Manual of Data Control in the DiDb System

Data controller of the DiDb system:

SECTRAN Kft.

Head office:

H-1033 Budapest Szentendrei út 89-93.
phone: +36-1-784-6830
email: office@didb.eu
web: www.didb.eu

Effective from: 1st January 2022, until revocation

TABLE OF CONTENT

1. The purpose and scope of effect of the Manual 4
2. Terms 5
3. The rules of data control 5
4. The data protection system of sectran 6
4.1. Responsibilities of CEO in data protection 6
4.2. Responsibilities of Data Protection Officer (DPO) 7
5. Rules of data security 7
6. Exercising the rights of the data subjects 8
6.1. Informing data subjects about their controlled personal data 9
6.2. Rectification rights of the data subject 10
6.3. Erasure rights of the data subject 10
6.3.1. General right to erasure 10
6.3.2. Withdrawal of consent 10
6.4. The right of data subjects to require restriction of data controlling 10
6.5. The right of data subjects to object to controlling of personal data 11
6.6. Exercising the data subjects' right to data portability 12
6.7. Legal remedies 12
7. Data control in connection with the operation of the DiDb system 12
7.1. Information concerning the data controller 12
7.2. Presentation of the purpose of data processing 13
7.3. Legal grounds for the processing of personal data 13
7.3.1. Legal ground: Article 6 (1) c) of the GDPR 13
7.3.2. Legal ground: Article 6 (1) f) of the GDPR 14
7.4. Time limit of data storage of personal data 14
7.5. Place of the processing of personal data 15
7.6. Processed personal data and categories 15
7.7. Detailed description of data processing in the DiDb system 15
7.7.1. Data controlling in the course of registration process 15
7.7.2. Frequently asked questions related to registration 16
7.8. Conclusion of legal membership 18
7.9. Avoidance of duplication of membership 19
7.10. Termination of DiDb membership 19
7.11. DiDb membership validation 19
7.12. Data controlling during the operation of DiDb system 20
7.13. Data processing operations performed by the users of the system 20
7.14. Special rules for data controlling regarding extraordinary events in association with deliveries 21
7.14.1. Legal ground for data controlling 21
7.14.2. Result of investigation 21
7.14.3. Rules concerning investigation documentation 21
7.15. Material breach of contract – exclusion of a member from didb-system 23
7.15.1. Definite or indefinite exclusion 23
7.15.2. Processing of the data of excluded persons 23
Appendix No. 1 24
On the appointment of the data protection officer of SECTRAN 24
Appendix No. 2 25
Third parties involved in the data processing as data processors: 25
Appendix No. 3 26
Appendix No. 4 27
Table of processed data 27

SECTRAN Kft. (hereafter referred to as SECTRAN) has created the Handbook of "Manual of Data Control in the DiDb System" (hereinafter referred to as Manual) for the purpose of ensuring the rights of the data subjects concerned, and in order to ensure the accessibility and transparency of data processing practices related to the operation of the DiDb (Driver Intelligence Database, hereinafter referred to as DiDb) system, which has been developed and is being operated exclusively by SECTRAN.

The primary legal background of the data processing is 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) [hereinafter: GDPR] which entered into effect on 25 May 2018. However, Hungary, the Member State where SECTRAN has its registered office, has only introduced the legislative acts required by GDPR after that, and the enforcement case law is also constantly evolving. Therefore, based on the consequences and experience gained from the above, SECTRAN reviewed its regulation established as a result of the GDPR, and modified its rules of data protection processes with entry into effect from 1 February 2020.

Name of the controller:	SECTRAN Kft.
CRN of the controller:	Cg.16-09-016061
Registered office of the controller:	H-5008 Szolnok, Fazekas Mihály u. 42.
Email of the controller:	info@sectran.eu
Representative of the controller:	Tímea Garai, managing director

1. THE PURPOSE AND SCOPE OF EFFECT OF THE MANUAL

Although GDPR does not explicitly stipulate an obligation for SECTRAN to create a data protection manual, however, considering Article 24 (2) of the GDPR and Paragraph (78) of the Preamble, as well as the direction given by the Hungarian National Authority for Data Protection and Freedom of Information under case numbers NAIH/2018/1212/2/K and NAIH/2018/1594/2/K regarding the data protection reform, SECTRAN has elected to publish the data processing practices of the DiDb-system in this Manual, in order to ensure the rights of those involved.

SECTRAN ensures the rights of the data subjects as specified in Chapter 3 of the GDPR by creating this Manual and making it available, as it defines SECTRAN's practical implementation of the principles of data protection and its data protection procedures. The aim of the present Manual is to provide adequate information about the data controlled by SECTRAN and data processors commissioned by SECTRAN, their source, the aim of, legal ground for, duration of data control, the data processors, and their activity in connection with data process, and – in case of the transfer of personal data – the recipient of and legal ground for data transfer. The Manual is also considered as information provision under Article 13 (1)-(2) of the GDPR, since the Manual is available for all data subjects and contains all the information which shall be provided to the data subjects by SECTRAN as controller.

In regard to the personal scope of the Manual, it applies to all persons who, through their legal relationship with SECTRAN and especially in capacities such as those granted by employment, data processing agreement or agency relationship, gain access to or take possession of personal data.

The material scope of the Manual covers all processes of the DiDb system in which processing of personal data, as defined in Article 4 (1) of the GDPR, is carried out.

The temporal scope of the Manual shall extend from 25 May 2018 the date of implementation of the GDPR, until it is repealed, its current version (with the serial number MDC-ENv-22.1) is valid from 1 January 2022.

SECTRAN hereby states that it is a legal person registered and listed in Hungary, a Member State of the European Union. Considering that data subjects of the data processing activities are not exclusively Hungarian citizens, and that not only legal persons registered and listed in Hungary perform data processing activities as processors, respecting the redress and enforcement rights of all data subjects, SECTRAN states that its main supervisory authority under Article 56 of the GDPR is **the Hungarian supervisory authority, the National Authority for Data Protection and Freedom of Information.** Naturally, the identification of the main supervisory authority does not result in the violation of data subjects' right under Article 77 (1) of the GDPR, which means that any and all natural persons the data of whom are processed by SECTRAN continue to be entitled to lodge a complaint with another supervisory authority – in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement.

2. TERMS

The terms and their definitions used in this Manual are the same as those defined in Article 4 of the GDPR. However, SECTRAN wishes to comply with the principle of transparency [Article 5 (1) a) of the GDPR], therefore, in order to ensure the expected plain communication, and easy interpretation of legal terms, it explains them as follows:

- ***personal data:*** any information that is associated with, or may be associated with, a particular living individual, and which information may potentially be used to infer further information. The data must be associated with a person who is alive (there are no personal data associated with the deceased), and the data and the person does not necessarily have to be associated with each other, as long as it is possible to associate them, it is considered personal data. Therefore, any information may become personal data if that information allows one to associate it with a particular person; this way practically anything can become personal data, starting from names, places and dates of birth, through lists of phone numbers dialled to dedicated IP addresses.
- ***data subject:*** the person whom the personal data may be associated with, so literally the "subject" of the data; in regard to the procedures described in this Manual, it shall mean DiDb member (driver)
- ***data processing:*** data processing shall mean any operation involving personal data
- ***data controller:*** any person other than the data subject who is involved in performing operations on personal data on their own terms; in regard to the procedures described in this Manual, it shall mean SECTRAN
- ***data processor:*** a third party, other than the data controller and the data subject, who takes possession of personal data in the course of data processing. Anyone who performs any operation on behalf of the data controller is considered data processor. SECTRAN's partners who register drivers into the DiDb system, or who check the DiDb membership of drivers via the DiDb system during the entry and exit controlling procedure to logistics sites, are considered data processors
- ***data transfer:*** the personal data is transferred to a third party from the data controller, however, following transfer of said data, no legal relationship exists between the data controller and the third party; the recipient third party becomes a data controller itself, and an independent legal relationship is created between this third party and the data subject.

3. THE RULES OF DATA CONTROL

As informational self-determination is a basic right of every natural person established in the Fundamental Law of Hungary, SECTRAN may only process data during its proceedings on the basis of effective legal regulations, especially:

SECTRAN shall control personal data only as specified in Article 6 (1) of the GDPR.

In addition to the rule set forth in the previous paragraph, SECTRAN shall control personal data [Article 9 (1) of the GDPR] only in accordance with the provisions in Article 9 (2) of the GDPR, or if conditions specified in the legal regulation established under Member State authorization by the GDPR are met.

Any personal data that SECTRAN processes shall remain personal data in the course of data processing as long as they concern identified or identifiable natural persons. SECTRAN shall consider a piece of data to be personal data if it has the technical means to identify the data subject from that piece of data. If data have been anonymized by someone (either SECTRAN or someone else) in a way that as a result of which the data subject cannot be identified or cannot be identified anymore, SECTRAN shall not apply the principles of data protection to the anonymized information. SECTRAN shall provide information on the time and means of data anonymization at the time of the specific process.

Through the publication of this Manual or the disclosure of the controlling description regarding specific data controlling activities, SECTRAN shall, in every instance, inform the data subject about the purpose of data controlling, the legal grounds for such controlling, and the facts associated with data controlling as specified under Articles 13 and 14 of the GDPR.

SECTRAN shall make use of O&M, physical, IT and authorisation tools in order to ensure that no unauthorised person may gain knowledge of any personal data.

The employees of SECTRAN and the staff of any organisation involved in data processing, performing any part of the data processing operations, shall treat the personal data disclosed to them during the course of processing as confidential information.

4. THE DATA PROTECTION SYSTEM OF SECTRAN

Taking into consideration the company's characteristic features, the leading representatives of SECTRAN define the organisation of data protection and the sphere of tasks and authority for and in connection with data protection and appoint a person for the supervision of data control.

The employees of SECTRAN make sure during their work that unauthorised persons may not inspect personal data, and that the storage of personal data is carried out in such a way that they may not be accessible, identifiable, modifiable and destroyed by unauthorised persons.

The supervision of SECTRAN's data protection system is carried out by the CEO via a data protection officer appointed by him/her. The name and e-address of the data protection officer can be found in *Appendix 1.*

4.1. RESPONSIBILITIES OF CEO IN DATA PROTECTION

a) ensuring the conditions necessary for the data subjects to exercise their rights as specified under Article 6 below
b) provision the resources in staff and equipment for the protection of personal data controlled by SECTRAN;
c) elimination of shortcomings and illegitimate conditions disclosed during the inspection of data control, and initiating and conducting proceedings in order to establish personal liability;
d) overseeing the work of the person responsible for data protection;
e) launch an internal audit assessing data protection in case of necessity;
f) submission the internal regulations of SECTRAN concerning data protection;

g) in case of extremely severe violation of the law, the CEO, pursuant to the provisions of employment laws, shall initiate disciplinary action against the person who has processed personal data in a way that violated legislations.

4.2. RESPONSIBILITIES OF DATA PROTECTION OFFICER (DPO)

a) provision assistance in the enforcement of the rights of the data subject included in Chapter 6;
b) submission of an annual report on the execution of SECTRAN data protection tasks for the senior officer until January 15,
c) monitoring the observance of the present Manual at the individual organisational units;
d) investigation of compliance with the legal provisions of the GDPR and other legislations, including compliance with the provisions of the Manual and the requirements for data security, and shall inform the CEO about the results of the investigation;
e) monitoring the legislative changes concerning data protection, and if justified, initiates the modification of the present Manual;
f) responding to any queries sent to SECTRAN by the supervisory authorities and in any procedures initiated by the supervisory authorities;
g) submission a request towards the Authority should an issue concerning data protection arise that cannot be addressed on the basis of statutory interpretation;
h) investigation of any notification it receives; and if unauthorised data processing or its possibility is detected, the DPO shall request SECTRAN or the data processor to refrain from such practices;
i) making recommendations for necessary steps to be taken based on the findings of the above investigations and on the reports submitted regarding violations of the data protection provisions;
j) supervision of the completion of requests received from external organisations affecting personal data,
k) ensuring that training is provided regarding data protection,
l) active participation and assistance with making decisions regarding data processing,
m) if requested, providing information on the issues of data protection to the associates of SECTRAN,
n) commenting on sections of policies and procedures documentations to be published by SECTRAN that deal with the issues of data protection,
o) performing the duties associated with data protection that legislations require them to perform.

5. RULES OF DATA SECURITY

SECTRAN applies the following measures for the security of paper-based personal data:

- the data may be inspected by authorised personnel only and may not be disclosed to any other third party;
- the documentation is kept in a locked and dry room equipped with a fire- and property protection device;
- actively controlled documents may only be accessed by authorised personnel;
- SECTRAN's employee may only leave the room where data control is performed after locking up the data storage medium or locking the door of the room;
- when data control is finished, SECTRAN's employee must lock up the paper-based data carrier;
- should the data controlled on paper be digitalised, SECTRAN's rules for digitally stored documents become applicable

SECTRAN applies and guarantees the following measures for the security of personal data stored on computers or the network:

- the computers used during data control are owned by the company or the company holds proprietorship that complies with the full ownership of the device;

- data stored on the computers may only be accessed with a valid, personal and identifiable permission – at least a username and a password – and SECTRAN makes sure that the passwords are regularly changed;
- every computer record is traceable and stored in a log file;
- data stored on cloud-based, network servers (hereinafter: servers) may only be accessed with the necessary permissions and by appointed personnel;
- regulates and publishes in a separate document its data storage and data management and encryption protocols implemented on cloud-based servers;
- the active data of databases of personal data are periodically saved, the scope of the save is the central server's entire data set;
- should the objective of data control be carried out and the time-limit of data control is over, the file containing the data is irrevocably deleted and the data is unrecoverable;
- SECTRAN makes sure about continuous virus protection on the network where the control of personal data is carried out;
- SECTRAN prevents unauthorised access to the network with its available IT equipment.

6. EXERCISING THE RIGHTS OF THE DATA SUBJECTS

In the course of operating the DiDb system, SECTRAN controls personal data. According to Articles 15 through 21 of the GDPR, the data subjects have the following options to enforce their rights with respect to SECTRAN's control of their personal data:

- The data subjects may ask for information about how their personal data is controlled as specified in Article 6.1,
- ask for the rectification of their personal data as specified in Article 6.2,
- ask for the deletion of their personal data as specified in Article 6.3,
- ask for restrictions in controlling their personal data as specified in Article 6.4,
- ask for objection to controlling their personal data as specified in Article 6.5,
- exercise their right to the portability of their personal data as specified in Article 6.6.
- file a complaint or take legal actions as specified in Article 6.7.

Hereby in Article 6, SECTRAN specifies the rights, obligations and procedural requirements of data subjects that allow them to exercise their rights.

SECTRAN shall always strive to provide information to the data subjects in a way that is as concise, transparent, understandable, easily accessible, clear and nontechnical as possible, while meeting the requirements set forth in the GDPR.

By default, SECTRAN shall provide all information to the data subjects in writing, which also includes information in electronic form.

If the data subject requests information communicated orally, then authorised representatives of SECTRAN can comply with this request once the data subject identifies herself/himself.

SECTRAN shall provide information to data subject only if authorised SECTRAN employee has verified the data subject's identity.

The identity of data subject is considered verified if:

- the data subject provides proof of identification to authorised SECTRAN employee as specified in current Hungarian legislations (by submitting documentation such as Personal ID card, passport, driver's licence, or other legally allowed documents),

- the data subject provides proof of identification to authorised SECTRAN employee as specified in legislations of the EU,
- the request of the data subject is known from earlier contacts made, arrives from an email address associated with the data subject,
- the request from the data subject arrives via a channel that is insured by SECTRAN, one that is not public and may only be used following appropriate identification of the data subjects.

SECTRAN does not accept verification of someone's identity via the telephone; for this reason, data subject may not initiate asserting her/his rights specified in Article 6 on the phone.

If the identity of the data subject is not verified, SECTRAN shall decline any request to assert rights regarding the data processing.

In case of a request regarding the data subject's rights specified in Article 6, SECTRAN shall send information to the data subject within one month of receipt of such request.

The request is considered received by SECTRAN if:

- the data subject discloses her/his request in person to the authorised employee of SECTRAN who will verify the subject's identity,
- a written request arrives officially to SECTRAN.

SECTRAN may extend this time period by a maximum of two months if the complexity of the request or the high number of requests being handled at the time makes this necessary.
SECTRAN shall send electronic notification to the data subject regarding the extension of the deadline within one month of the receipt of the request, including reasons for such delay.
If SECTRAN fails to take steps upon a request by data subject, then the data subject may exercise her/his right to appeal as specified in Article 6.7.

SECTRAN shall provide information and take measures in connection with the rights of the data subject free of charge.

The Data Protection Officer of SECTRAN is responsible for providing information and taking the necessary measures in connection with the rights of the data subjects.

The information provided under Section 6.1 shall contain in all cases information on the possibility to exercise further redress and enforcement rights of the data subject.

For further information on data subjects' rights related to the specific data, please check Appendix No. 4.

6.1. INFORMING DATA SUBJECTS ABOUT THEIR CONTROLLED PERSONAL DATA

If the data subjects decide to exercise their access rights as defined in Article 15 of the GDPR, SECTRAN shall disclose the following in its response:

- the purpose(s) of data processing,
- the categories of personal data concerned,
- the recipients or categories of recipients to whom the personal data have been or will be disclosed by SECTRAN,
- the envisaged period for which the personal data will be stored, or, if it is not possible, the criteria used to determine that period,
- the procedures for exercising the right to rectification,
- the procedures for exercising the right to erasure,
- the procedures for exercising the right to restrict controlling,
- the procedures for exercising the right to object to controlling,
- the right to lodge a complaint with the supervisory authority,

- if the personal data is not collected from the data subject, then all available information as to their source,
- the existence of automated decision-making algorithms if the data controlling uses such systems, along with meaningful information on the logic applied.

In the course of providing the above information and upon request from the data subjects involved, SECTRAN shall provide a copy of the relevant personal data to the data subjects.

None of the employees of SECTRAN shall provide information by phone regarding any particular personal data controlled by SECTRAN.

6.2. RECTIFICATION RIGHTS OF THE DATA SUBJECT

If the data subject requests rectification of his/her personal data and such personal data is available, SECTRAN shall rectify such personal data and inform the data subject about this fact as well as the date of rectification.

If the data subject requests rectification of their personal data, but the personal data to replace the already processed data is not available, then SECTRAN shall ask the data subject to provide the missing data.

6.3. ERASURE RIGHTS OF THE DATA SUBJECT

If the data subject exercises his right to erasure, SECTRAN shall erase the personal data so that they cannot be restored anymore. If the personal data cannot be erased from the data storage media, SECTRAN shall destroy the data storage media.

6.3.1. GENERAL RIGHT TO ERASURE

SECTRAN shall erase the controlled personal data without delay if one of the following conditions exists:

- The personal data are no longer needed for the purpose SECTRAN has been processing them, that is the DiDb member ceases to be a member for any reason
- the data subject successfully objects to the data processing in accordance with Section 6.5,
- SECTRAN is advised that the processing of such personal data does not follow legislations,
- personal data shall be erased in order to comply with a legal provision set forth in the EU or Hungarian law applicable to SECTRAN.

6.3.2. WITHDRAWAL OF CONSENT

SECTRAN shall erase the controlled personal data without delay if the legal ground for data processing is the consent of the data subject [Article 6 (1) a) of the GDPR], and the data subject withdraws his consent.

SECTRAN states that although with the withdrawal of the consent, SECTRAN cannot process the data anymore, but the DiDb membership may be maintained in the absence of such data, therefore, the data may be provided again later based on the decision of the data subject. No disadvantages may arise from failure to provide data or withdrawal of the consent.

6.4. THE RIGHT OF DATA SUBJECTS TO REQUIRE RESTRICTION OF DATA CONTROLLING

The data subject may request SECTRAN to mark their personal data stored by SECTRAN with the purpose of restricting any future processing.

Upon receipt of such request by the data subject, SECTRAN shall restrict data controlling if one of the following conditions exists:

- the request of the data subject questions the accuracy of their personal data; in this case the restriction shall apply to the period of time needed for SECTRAN to verify the accuracy of such personal data,
- the controlling of the relevant data does not follow legislations, but the data subject objects to the erasure of his/her data, instead, he/she requests restriction of processing,
- SECTRAN does not need the personal data to be controlled any longer to achieve the objectives set forth prior to data controlling, but the data subject requests such data in order to file, assert or protect legal claims.

If SECTRAN restricts controlling of personal data, then during the period of restriction, such personal data may only be controlled with the approval of the data subjects, or in association with filing, asserting or protecting legal claims, to protect the rights of other natural or legal persons, or to ensure important public interests of the European Union or its member states.

The restriction does not apply to the storage of personal data as data controlling operation; such an operation must be carried out by SECTRAN even during the period of restriction.

When SECTRAN lifts the restriction on data controlling, SECTRAN shall, at the same time, send notification of this fact to the data subject who requested the restriction.

6.5. THE RIGHT OF DATA SUBJECTS TO OBJECT TO CONTROLLING OF PERSONAL DATA

Data subjects may only object to data processing operations the legal ground for which is the legitimate interest of the data processor or any third party in accordance with Article 6 (1) f) of the GDPR.

In such cases, SECTRAN shall assess whether there are compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

During the assessment, SECTRAN shall review the interest assessment test supporting the data processing under Article 6 (1) f) of the GDPR, taking into account all important circumstances of the case related to the right enforcement subject to the objection, and create a summary thereof. The summary may not contain any data which may be considered personal data of the person exercising his right. The summary shall be prepared by the data protection officer.

If SECTRAN finds during the assessment, that the data processing activity is justified by legitimate reasons, it shall inform the data subject exercising his/her right to objection and may continue to process such data. In such cases, the objection of the data subject shall be considered invalid.

If SECTRAN finds during the assessment, that the data processing activity is not justified by legitimate reasons, it shall immediately terminate data processing. In such cases, the objection of the data subject shall be considered successful. However, SECTRAN informs all data subjects, that it has established its data processing system in a way that in its professional opinion, in the absence of all data processed on the legal ground specified in Article 6 (1) f) of the GDPR, the purposes of data processing may not be obtained. Therefore, if

the data subject successfully objects to the data processing, upon erasure of the data, SECTRAN will erase all other data of the data subject related to his DiDb membership, considering that the purpose of the data processing may not be obtained with respect to the data subject in question. (Data processed on the legal ground under Article 6 (1) c) of the GDPR – data processing required by law – shall be exceptions to this rule, since they cannot be deleted within the deadline specified in the legislation.)

6.6. EXERCISING THE DATA SUBJECTS' RIGHT TO DATA PORTABILITY

If the legal ground for any of the data processing activities detailed in Section 7 is a contractual relationship under Article 6 (1) b) of the GDPR, the data subject has the right to receive any of his/her processed personal data in a structured, widely used, machine readable format.

SECTRAN shall comply with Article 6.6 as specified here primarily in .xml, .csv or .doc format, depending on the nature of the relevant personal data.

Data subject may further requests SECTRAN to transfer his/her personal data, if this is technically feasible, to another data controller clearly identified by the data subject.

6.7. LEGAL REMEDIES

In accordance with Paragraph (1), Article 77 of the GDPR, the data subject may file a complaint with the supervisory authority regarding the data processing practices of SECTRAN.

In accordance with Paragraph (1), Article 79 of the GDPR, data subject may take legal actions at the competent court of their permanent address or place of residence regarding any legal non-compliance during data processing by SECTRAN.

7. DATA CONTROL IN CONNECTION WITH THE OPERATION OF THE DIDB SYSTEM

In the course of operating the DiDb system, SECTRAN controls personal data of data subject. The main purpose of data controlling is the same for all data processing operations: the operation of the DiDb system. However, SECTRAN divided its data processing processes to sub-purposes, since not all processes are based on the same legal ground.

Therefore, in this Section 7, SECTRAN specifies and explains all data processing activities with different purposes. If SECTRAN obtains personal data necessary for data processing directly from the data subject, these process descriptions shall be considered provision of information to the data subject under Article 13 of the GDPR. If SECTRAN does not obtain personal data necessary for data processing directly from the data subject, the Manual explicitly mentions this, and provides information to the data subject on a case-by-case basis.

7.1. INFORMATION CONCERNING THE DATA CONTROLLER

The identity and contact details of the data controller: see the introductory provisions of this Manual

The contact details of the DPO, if any: the name and contact details are provided in Appendix 1

Third parties included as data processors in the data processing activities of the data controller: during the operation of the DiDb system, SECTRAN cooperates with several partners. These partners may perform two tasks: they register drivers into the DiDb system or check the DiDb membership of drivers on-site by applying the DiDb system. None of the above processes may take place without the personal presence of the driver, therefore, SECTRAN shall provide information on the data controller on-site in all cases.

7.2. PRESENTATION OF THE PURPOSE OF DATA PROCESSING

PURPOSE OF PROCESSING PERSONAL DATA: DiDb system operation

The purpose of DiDb is to reduce driver related risks and losses in ground transportation. By operating the DiDb system, SECTRAN aims to protect the supply chain sector from systematic cargo crime, whereby individual drivers are given the opportunity to register their good and reliable behavior in the independent system of DiDb.

DiDb operated by SECTRAN is neither a professional chamber, nor a union, membership is not obligatory for the drivers! SECTRAN's mission is to decrease the number of crimes against or during ground transportation, which has been increasing every year. The DiDb system is a database registering qualified and supervised truck drivers and shared by the participants of logistics market. Naturally, it does not mean that all members of DiDb are reliable. However, market participants may decide to become part of the DiDb system, and only appoint drivers who have satisfactorily proved during the years that they are in fact reliable.

Therefore, SECTRAN states that by entering the DiDb system, no one will have any disadvantage which may render his employment impossible. To SECTRAN's knowledge, there are no companies in Europe which set DiDb membership as a condition for employment!

However, DiDb membership may present several advantages to those who wish to become part of the system as drivers. In the system which is based on score collection, it can be monitored whether someone has in fact performed his work in a reliable manner, and the clients regularly provide feedback on the performance of drivers, thus contributing to the collective qualification of drivers registered in the database.

DiDb membership is based on the individual decision of drivers: whether they wish to become DiDb members or not. If yes, they shall conclude a contract with SECTRAN.

7.3. LEGAL GROUNDS FOR THE PROCESSING OF PERSONAL DATA

A contractual relationship is established between SECTRAN and the driver wishing to register in the DiDb system. SECTRAN draws the attention of the data subject to the fact that personal data are included in Appendix 4 of this manual is a precondition for the conclusion of the contract. If this information is not provided to SECTRAN by the data subject, the contractual relationship does not enter into effect.

There are several legal bases for data processing in order to achieve the purpose of data processing:

7.3.1. LEGAL GROUND: ARTICLE 6 (1) C) OF THE GDPR

For certain categories of data, the Hungarian law sets forth legal obligations for SECTRAN which may only be complied with the processing of such data. There are two categories of data concerned:

- accounting documents directly and indirectly supporting accounting in accordance with the provision of Section 169 (2) of Act C of 2000 on Accounting shall be retained for at least 8 years, in legible form, in a way retrievable based on accounting records. SECTRAN complies with this provision by keeping accounting documents for the end of 8th year after they are issued. Therefore, due to this requirement, data related to financial performance are kept regardless of the DiDb membership, considering that they are indicated on invoices.
- since SECTRAN's service for members is a service provided for natural persons, members may exercise their rights related to consumer protection. Section 17/A (2) of Act CLV of 1997 on consumer protection

states with respect to the enforcement of consumer rights that the consumer may communicate his complaint to the business orally or in writing. However, in addition to natural persons, SECTRAN provides the right to lodge a complaint for its partners as well. Therefore, if a complaint is lodged, SECTRAN files it, and shall keep the minutes recorded in accordance with Section 17/A (7) of the Act and the copy of the response for five years.

7.3.2. LEGAL GROUND: ARTICLE 6 (1) F) OF THE GDPR

The processing of certain data indicated in Appendix No. 4 is the legitimate interest of SECTRAN and its partners involved in ground transportation. In order to achieve the purpose of operating the DiDb system, the processing of data categories specified there is absolutely necessary. In order to determine whether such data can be processed or not, SECTRAN performed a so-called interest assessment test, and found with respect to all data indicated so in the Manual that they are necessary for the legitimate interests of SECTRAN and its partners related to the operation of the DiDb system and its purposes, and their processing does not result in the excessive restriction or violation of the interests, basic rights and freedoms of the members.
It is the legitimate interest of SECTRAN and its partners to employ reliable persons for the transportation of goods whose personal data are known to the freight operator and SECTRAN, who has no criminal record and with respect to whom it can be stated with a high level of confidence that they would not commit an act to the detriment of the beneficiaries of the transport. It is an overriding interest composed of several individual cases that DiDb system is able to fulfil its function for which it has been established: it aims to be the white list of reliable drivers, thus decreasing the number and volume of incidents incurring during ground transportation.

7.4. TIME LIMIT OF DATA STORAGE OF PERSONAL DATA

As general rule, data related to DiDb membership are stored as follows – regardless of the legal ground:

- for applicants who do not become members:
  - for applicants, whose application for registration has been refused, the time limit for data storage by SECTRAN is 30 days, as described in the process description
- for applicants who become members:
  - until termination of DiDb membership:
    - for applicants who become members, from commencement of the membership until 2+2 years after the last renewal of the membership as detailed in 'DiDb membership validation'
    - or until termination of the membership by the data subject or SECTRAN

Additional deadline for data processing:

- For data processed on the legal ground specified in Article 6 (1) a) of the GDPR, SECTRAN shall also erase data if the data subject withdraws his consent for the processing [for more information see Section 6.3.2]
- SECTRAN shall store complaints received by SECTRAN, minutes recorded and the copy of the response for five years regardless of the DiDb membership in accordance with Section 17/A (7) of Act CLV of 1997 on consumer protection [hereinafter: Consumer Protection Act].
- SECTRAN shall retain accounting documents for 8 years after they were issued in accordance with Section 169 (2) of Act C of 2000 on accounting [hereinafter: Act on Accounting], and this provision is performed by SECTRAN by retaining such documents for the end of the 8th year after they were issued.

Rule concerning data not considered as personal data:
After erasure of personal data concerning the data subject by SECTRAN due to the withdrawal of the consent or termination of the membership, it further processes data which are not considered personal data: date of DiDb registration, DiDb membership identifier, DiDb status, DiDb membership validity, DiDb qualifications (number of points and stars) and HASH code. Such data related to the DiDb membership number are retained in order to ensure that the same number is not distributed for a second time. However, such data are not considered personal data, as there is no possibility to link them with identified or identifiable natural persons, and SECTRAN permanently terminates the link between the data and the data subject.

7.5. Place of the processing of personal data

The place of the data processing is the head office of SECTRAN, but the data registration and checks during loading and unloading may also take place at the partners of SECTRAN.

7.6. PROCESSED PERSONAL DATA AND CATEGORIES

With Appendix No. 4 of the Manual, SECTRAN has prepared an easily understandable summary table which contains all data categories with other relevant information concerning the data.

During scanning we are masking all data on identity document, which are not processed by SECTRAN in accordance to make them invisible.

7.7. DETAILED DESCRIPTION OF DATA PROCESSING IN THE DIDB SYSTEM

The main purpose of DiDb system is to reduce the driver related risks and losses in ground transportation. DiDb is a shared whitelist of checked and qualified truck drivers, consisting of those previously registered drivers who – on basis of their voluntary decision – wish to be members of a database which assesses the reliability and work quality of its members with a positive approach. Registration or membership validation can be done at one of SECTRAN's customer service offices or at a registration point operated by a partner - during the assessment, candidates must undergo a compliance procedure based on the data they provide. If the registration is successful, the driver is entered into the system and can prove his membership with the DiDb card issued to him at the companies using the DiDb system.

During registration or membership validation process, the following data groups can be communicated to SECTRAN by data subjects:

- ***obligatory data:*** data in this group are required to provide for the assessment of the application, obtaining and maintaining the membership
- ***optional data:*** data in this group can be divided into two sub-groups:
    - data beneficial for the assessment of the application (information in accordance with the purpose of the DiDb system, which may facilitate the decision whether the driver is worthy of the membership);
    - data that may support easy contact.

It should be noted that those applicants who provide all the obligatory data and are worthy of the membership will become members, and not submitting optional data will not be a disadvantage during the assessment process of registration.

7.7.1. DATA CONTROLLING IN THE COURSE OF REGISTRATION PROCESS

In order to start the assessment process of the driver membership application, the applicants must submit the data which are summarized in Appendix 4.

For data categories the provision of which is compulsory, in the absence of the data the contract cannot be concluded between SECTRAN and the driver.
For data categories the provision of which is not compulsory, in the absence of the data the contract can be concluded between SECTRAN and the driver, but the lack of data may present an obstacle to the performance of transports based on the individual decision of the freight operators. This is however the individual decision of the freight operator, regardless of the DiDb system. The driver may provide such data to the freight operator for the performance of the transport not only via the DiDb system, but also directly. The legal ground for data processing by SECTRAN is the voluntary consent of the driver in accordance with Article 6 (1) a) of the GDPR, and this consent may be withdrawn at any time. This means that if the driver decides that he/she does not want SECTRAN to process data the provision of which is not compulsory, he/she may request their erasure from the DiDb system anytime.

7.7.2. FREQUENTLY ASKED QUESTIONS RELATED TO REGISTRATION

Why is it required to keep a record of the expiry date of all three personal documents?
Each document is concerned with different questions of authority:

- ***ID card:*** with an expired ID card, the driver may be stopped during a roadside check if he/she is not able to prove his/her identity with another document;
- ***driving license:*** with an expired driving license the driver may be stopped during a roadside check and is officially ineligible to drive in traffic;
- ***passport:*** with an expired passport the driver may not enter destinations (or transit countries) which are outside of the Schengen Area

This information is crucial for the determination of certain routes.

During the data are obtained, the image of the identity documents is scanned. The data uploaded by the data processor is compared with the data on the identity document. The purpose of the scanning is to double-check the data entering the system on the basis of the "four eyes principle" and to ensure that only the real, actual data about the data subject should be entered into the database - this is the legitimate interest of the data subject and the SECTRAN too. The check is carried out in order to enforce the principle of accuracy.

We emphasize: scanned images are only stored and processed until the time of the data check, after it the data will be erasured.

What determines whether the name of the driver's mother or father is required by SECTRAN?
In certain European countries – unlike in Hungary – applicants must provide their father's name and not their mother's name; and there are other countries where none or both parents' name shall be provided. This is why the applicant's citizenship is obligatory to be given, as when the registration form is completed electronically the citizens of the specified countries do not give their mother's name, but their father's name or both or none.

The list showing the right categories for the citizenship is detailed in App. 3.

Why is a high-definition photograph taken of the driver during registration?
In order to start the assessment process of the membership application, SECTRAN takes a high-quality and high-definition photograph for the future identification of the driver.

In the future, the photograph shall only be accessible by the users of DiDb system, contracted with SECTRAN in the presence of the data subject, as the identification of the driver's data requires his/her own personal DiDb card and PIN number.

(For a more detailed description, please check the "DiDb system - User's Manual")

We will also process the photographs on the identity document During the data are obtained, but only until the double-check of data described in the previous paragraphs. This is also carried out in order to enforce the principle of accuracy.

The purpose of comparing the photograph taken at the time of registration with the photograph on the document is to ensure, on the basis of the 'four eyes principle', that the data are indeed registered for the right person.

Why is it required to submit a Certificate of Good Conduct?
In order to start the assessment process of the membership application, the driver must submit a valid Certificate of Good Conduct to SECTRAN.

Given that the DiDb is a database of reliable drivers, SECTRAN reserves the right to harmonise the admission of drivers to the database with the purposes of the system.

The condition of the DiDb membership is clean criminal history, which is why admission is linked to a valid Certificate of Good Conduct.

The character of legal relationship between SECTRAN and the drivers – as a result of the purpose of the DiDb system – is a confidential relationship, the foundation of which requires the clean criminal history of the driver.

In course of the registration the applicant is required to present a valid Certificate of Good Conduct that is not older than 96 days, in connection with the prescriptions of data protection and data security are enforced by SECTRAN via the regulations presented below.

For which purpose SECTRAN uses the Certificate of Good Conduct?
As on basis of the legal relationship between SECTRAN and its contractual partners (manufacturers, freight forwarders and carriers), SECTRAN only allows drivers in the DiDb database who are morally acceptable for the purposes of the DiDb-system, the customer service administrator examines the Certificates':

- validity (in a way that is accessible for anyone);
- content on basis of the requirements of the registration.

How does SECTRAN handle the information included in the Certificate of Good Conduct?
Prior to processing being initiated, SECTRAN informs the data subject that the objective of the presentation of the Certificate of Good Conduct is to decide whether the applicant is worthy of the DiDb membership, so the provision of such data is indispensable for SECTRAN.

Who can access the personal data on the Certificate of Good Conduct?
The registration process is always carried out in one of SECTRAN's or its contracted partner's customer services or dedicated registration points, located within the EU. Data on the Certificate of Good Conduct become known to the customer service employee, when examining the presented Certificate of Good Conduct, and deciding whether the applicant has indeed no criminal records, which is a prerequisite for registration.

Does SECTRAN store any data in connection with the Certificate of Good Conduct?
On basis of the legal relationship between SECTRAN and the partners using the DiDb system, SECTRAN guarantees that it only allows the admission of applicants who comply with the conditions defined in DiDb.
In order to make sure that SECTRAN can prove that

- the validity of the Certificate of Good Conduct during the registration process has been examined

- on the basis of which data, it awarded the membership to the applicant during the membership management process

SECTRAN records the following data along with the data required for maintaining the DiDb membership with the same method of storage and storage deadline:

- date of issue, date of submission, issuing authority of the Certificate of Good Conduct
- registration number of CR
- request identifier of CR

According to the effective law, these data are not considered as sensitive personal data, as they are not criminal personal data.

Does SECTRAN store an electronic copy of the Certificate of Good Conduct?
It does not.

What happens to the applicant who is unable to submit a valid Certificate of Good Conduct in the course of the registration? May he/she be allowed to scan his/her valid Certificate of Good Conduct and send it to SECTRAN electronically?
If the driver is unable to present a Certificate of Good Conduct during the membership process, he/she can send it to SECTRAN afterwards.
SECTRAN does not make a digital copy of the certificate submitted and destroys it once the decision procedure is completed. The only exception to this is if the applicant also sends a stamped and addressed reply envelope together with the Certificate of Good Conduct - in this case, SECTRAN will return the Certificate in the stamped and addressed reply envelope to the indicated address.

A digital scan of a valid Certificate of Good Conduct as a supplementing document is not accepted by SECTRAN, as in this case no SECTRAN employee may be able to assess the visual and textual authenticity of the electronic copy, therefore it is not guaranteed that the electronic copy has not been modified until submission.

What measures are applied by SECTRAN for the security of the personal data controlled?

The regulations regarding data security can be found in No. 5 of this manual.

What are the data the applicant is not obliged to provide during his registration? If he changes his mind later, can such data be provided subsequently?
In order to facilitate keeping contact in the future and to decide on the driver's ability to carry out freight assignments which assume special transport qualifications, the driver may give the following information electronically during the registration process:

- certain types of contact data
- data for verification of professional competence for the fulfilment of transport assignment.

All these data can be given later, during the membership of the driver.
For more information on non-compulsory data, please check Appendix No. 4.

7.8. CONCLUSION OF LEGAL MEMBERSHIP

In case the driver successfully registers to the system, provides the mandatory data, and receives a positive evaluation by SECTRAN in accordance with this present document, a fixed legal relationship is established between SECTRAN and the driver on basis of the following terms:

- commencement of the legal relationship is the acceptance by SECTRAN of the Membership Declaration and Information on Data Controll filled out and signed by the driver;
- the legal relationship is established for a fixed term of two years;

– following the expiration of the fixed term, the driver may prolong his/her membership in accordance with the conditions under "Membership Validation".

7.9. AVOIDANCE OF DUPLICATION OF MEMBERSHIP

With the aim of avoiding the duplication of applications/registrations in the system as well as of avoiding the possibility for any abusement and misuse of personal data, the next procedures are applied by SECTRAN:

– A special HASH code is generated by using some personal data of the data subject given during the registration process. For the HASH code generation, a special math algorithm is used by SECTRAN. The code is unique and irreversible even if the algorithm generates the same HASH code by using the same personal data. It means that this code shall not be entitled as personal data and stored by SECTRAN in a separated database where no personal data may be linked to any person. Each newly generated HASH code will be compared to the existing ones. In case of matching, the system warns the applicants that the registration cannot be made and the application will be refused with the concerned personal data.

7.10. TERMINATION OF DIDB MEMBERSHIP

The legal relationship due to DiDb membership may be terminated prior to expiry:

– by mutual consent between SECTRAN and the driver, according to the specified therein;
– upon the termination of SECTRAN without a legal successor;
– upon the termination of the driver's capacity to act;
– upon the driver's death;
– upon termination by ordinary notice addressed to the other Party by either SECTRAN or the driver on the day of receipt;
– by termination with cause addressed by the other Party to the defaulting Party specifying the reasons for termination upon severe, repeated or willful misconduct, on the day of receipt.

7.11. DIDB MEMBERSHIP VALIDATION

Following the expiry of the two-year fixed term, membership may be prolonged in a membership renewal process due in every two years

- all the driver's data are updated, new data (previously unspecified "optional data") may be recorded. Data recording is performed as per specified in the registration process. Invalid or incorrect data are permanently deleted.
- the driver submits a new (not older than 96 days) Certificate of Good Conduct. The Certificate of Good Conduct is managed as per specified in the registration process.
- a new photograph is taken of the driver, which is uploaded to the DiDb system, while the old photograph is permanently deleted.

Should the driver fail to renew his/her membership within two years after the expiry date of the membership, all of his/her controlled personal data will be deleted from the DiDb system (following the rule of 2+2 years for time limit for data storage and controlling). The following data are excluded from erasure: date of DiDb registration, DiDb membership identifier, DiDb status, DiDb membership validity, DiDb qualifications (number of points and stars) and HASH code, which is not considered personal data. The driver's DiDb status will be changed to "Dormant" in the system and can be renewed only by recording all the obligatory personal data again (so called reactivation of the membership). Renewal of membership (so called reactivation) may only be possible by recording the personal data again.

7.12. DATA CONTROLLING DURING THE OPERATION OF DIDB SYSTEM

SECTRAN as data controller may access and control all data in the system.
The users of the DiDb system (operator of contracted clients) may access only the following data during the DiDb card checking procedure via a dedicated software application:

- status of DiDb card;
- validity of DiDb membership (valid/ invalid);
- in case of a valid membership:
  - DiDb status stored in the system (approved/suspended/rejected/banned);
  - DiDb card number;
  - date of DiDb registration;
  - expiry date of DiDb membership validity
  - DiDb qualification (number of points and stars)
  - transports fulfilled in last week;
  - qualifications and trainings of the driver (if data related to qualifications, trainings and courses (specifying the name of freight-related qualifications and courses, date of issuing and period of validity, name of issuing authority; specifying the name of freight-related trainings, type of training, date) were recorded during registration or membership renewal process.)
- the DiDb operator may identify the driver arriving for loading on basis of next data, and compare him/her with the person registered in the database on the basis of the documents handed over on the site before loading the cargo
  - name, place and date of birth, name of mother/father, expiry dates of ID, driving licence and passport;
  - high-definition photograph;

All above described data can be accessed by the operator only in case the driver consents to the identity check by putting at disposal his/her DiDb card and the belonging PIN code, known only by the driver.

7.13. DATA PROCESSING OPERATIONS PERFORMED BY THE USERS OF THE SYSTEM

Data processors of the DiDb system may perform the following operations in addition to and along with those specified in the previous section:

- prior to starting a delivery, the users of the DiDb system (operators) may **query**:
  - personal identification data,
  - data regarding professional qualifications to pick up and deliver cargo,
  - data regarding authorized eligibility to pick up and deliver cargo,
  - DiDb membership-related data.

- data related to the transport in question, concerning the vehicle and the consignment, as well as the categories of transport may be **recorded** by the users of the DiDb system

- in case of an extraordinary event in association with the fulfilment of delivery, those users of the DiDb system specified in prior agreement and authorized to investigate extraordinary events **may record, modify, and change** data regarding the extraordinary event and its investigation within their own scope of interest:
  - in the section containing data regarding extraordinary events in association with deliveries.

- if SECTRAN appoints a third party to complete registration process, the third party may, in the course of the registration process, **record**:
  - personal identification data,

- contact information data,
- financial data,
- data regarding professional qualifications to pick up and deliver cargo,
- data regarding authorized eligibility to pick up and deliver cargo,
- data regarding the certificate of good conduct

7.14. SPECIAL RULES FOR DATA CONTROLLING REGARDING EXTRAORDINARY EVENTS IN ASSOCIATION WITH DELIVERIES

If an extraordinary event (incident) occurs in association with the fulfilment of a delivery, any involved party (e.g. owner of the cargo, supplier, transporter, customer or appointed representatives of the above) may initiate the procedure concerning the extraordinary event. In this case, the person(s) specified in the user agreement of the DiDb-system and authorized to investigate extraordinary events shall enter data about the driver of the vehicle regarding the extraordinary event and its investigation within their own scope of interest.

7.14.1. LEGAL GROUND FOR DATA CONTROLLING

The legal ground for the controlling of such data is the legitimate interest of SECTRAN and its partners in accordance with Article 6 (1) f) of the GDPR: it is the basic concept of the DiDb system, that only drivers who comply with the conditions for membership continuously, and not only at the time of registration, may be members of the DiDb. Therefore, if as a result of the assessment of an extraordinary event, it is demonstrated that a driver is concerned, then SECTRAN may withdraw his DiDb membership. Detailed rules for the above are included in the Incident Management Rules which is available for applicants during the registration process and for members.

7.14.2. RESULT OF INVESTIGATION

If the investigation establishes that the driver concerned has not infringed the legitimate interests of SECTRAN or its partner, no breach of contract has occurred.

If during the investigation it is found that the driver has violated the legitimate interest of SECTRAN or its partner as specified in the Incident Management Rules, it shall be considered as material breach of contract. The extent of the material breach of contract is specified by SECTRAN in the Incident Management Rules, whereas legal consequences on the membership are detailed in Section 7.15.

SECTRAN is engaged to protect the privacy of data subjects, therefore, it includes the concerned driver in the assessment of the event in all cases. The driver is not obliged to cooperate with SECTRAN during the assessment of the extraordinary event, but it is considered as a material breach of contract which results in the termination of his/her membership and shall result in an indefinite ban based on clause 17.5.1.

7.14.3. RULES CONCERNING INVESTIGATION DOCUMENTATION

At the end of each investigation process, SECTRAN composes the entire documentation into a digital file and assigns a digital connection code to the digital file. The connection code is the name of the member, the date of the decision in YYYY-MM-DD format (eg, 2020-01-01) and the DiDb card number of the member. Apart from the digital file, SECTRAN will delete or destroy all documents available during the investigation.

SECTRAN is neither an investigation authority, nor a court, it may only make decision on the material breach of contract based on the data available at the time of assessment of the case. Since the material breach results in the

exclusion of the member from the DiDb system as specified in Section 7.15, SECTRAN keeps all data related to investigations according to which the case is considered as material breach of contract. This is explained by the fact that even court proceedings may be initiated against the individual decision of SECTRAN, and SECTRAN may only prove the validity of its decision in an individual court proceeding if the data available at the time of the decision are still available during the court proceeding.

SECTRAN has an undeniable legitimate interest in having access to data in the course of legal proceedings, SECTRAN therefore applies the following time limits and procedures for data controlling:

A) Result of the investigation: no breach of contract
The file will be kept by SECTRAN until the limitation period for claims for legal enforcement in connection with the decision – as it is specified in Act V of 2013, Article 6:22 of the Civil Code in force in Hungary. (1) - (2) – until the end of the fifth year from the date of the decision.

B) Result of investigation: definite exclusion referred to in chapter 7.15.1
In the case of a definite exclusion, the DiDb member may not regain its "approved" status in the DiDb system for the period of time specified in the decision, so the decision may have an effect on the driver until the end of the definite exclusion. Therefore, SECTRAN files the case - in accordance with the Act V of 2013, 6:22. (1) of the Civil Code in force in Hungary regulating claims for legal enforcement or remedy - until the end of the fifth year following the expiration of the exclusion.

C) Result of investigation: indefinite exclusion referred to in chapter 7.15.2
Considering that as a result of an indefinite exclusion, a member will never be able to regain his or her "approved" status in the DiDb system, the decision may have an impact on the driver at any time in the future.

However, according to SECTRAN's privacy point of view, it does not justify the possibility to store the file of all cases closed with a decision for exclusion based on chapter 7.15.2. without time limitation, as SECTRAN recognizes that not all of its individual decisions will be subject to legal remedy.
Data processing based on the possibility of an eventual legal proceeding which may conditionally occur would be data processing activity without an actual purpose, therefore, it would be unlawful.

However, given that SECTRAN's decision may be subject to a legal remedy risen by the data subject at any time, it is the legitimate interest of SECTRAN that the file should be available in any legal proceedings.

Therefore, SECTRAN applies the following solution:
C1) in each calendar year, SECTRAN saves the digital file of each case closed in accordance with section 7.15.2. on a password-protected digital medium.

C2) SECTRAN hands over the digital medium created in accordance with C1) to custody in accordance with Section 158 of Act XLI of 1991 on civil law notaries. In accordance with the Hungarian law, the law confers the status of public official on notaries so that they may provide parties with impartial legal services in order to prevent litigation, therefore, SECTRAN has selected custody by notaries to keep the documents.

C3) SECTRAN keeps a register on each digital medium and documents stored, it has handed over to the notary.
C4) In accordance with the rules on custody, the notary public shall keep the documents which may be taken over by SECTRAN from the notary public exclusively in the case of a legal proceeding and only for the purpose of enforcing legal claims.

7.15. MATERIAL BREACH OF CONTRACT – EXCLUSION OF A MEMBER FROM DIDB-SYSTEM

If a member is found to have behaved in a manner that endangers the purposes of the DiDb-system, has violated the legitimate interests of SECTRAN and / or its partners, the member's membership shall be terminated, and member shall be excluded.

7.15.1. DEFINITE OR INDEFINITE EXCLUSION

Depending on the severity of the breach of contract, the exclusion may be for a definite or an indefinite period. The detailed rules on which conduct results in what type and length of exclusion are included in the Incident Management Rules.

Exclusion for a definite period shall mean that SECTRAN excludes the member from the system for a definite period defined in years in accordance with its Incident Management Rules. In this case, the member may regain his/her approved status after expiry of the definite period.
It shall be considered as indefinite exclusion, if the conduct serving as a basis for exclusion is so serious that the member may not regain his/her membership in the system anymore, so the exclusion is final.

Considering that the DiDb is not an obligatory professional chamber, and anyone can work without being a member of the DiDb as driver, and DiDb is a system operated by not a public, but a private economic operator, therefore there is nothing to prevent SECTRAN to permanently exclude anyone who engages in a material breach from the persons who may use its services.

There are several examples to the above in Europe, such as:
– European football clubs may permanently exclude supporters from their stadiums who engage in a racist or otherwise violating activity,
– in certain countries, people who engaged in an activity beneath the standards of the building of the Parliament may be excluded from the building of the Parliament forever,
– European airlines may exclude passengers who cause any disturbances at their flights from their flights forever.

7.15.2. PROCESSING OF THE DATA OF EXCLUDED PERSONS

SECTRAN will delete any personal data that is not legally required to be retained after a member is excluded from DiDb.

However, in order to prevent a member from re-registering and also to not processing personal data, SECTRAN applies the method of HASH coding in accordance with section 7.9. The banned member's HASH code will be marked "excluded" by SECTRAN in order to prevent the excluded member from re-registering in the future. However, in order to protect the privacy of an excluded member, only a message will appear to the customer service administrator during the re-registration trial stating that this information does not allow re-registration to the DiDb database but does not provide information on the actual cause.

For a definite excluded member's HASH code, SECTRAN assigns the "excluded" flag until the end of the definite period, and after the expiration date, the "excluded" flag disappears from the HASH code, allowing the excluded member to re-register or validate.

An indefinite excluded member's HASH code will be assigned an "excluded" flag by SECTRAN without time limit, so the member will never be able to register again.

APPENDIX NO. 1

On the appointment of the data protection officer of SECTRAN

In order to ensure data subjects' rights, SECTRAN appointed a data protection officer,

whose name it reported to the supervisory authority in accordance with Article 37 (7) of the GDPR.

Data protection officer
– **name**: dr. Gábor Pataki LL.M, attorney specialized in data protection
- **contact details**: dataprotection@sectran.eu

APPENDIX NO. 2

Third parties involved in the data processing as data processors:

The list of DiDb users and SECTRAN partners may change continuously due to contractual freedom; in each case, during the given administration, we individually identify the third party and its authorization related to the operation of the DiDb system for the person concerned.

The current list of data processors can be viewed on the website www.didb.eu.

APPENDIX NO. 3

Citizens of the following countries are required to provide their father's name	Citizens of the following countries are required to provide their mother's name	Citizens of the following countries are not required to provide the name of their father or mother
Bulgaria	Hungary	Slovakia
Portugal	Poland	The Netherlands
	Portugal	Czech Republic
	Ukraine	Latvia
	Belarus	Lithuania
		Germany
		Croatia
		Italy
		Romania
		Spain
		France
		Belgium
		Austria
		Slovenia
		Estonia
		Turkey
		Cuba
		Macedonia
		Kenya
		Egypt
		Bosnia-Herzegovina
		Serbia

APPENDIX NO. 4

Table of processed data

Category of personal data	Named personal data	Is it obligatory[1]	Source of the data[2]			Legal grounds for data processing	Deadline for data processing[3]	Data subject's right which may be enforced[4]							
			DS	D	P			6.1.	6.2.	6.3.1.	6.3.2.	6.4.	6.5.	6.6.	6.7.
data for personal identification	name	yes	X			Article 6 (1) f)	g.r.	Y	Y	Y	X	Y	X	Y	Y
	birth name	yes	X			Article 6 (1) f)	g.r.	Y	Y	Y	X	Y	X	Y	Y
	place and date of birth	yes	X			Article 6 (1) f)	g.r.	Y	Y	Y	X	Y	X	Y	Y
	country of birth	yes	X			Article 6 (1) f)	g.r.	Y	Y	Y	X	Y	X	Y	Y
	citizenship	yes	X			Article 6 (1) f)	g.r.	Y	Y	Y	X	Y	X	Y	Y
	name of mother/father	See: Appendix No. 3	X			Article 6 (1) f)	g.r.	Y	Y	Y	X	Y	X	Y	Y
	high-definition photograph	yes (prepared at the place of registration)	X			Article 6 (1) f)	g.r.	Y	Y	Y	X	Y	X	Y	Y
contact data	home address	yes	X			Article 6 (1) f)	g.r.	Y	Y	Y	X	Y	X	Y	Y
	mail address	no	X			Article 6 (1) f)	g.r.	Y	Y	Y	Y	Y	X	Y	Y
	phone number(s)	yes	X			Article 6 (1) f)	g.r.	Y	Y	Y	X	Y	X	Y	Y
	e-mail address	no	X			Article 6 (1) f)	g.r.	Y	Y	Y	Y	Y	X	Y	Y
	language of communication	yes	X			Article 6 (1) f)	g.r.	Y	Y	Y	X	Y	X	Y	Y
	name, address, phone number and email address of the employer	no	X			Article 6 (1) f)	g.r.	Y	Y	Y	Y	Y	X	Y	Y
financial data	billing name and address	yes	X			Article 6 (1) c)	for 8 years after it is issued [Act on Accounting, Section 169 (2)]	Y	Y	Y	X	Y	X	X	Y
	name and address of the employer (if the membership fee is paid by the employer)	only if the membership fee is paid by the employer	X			Article 6 (1) c)		Y	Y	Y	X	Y	X	X	Y

data for verification of professional competence for the fulfilment of transport assignment	name of qualification(s) and training(s) connected to ground transportation	no	X			Article 6 (1) f)	g.r.	Y	Y	Y	Y	Y	X	Y	Y
	date of issue and expiry date of the qualification and training related to transport	no	X			Article 6 (1) f)	g.r.	Y	Y	Y	Y	Y	X	Y	Y
	name of authority issuing the certification about the qualification(s) and training(s)	no	X			Article 6 (1) f)	g.r.	Y	Y	Y	Y	Y	X	Y	Y
	information on the type of training (theoretical or practical or e-learning)	no	X			Article 6 (1) f)	g.r.	Y	Y	Y	Y	Y	X	Y	Y
	date of the training related to transportation	no	X			Article 6 (1) f)	g.r.	Y	Y	Y	Y	Y	X	Y	Y
data for verification of authorised eligibility for the fulfilment of transport assignment	nr. and expiry date of ID card	yes	X			Article 6 (1) f)	g.r.	Y	Y	Y	X	Y	X	Y	Y
	expiry date of medical certificate of driving licence	yes	X			Article 6 (1) f)	g.r.	Y	Y	Y	X	Y	X	Y	Y
	nr. and expiry date of passport	yes	X			Article 6 (1) f)	g.r.	Y	Y	Y	X	Y	X	Y	Y
data of Certificate of good conduct (CR)	issue date of CR	yes	X			Article 6 (1) f)	g.r.	Y	Y	Y	X	Y	X	Y	Y
	number of CR	yes	X			Article 6 (1) f)	g.r.	Y	Y	Y	X	Y	X	Y	Y
	request identifier of CR	yes	X			Article 6 (1) f)	g.r.	Y	Y	Y	X	Y	X	Y	Y
	issuing authority of CR	yes	X			Article 6 (1) f)	g.r.	Y	Y	Y	X	Y	X	Y	Y
data related to the transport assignment	data related to the truck, trailer and cargo	N.A.: *data are generated only if the data are recorded by the user of the DiDb system*		X		Article 6 (1) f)	g.r.	Y	Y	Y	X	Y	Y	Y	Y
	transport category (domestic/domestic high	N.A.: *data are*		X		Article 6 (1) f)	g.r.	Y	Y	Y	X	Y	Y	Y	Y

	value/international/international high value)	*generated during the transport starting depending on the selected category*													
data concerning complaints	all data included in the complaint submitted to SECTRAN, the source of which is the complainant, but their data subject can be other persons as well	N.A.*: data are generated only if complaints are submitted*	X	X	X	Article 6 (1) c)	until the end of the fifth year after assessment of the complaint [Act on Consumer Protection, Section 169 (2)]	Y	Y	Y	X	Y	X	X[5]	Y
data of an extraordinary event related to the fulfilment of a transport assignment	location, time, description, involved parties and documents (such as photos etc.) connected to the extraordinary event	N.A.: *data are generated only if an extraordinary event happens during the fulfilment of the transport*			X	Article 6 (1) f)	g.r.	Y	Y	Y	X	Y	Y	Y	Y
	data connected to the truck, trailer and cargo concerned to the extraordinary event				X	Article 6 (1) f)	g.r.	Y	Y	Y	X	Y	Y	Y	Y
data in association with DiDb membership	status of DiDb card	N.A. *data are generated after the registration and updated continuously during the membership*		X		Article 6 (1) f)	g.r.	Y	Y	Y	X	Y	Y	Y	Y
	status of DiDb membership validity			X		Article 6 (1) f)	g.r.	Y	Y	Y	X	Y	Y	Y	Y
	DiDb status stored in the system			X		Article 6 (1) f)	g.r.	Y	Y	Y	X	Y	Y	Y	Y
	DiDb card and DiDb membership number			X		Article 6 (1) f)	g.r.	Y	Y	Y	X	Y	Y	Y	Y
	DiDb qualifications			X		Article 6 (1) f)	g.r.	Y	Y	Y	X	Y	Y	Y	Y
	date of DiDb registration and expiry date of DiDb membership			X		Article 6 (1) f)	g.r.	Y	Y	Y	X	Y	Y	Y	Y

	transports fulfilled last week			X		Article 6 (1) f)	g.r.	Y	Y	Y	X	Y	Y	Y	Y

[1]***Is it obligatory to provide:***
yes: the data subject is obliged to provide the data at the time of registration, otherwise the contract cannot be concluded between SECTRAN and the data subject
no: for such data, the data subject may freely decide whether he wishes to provide them for SECTRAN
N.A.: not applicable, that is, data are not provided by the data subject, after the colon, explanation concerning generation of the data

[2]***In case of the source of data:***
DS: the source of data is the data subject himself; data are provided to SECTRAN by the data subject
D: the source of data is the DiDb system, the data are generated during use of the system
P: the source of data is a third party, the contracted partner of SECTRAN, SECTRAN received the data from them

[3]***Deadline for data processing:***
g.r: as a general rule, that is, until the data processing deadline specified in Section 7.4

[4]***Data subject's right which may be enforced:***
Whether the data subject may exercise the data subject's right detailed in the specified section of the Manual concerning the data in question.

[5]***Right which may be enforced separately during complaint management:***
Although the data subject is not entitled to the right to data portability, but if the data subject is the complainant, then SECTRAN shall hand him over one copy of the minutes recorded on the complaint in accordance with Section 17/A (3) of the Act on Consumer Protection.