent of their parents or legal guardians. You have the right to lodge a complaint with the supervisory authority competent for data processing [CONTACT DETAILS OF THE SUPERVISORY AUTHORITY]".

4.3. Cookies clause

4.3.1 Reminder: Elements to mention in the cookies clause

This topic falls also under the scope of the future E-Privacy Regulation. Many websites already integrate clauses on cookies.

The important elements to mention when a website contains/uses cookies are:

- Type of cookies
- How cookies are used
- Possibility for the customer to refuse cookies

A clause on cookies can be really detailed or only make reference to a webpage providing more details on the cookies. It is important, in any case, that the customer has the choice to refuse such cookies; such a possibility must be available in the website.

4.3.2 Example 1: Short version of a cookies clause

The short version regarding cookies would be to have a link where all the information is provided:

"This website uses cookies and analytics tools. Further information can be found under Privacy Policy"[64]

[63] https://www.intercity.pl/en/dokumenty/formularze/formularz_en.pdf.
[64] Example derived from: https://www.cit-rail.org/en/datenschutzerklarung-en/.

and there will be a box where the customer can decide whether to accept or refuse the use of such cookies.

An alternative would be:

> "This website uses cookies. By continuing to browse the website, you are agreeing to our use of cookies. You can block them through your browser. However, some areas will not work properly. For more information, visit our Privacy Policy".[65]

and there will be a box where the customer can decide whether to accept or refuse the use of such cookies.

Under the privacy policy, the following clause will then be found:[66]

"**Cookies policy**

Cookies are files that are placed in the browser on the user's computer or terminal when it browses the [NAME] site. These files are subsequently automatically sent by the browser to the servers of [COMPANY] during your browsing, in order:

- to enable browsing on [COMPANY] sites (management of shopping baskets, customer account connection sessions, proof of authentication for the "remember me" function, servers used, etc.) or to adapt to the user's terminal (language used, display resolution, operating system of the site);
- to monitor customer browsing on [COMPANY] sites and to measure audiences to optimise and improve the sites;
- to personalise the click path and the offers;
- to manage advertising on [COMPANY] and other sites.

Who are the cookies placed by?

These files are placed:

- Either by [COMPANY]
- Or by third parties: when browsing [COMPANY] site, cookies are issued by third-party companies (companies providing user help, advertising service providers, communications agency, audience measurement companies, etc.), subject to choices that the user has made previously with their services, or at any time under the conditions described below.

These cookies are mainly intended to provide the user with advertising content likely to correspond to your centres of interest according to the data collected during your browsing on the sites of [COMPANY].

These cookies may also enable:

- counting of the number of displays of advertising content disseminated via the advertising spaces on the sites of [COMPANY], identification of the advertisements displayed and the number of users who clicked on each advertisement, in order to calculate amounts due and prepare statistics;
- recognition of the user's computer or terminal during his browsing on any other site in order to adapt the advertisements that are disseminated there.

The issue, use and management of these third-party cookies are subject to the confidentiality and data-protection policies of these third-party companies. However, when [COMPANY] actually knows the purpose and means of management of these cookies, it will inform the user.

[65] Example derived from: https://www.cp.pt/passageiros/en/passenger-information/Contacts.
[66] Example derived from different websites, in particular:
https://en.oui.sncf/en/privacy.
https://www.cp.pt/passageiros/en/privacy.
https://www.cit-rail.org/en/datenschutzerklarung-en/.

Also, if the computer or terminal is used by several persons, or if it has several browsers, it is not possible for [COMPANY] to be sure that the services and advertisements correspond to the user's use of [COMPANY] sites and not that of another user. This choice of sharing and configuration is the user's free choice and responsibility.

Detailed description of the cookies of [COMPANY]:

- Strictly necessary cookies:
    - browsing sessions (connection to customer account, technical browsing session, servers used);
    - simplification of the visit, with adaptation of display criteria to your computer or terminal (language used, display resolution, operating system, browser used, accessibility parameter);
    - detection of a previous visit;
    - registration of customer preferences;
    - automatic re-connection to the customer account (when activated).

  These cookies are necessary for the correct functioning of the website of [COMPANY] and for browsing.
- Analytical cookies:
    - audience measurement: statistical data on traffic and the use of the sites of [COMPANY] (sections and content targeted, click path) in order to measure and study the functioning and efficiency of [COMPANY] sites, and thus improve the benefit and ergonomics of the services of [COMPANY];
    - comparative tests of several versions of the site (AB Testing).

  These cookies enable the continuous improvement of the sites and services of [COMPANY] (benefits, ergonomics,…).
- Functional cookies:
    - personalisation, in real-time, of browsing on the sites of [COMPANY] and proposal of relevant and personalised offers;
    - improvement of ergonomics;
    - identification of browsing problems in order to offer the assistance of a call-centre agent.

  These cookies enable the user to be offered products and services that are personalised and in accordance with his requirements and centres of interest.
- Advertising cookies:
    - counting and personalisation of content and advertisements proposed when the user visits the sites of [COMPANY];
    - connections to social network services, sharing information on social networks.

  These cookies enable the most relevant offers to be provided to the user.

How are they put in place?

When browsing the sites of [COMPANY]:

- the user is informed of the existence of cookies via the navigation banner that appears when he first visits or in case he deletes the cookies placed by [COMPANY];

- he consents to the placing and use of cookies by every browsing act.

How do I express my choices concerning cookies?

In most cases, the cookies are deleted when you close your browser (session cookies). Some cookies are more persistent and remain in the user's browser until they expire or until the user deletes them.

The user can change the definitions of his browser to block or delete cookies, or to warn him every time a new cookie is stored on his computer, enabling him to decide whether or not to accept it. If he decides to block or delete the cookies, he may not be able to access all the services and it may have some impact on the performance of the website in his system.

More information regarding the setting of each type of browser (e.g. Firefox, Chrome, Explorer, Opera) can be found in the corresponding institutional websites".

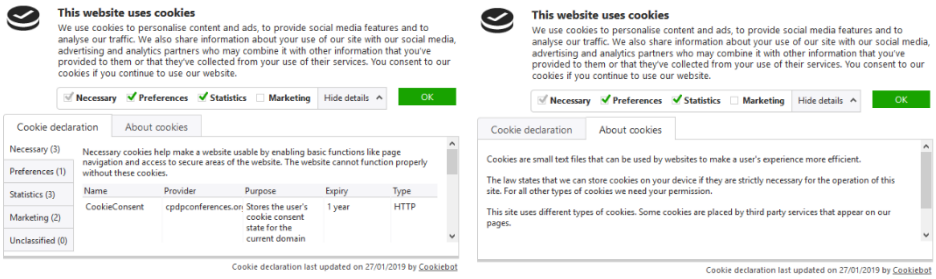
4.3.3 Example 2: Long version of a cookies clause

Another option is to provide all the information directly when the user arrives on the website, by also giving the user the opportunity to choose if and which cookies he accepts.

The following solution has been found on different websites[67] and seems to be the most effective way to provide information and obtain valid consent from the customer, when dealing with cookies.

- Definition of cookies
- Purpose of the use of cookies
- Types of cookies, their name, provider, purpose and expiry date
- Boxes that the customer can tick, and which permit him to decide whether he wants to accept the use of cookies or not (and which cookies he wants to accept), with the limitation that it is not possible to refuse the use of "necessary cookies".

[67] See in particular:
https://www.cpdpconferences.org/
https://www.swissbanking.org/en/topics/information-for-private-clients/privacy-and-data-protection



4.4. Links

4.4.1 Reminder: Elements to mention about links

On websites, it is often the case that links to other pages are provided. It might be useful to include in the privacy policy a point explaining that there is no responsibility regarding data protection for other websites.

4.4.2 Example of a clause about links on a website[68]

“In its website, [COMPANY] has included links to other Internet pages or to resources managed by third parties, including its partners. [COMPANY] assumes no responsibility for the consent, accuracy, availability and privacy practices of such Internet pages or external resources. [COMPANY] shall not be liable, directly or indirectly, for damages, losses or violations caused by, or perceived to be caused by, or related to the use of such Internet pages or external resources.”

[68] Example from: https://www.cp.pt/passageiros/en/privacy.

5 Boilerplate contracts on data processing

5.1 CIT Model Data Processing Contract

Preamble

This model Data Processing Contract is provided to CIT members to assist them in drafting their data processing contracts with data processors. The model contract is in line with Article 28 of the GDPR. CIT members shall adjust this model contract to include any additional obligations required by national data protection laws and regulations.

Contract

between

Undertaking X (name, address), <private> company <with limited liability> <NAME>, with its registered office and principal place of business at <address>, (<post code>) <town/city>, trade register number <number>, legally represented by <position + name>, acting as the "Data Controller", hereinafter referred to as "**[CIT Member**]"

and

Undertaking Y (name, address, customer code), <private> company <with limited liability> <NAME>, with its registered office and principal place of business at <address> in (<post code>) <town/city>, creditor number <number>, trade register number <number>, legally represented by <position + name>, hereinafter referred to as the **"Data Processor"**,

hereinafter collectively referred to as the **"Parties"** or separately as a **"Party"**.

1 Subject-matter of the Data Processing Contract

1.1 [CIT Member] subcontracts certain Services (as defined below), that require the processing of personal data, to the Data Processor. This Data Processing Contract contains the entire agreement and understanding between the Parties with respect to the subject matter hereof.

1.2 This Data Processing Contract lays down the rights and obligations of the Parties in accordance with Article 28 of the GDPR[69] .

1.3 The legal terms used in this Data Processing Contract shall have the meaning defined in Article 4 of the GDPR. GDPR refers to the EU General Data Protection Regulation 2016/679. All other legal terms are defined in the CIT Glossary.

1.4 This Data Processing Contract consists of eighteen Points and four Appendices, which are deemed to be an inseparable part of this Data Processing Contract:

Appendix 1: Service Description and Pricing

Appendix 2: Data Processing, Technical and Organisational Security Measures

Appendix 3: Dealing with Data Breaches

Appendix 4: Transfer of Personal Data to Data Processors outside the European Economic Area

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

2 Object and purpose of the Data Processing Contract

This Data Processing Contract applies to the processing of Personal Data in the context of the fulfilment of the Services set out in **Appendix 1**.

3 Pricing and Payment

3.1 In return for the Services provided, [CIT Member] shall pay the Data Processor the amounts indicated in **Appendix 1**.

3.2 All amounts mentioned in this Data Processing Contract are exclusive of VAT.

3.3 Unless agreed otherwise by the Parties, invoices shall be paid within a period of thirty (30) days following receipt thereof.

4 Relationship between the Parties

4.1 In accordance with this Data Processing Contract, [CIT Member] gives the Processor instructions to process Personal Data for the fulfilment of the Services described in **Appendix 1**.

4.2 With respect to the processing of Personal Data, [CIT Member] is the Data Controller, whereas [XXX] is the Data Processor, as defined in the GDPR. [CIT Member] has and retains independent control of the purpose for which the Personal Data is processed and of the resources used to do so.

4.3 Prior to entering into this Data Processing Contract, the Data Processor shall ensure that [CIT Member] is sufficiently informed about the Service(s) provided by the Data Processor and about the data processing to be carried out. The information provided must enable [CIT Member] to make a choice in relation to the services offered as such, and also to make a separate choice for any optional services offered. In order to be covered by this Data Processing Contract, the Services referred to in **Point 2**, including any optional services, must be listed in **Appendix 1**.

4.4 [CIT Member] and the Data Processor will give each other all the required information to ensure proper compliance with the relevant legislation and regulations regarding privacy.

5 Processing of Personal Data and related obligations of the Data Processor

5.1 The processing of Personal Data as part of the performance of the Services mentioned in **Appendix 1** shall comply with the applicable data protection laws and regulations, including the GDPR and any additional national legislation.

5.2 The Data Processor shall undertake not to use the Personal Data obtained from [CIT Member] for other purposes or in any other way than that for which the data has been transmitted or disclosed. The Data Processor is therefore not authorised to carry out any data processing operations other than those entrusted to it by [CIT Member]. This obligation applies both during the term of this Data Processing Contract and after this Data Processing Contract has ended for [XX] years.

5.3 **Appendix 1** to this Data Processing Contract contains a summary of the Personal Data categories used.

5.4 The Data Processor shall:

5.4.1 create and maintain a record of its data processing activities under this Data Processing Contract; if requested to do so, the Data Processor shall, at the first time of asking, make the record available to [CIT Member], any auditor appointed by the latter, and/or the supervisory authority;

5.4.2 promptly inform [CIT Member] if it is not able to comply with [CIT Member's] instructions with respect to the processing of the Personal Data or with any other obligation under this Data Processing Contract;

5.4.3 inform [CIT Member] immediately if it believes that any instructions from [CIT Member] infringe the GDPR or other applicable data protection laws and regulations;

5.4.4 deal promptly and properly with all reasonable inquiries from [CIT Member] relating to the processing of Personal Data under this Data Processing Contract;

5.4.5 make available to [CIT Member] all information necessary to demonstrate compliance with the GDPR or other applicable data protection laws and regulations;

5.4.6 not process the Personal Data for longer than the required retention period. [CIT Member] will adequately inform the Data Processor about the (legal) retention periods applicable to the processing of the Personal Data;

5.4.7 submit its data processing facilities for audit or control of the data processing activities, in accordance with **point 7.7** of this Data Processing Contract;

5.4.8 promptly notify [CIT Member] of:

a) any legally binding request for disclosure of the Personal Data by a data subject or by a judicial or regulatory authority (unless prohibited from doing so, for example by an obligation under criminal law to preserve the confidentiality of a judicial investigation), and to assist [CIT Member] herewith,

b) any accidental or unauthorized access, and any unlawful processing more generally, and to assist the [CIT Member] herewith;

5.4.9 not pass Personal Data on to Third Parties, unless this exchange takes place on the instructions of [CIT Member] or if it is necessary to meet a legal obligation imposed on the Data Processor. The Data Processor shall ensure that everyone involved in processing the Personal Data, including its employees, representatives and/or Sub-processors, has entered into a confidentiality agreement or accepted a confidentiality clause. Should transfer to Third Parties be required by a legal obligation, the Data Processor shall verify the basis for the request and the identity of the requesting party prior to transferring any Personal Data. In addition, if legally allowed to do so, the Data Processor shall notify [CIT Member] immediately of the transfer, if possible prior to transferring the Personal Data;

5.4.10 refrain from engaging any Data Sub-processor without the prior written consent of [CIT Member]. See the additional conditions with respect to Data Sub-processors as detailed in **point 10** and **Section E** of **Appendix 1**;

5.4.11 [subject to additional compensation agreed in advance], assist [CIT Member] in complying with the Data Controller's obligations under the applicable data protection laws and regulations.

5.5 The personal data subject to this Data Processing Contract shall not be transferred to any country outside the European Economic Area without prior written consent from [CIT Member]. If the Personal Data is transferred to a country outside the European Economic Area, the Parties shall ensure that said Personal Data is adequately protected in line with the GDPR. Any transfer of Personal Data to a country outside the European Economic Area shall be subject to the conditions of **Appendix 4**, unless the country of destination to which the Personal Data is transferred is covered by an adequacy decision of the European Commission.

6 Confidentiality

6.1 Each Party to this Data Processing Contract acknowledges that during the performance of its obligations, a Party (the "receiving Party") may become privy to confidential information which is disclosed by the other Party (the "disclosing Party").

6.2 The receiving Party shall keep confidential all such confidential information as well as the Personal Data, and shall not disclose it to any third party or use it for any other purposes than those of this Data Processing Contract.

6.3 Each Party agrees that before any of its employees, Sub-processors or agents are given access to confidential information and/or Personal Data, each of them shall agree to be bound by a confidentiality agreement under comparable terms and conditions to those defined in this Data Processing Contract.

6.4 The Data Processor shall ensure in each case that access is strictly limited to those individuals who need to know / access the Personal Data for the purposes of this Data Processing Contract.

6.5 If the receiving Party has a legal duty to disclose confidential information, e.g. by a court order, the receiving Party shall, to the extent possible, inform the disclosing Party of this fact without delay, thereby enabling the disclosing Party to seek an interlocutory injunction or other appropriate remedy.

7 Security and checks

7.1 The Data Processor shall take appropriate technical and organisational measures to secure Personal Data against loss or against any form of unlawful data processing. These measures shall ensure an appropriate level of security, taking into account technical developments and implementation costs, and having regard to the risks associated with the processing of Personal Data and the nature of the Personal Data to be protected.

7.2 The measures referred to in **point 7.1** shall include, at the very least:

- pseudonymisation and encryption of the Personal Data;
- measures enabling the availability of and access to the Personal Data to be restored in a timely manner in the event of a physical or technical incident;
- measures guaranteeing that only authorised employees have access to the Personal Data being processed under the Data Processing Contract;
- measures protecting the Personal Data, in particular against unintentional or unlawful destruction, unintentional loss or modification, or unauthorised or unlawful storage, processing, access or publication;
- measures whereby weak spots in the processing of Personal Data can be regularly identified in the systems used for providing services to [CIT Member];
- an appropriate information security policy for processing Personal Data.

7.3 The Data Processor shall evaluate and strengthen, supplement or improve the information security measures it has taken, insofar as the requirements or technological or other developments give reason to do so.

7.4 The agreements between the Parties on the technical and organisational measures to be taken and the content and frequency of the reports to be supplied by the Data Processor to [CIT Member] on the security measures shall be recorded in **Appendix 2**. These measures shall be compliant with the security measures that [CIT Member] is required to take.

7.5 The Data Processor may use its adherence to an approved code of conduct or an approved certification mechanism to demonstrate its compliance with the technical and organisational measures required.

7.6 The Data Processor shall enable [CIT Member] to comply with its legal obligations to monitor compliance by the Data Processor, in particular with the technical and organisational security measures, and with the obligations regarding Data Breaches as stated in **Point 8**.

7.7 [CIT Member] may at any time audit (or commission an audit of) the technical and organisational security measures taken by the Data Processor to ensure compliance with the GDPR, the applicable legislation and regulations, and this Data Processing Contract. This audit, the cost of which shall be

borne by [CIT Member], shall be arranged in consultation with the Data Processor, who shall be given reasonable notice thereof. The Parties may agree by mutual consent that the audit will be performed by a certified and independent auditor hired by the Data Processor; this auditor shall issue a Third-Party Memorandum (TPM). [CIT Member] shall be informed of the results of the audit. The costs of the audit shall be borne by the Data Processor if and insofar as it has breached either the applicable legislation and regulations or this Data Processing Contract.

8 Data Breaches

8.1 The Data Processor shall adopt an appropriate policy for handling Data Breaches.

8.2 If the Data Processor becomes aware of a Data Breach, it shall notify [CIT Member] as swiftly as possible, in accordance with the instructions in **Appendix 3** to this Data Processing Contract. In the event of a Data Breach, the Data Processor shall provide [CIT Member] with all the relevant information about the Data Breach, including:

a) the nature of the Data Breach,

b) the categories and approximate number of data subjects concerned,

c) the categories and approximate number of personal data records concerned,

d) any further developments regarding the Data Breach,

e) the likely consequences of the Data Breach,

f) the measures taken by the Data Processor to mitigate the impact of the Data Breach and prevent recurrence on its side.

8.3 If it transpires that the security breach is likely to have adverse effects on the privacy of the data subjects, the Data Processor shall notify [CIT Member] as swiftly as possible.

8.4 In the event of a Data Breach, the Data Processor shall allow [CIT Member] to take suitable follow-up steps in relation to the Data Breach; the Data Processor shall use the existing processes that [CIT Member] has set up for this purpose. The Parties undertake to take all reasonably required measures as quickly as possible in order to prevent or reduce (further) infringement or breaches concerning the processing of Personal Data and, in particular, (further) infringements or breaches of the GDPR or other data protection laws and regulations.

8.5 In the event of a Data Breach, [CIT Member] will in turn notify the [National Data Protection Authority] of the Data Breach within 72 hours of [CIT Member] being informed of it by the Data Processor, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

9 Procedural Rights of Data Subjects

9.1 Complaints or requests from a data subject relating to the processing of the Personal Data shall be forwarded to [CIT Member] by the Data Processor without delay, since [CIT Member] is responsible for handling such requests.

9.2 The Data Processor shall, to the extent possible, cooperate fully with [CIT Member] in order to meet the obligations pursuant to Articles 16-22 GDPR, in particular the rights of data subjects to request the inspection, correction, addition or deletion of Personal Data, and shall do so within the legally defined time limits. The Parties shall consult in good faith on the reasonable distribution of any costs related to guaranteeing the procedural rights of data subjects.

10 Sub-Processors

10.1 The Data Processor may not commission a Sub-Processor to process Personal Data without the explicit prior written permission of [CIT Member]. [CIT Member] shall not refuse permission without reasonable grounds.

10.2 If a Sub-Processor is hired in with permission from [CIT Member], the identity and business particulars of the Sub-Processor shall be included in **Appendix 1**.

10.3 The Data Processor shall contractually require each Sub-Processor to comply with at least the same obligations as those set out in this Data Processing Contract.

10.4 Irrespective of the permission given by [CIT Member], the Data Processor shall remain liable for the actions of its Sub-Processors as stated in **point 10.1**.

10.5 In any event, the Data Processor shall make contractually certain that no Sub-Processor processes Personal Data further than has been agreed as part of this Data Processing Contract.

11 Liability and Indemnification

11.1 The Data Processor shall be independently liable for damages that are the result of it failing to comply with its obligations pursuant to this Data Processing Contract, or of it failing to do so properly within the stipulated deadline, and/or of it failing to comply with its own obligations, including those pursuant to the applicable legislation and regulations.

11.2 The Data Processor shall indemnify [CIT Member] fully against liability claims by third parties and reimburse it for all current and future damages and reasonably incurred costs, whether or not related to the case, that are caused by or associated in any way with an attributable shortcoming by the Data Processor in meeting the obligations described in **point 11.1**. The Data Processor is liable for damages or negative consequences resulting from non-compliance with the applicable legislation and regulations or this Data Processing Contract, insofar as said damages or negative consequences can be attributed to its work as a Data Processor for [CIT Member].

11.3 If [CIT Member] is held liable, [CIT Member] can claim recourse against the Data Processor if the Data Processor can be shown to have failed to comply with its obligations under this Data Processing Contract, or by virtue of the GDPR and the applicable data protection laws and regulations. The Data Processor shall indemnify [CIT Member] against all liability claims by third parties if these are attributable to the Data Processor's failure to comply with its obligations.

11.4 [CIT Member] shall indemnify the Data Processor against and shall compensate the Data Processor for all claims, actions and liability claims of third parties that result from a shortcoming by [CIT Member] in complying with its obligations under this Data Processing Contract or by virtue of the GDPR and the other applicable data protection laws and regulations, unless the claims, actions or liability claims of third parties are attributable to failure on the part of the Data Processor to comply with its obligations.

11.5 Neither Party shall be liable towards the other for any indirect or consequential damages, such as loss of revenue, loss of profit, loss of opportunity, or loss of goodwill.

12 Provisions contrary to law and loopholes in the Data Processing Contract

12.1 Should any individual provision of this Data Processing Contract prove to be wholly or partly invalid or inoperable, this shall not affect the other provisions of the Data Processing Contract or the validity of the Data Processing Contract. In place of the invalid or inoperable provision, the parties shall agree on a valid and operable provision which is as close as possible to the meaning and objective of the invalid provision.

12.2 If this Data Processing Contract proves to have loopholes, the parties shall agree on provisions which correspond to the meaning and objectives of the contract and which would have been agreed had the loopholes been detected.

13 Languages

13.1 The Parties may choose between the two following options:

Option 1:
If the Data Processing Contract or its appendices are drawn up in several languages, the texts in the various languages are equally authoritative.

If a comparison of the texts discloses a difference of meaning which cannot be resolved using general rules for interpretation, the meaning which best reconciles the texts, having regard to the object and purpose of the Data Processing Contract, is to be adopted.

Option 2:
If the Data Processing Contract or its appendices are drawn up in several languages, the ..... [language] version is authoritative. Translations may only be used internally by the Parties.

14 Amendment of the Data Processing Contract

14.1 Any amendments to this Data Processing Contract must be agreed in writing by both Parties.

14.2 Should a Party fail to exercise any of its rights under this Data Processing Contract, or should it fail to react in the event of a breach of obligations by the other Party, this shall not be interpreted as that Party waiving its right, nor shall it preclude any further exercise of any such rights in future. Any waiver of a right must be given expressly and in writing. If one Party has given an express written waiver of a right following a specific failure by a Party, this waiver cannot be invoked by the other Party in favour of a new failure, whether similar to the first or of any other kind.

15 Intellectual Property Rights

15.1 The Parties may choose between the two following options:

Option 1:
If the processing of the Personal Data by the Data Processor results in any intellectual property rights or similar liabilities, the Data Processor shall transfer those rights and/or claims to [CIT Member] without delay.

Option 2:
The Data Processor is and shall remain the owner of any materials used or made available in the context of the fulfilment of the Services.

15.2 The Data Processor grants [CIT Member] a limited, personal, non-exclusive, non-transferable right to use any material provided in the context of the fulfilment of the Services. The license is coterminous with this Data Processing Contract.

16 Duration and Termination

16.1 The duration of this Data Processing Contract shall be [e.g. one year] from the date of signature.

16.2 The Parties may choose between the two following options:

Option 1:
Either Party shall have the right to terminate this Data Processing Contract in whole or in part by sending [30 days'] written notice of termination to the other Party, specifying the reasons for the termination, including in case of:

a) material breach of any obligations under this Data Processing Contract by the other Party;

b) failure to remedy a significant breach caused by one Party despite a written request to do so from the other Party;

c) force majeure that prevails for a duration of over [XXX];

d) insolvency or liquidation of one of the Parties.

Option 2:
If [CIT Member] believes that the obligations have not been met or not met in full by the Data Processor, it is entitled to suspend the execution of the Data Processing Contract with immediate effect. If [CIT Member] exercises this right, it shall issue a notice of default to the Data Processor and give it a reasonable period of time within which to meet its obligations. If the Data Processor remains in default and fails to meet its obligations, [CIT Member] is entitled to terminate further execution of processing by the Data Processor with immediate effect. No compensation shall be payable by [CIT Member] to the Data Processor in the event that [CIT Member] exercises one or more of the rights stated in this paragraph. If the Data Processor fails to meet the obligations of this Data Processing Contract, [CIT Member] shall be entitled to terminate the contract at any time by issuing a unilateral written statement to this end, to take immediate effect and with no compensation for damages payable to the Data Processor.

16.3 Termination of this Data Processing Contract shall not release the Parties from their obligations under this Data Processing Contract, which because of their nature are deemed to continue even after termination.

17 Destruction of Personal Data

17.1 The Data Processor is obliged by [CIT Member] to transfer the Personal Data processed on the instructions of [CIT Member] within [fourteen (14)] days after the termination of the Data Processing Contract to [CIT Member], or within [fourteen (14)] days after the first instruction in writing by [CIT Member] to do so, and to delete it from its systems and to destroy it or have it destroyed, unless the Personal Data has to be stored for a longer period, for example as a consequence of legal or other obligations, or on request by [CIT Member].

17.2 The Data Processor shall confirm to [CIT Member] (in writing or electronically) that the destruction of the processed Personal Data has taken place. [CIT Member] may carry out a check that the destruction has taken place at its own expense.

17.3 The Data Processor shall inform all Sub-Processors involved in the processing of Personal Data of the termination of the Data Processing Contract, and shall guarantee that all Sub-Processors destroy the Personal Data or have it destroyed.

18 Jurisdiction and Applicable Law

18.1 The Parties can choose between the following options for the applicable law:

Option 1:
This Data Processing Contract between [CIT Member] and the Data Processor shall be subject to [specify the national law] law only.

Option 2:
This Data Processing Contract between [CIT Member] and the Data Processor shall be subject to the law of the competent court.

18.2 The Parties can choose between the following options for the competent court:

Option 1:
The competent court [specify the court] shall have exclusive jurisdiction in all disputes resulting from or related to this Data Processing Contract or the execution thereof.

Option 2:
The competent courts and tribunals shall be those of the defendant.

List of Appendices:

Appendix 1: Service Description and Pricing

Appendix 2: Data Processing, Technical and Organisational Security Measures

Appendix 3: Dealing with Data Breaches

Appendix 4: Transfer of Personal Data to Data Processors outside the European Economic Area

Agreed and signed in duplicate by:

[Contracting CIT Member]
……
……

……
……

[Date and Place]

[Signature]

[Name and title of representative]

Data Processor

……
……

……
……

[Date and Place]

[Signature]

[Name and title of representative]

Appendix 1 to CIT Model Data Processing Contract – Service Description and Pricing

Version [number] of [date of last modification]

A General information

- Name of Service(s):
- Name of Data Processor and location details:
- Brief explanation and operation of the Service(s):

B The specific services

Description of the specific services provided and associated data processing:

1 Processing that is deemed to be an inseparable part of the service offered;

[….]

2 Description of optional processing that the Data Processor offers.

[….] **Comment: This concerns additional services and associated data processing that are not an inseparable part of the services offered. [CIT Member] has the right to choose who should perform the optional processing.**

C Pricing

- Description of the pricing conditions:
- Amounts

D Categories and types of personal data

- Description and summary of the Personal Data categories used:
- Types of data (such as special data or financial data):

E General information about the security measures taken

See **Appendix 2** to the Data Processing Contract for a general description of the security measures taken.

- Specific security measures for this service/product [if applicable]:
- Certifications, if any:
- Audits/third-party memoranda:
- City/country in which the Personal Data will be stored and processed:

F Sub-Processors

(Only with written permission from [CIT Member])

The Data Processor has appointed the following Sub-Processors for the service/product: [name, brief description of task/service that shows what information this Sub-Processor is processing]

City/country in which the Personal Data will be stored and processed (if the Personal Data is processed outside the EEA, the prior written permission of [CIT Member] is required, along with a separate statement listing the countries in which the Personal Data is processed).

G Contact details

For any questions or comments about this appendix or the fulfilment of this product or service, please contact: [contact details].

Appendix 2 to CIT Model Data Processing Contract – Technical and organisational security measures

Version [number] of [date of last modification]

In accordance with the GDPR and [the national law implementing the GDPR], the Data Processor is obliged to take technical and organisational measures to ensure the secure processing of Personal Data.

Description of the measures referred to in **point 8.2** of this Data Processing Contract

a) …

b) ….

c) ….

Reporting

The Data Processor shall report periodically, every […], to [CIT Member] about the technical and organisational security measures taken by the Data Processor and any points requiring attention.

[Contact details of the helpdesk/service desk for security incidents]

Appendix 3 to CIT Model Data Processing Contract – Dealing with Data Breaches

Version [number] of [date of last modification]

1 Handling Data Breaches

Data Breaches shall be handled in line with Article 33 GDPR, the applicable data protection laws and regulations, and **point 9** of this Data Processing Contract.

2 Notifying Data Breaches and/or incidents relating to security

[CIT Member] shall report all data breaches to the [National] Data Protection Authority. In order to meet this obligation, the Data Processor must report any data breaches to the [indicate the responsible unit within the CIT Member] within 24 hours of becoming aware of the data breach.

The [unit of the CIT Member] can be contacted 24/7 on the following telephone number: [insert the emergency contact phone number to deal with personal data breaches].

When notifying [CIT Member], you must explicitly state that the report concerns a data breach of personal data. In addition, please ensure that you supply the information set out in the **table below** *as* **fully as possible**.

[Provide any additional information that could be of use to the responsible unit in dealing with the Data Breach.]

Model data breach report by the Data Processor to [CIT Member]

Contact details of reporting party	Company name/supplier of services: a) Name of reporting party b) E-mail address of reporting party c) Telephone number of reporting party d) Alternative telephone number of reporting party
Contact details for further information	Reporting party (see above) or details of contact: a) Name of contact b) Position of contact c) E-mail address of contact d) Telephone number of contact e) Alternative telephone number of contact
Number or description of the contract governing the work carried out	
Summary of the incident, such as: - Features and nature of the incident (what aspect of data security was involved, how did it occur?) - Cause of the security incident (if known, such as a breach, human error or system error) - Measures taken in order to prevent any damage and/or further damage	
How much personal data of how many people was affected by the breach? (Give numbers, if known)	a) At least: (fill in) b) At the most: (fill in)
Describe (if known) the group of people whose personal data is affected by the breach and who may experience the consequences of the incident (including the expected extent to which this will happen)	
When did the breach take place? (Choose one of the following options and add information, where necessary.)	a) Date and time b) Between (starting date of the period) and (end date of the period) c) Not yet known
What is the nature of the breach? **You can tick multiple possibilities.**	a) Reading (confidentiality) b) Copying c) Modification (integrity) d) Deletion or destruction (availability) e) Theft f) Not yet known
What type of personal data is involved? **(special data in particular, or data of a sensitive nature, including access details or identification data or financial data).** **You can tick multiple possibilities.**	a) Data about name, address and place of residence b) Telephone numbers c) E-mail addresses or other addresses for electronic communication d) Access data or identification data (e.g. username and password or client number) e) Financial data (e.g. account number, credit card number) f) Citizen Service Number (BSN) or social insurance number g) Passport copies or copies of other ID documents h) Gender, date of birth and/or age i) Special personal data (e.g. race, ethnicity, criminal records, political opinion, trade union membership, religion, sexual life, medical records) j) Public transport smartcard data k) Other data, namely: ……..

Which measures have you already taken to minimise the negative effect of the Data Breach on the rights of the affected data subjects?	
Which measures do you plan to adopt to prevent recurrence of similar incidents?	

Appendix 4 to CIT Model Data Processing Contract – Transfer of Personal Data to Data Processors outside the European Economic Area

1 In line with Article 46 § 1 GDPR and Article XX of the *[national law of the EU Member State],* the Parties shall provide appropriate safeguards and ensure that enforceable data subjects' rights and effective legal remedies for data subjects are available when the personal data is transferred to a Data Processor or a Sub-Processor in a third country outside the EEA.

2 In line with Article 49 GDPR, when transferring personal data to a third country outside the EEA this Appendix does not apply when:

- the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfer for the data subject due to the absence of an adequacy decision and appropriate safeguards. It is up to the Data Controller to request such consent from the data subject, unless it has authorised the Data Processor to do so;
- the transfer is necessary for the performance of the contract between the data subject and the Data Controller or the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the establishment, exercise or defence of legal claims;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the purposes of compelling legitimate interests pursued by the Data Controller which are not overridden by the interests or rights and freedoms of the data subject, and the Data Controller, after assessing all the relevant circumstances, has provided suitable safeguards with regard to the protection of personal data. Before transferring the personal data, the Data Controller shall also inform the data subject of the compelling legitimate interests that are pursued with this transfer;
- the transfer is not repetitive and concerns only a limited number of data subjects.

The Data Controller, and where applicable the Data Processor, shall each keep records of such transfers; each record shall include a reference to one of the grounds mentioned in this paragraph and the suitable safeguards, whenever required.

3 In line with **point 1** of this **Appendix**, the transfer of personal data subject to this Data Processing Contract is based on …

Option 1:
… XXXX [a legally binding and enforceable instrument between public authorities or bodies]. The transfer of personal data to [a third country outside the EEA] in line with [instrument] shall comply at least with the following requirements:

- …
- …
- …

Option 2:

… [binding corporate rules adopted on….] in line with Articles 46 § 2 b) and 47 GDPR.

The binding corporate rules contain the following requirements:
[…. list the requirements contained in the binding corporate rules with respect to:

1 the structure and contact details of the group of undertakings or group of enterprises engaged in a joint economic activity and of each of its members;

2 their legally binding nature, both internally and externally;

3 the application of general data protection principles (according to this Data Processing Contract, the GDPR) and the applicable national law of the EU Member State, in particular: purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules;

4 the rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling, in accordance with Article 22 GDPR, the right to lodge a complaint with the competent supervisory authority and before the competent courts of the Member States in accordance with Article 79 GDPR, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;

5 the acceptance by the Data Controller or Data Processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member concerned not established in the Union; the Data Controller or the Data Processor shall be exempt from that liability, in whole or in part, only if it proves that that member is not responsible for the event giving rise to the damage;

6 how the information on the binding corporate rules, in particular on the provisions referred to under numbers 3-5 above-mentioned (pursuant to Article 47 § 1 d), e) and f) GDPR), is provided to the data subjects in addition to Articles 13 and 14 GDPR;

7 the tasks of any data protection officer designated in accordance with Article 37 GDPR or any other person or entity in charge of the monitoring compliance with the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling;

8 the complaint procedures;

9 the mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity, for ensuring the verification of compliance with the binding corporate rules. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. The results of such verification should be communicated to the person or entity referred to under number 7 above-mentioned [pursuant to Article 47 § 1 h) GDPR] and to the board of the controlling undertaking of a group of undertakings, or of the group of enterprises engaged in a joint economic activity, and should be available upon request to the competent supervisory authority;

10 the mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authority;

11 the cooperation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, or group of enterprises engaged in a joint economic activity, in particular by making available to the supervisory authority the results of verifications of the measures referred to under number 9 above-mentioned [pursuant to article 47 § 1 j) GDPR];

12 the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity, is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and

13 the appropriate data protection training to personnel having permanent or regular access to personal data.]

Option 3:
… [the European Commission decision containing the standard data protection clauses] in line with Article 46 § 2 c) GDPR.

Option 4:
…. [the decision taken by a national supervisory authority with reference to its own standard data protection clauses approved by the European Commission according to Article 93 § 2 GDPR] in line with Article 46 § 2 d) GDPR.

Option 5:
…. [code of conduct approved by the supervisory authority XYZ] in line with Articles 46 § 2 e) and 40 GDPR.

Option 6:
… [approved certification mechanism] in line with Article 46 § 2 f) and Article 42 GDPR. [add any details necessary pertaining to the approved certification mechanism]

Option 7:
… the following contractual clauses approved by the [supervisory authority] subject to the consistency mechanism:

3.1 Data Processors located in third countries outside the European Economic Area agree to comply with their obligations under this Data Processing Contract; in the event that Sub-Processors as described in **point 10.3** of this Data Processing Contract are used, the Sub-Processor(s) shall comply with the Data Sub-Processing Contract, which shall impose at least the same obligations on the Sub-Processor as this Data Processing Contract.

3.2 If a Data Processor cannot comply, for whatever reason, with any of the provisions of this Data Processing Contract, it shall promptly inform the Data Controller of its inability to comply, in which case the Data Controller is entitled to suspend the transfer of data and/or terminate the Data Processing Contract. This provision applies mutatis mutandis to the relationship between the Data Processor and a Sub-Processor located in a third country outside the EEA.

3.3 Data Processors located in a third country outside the EEA shall guarantee that they have no reason to believe that the legislation applicable to them prevents them from fulfilling the instructions received from the Data Controller and their obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on their obligations under this Data Processing Contract, they will promptly notify the change to the Data Controller as soon as they are aware of it, in which case the Data Controller is entitled to suspend the transfer of data and/or terminate the contract. The Data Controller shall forward any such notification received from the Data Processor to the supervisory authority if the Data Controller decides to continue the transfer or to lift the suspension.

3.4 The Data Processor and Data Controller shall make available to the data subjects upon request a copy of the relevant provisions of this Data Processing Contract, unless they contain confidential or commercial information, and a summary description of the security measures implemented by any Data Processors located in third countries outside the EEA.

3.5 If the data subject is unable to bring a claim for compensation against the Data Controller due to the damage suffered as a result of any breach by the Parties of the obligations contained in this Appendix because the Data Controller has ceased to exist physically or in law or has become insolvent, the Data Processor agrees that the data subject may issue a claim against the Data Processor as if it were the Data Controller, unless the successor entity has assumed in full the legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against said successor entity.

5.2 CIT Model Data Processing Contract, Appendix …… to the Agreement concluded on ……

Preamble

This Model Data Processing Contract is provided to CIT members to assist them in drafting their data processing contracts with data processors, where data processing is an ancillary service provided in addition to other services contractually agreed upon between CIT members, or between the CIT member and a third party. The model contract is in line with Article 28 of the GDPR. CIT members shall adjust this model contract to include any additional obligations required by national data protection laws and regulations.

Contract

between

Undertaking X (name, address), <private> company <with limited liability> <NAME>, with its registered office and principal place of business at <address>, (<post code>) <town/city>, trade register number <number>, legally represented by <position + name>, acting as the "Data Controller", hereinafter referred to as **"[CIT Member]"**

and

Undertaking Y (name, address, customer code), <private> company <with limited liability> <NAME>, with its registered office and principal place of business at <address> in (<post code>) <town/city>, creditor number <number>, trade register number <number>, legally represented by <position + name>, hereinafter referred to as the **"Data Processor"**,

hereinafter collectively referred to as the **"Parties"** or separately as a **"Party**".

1 Subject-matter of the Data Processing Contract

1.1 On <date>, [CIT Member] and the Data Processor entered into an agreement with reference <number> relating to <subject of agreement> (hereinafter referred to as "the Agreement");

1.2 As part of the fulfilment of its obligations pursuant to the Agreement, the Data Processor shall process personal data for or on behalf of [CIT Member];

[The Data Processing Contract is in that respect an appendix to the existing agreement between the Data Controller and the Data Processor. These two terms (contract and agreement) are therefore not used as synonyms in this document.]

1.3 This Data Processing Contract lays down the rights and obligations of the Parties in accordance with Article 28 of the GDPR[70] .

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

1.4 The legal terms used in this Data Processing Contract shall have the meaning defined in Article 4 of the GDPR. GDPR refers to the EU General Data Protection Regulation 2016/679. All other legal terms are defined in the CIT Glossary.

1.5 This Data Processing Contract is an integral and inseparable part of the Services Agreement concluded on ….. .

1.6 In case of conflict between the provisions of this Data Processing Contract and those of the Agreement, the provisions of this Data Processing Contract shall prevail.

1.7 This Data Processing Contract consists of eighteen Points and four Appendices, which are deemed to be an inseparable part of this Data Processing Contract:

Appendix 1: Service Description and Pricing

Appendix 2: Data Processing, Technical and Organisational Security Measures

Appendix 3: Dealing with Data Breaches

Appendix 4: Transfer of Personal Data to Data Processors outside the European Economic Area

2 Object and purpose of the Data Processing Contract

This Data Processing Contract applies to the processing of Personal Data in the context of the fulfilment of the Services set out in the Agreement and specified in **Appendix 1**.

3 Pricing and Payment

3.1 In return for the data processing, [CIT Member] shall pay the Data Processor the amounts indicated in **Appendix 1**.

3.2 All amounts mentioned in this Data Processing Contract are exclusive of VAT.

3.3 Unless agreed otherwise by the Parties, invoices shall be paid within a period of thirty (30) days following receipt thereof.

4 Relationship between the Parties

4.1 In accordance with this Data Processing Contract, [CIT Member] gives the Data Processor instructions to process Personal Data for the fulfilment of the Services described in **Appendix 1**.

4.2 With respect to the processing of Personal Data, [CIT Member] is the Data Controller, whereas [XXX] is the Data Processor, as defined in the GDPR. [CIT Member] has and retains independent control of the purpose for which the Personal Data is processed and of the resources used to do so.

4.3 Prior to entering into this Data Processing Contract, the Data Processor shall ensure that [CIT Member] is sufficiently informed about the Service(s) provided by the Data Processor and about the data processing to be carried out. The Services referred to in the Agreement are covered by this Data Processing Contract. Further specifications, e.g. the type of data processing for a specific service, and any optional data processing which is not an inseparable part of the services offered, shall be indicated in **Appendix 1**.

4.4 [CIT Member] and the Data Processor will give each other all the required information to ensure proper compliance with the relevant legislation and regulations regarding privacy.

5 Processing of Personal Data and related obligations of the Data Processor

5.1 The processing of Personal Data as part of the performance of the Services mentioned in the Agreement and specified in **Appendix 1** shall comply with the applicable data protection laws and regulations, including the GDPR and any additional national legislation.

5.2 The Data Processor shall undertake not to use the Personal Data obtained from [CIT Member] for other purposes or in any other way than that for which the data has been transmitted or disclosed. The Data Processor is therefore not authorised to carry out any data processing operations other than those entrusted to it by [CIT Member]. This obligation applies both during the term of this Data Processing Contract and after this Data Processing Contract has ended for [XX] years.

5.3 **Appendix 1** to this Data Processing Contract contains a summary of the Personal Data categories used.

5.4 The Data Processor shall:

5.4.1 create and maintain a record of its data processing activities under this Data Processing Contract; if requested to do so, the Data Processor shall, at the first time of asking, make the record available to [CIT Member], any auditor appointed by the latter, and/or the supervisory authority;

5.4.2 promptly inform [CIT Member] if it is not able to comply with [CIT Member's] instructions with respect to the processing of the Personal Data or with any other obligation under this Data Processing Contract;

5.4.3 inform [CIT Member] immediately if it believes that any instructions from [CIT Member] infringe the GDPR or other applicable data protection laws and regulations;

5.4.4 deal promptly and properly with all reasonable inquiries from [CIT Member] relating to the processing of Personal Data under this Data Processing Contract;

5.4.5 make available to [CIT Member] all information necessary to demonstrate compliance with the GDPR or other applicable data protection laws and regulations;

5.4.6 not process the Personal Data for longer than the required retention period. [CIT Member] will adequately inform the Data Processor about the (legal) retention periods applicable to the processing of the Personal Data;

5.4.7 submit its data processing facilities for audit or control of the data processing activities, in accordance with **point 7.7** of this Data Processing Contract;

5.4.8 promptly notify [CIT Member] of:

a) any legally binding request for disclosure of the Personal Data by a data subject or by a judicial or regulatory authority (unless prohibited from doing so, for example by an obligation under criminal law to preserve the confidentiality of a judicial investigation), and to assist the [CIT Member] herewith,

b) any accidental or unauthorized access, and any unlawful processing more generally, and to assist the [CIT Member] herewith;

5.4.9 not pass Personal Data on to Third Parties, unless this exchange takes place on the instructions of [CIT Member] or if it is necessary to meet a legal obligation imposed on the Data Processor. The Data Processor shall ensure that everyone involved in processing the Personal Data, including its employees, representatives and/or Sub-processors, has entered into a confidentiality agreement or accepted a confidentiality clause. Should transfer to Third Parties be required by a legal obligation, the Data Processor shall verify the basis for the request and the identity of the requesting party prior to transferring any Personal Data. In addition, if legally allowed to do so, the Data Processor shall notify [CIT Member] immediately of the transfer, if possible prior to transferring the Personal Data;

5.4.10 refrain from engaging any Data Sub-processor without the prior written consent of [CIT Member]. See the additional conditions with respect to Data Sub-processors as detailed in **point 10** and **Section E** of **Appendix 1**;

5.4.11 [subject to additional compensation agreed in advance], assist [CIT Member] in complying with the Data Controller's obligations under the applicable data protection laws and regulations.

5.5 The personal data subject to this Data Processing Contract shall not be transferred to any country outside the European Economic Area without prior written consent from [CIT Member]. If the Personal Data is transferred to a country outside the European Economic Area, the Parties shall ensure that said Personal Data is adequately protected in line with the GDPR. Any transfer of Personal Data to a country outside the European Economic Area shall be subject to the conditions of **Appendix 4**, unless the country of destination to which the Personal Data is transferred is covered by an adequacy decision of the European Commission.

6 Confidentiality

6.1 Each Party to this Data Processing Contract acknowledges that during the performance of its obligations, a Party (the "receiving Party") may become privy to confidential information which is disclosed by the other Party (the "disclosing Party").

6.2 The receiving Party shall keep confidential all such confidential information as well as the Personal Data, and shall not disclose it to any third party or use it for any other purposes than those of this Data Processing Contract.

6.3 Each Party agrees that before any of its employees, Sub-processors or agents are given access to confidential information and/or Personal Data, each of them shall agree to be bound by a confidentiality agreement under comparable terms and conditions to those defined in this Data Processing Contract.

6.4 The Data Processor shall ensure in each case that access is strictly limited to those individuals who need to know / access the Personal Data, for the purposes of this Data Processing Contract.

6.5 If the receiving Party has a legal duty to disclose confidential information, e.g. by a court order, the receiving Party shall, to the extent possible, inform the disclosing Party of this fact without delay, thereby enabling the disclosing Party to seek an interlocutory injunction or another appropriate remedy.

7 Security and checks

7.1 The Data Processor shall take appropriate technical and organisational measures to secure Personal Data against loss or against any form of unlawful data processing. These measures shall ensure an appropriate level of security, taking into account technical developments and implementation costs, and having regard to the risks associated with the processing of Personal Data and the nature of the Personal Data to be protected.

7.2 The measures referred to in **point 7.1** shall include, at the very least:

- pseudonymisation and encryption of the Personal Data;
- measures enabling the availability of and access to the Personal Data to be restored in a timely manner in the event of a physical or technical incident;
- measures guaranteeing that only authorised employees have access to the Personal Data being processed under the Data Processing Contract;
- measures protecting the Personal Data, in particular against unintentional or unlawful destruction, unintentional loss or modification, or unauthorised or unlawful storage, processing, access or publication;

- measures whereby weak spots in the processing of Personal Data can be regularly identified in the systems used for providing services to [CIT Member];
- an appropriate information security policy for processing Personal Data.

7.3 The Data Processor shall evaluate and strengthen, supplement or improve the information security measures it has taken, insofar as the requirements or technological or other developments give reason to do so.

7.4 The agreements between the Parties on the technical and organisational measures to be taken and the content and frequency of the reports to be supplied by the Data Processor to [CIT Member] on the security measures shall be recorded in **Appendix 2**. These measures shall be compliant with the security measures that [CIT Member] is required to take.

7.5 The Data Processor may use its adherence to an approved code of conduct or an approved certification mechanism to demonstrate its compliance with the technical and organisational measures required.

7.6 The Data Processor shall enable [CIT Member] to comply with its legal obligations to monitor compliance by the Data Processor, in particular with the technical and organisational security measures, and with the obligations regarding Data Breaches as stated in **point 8**.

7.7 [CIT Member] may at any time audit (or commission an audit of) the technical and organisational security measures taken by the Data Processor to ensure compliance with the GDPR, the applicable legislation and regulations, and this Data Processing Contract. This audit, the cost of which shall be borne by [CIT Member], shall be arranged in consultation with the Data Processor, who shall be given reasonable notice thereof. The Parties may agree by mutual consent that the audit will be performed by a certified and independent auditor hired by the Data Processor; this auditor shall issue a Third-Party Memorandum (TPM). [CIT Member] shall be informed of the results of the audit. The costs of the audit shall be borne by the Data Processor if and insofar as it has breached either the applicable legislation and regulations or the Agreement and this Data Processing Contract.

8 Data Breaches

8.1 The Data Processor shall adopt an appropriate policy for handling Data Breaches.

8.2 If the Data Processor becomes aware of a Data Breach, it shall notify [CIT Member] as swiftly as possible, in accordance with the instructions in **Appendix 3** to this Data Processing Contract. In the event of a Data Breach, the Data Processor shall provide [CIT Member] with all the relevant information about the Data Breach, including

a) the nature of the Data Breach,

b) the categories and approximate number of data subjects concerned,

c) the categories and approximate number of personal data records concerned,

d) any further developments regarding the Data Breach,

e) the likely consequences of the Data Breach,

f) the measures taken by the Data Processor to mitigate the impact of the Data Breach and prevent recurrence on its side.

8.3 If it transpires that the security breach is likely to have adverse effects on the privacy of the data subjects, the Data Processor shall notify [CIT Member] as swiftly as possible.

8.4 In the event of a Data Breach, the Data Processor shall allow [CIT Member] to take suitable follow-up steps in relation to the Data Breach; the Data Processor shall use the existing processes that [CIT Member] has set up for this purpose. The Parties undertake to take all reasonably required measures as quickly as possible in order to prevent or reduce (further) infringement or

breaches concerning the processing of Personal Data and, in particular, (further) infringements or breaches of the GDPR or other data protection laws and regulations.

8.5 In the event of a Data Breach, [CIT Member] will in turn notify the [National Data Protection Authority] of the Data Breach within 72 hours of [CIT Member] being informed of it by the Data Processor, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

9 Procedural Rights of Data Subjects

9.1 Complaints or requests from a data subject relating to the processing of the Personal Data shall be forwarded to [CIT Member] by the Data Processor without delay, since [CIT Member] is responsible for handling such requests.

9.2 The Data Processor shall, to the extent possible, cooperate fully with [CIT Member] in order to meet the obligations pursuant to Articles 16-22 GDPR, in particular the rights of data subjects to request the inspection, correction, addition or deletion of Personal Data, and shall do so within the legally defined time limits. The Parties shall consult in good faith on the reasonable distribution of any costs related to guaranteeing the procedural rights of data subjects.

10 Sub-Processors

10.1 The Data Processor may not commission a Sub-Processor to process Personal Data without the explicit prior written permission of [CIT Member]. [CIT Member] shall not refuse permission without reasonable grounds.

10.2 If a Sub-Processor is hired in with permission from [CIT Member], the identity and business particulars of the Sub-Processor shall be included in **Appendix 1**.

10.3 The Data Processor shall contractually require each Sub-Processor to comply with at least the same obligations as those set out in this Data Processing Contract.

10.4 Irrespective of the permission given by [CIT Member], the Data Processor shall remain liable for the actions of its Sub-Processors as stated in **point 10.1**.

10.5 In any event, the Data Processor shall make contractually certain that no Sub-Processor processes Personal Data further than has been agreed as part of this Data Processing Contract.

11 Liability and Indemnification

11.1 The Data Processor shall be independently liable for damages that are the result of it failing to comply with its obligations pursuant to this Data Processing Contract, or of it failing to do so properly within the stipulated deadline, and/or of it failing to comply with its own obligations, including those pursuant to the applicable legislation and regulations.

11.2 The Data Processor shall indemnify [CIT Member] fully against liability claims by third parties and reimburse it for all current and future damages and reasonably incurred costs, whether or not related to the case, that are caused by or associated in any way with an attributable shortcoming by the Data Processor in meeting the obligations described in **point 11.1**. The Data Processor is liable for damages or negative consequences resulting from non-compliance with the applicable legislation and regulations or this Data Processing Contract, insofar as said damages or negative consequences can be attributed to its work as a Data Processor for [CIT Member].

11.3 If [CIT Member] is held liable, [CIT Member] can claim recourse against the Data Processor if the Data Processor can be shown to have failed to comply with its obligations under this Data Pro-

cessing Contract, or by virtue of the GDPR and the applicable data protection laws and regulations. The Data Processor shall indemnify [CIT Member] against all liability claims by third parties if these are attributable to the Data Processor's failure to comply with its obligations.

11.4 [CIT Member] shall indemnify the Data Processor against and shall compensate the Data Processor for all claims, actions, and liability claims of third parties that result from a shortcoming by [CIT Member] in complying with its obligations under this Data Processing Contract, or by virtue of the GDPR and the other applicable data protection laws and regulations, unless the claims, actions or liability claims of third parties are attributable to failure on the part of the Data Processor to comply with its obligations.

11.5 Neither Party shall be liable towards the other for any indirect or consequential damages, such as loss of revenue, loss of profit, loss of opportunity, or loss of goodwill.

12 Provisions contrary to law and loopholes in the Data Processing Contract

12.1 Should any individual provision of this Data Processing Contract prove to be wholly or partly invalid or inoperable, this shall not affect the other provisions of the Data Processing Contract or the validity of the Data Processing Contract. In place of the invalid or inoperable provision, the parties shall agree on a valid and operable provision which is as close as possible to the meaning and objective of the invalid provision.

12.2 If this Data Processing Contract proves to have loopholes, the parties shall agree on provisions which correspond to the meaning and objectives of the contract and which would have been agreed had the loopholes been detected.

13 Languages

13.1 The Parties may choose between the two following options:

Option 1:
If the Data Processing Contract or its appendices are drawn up in several languages, the texts in the various languages are equally authoritative.

If a comparison of the texts discloses a difference of meaning which cannot be resolved using general rules for interpretation, the meaning which best reconciles the texts, having regard to the object and purpose of the Agreement and the Data Processing Contract, is to be adopted.

Option 2:
If the Data Processing Contract or its appendices are drawn up in several languages, the ..... [language] version is authoritative. Translations may only be used internally by the Parties.

14 Amendment of the Data Processing Contract

14.1 Any amendments to this Data Processing Contract must be agreed in writing by both Parties.

14.2 Should a Party fail to exercise any of its rights under this Data Processing Contract, or should it fail to react in the event of a breach of obligations by the other Party, this shall not be interpreted as that Party waiving its right, nor shall it preclude any further exercise of any such rights in future. Any waiver of a right must be given expressly and in writing. If one Party has given an express written waiver of a right following a specific failure by a Party, this waiver cannot be invoked by the other Party in favour of a new failure, whether similar to the first or of any other kind.

15 Intellectual Property Rights

15.1 The Parties may choose between the two following options:

Option 1:
If the processing of the Personal Data by the Data Processor results in any intellectual property rights or similar liabilities, the Data Processor shall transfer those rights and/or claims to [CIT Member] without delay.

Option 2:
The Data Processor is and shall remain the owner of any materials used or made available in the context of the fulfilment of the Services.

15.2 The Data Processor grants [CIT Member] a limited, personal, non-exclusive, non-transferable right to use any material provided in the context of the fulfilment of the Services. The license is coterminous with this Data Processing Contract.

16 Duration and Termination

16.1 Unless otherwise agreed between the Parties, the term of this Data Processing Contract shall be the same as that of the Agreement between the Parties, including any extensions thereto. Termination of the Agreement shall automatically trigger the termination of this Data Processing Contract. Termination of this Data Processing Contract shall not release the Parties from their obligations under this Data Processing Contract, which by their nature are expected to continue after termination.

16.2 If [CIT Member] believes that the obligations have not been met or not met in full by the Data Processor, it is entitled to suspend the execution of the Data Processing Contract with immediate effect. If [CIT Member] exercises this right, it shall issue a notice of default to the Data Processor and give it a reasonable period of time within which to meet its obligations. If the Data Processor remains in default and fails to meet its obligations, [CIT Member] is entitled to terminate further execution of processing by the Data Processor with immediate effect. No compensation shall be payable by [CIT Member] to the Data Processor in the event that [CIT Member] exercises one or more of the rights stated in this paragraph.

16.3 Upon termination or expiry of this Data Processing Contract, any Personal Data that remains in the possession of the Data Processor and which is not relevant for the provision of the Services in accordance with the Agreement, shall be deleted or returned to [CIT Member]. This includes any existing copies of such Personal Data, unless the retention of this Personal Data is required by law.

17 Destruction of Personal Data

17.1 The Data Processor is obliged by [CIT Member] to transfer the Personal Data processed on the instructions of [CIT Member] within [fourteen (14)] days after the termination of the Data Processing Contract to [CIT Member], or within [fourteen (14)] days after the first instruction in writing by [CIT Member] to do so, and to delete it from its systems and to destroy it or have it destroyed, unless the Personal Data has to be stored for a longer period, for example as a consequence of legal or other obligations, or on request by [CIT Member].

17.2 The Data Processor shall confirm to [CIT Member] (in writing or electronically) that the destruction of the processed Personal Data has taken place. [CIT Member] may carry out a check that the destruction has taken place at its own expense.

17.3 The Data Processor shall inform all Sub-Processors involved in the processing of Personal Data of the termination of the Data Processing Contract, and shall guarantee that all Sub-Processors destroy the Personal Data or have it destroyed.

18 Jurisdiction and Applicable Law

18.1 The Parties can choose between the following options for the applicable law:

Option 1:
This Data Processing Contract between [CIT Member] and the Data Processor shall be subject to [specify the national law] law only.

Option 2:
This Data Processing Contract between [CIT Member] and the Data Processor shall be subject to the law of the competent court.

18.2 The Parties can choose between the following options for the competent court:

Option 1:
The competent court [specify the court] shall have exclusive jurisdiction in all disputes resulting from or related to this Data Processing Contract or the execution thereof.

Option 2:
The competent courts and tribunals shall be those of the defendant.

List of Appendices:

Appendix 1: Service Description and Pricing

Appendix 2: Data Processing, Technical and Organisational Security Measures

Appendix 3: Dealing with Data Breaches

Appendix 4: Transfer of Personal Data to Data Processors outside the European Economic Area

Agreed and signed in duplicate by:

[Contracting CIT Member]
……..
……..

……..
……..

[Date and Place]

[Signature]

[Name and title of representative]

Data Processor

……
……...

……
……...

[Date and Place]

[Signature]

[Name and title of representative]

Appendix 1 to CIT Model Data Processing Contract, Appendix ….. to the Agreement concluded on ….. – Service Description and Pricing

Version [number] of [date of last modification]

A General information

- Name of Service(s):
- Name of Data Processor and location details:
- Brief explanation and operation of the Service(s) (or reference to the provision in the Agreement):

B The specific services

Description of the specific services provided and associated data processing:

1. Processing that is deemed to be an inseparable part of the service offered;

   [….]

2. Description of optional processing that the Data Processor offers.

[….] **Comment: This concerns additional services and associated data processing that are not an inseparable part of the services offered. [CIT Member] has the right to choose who should perform the optional processing.**

C Pricing

- Description of the pricing conditions:
- Amounts

D Categories and types of personal data

- Description and summary of the Personal Data categories used:
- Types of data (such as special data or financial data):

E General information about the security measures taken

See **Appendix 2** to the Data Processing Contract for a general description of the security measures taken.

- Specific security measures for this service/product [if applicable]:
- Certifications, if any:
- Audits/third-party memoranda:
- City/country in which the Personal Data will be stored and processed:

F Sub-Processors

(Only with written permission from [CIT Member])

The Data Processor has appointed the following Sub-Processors for the service/product: [name, brief description of task/service that shows what information this Sub-Processor is processing]

City/country in which the Personal Data will be stored and processed (if the Personal Data is processed outside the EEA, the prior written permission of [CIT Member] is required, along with a separate statement listing the countries in which the Personal Data is processed).

G Contact details

For any questions or comments about this appendix or the fulfilment of this product or service, please contact: [contact details].

Appendix 2 to CIT Model Data Processing Contract, Appendix ….. to the Agreement concluded on ….. –
Technical and organisational security measures

Version [number] of [date of last modification]

In accordance with the GDPR and [the national law implementing the GDPR], the Data Processor is obliged to take technical and organisational measures to ensure the secure processing of Personal Data.

Description of the measures referred to in **point 8.2** of this Data Processing Contract

a) …

b) ….

c) ….

Reporting

The Data Processor shall report periodically, every […], to [CIT Member] about the technical and organisational security measures taken by the Data Processor and any points requiring attention.

[Contact details of the helpdesk/service desk for security incidents]

Appendix 3 to CIT Model Data Processing Contract, Appendix ….. to the Agreement concluded on ….. – Dealing with Data Breaches

Version [number] of [date of last modification]

1 Handling Data Breaches

Data Breaches shall be handled in line with Article 33 GDPR, the applicable data protection laws and regulations, and **point 9** of this Data Processing Contract.

2 Notifying Data Breaches and/or incidents relating to security

[CIT Member] shall report all data breaches to the [National] Data Protection Authority. In order to meet this obligation, the Data Processor must report any data breaches to the [indicate the responsible unit within the CIT Member] within 24 hours of becoming aware of the data breach.

The [unit of the CIT Member] can be contacted 24/7 on the following telephone number: [insert the emergency contact phone number to deal with personal data breaches].

When notifying [CIT Member], you must explicitly state that the report concerns a data breach of personal data. In addition, please ensure that you supply the information set out in the **table below** *as* **fully as possible**.

[Provide any additional information that could be of use to the responsible unit in dealing with the Data Breach.]

Model data breach report by the Data Processor to [CIT Member]

Contact details of reporting party	Company name/supplier of services: a) Name of reporting party b) E-mail address of reporting party c) Telephone number of reporting party d) Alternative telephone number of reporting party
Contact details for further information	Reporting party (see above) or details of contact: a) Name of contact b) Position of contact c) E-mail address of contact d) Telephone number of contact e) Alternative telephone number of contact
Number or description of the contract governing the work carried out	
Summary of the incident, such as: - Features and nature of the incident (what aspect of data security was involved, how did it occur?) - Cause of the security incident (if known, such as a breach, human error or system error) - Measures taken in order to prevent any damage and/or further damage	
How much personal data of how many people was affected by the breach? (Give numbers, if known)	a) At least: (fill in) b) At the most: (fill in)
Describe (if known) the group of people whose personal data is affected by the breach, and who may experience the consequences of the incident (including the expected extent to which this will happen)	
When did the breach take place? (Choose one of the following options and add information, where necessary.)	a) Date and time b) Between (starting date of the period) and (end date of the period) c) Not yet known
What is the nature of the breach? **You can tick multiple possibilities.**	a) Reading (confidentiality) b) Copying c) Modification (integrity) d) Deletion or destruction (availability) e) Theft f) Not yet known
What type of personal data is involved? **(special data in particular, or data of a sensitive nature, including access details or identification data or financial data).** **You can tick multiple possibilities.**	a) Data about name, address and place of residence b) Telephone numbers c) E-mail addresses or other addresses for electronic communication d) Access data or identification data (e.g. username and password or client number) e) Financial data (e.g. account number, credit card number) f) Citizen Service Number (BSN) or social insurance number g) Passport copies or copies of other ID documents h) Gender, date of birth and/or age i) Special personal data (e.g. race, ethnicity, criminal records, political opinion, trade union membership, religion, sexual life, medical records) j) Public transport smartcard data k) Other data, namely: ……

Which measures have you already taken to minimise the negative effect of the Data Breach on the rights of the affected data subjects?	
Which measures do you plan to adopt to prevent recurrence of similar incidents?	

Appendix 4 to CIT Model Data Processing Contract, Appendix ….. to the Agreement concluded on ….. – Transfer of Personal Data to Data Processors outside the European Economic Area

1 In line with Article 46 § 1 GDPR and Article XX of the *[national law of the EU Member State]*, the Parties shall provide appropriate safeguards and ensure that enforceable data subjects' rights and effective legal remedies for data subjects are available when the personal data is transferred to a Data Processor or a Sub-Processor in a third country outside the EEA.

2 In line with Article 49 GDPR, when transferring personal data to a third country outside the EEA this Appendix does not apply when:

- the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfer for the data subject due to the absence of an adequacy decision and appropriate safeguards. It is up to the Data Controller to request such a consent from the data subject, unless it has authorised the Data Processor to do so;
- the transfer is necessary for the performance of the contract between the data subject and the Data Controller or the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the establishment, exercise or defence of legal claims;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the purposes of compelling legitimate interests pursued by the Data Controller which are not overridden by the interests or rights and freedoms of the data subject, and the Data Controller, after assessing all the relevant circumstances, has provided suitable safeguards with regard to the protection of personal data. Before transferring the personal data, the Data Controller shall also inform the data subject of the compelling legitimate interests that are pursued with this transfer;
- the transfer is not repetitive and concerns only a limited number of data subjects.

The Data Controller, and where applicable the Data Processor, shall each keep records of such transfers; each record shall include a reference to one of the grounds mentioned in this paragraph and the suitable safeguards, whenever required.

3 In line with **point 1** of this **Appendix**, the transfer of personal data subject to this Data Processing Contract is based on …

Option 1:
… XXXX [a legally binding and enforceable instrument between public authorities or bodies]. The transfer of personal data to [a third country outside the EEA] in line with [instrument] shall comply at least with the following requirements:

- …

- …
- …

Option 2:
… [binding corporate rules adopted on….] in line with Articles 46 § 2 b) and 47 GDPR.

The binding corporate rules contain the following requirements:
[…. list the requirements contained in the binding corporate rules with respect to:

1 the structure and contact details of the group of undertakings or group of enterprises engaged in a joint economic activity and of each of its members;

2 their legally binding nature, both internally and externally;

3 the application of general data protection principles (according to this Data Processing Contract, the GDPR) and the applicable national law of the EU Member State, in particular: purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules;

4 the rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling, in accordance with Article 22 GDPR, the right to lodge a complaint with the competent supervisory authority and before the competent courts of the Member States in accordance with Article 79 of the GDPR, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;

5 the acceptance by the Data Controller or Data Processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member concerned not established in the Union; the Data Controller or the Data Processor shall be exempt from that liability, in whole or in part, only if it proves that that member is not responsible for the event giving rise to the damage;

6 how the information on the binding corporate rules, in particular on the provisions referred to under numbers 3-5 above-mentioned [pursuant to Article 47 § 1 d), e) and f) GDPR], is provided to the data subjects in addition to Articles 13 and 14 GDPR;

7 the tasks of any data protection officer designated in accordance with Article 37 GDPR or any other person or entity in charge of the monitoring compliance with the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling;

8 the complaint procedures;

9 the mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity, for ensuring the verification of compliance with the binding corporate rules. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. The results of such verification should be communicated to the person or entity referred to under number 7 above-mentioned [pursuant to Article 47 § 1 h) GDPR] and to the board of the controlling undertaking of a group of undertakings, or of the group of enterprises engaged in a joint economic activity, and should be available upon request to the competent supervisory authority;

10 the mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authority;

11 the cooperation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, or group of enterprises engaged in a joint economic activity, in particular by making available to the supervisory authority the results of verifications of the measures referred to under number 9 above-mentioned [pursuant to article 47 § 1 j) GDPR];

12 the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in

a joint economic activity, is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and

13 the appropriate data protection training to personnel having permanent or regular access to personal data.]

Option 3:
… [the European Commission decision containing the standard data protection clauses] in line with Article 46 § 2 c) GDPR.

Option 4:
…. [the decision taken by a national supervisory authority with reference to its own standard data protection clauses approved by the European Commission according to Article 93 § 2 GDPR] in line with Article 46 § 2 d) GDPR.

Option 5:
…. [code of conduct approved by the supervisory authority XYZ] in line with Articles 46 § 2 e) and 40 GDPR.

Option 6:
… [approved certification mechanism] in line with Article 46 § 2 f) and Article 42 GDPR. [add any details necessary pertaining to the approved certification mechanism]

Option 7:
… the following contractual clauses approved by the [supervisory authority] subject to the consistency mechanism:

3.1 Data Processors located in third countries outside the European Economic Area agree to comply with their obligations under this Data Processing Contract; in the event that Sub-Processors as described in **point 10.3** of this Data Processing Contract are used, the Sub-Processor(s) shall comply with the Data Sub-Processing Contract, which shall impose least the same obligations on the Sub-Processor as this Data Processing Contract.

3.2 If a Data Processor cannot comply, for whatever reason, with any of the provisions of this Data Processing Contract, it shall promptly inform the Data Controller of its inability to comply, in which case the Data Controller is entitled to suspend the transfer of data and/or terminate the Data Processing Contract. This provision applies mutatis mutandis to the relationship between the Data Processor and a Sub-Processor located in a third country outside the EEA.

3.3 Data Processors located in third countries outside the EEA shall guarantee that they have no reason to believe that the legislation applicable to them prevents them from fulfilling the instructions received from the Data Controller and their obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on their obligations under this Data Processing Contract, they will promptly notify the change to the Data Controller as soon as they are aware of it, in which case the Data Controller is entitled to suspend the transfer of data and/or terminate the contract. The Data Controller shall forward any such notification received from the Data Processor to the supervisory authority if the Data Controller decides to continue the transfer or to lift the suspension.

3.4 The Data Processor and Data Controller shall make available to the data subjects upon request a copy of the relevant provisions of this Contract, unless they contain confidential or commercial information, and a summary description of the security measures implemented by any Data Processors located in third countries outside the EEA.

3.5 If the data subject is unable to bring a claim for compensation against the Data Controller due to the damage suffered as a result of any breach by the Parties of the obligations contained in this Appendix because the Data Controller has ceased to exist physically or in law or has become insolvent, the Data Processor agrees that the data subject may issue a claim against the Data Processor as if it were the Data Controller, unless the successor entity has assumed in full

the legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against said successor entity.