Data controller of 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

Description of Data Control in the DiDb System (handbook)

in effect from 1st Febr, 2019 until revocation

Content

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

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

1. The purpose and scope of effect of the Handbook

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]*, 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 controlling and 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 Handbook 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.

In regards 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.

2. Terms

The terms and their definitions used in this Manual are the same as those defined in Article 4 of the GDPR, but to improve readability of the Manual, the most important terms are included below:

- ***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 regards 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 regards 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 that the data controller will not or cannot perform due to economic, professional, or any other reason is considered data processor. By default, the data controller is responsible for the activities of the data processor; the activities of the data processor follow legislations only if the complete description of such activities is specified in a contract. There is no legal relationship between the data subject and the data processor involving the processing of data.
- ***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, SECTRAN may only control data during its proceedings on the basis of effective legal regulations, especially:

SECTRAN shall control personal data only as specified in Article 6 of the GDPR, and shall control special categories of personal data only in accordance with the provisions in Article 9 (2) of the GDPR, for the purposes of exercising its rights or performing its obligations.

Rights and obligations associated with any particular data controlling activity may arise on part of SECTRAN, the data subject, or a third party.

Any personal data that SECTRAN controls shall remain personal data in the course of data controlling as long as it does, or can be used to, identify the data subject. 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.

SECTRAN shall pursue data controlling activities only if every stage of the controlling process is in line with its purpose.

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.

Every organisational unit leader is responsible for the keeping of the rules prescribed in the Handbook.

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 an annual report on the execution of SECTRAN data protection tasks for the CEO until January 15;
c) monitoring the observance of the present Handbook 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 Handbook;
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 network servers (hereinafter: servers) may only be accessed with the necessary permissions and by appointed personnel;
- 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;
- the servers for data storage are kept in separate air-conditioned computer rooms with excellent infrastructure, continuous network monitoring, IP consoles and fire-extinguishers to ensure high availability. As a result of this so-called HA environment, data loss and fatal shutdowns can be avoided.
- the active data of databases of personal data are periodically saved; the scope of the save is the central server's entire data set and is performed onto a magnetic data storage media;
- the magnetic data storage media are kept in a fire-proof safe;
- 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 subjects request information communicated orally, then authorised representatives of SECTRAN can comply with this request once the data subjects identify themselves.

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

The identity of data subjects is considered verified if:

- the data subjects provide 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 subjects provide proof of identification to authorised SECTRAN employee as specified in legislations of the EU,
- the request of the data subjects is known from earlier contacts made, arrives from an email address associated with the data subjects,
- 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 subjects may not initiate asserting their rights specified in Article 6 on the phone.

If the identity of the data subjects is not verified, SECTRAN shall decline any request to assert rights in regards to data processing.

In case of a request regarding the data subjects' 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 subjects disclose their request in person to the authorised employee of SECTRAN who will verify the subjects' 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 subjects 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 subjects, then the data subjects may exercise their right to appeal as specified in Article 6.7.

SECTRAN shall provide information and take measures in connection with the rights of the data subjects 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.

6.1Informing 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 over the telephone 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

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.
- SECTRAN is advised that the processing of such personal data does not follow legislations.

SECTRAN shall erase personal data so that their recovery would never be possible.

If the personal data cannot be deleted from the data storage medium that stores such personal data, SECTRAN shall physically destroy such medium.

6.4 The right of data subjects to require restriction of data controlling

The data subjects 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 subjects, SECTRAN shall restrict data controlling if one of the following conditions exists:

- the request of the data subjects 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 subjects object to the erasure of their data, instead, they request 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 subjects request 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 do not have this right, because data processing as specified in Article 7 below is not based on Paragraph e) or f) of Article 6 of the GDPR.

6.6 Exercising the data subjects' right to data portability

Since Article 6 (1) b) of the GDPR provides the legal grounds to data processing in the form of a contractual relationship, the data subjects have the right to receive any of their 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 subjects may further request SECTRAN to transfer their personal data, if this is technically feasible, to another data controller clearly identified by the data subjects.

6.7 Legal remedies

In accordance with Paragraph (1), Article 77 of the GDPR, the data subjects 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 subjects 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 subjects. Since SECTRAN obtains such personal data directly from the data subjects – excluded those data, which are connected to the fulfilment of the transport assignments and those ones, which are connected to extraordinary events during the fulfilment of transport assignments - SECTRAN shall disclose the following information to the data subjects as required by Article 13 of the GDPR:

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

The identity and contact details of the data controller's representative: see the opening provisions of this Manual.

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

Any third party involved in the data processing as data processors: the names and contact details are provided in Appendix 2, along with a description of their activities as data processors**.**

Purpose of processing personal data: operation the DiDb system

Legal grounds for processing personal data: registration in the DiDb database establishes a contract between SECTRAN and the data subject; in accordance with Article 6 (1) b) of the GDPR, fulfilment of such contract provides the necessary legal grounds: when the data subject and SECTRAN enter into a contractual relationship, SECTRAN becomes liable to provide services for the data subject and the controlled personal data are necessary to fulfil obligations set forth in such contract.

SECTRAN hereby informs the data subjects that they must provide the personal data and all contact details necessary to comply with this contract as specified in the Manual, since the provision of personal data is a prerequisite to entering into the contractual relationship as described in this Manual. If such personal data is not provided to SECTRAN, the contractual relationship does not exist.

Time limit of data storage of personal data:

- for applicants whose application for registration has been refused, the time limit for data storage is 30 days, as described in the process description
- for members whose application for registration has been approved the time limit for data storage is 2+2 years, as described in the process description and also in Chapter 7.7. (DiDb membership validation)

Location for data controlling: head office of SECTRAN

7.1 Categories of controlled personal data in DiDb system

Category of personal data	Named personal data
data for personal identification	– name – birth name – place, country and date of birth – citizenship – name of mother/father – high res. photo
contact data	– home address – postal address – phone number(s)

	– e-mail address – native language – spoken language(s) – name, address, phone number and email address of the driver's employer
financial data	– invoicing name and address – name and address of employer (in case employer pays for membership fee)
data for verification of professional competence for the fulfilment of transport assignment	– name of qualifications and trainings connected to ground transportation – date of issue and expiry date of the above qualifications and trainings – name of authority issuing the certification about the qualifications – information on the type of training (theoretical or practical or e-learning) – date of the training or qualification when it was executed by the driver
data for verification of authorized eligibility for the fulfilment of transport assignment	– expiry date of ID card – expiry date of medical certificate of driving license – expiry date of passport
data for Certificate of good conduct (CR)	– issue date of CR – registration number of CR – request identifier of CR – issuing authority of CR
data connected to Naturalization Certificate (only in case of owing dual membership)	– name – birth name – place of birth – date of birth – issue date of certificate
	– registration number of certificate – issuing authority of certificate
data connected to the fulfilment of transport assignment	– data related with the truck, trailer and cargo – transport category (domestic/domestic high value/international/international high value) queried by the operator of the system
data connected to extraordinary event during the fulfilment of transport assignments	– location, time, description, involved parties and documents (such as photos etc.) connected to the extraordinary event – data related to the truck, trailer and cargo involved in the extraordinary event
data connected to DiDb membership	– status of DiDb card (valid/deleted) – status of DiDb membership validity (valid/ valid but with expired personal docs/invalid) – DiDb status recorded in the system (approved/suspended) – DiDb card number (membership identifier) – DiDb qualification (number of points and stars) – date of DiDb registration – expiry date of DiDb membership – transports fulfilled in last week

7.2 Detailed description of data controlling in DiDb system

The main purpose of DiDb system is to reduce the driver related risks and losses in ground transportation. DiDb is a shared white list of checked and qualified truck drivers, consisting of those previously registered drivers who – on the 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.

Without exception, registration is carried out personally in one of SECTRAN's customer service offices or dedicated registration points – during the assessment the applicants go through a process of adequacy on the basis of

the data they provided. Should registration be successful, the driver will be included in the database and can prove his/her membership to companies using the DiDb system with a personal DiDb card.

During registration, the following data groups can be communicated to SECTRAN by data subjects:

- ***obligatory data:*** data in this group are required to communicate for the assessment of the application and obtaining 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.

7.3 Data controlling in the course of registration process

7.3.1. REGISTRATION – obligatory data

In order to start the assessment process of the driver membership application, during registration the applicants must submit the following obligatory data:

Category of personal data	Named personal data	Obligatory data
data for personal identification	name	yes
	given name	yes
	place, country and date of birth	yes
	citizenship	yes
	name of mother/father	as per Appendix 3
	high res. photo	taken on spot
contact data	home address	yes
	postal address	no
	phone number(s)	yes
	e-mail address	no
	native language	yes
	spoken language(s)	no
	name, address, phone number and email address of the employer	no
financial data	billing name and address	yes
	name and address of the employer (if the membership fee is paid by the employer)	yes (if the membership fee is paid by the employer)
data for verification of professional competence for the fulfilment of transport assignment	name of qualification(s) and training(s) related to ground transportation	none of them is obligatory
	date of issue and expiry date of the qualification and training	
	name of authority issuing the certification about the qualification	
	information on the type of training (theoretical or practical or e-learning)	
	date of the training or qualification when it was executed by the member	
data for verification of authorised eligibility for the	expiry date of ID card	each data is obligatory
	expiry date of medical certificate of driving licence	

fulfilment of tranport assignment	expiry date of passport	
data of Certificate of good conduct (CR)	issue date of CR	yes
	registration number of CR	no
	request identifier of CR	yes
	issuing authority of CR	yes
data of Naturalization Certification (in case of owing dual citizenship)	data for identification (name, birth name, place and date of birth, home address)	yes
	issue date of certification	yes
	registration number of certificate	no
	issuing authority of certificate	no
data related to the transport assignment	data related to the truck, trailer and cargo	data are generated only if the data are recorded by the operator
	transport category (domestic/domestic high value/international/international high value)	data are generated during the transport starting, chosen by the operator in the app
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	data are generated only if an extraordinary event happens during the fulfilment of the transport
	data connected to the truck, trailer and cargo concerned to the extraordinary event	
data in association with DiDb	status of DiDb card (valid/deleted)	data are generated after the
membership	status of DiDb membership validity (valid/valid with expired personal docs/invalid)	registration and updated continuously during the membership
	DiDb status recorded in DiDb system (approved/suspended)	
	DiDb card number (membership identifier)	
	DiDb qualifications (no. of points and stars)	
	date of DiDb registration	
	expiry date of DiDb membership validity	
	transports fulfilled in last week	

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.

These information are crucial for the determination of certain routes.

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 indicate their father's name and not their mother's name; and there are other countries where none or both parent's name shall be indicated. 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 in Appendix 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 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 User's Manual", which can be found on www.didb.eu.)

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.
One of the conditions 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 submit 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 the 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 director of the Registration Department examines the Certificates':

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

How does SECTRAN handle the information included in the Certificate of Good Conduct?
SECTRAN may only control criminal personal data with the written consent of the data subject. Prior to control being initiated, SECTRAN informs the data subject that the objective of the control of personal data is to decide whether the applicant is worthy of the DiDb membership, so the data is only controlled until this purpose is achieved i.e. until the decision is made.

SECTRAN specifies clean criminal record as a condition of membership. In certain cases, however, the CEO of SECTRAN in his/her private authority and on the basis of his/her individual judgement may decide to accept a member even if the Certificate of Good Conduct contains a record which:

- depending on the type and severity of the act is not incompatible with the principles of DiDb;
- is in the relief period;
- is close to the relief period;
- for other reasons does not endanger the purposes and principles of DiDb.

Who can access the personal data on the Certificate of Good Conduct?

The registration process is always carried out in one of SECTRAN's customer services or dedicated registration points. All data are recorded by a SECTRAN employee or contracted partner and forwarded to the authorised decision-makers. In every case the assessment of membership applications falls into the sphere of authority of the manager of the SECTRAN's Registration Department. Data submitted during registration can only be disclosed to the employee working at the registration point assisting in the registration process, the employees of the Registration Department and the CEO of SECTRAN.

No other person may have any access to the data, including any other employee of SECTRAN or person in a legal relationship with the company.

Due to the fact that during the registration process SECTRAN pays special attention on ensuring that the personal data of those concerned may only be accessed within the narrowest possible limits, SECTRAN manages the Certificate of Good Conduct submitted on the basis of the following principles and processes:

- SECTRAN is aware that the Certificate of Good Conduct may be submitted to more than one administrative process, which is why SECTRAN – in order to allow its applicants to use their Certificates of Good Conduct for purposes outside of the registration to DiDb – does not restrict the privacy of the persons concerned by taking away their Certificate of Good Conduct.
- in order to allow the manager of the Registration Department to decide whether or not the applicant complies with DiDb membership requirements specified by SECTRAN, the customer service employee makes an electronic copy of the Certificate of Good Conduct.

What happens to the scan of the Certificate of Good Conduct and the data therein?

The customer service employee makes an electronic copy of the applicant's Certificate of Good Conduct with a dedicated image scanning device, provided at every customer service or dedicated registration point operated by SECTRAN. The visual and textual authenticity of the electronic copy (i.e. whether the copy indeed contains the same data as the paper-based document) is determined by the customer service employee. The dedicated image scanning device encrypts the electronic copy with a key only known to the manager of the Registration Department, which means the contents of the electronic copy – i.e. the Certificate of Good Conduct – may only be accessed by that person. Should the manager of the Registration Department make a decision on the registration within the scope of his/her own authority, the contents of the Certificate of Good Conduct are not to be disclosed to any other person. The manager of the Registration Department may only disclose the contents of the electronic copy of the Certificate of Good Conduct to the CEO should the document contain a record which requires a managerial decision.

Does SECTRAN store any data in connection with the Certificate of Good Conduct?

On the 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

- it examines the validity of the Certificate of Good Conduct during the registration process;
- on the basis of which data it awarded the membership to the applicant during the registration 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 and issuing authority of the Certificate of Good Conduct;
- registration number of the Certificate of Good Conduct;
- request identification number of the Certificate of Good Conduct;

According to the effecive law, these data are not considered as special data, as they are not criminal personal data.

Does SECTRAN store an electronic copy of the Certificate of Good Conduct?
It does not. Once the decision has been made regarding membership, SECTRAN irrevocably deletes the electronic copy without the possibility to restore any data.

Why is it required to submit a Naturalization Certification in case of owing a dual citizenship?
The framework decisions (2009/315/JHA and 2009/316/JHA) of the European Council provides guidance for the policy of information exchanging process of criminal records between the Member States of the EU. Based on these framework decisions, all Member States are obliged to report all convictions and decisions made by their own juries to the competent judicial Authority, which is equal to the Authority where the person was born (being the primary citizenship of the driver). By following the above direction, SECTRAN can accept for applications submitted by the driver only a criminal record which has been issued by the judicial Authority matching with the driver's primary citizenship. Exception may be made only in case of having a dual membership by the driver. In this case a certificate of good conduct can be accepted issued by both judicial Authorities. For the verification of having dual citizenship, SECTRAN prescribes for the drivers to submit a Naturalization Certification. The certificate shall be submitted to the administrator only once – when applying for registration or membership validation. All data controlling processes connected to the data being on the Naturalization Certificate are equal to the processes connected to data being on the Certificate of Good Conduct, and all deadlines for data controlling are the same as well.

What happens to the candidate 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?
Should the driver be unable to submit a Certificate of Good Conduct on the site, he/she may send it to SECTRAN by post as a supplementing document. In such cases the decision on membership is made by the manager of the Registration Department within 30 days after registration. SECTRAN does not make a digital copy of Certificates of Good Conduct submitted as supplementing documents; it destroys the Certificate of Good Conduct following the decision-making process. An exception may be made if the applicant sends the Certificate of Good Conduct along with a stamped and addressed return envelope – in such cases SECTRAN returns the Certificate of Good Conduct in said envelope to the address specified.

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, that is, 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 forms and documents required for registration are digitized; SECTRAN's rules for digitally stored documents become applicable to ensure the safety of digital documents and electronic copies;
- the documents required for registration are kept in a locked and dry room equipped with a fire- and property protection device;
- documents being actively controlled may only be accessed by authorized personnel (Registration Department, managing directors);

The manager of the Registration Department is obliged to make a decision on the basis of the electronic copy within 30 days after registration.
Following the decision on registration, SECTRAN does not control any special personal data.

7.3.2. REGISTRATION – optional data

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:

Category of personal data	Named personal data	Optional data
contact data	spoken language(s)	yes
	email address	yes

	postal address	yes
	name, address, phone number and email address of the employer	yes
data for verification of professional competence for the fulfilment of transport assignment	name of qualification(s) and training(s) connected to ground transportation	all of them can be given optionally
	date of issue and expiry date of the qualification and training	
	name of authority issuing the certification about the qualification	
	information on the type of training (theoretical or practical or e-learning)	
	date of the training or qualification when it was executed by the driver	

All of these data can be given later, during the membership of the driver.

7.4 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, 2-year term legal relationship is established between SECTRAN and the driver on the basis of the following terms:

- the commencement of the legal relationship is the acceptance of the Terms and Conditions of Registration by SECTRAN;
- 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".

7.5 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 any 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.

7.6 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 terms and conditions 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.

7.7 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), excluded: date of DiDb registration, DiDb membership identifier, DiDb status, DiDb membership validity, status of DiDb card, DiDb qualifications (number of points and stars) and HASH code. 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).

7.8 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 (valid/deleted);
- validity of DiDb membership (valid/valid but with expired personal documents/invalid);
- in the case of a valid membership:
  - DiDb status stored in the system (approved/suspended);
  - DiDb card number (DiDb membership identifier);
  - date of DiDb registration;
  - expiry date of DiDb membership validity
  - 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 the 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.

7.9 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 (those managing clients) 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

- 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
  - data regarding the naturalization certificate

7.10 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. Since the source of this data is not the data subject, SECTRAN shall, to comply with Article 14 of the GDPR, notify the data subject in registered mail of all information recorded about the data subject in regards to the extraordinary event, as specified in Article 14, Paragraphs (1) and (2). Any data already known by the data subject is exempt from this notification.