Personal data privacy policy

Version:	1.1
Version dated:	18/05/2018
Created by:	Bruce GARNIER
Approved by:	Philippe GANGNEUX , Olivier NOVASQUE
Level of confidentiality:	Public

Modification history

Date	Version	Created by	Modification description
18/05/2018	0.1	Bruce GARNIER	Creation
08/03/2018	0.9	Bruce GARNIER	Minor changes and translation
10/05/2018	1.0	Olivier NOVASQUE	Comments
10/05/2018	1.1	Olivier NOVASQUE	Validation

Table of contents

I. CONTEXT 4

I.1 AIMS 4
I.2 SCOPE 4
I.3 EXEMPTIONS 4
I.4 DOCUMENTARY MONITORING 5

II. GOVERNANCE AND RESPONSIBILITIES OF STAKEHOLDERS 5

II.1 GENERAL MANAGEMENT AND EXCOM 5
II.2 ROLES AND RESPONSIBILITIES OF THE DATA PROTECTION OFFICER (DPO) 5
II.3 ROLES AND RESPONSIBILITIES OF THE OPERATIONAL TEAMS (OPERATIONS AND IT) 6
II.4 OPERATIONS AND COUNTRY PRIVACY OFFICERS 6
II.5 INFORMATION SYSTEMS DEPARTMENT 7
II.6 LEGAL DEPARTMENT 7
II.7 PROTECTION OF PRIVACY COMMITTEE 7

III. PRINCIPLES OF PROTECTION OF PRIVACY 8

III.1 DEFINITIONS 8
III.2 PRINCIPLES OF PROTECTION OF PRIVACY (PRINCIPLE OF ACCOUNTABILITY) 8

IV. PROTECTION OF PRIVACY RULES (ACCOUNTABILITY RULES) 9

IV.1 GOVERNANCE OF DATA PROTECTION 10
IV.1.1 Organisation 10
IV.1.2 Processing liability 10
IV.1.3 Relations with the supervisory authority 11
IV.2 PROCESSING SECURITY 11
IV.3 DATA LIFE-CYCLE 12
IV.3.1 Prior information 12
IV.3.2 Management of data collection 12
IV.3.3 Management of exercise of rights 14
IV.3.4 Retention period management 15
IV.4 MANAGEMENT OF PRIVACY IN PROJECTS 15
IV.4.1 Data minimisation 15
IV.4.2 Access management 15
IV.4.3 Privacy by Design/by Default & DPIA 15
IV.5 MANAGEMENT OF RELATIONS WITH THIRD PARTIES AND/OR SUBCONTRACTORS 16
IV.6 MANAGEMENT OF PERSONAL DATA TRANSFERS (SIDETRADE INTERNAL AND OUTSIDE THE EU) 17
IV.7 PERSONAL DATA BREACH MANAGEMENT 17
IV.8 TRAINING/AWARENESS 18

I. Context

In accordance with the General Data Protection Regulation (GDPR), Sidetrade is committed to respect the principles of protection of data subjects (users, staff, third parties, etc…) personal data collected and used for the purpose of their activity.

I.1 Aims

This personal data protection policy defines the guiding principles to be put in place at Sidetrade, particularly regarding the requirements of the EU General Data Protection Regulation (GDPR).

Those guiding principles will enable the establishment of necessary and appropriate procedures to Sidetrade's context to meet the following requirements:

- Define a framework of requirements in terms of data protection to meet Sidetrade's commitments
- Notify the organisation, staff and contract workers (full-time/part-time employees, contractors, internal teams, temps and other persons engaged by Sidetrade), unless this breaches local regulations in force in the context of the organisation
- Supporting ongoing business operations to meet appropriate data protection standards
- Complying with applicable regulations such as the GDPR and other national laws

I.2 Scope

All Sidetrade's subsidiaries in France and internationally are required to comply with this policy and to process personal data in accordance with the GDPR and/or applicable regulations according to the principles described in this document.

This policy is issued to all Sidetrade staff. The location of the reference version is specified in appendices.

Certain principles of the policy also apply to third parties in relations with Sidetrade. This information is specified in a chapter included for this purpose.

I.3 Exemptions

Any exemption of this policy must be documented and justified by the person requesting it, and formally approved by Sidetrade's Data Protection Officer (DPO).

In particular, if certain provisions breach local laws or regulations in force, an exemption may be made and additional rules may replace them to maintain an appropriate level of protection of personal data.

I.4 Documentary monitoring

The personal data protection policy is reviewed at least every year by Sidetrade's Data Protection Officer, particularly in case of legislative changes with a potential impact on management of personal data.

Before publication, this policy must be approved by the legal department.

Whenever the document is updated, this policy is issued to all Sidetrade subsidiaries.

II. Governance and responsibilities of stakeholders

This policy is implemented Sidetrade-wide. The subsidiaries for each Country may choose to implement this policy directly or otherwise to adapt it, on condition that the local policy remains in line with the principles described in the Sidetrade main policy.

The stakeholders described below represent the compliance system

II.1 General Management and EXCOM

General Management is responsible for implementation of and compliance with this policy and compliance with the applicable regulatory requirements.

They ensure that sufficient resources are available to achieve and maintain Sidetrade's compliance, at each of the relevant subsidiaries.

Also, in order to ensure the consistency and monitoring of the compliance system's implementation and maintenance actions, General Management must have visibility on the actions taken and their monitoring. This visibility is provided by the DPO (see description below)

The DPO makes an annual presentation to the Group Executive Committee to:

- Approve the budget allocated to data protection
- Present the key issues identified in terms of data protection and Sidetrade's progress on those issues
- Share their review of the past year: key events, areas requiring attention and trade-off requirements.

In particular, the DPO informs General Management of all developments (organisational, regulatory, etc.) likely to have an impact on data protection.

II.2 Roles and responsibilities of the Data Protection Officer (DPO)

The "Data Protection Officer" or DPO is in charge of controlling and monitoring the development of the implementation of Sidetrade's personal data policy.

He promotes the transfer of knowledge between local subsidiaries to improve Sidetrade's compliance programme and promotes a consistent approach with the programme's objectives, all while fulfilling Sidetrade's specific legal requirements.

The DPO is the point of contact with the supervisory authorities in terms of personal data protection. He is in charge of liaising and cooperating with the supervisory authorities if necessary.

Their duties are as follows:

- Putting in place and coordinating data protection governance
- Informing, advising and assisting
- Representing, consulting and cooperating
- Coordinating and steering programmes and projects related to protection of the data privacy
- Assessing, controlling and recommending
- Managing personal data protection watch

Additional information on all the DPO's duties is available in the DPO job description.

II.3 Roles and responsibilities of the operational teams (operations and IT)

The operational departments are responsible, within the scope of their activity, for compliance with regulations in force and with this policy.

In particular, they are responsible, within their scope of activity, for:

- Identification and keeping of personal data processing documents and their respective scope
- Integration of the principles of protection of privacy by design and by default in their activities and particularly in the development of their projects
- Conducting personal data processing privacy impact assessments if necessary
- Forwarding rights requests from data subjects to the relevant teams
- Alerting the DPO as early as possible in case of suspected breach of personal data

Accordingly, they can request the opinion of and advice from the DPO in the achievement of these duties.

II.4 Operations and Country privacy officers

At least one privacy officer is appointed for each of Sidetrade group's European subsidiaries. If an officer is not formally appointed, the subsidiary manager takes on this role.

The privacy officer is in charge within their scope, of:

- Locally adapting if necessary the principles and rules of protection of privacy, in coordinated fashion with the DPO.
- Checking the proper set up or implementation of Sidetrade group protection of privacy rules or their local adaptation

- Appointing a local representative for issues related to protection of privacy and compliance with the GDPR

II.5 Information Systems Department

The Information Systems Department has a role supporting the Data Protection Officer, particularly in connection with their IT expertise and in particular, their knowledge of Sidetrade's information systems security.

It is a key stakeholder in the GDPR compliance project in view of the personal data protection measures relating to information systems security. It will play an essential role particularly for issues of management of personal data retention, compliance with the rights of data subjects, privacy impact assessments, as well as technical and operational measures for the protection and securing of personal data.

II.6 Legal Department

The Legal Department has a role regarding Data Protection, particularly in connection with its IT Department and particularly its knowledge of the GDPR and other regulations specific to Sidetrade's activity.

It plays an essential role particularly for issues of third-party management (i.e.: subcontractor, customers, etc.) and related contract reviews, legal bases and consent management, but also staff contract aspects. If there is no legal department, third-party management aspects will be managed by the administrative and financial department, staff and applicant issues by the human resources department, and customer prospecting issues by the communication department.

II.7 Protection of privacy committee

This committee is dedicated to the monitoring and operational implementation of protection of privacy. It meets at least once per half-year and is comprised of the following persons:

- The Chief Executive Officer (chair of the committee)
- The Data Protection Officer
- The Chief Legal Officer or the appointed representatives
- The Operations and Country privacy officers

The purpose of this committee is to:

- Present and monitor the main GDPR compliance indicators at organisational, Operational and Country level.
- Determine and prioritise the key issues in terms of data protection
- Report information on protection of privacy issues encountered at Sidetrade (monitoring audits, data breaches, complaints from data subjects, etc.).

III. Principles of protection of privacy

III.1 Definitions

For the purposes of this policy, the following definitions apply:

- "Personal data" means any information relating to an identified or identifiable natural person (hereinafter referred to as "data subject"); an "identifiable natural person" is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; "Special categories of personal data" means any personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation

- "Data Subject" means the natural person who is the subject of the "Personal Data" and is identified or identifiable, directly or indirectly

- "Subcontractor or Third Party" (Data Processor) means a natural or legal person, public authority, agency or other body **which processes personal data** on behalf of the data controller
- "Data Controller" means legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing. When two or more data controllers jointly determine the purposes and means of the processing, they are called "joint data controllers"

- "Processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

- "Recipient" means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients. The processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing

- "Privacy by design/by default", the fact of guaranteeing the protection of the personal data processed by default and before the design of new services/processing/products.

III.2 Principles of protection of privacy (Principle of accountability)

Accountability means the obligation for companies to implement internal mechanisms and procedures enabling demonstration of compliance with data protection rules. More precisely, Sidetrade must meet the following requirements:

- Taking account of the type, scope, context and purposes of the processing as well as the risks [...] for rights and freedoms of natural persons, the data controller implements appropriate technical and organisational measures to ensure and be able to demonstrate that the processing is performed in accordance with this regulation. These measures are re-examined and updated if necessary.

- When this is proportional to the processing activities, the measures mentioned in the previous point include implementation of appropriate data protection policies by the data controller.

- The implementation of an approved code of conduct [...] can serve as evidence to demonstrate compliance with obligations incumbent upon the data controller.

The following principles of protection of personal data must be complied with and Sidetrade must be able to provide evidence of compliance therewith:

- **Liability:** For all processing of personal data, Sidetrade may be formally identified as data controller. If not, the CEO or CTO of the subsidiary is considered as data controller. The staff member is responsible for compliance with the personal data protection policy for the processing that they are in charge of. They are able to demonstrate that it is complied with
- **Lawfulness, loyalty and transparency**: personal data is processed lawfully, loyally and transparently with regard to the data subject
- **Determined purposes**: Personal data is collected only to carry out operations whose purposes/objectives are determined
- **Integrity and confidentiality**: personal data is processed in a manner guaranteeing their security using appropriate technical or organisational measures
- **Accuracy**: personal data remains accurate and, if necessary, updated;
- **Data minimisation**: the personal data collected, stored, exchanged and handled is systematically limited to appropriate, relevant data and restricted to what is necessary with regard to the purposes for which it is processed;
- **Limited retention**: personal data is not retained for longer than necessary to achieve the purposes of the processing for which the data is processed

Protection of privacy rules are established based on these principles (accountability rules)

IV. Protection of privacy rules (accountability rules)

In order to meet commitments regarding the principles of data protection, the following rules are defined.

They are particularly intended to guarantee Sidetrade's ability to provide evidence of its proper compliance with the Regulation.

The rules set out in this policy constitute minimum required practice.

The DPO checks that this policy is implemented appropriately at Sidetrade, under the supervision of General Management. The implementation of this policy is jointly managed and supervised with any local compliance system.

IV.1 Governance of data protection

IV.1.1 Organisation

Sidetrade's subsidiaries put in place clear procedures to guarantee compliance with the principles and rules of this policy. They guarantee their compliance via appropriate monitoring procedures.

Each Sidetrade subsidiary is responsible for performing an annual analysis of instances of non-compliance with the personal data protection policy, and forwarding to the Data Protection Officer, accompanied by the action plan drawn up to resolve the instances of non-compliance observed.

IV.1.2 Processing liability

In order to understand and comply with regulatory requirements on personal data protection, it is essential to identify Sidetrade's position regarding processing of personal data.

There are three positions at Sidetrade depending on the processing:

- Data controller
- Joint data controller
- Subcontractor

Reminder - the subcontractor is subject to the following requirements:

- Taking account of the type of processing, the subcontractor must assist the data controller, insofar as possible, in connection with the obligation to respond to rights of data subjects, particularly with appropriate technical and organisational measures.
- Helping the data controller to guarantee compliance with the obligations relating to personal data security (taking account of the type of processing and information made available to the data controller)
- Making available to the data controller any information required to demonstrate its compliance with the GDPR, enabling and contributing to the monitoring obligation to which the data controller is subject, including in case of inspections performed by the data controller or another auditor appointed by the data controller.

IV.1.3 Relations with the supervisory authority

The DPO is in charge of Sidetrade's relations with the supervisory authorities (CNIL - French Data Protection Authority - in France), in cooperation with the Communications Department.

The DPO is informed of any contact from a supervisory authority.

Sidetrade cooperates with the supervisory authorities. This cooperation involves several actions:

- Reporting to the supervisory authority in case of data breach, in accordance with the provisions of the personal data breach management procedure.
- Making available any documents providing evidence of taking of the compliance measures requested by the authority, coordinated by the DPO.

IV.2 Processing security

Sidetrade guarantees an appropriate level of personal data processing security.

The processing activities have a level of security appropriate to the risks to which they are likely to expose the data subjects.

This personal data must be protected at least like all the other data processed or retained by Sidetrade entities and in accordance with this policy.

To do so, technical monitoring measures must be put in place. These measures approved by risk management must enable (for example):

- **Access control**: makes it possible to prevent unauthorised persons from accessing systems where personal data is stored, for processing purposes or use of the customer's personal data;
- **Access control**: Persons authorised to use a data processing system have access only to personal data that they are authorised to access, and personal data **cannot be read, copied, altered or removed without authorisation** during processing, use and after recording;
- **Disclosure control**: Personal data cannot be read, copied, modified or deleted without authorisation during electronic transfer or transmission or during its recording on a data medium, and it is possible to verify the persons with the right to transfer
- **Input control**: It is possible to verify whether the personal data has been consulted, modified or removed from data processing systems and, if so, by whom;
- **Control of work done**: Personal data processed on behalf of other parties is processed strictly in accordance with the professional responsibilities of the persons accessing the personal data
- **Control of availability**: Personal data is protected against accidental destruction or loss
- **Clean desk policy**: No personal data must be left in an easily visible or accessible place when it is not used by data controllers. This personal data must be archived and stored properly and completely securely when it is not used
- **Confidentiality agreements** or **confidentiality clauses** in contract agreements must be put in place for all third parties with which Sidetrade interacts

- Employees and other parties must be vigilant during their business trips and their work off company premises. **Personal data must not be disclosed in public places**. Appropriate precautions must be taken if personal data is contained on Sidetrade media such as laptop computers, mobile telephones, etc.
- The system's personal data must be regularly backed up appropriately
- **Distribution of personal data** to any non-Sidetrade entity is **strictly prohibited**, except for third parties designated by customers or by Sidetrade, and **acting in the capacity for which they were designated**, and in accordance with applicable local laws. Any exception to this rule can be considered only if a Sidetrade entity is required to supply information to another party for legal and/or regulatory reasons. In this case, the distribution or transfer must be authorised by the local data protection officer.
- In situations where personal data is also considered as inside information, the insider trading and market abuse policy applies.

IV.3 Data life-cycle

IV.3.1 Prior information

When personal data is collected, the data controller is required to supply the data subject, when the data in question is obtained, with information on the **collection**, **purpose** and **use** of this data, in accordance with the principle of **transparency.**

This information is supplied by the data controller to the data subject at the time of collection, or within a reasonable amount of time after obtaining personal data if it is not directly collected from the data subject.

The above information obligations do not apply if the data subject:

- **already has information or if supplying this information is impossible or would require a disproportionate effort**. In this case, appropriate measures to protect the rights and freedoms of the data subject are taken, including by making the information accessible to the public.

IV.3.2 Management of data collection

Legal basis

The personal data must be obtained **fairly and legally**, which is why there are 6 possible legal bases for personal data processing:

- Data subjects have **given their consent** for processing of their personal data for one or several specific purposes
- Processing is necessary for the **performance of a contract** to which the data subject is party, or to take measures on demand from the data subject before entering into a contract
- The processing is necessary to comply with a **legal obligation** of a country in the European Union to which Sidetrade is subject
- The processing is necessary to protect the **vital interests** of the data subject or another natural person

- The processing is necessary to **perform a task in the public interest** or to perform the official duties entrusted to the data controller
- The processing is necessary **for legitimate interests** pursued by the data controller or by a third party, unless these interests are overridden by the interests or fundamental rights and freedoms of data subjects (particularly when the data subject is a child). The use of this basis as a legal basis for processing must be approved by the legal department

The legal basis for processing must be documented and justified, for example by ~~citing~~ mentioning the legal article that imposes a legal obligation, or with a documented assessment of legitimate interest.

Classification of personal data

Personal data has been divided into **3 categories according to its sensitivity** for data subjects

The categories are as follows:

Classification	Description	Principles
Personal – professional	Personal data that is **professional contact** information (*e.g.: name, job title, professional e-mail address or professional telephone number*)	-
Personal – standard	Personal data, **in a non-professional context** (*e.g.: personal address, personal e-mail address, gender, number of children, lifestyle, etc.*)	-
Personal - sensitive	This category includes specific categories of personal data such as racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health, sex life or sexual orientation, criminal convictions or offences, as well as official documents and identifiers (identity cards, driving licence, passport, social security number).	The use of this data is strictly prohibited, unless one of the conditions or exceptions applies (described in article 9 and 10 of the GDPR)

Consent

In case of certain processing of personal data, prior consent from the data subjects is necessary. In this case, Sidetrade must be able to demonstrate that the data subjects have given their consent for the use of their personal data.

Consent must be given "by a clear affirmative act" establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her.

The data subject is able to withdraw his/her consent as simply as it was given.

When the processing has several purposes, consent must be requested for **each** of the processing purposes.

In order to ensure its ability to demonstrate its proper compliance, Sidetrade is able to trace giving and withdrawal of consent.

Consent of the data subject means "any **freely given, specific, informed and unambiguous indication of the data subject's wishes** by which he or she, by a statement or by a **clear affirmative action**, signifies agreement to the processing of personal data relating to him or her."

It may be given by written statement, including by electronic means, or an oral statement. If the data subject’s consent is to be given following a request by electronic means, the request must be **clear, concise and not unnecessarily disruptive** to the use of the service for which it is provided.

Silence, pre-ticked boxes or inactivity should not therefore constitute consent.

IV.3.3 Management of exercise of rights

Sidetrade is required to respect the exercise of the rights of data subjects, i.e.:

- Transparency
- Right to information
- Right to access
- Right to rectification
- Right to be forgotten
- Right to restriction of processing
- Right to data portability
- Right to object to processing

The way in which data subjects can contact Sidetrade to exercise their right is specified in the prior information of data subjects.

Data subjects' requests are analysed and examined within a reasonable amount of time.

Data subjects are informed within a month of the outcome of their request.

Management of the exercise of rights is detailed in **the procedure on management of the rights of data subjects**.

IV.3.4 Retention period management

Personal data is not retained longer than necessary for the purposes for which it was obtained or recorded, or for a period longer than that required by applicable regulatory requirements.

The retention period of personal data is recorded in the personal data processing log.

When personal data is retained, **appropriate information, storage, archiving, ownership and classification** of the personal data is set up to secure and protect personal data in accordance with retention periods defined by Sidetrade (more specifically by the legal department).

Personal data must be deleted or anonymised when it is no longer necessary to retain it for the purposes for which it was obtained or recorded or for applicable legal or regulatory requirements.

The data retention procedure must be assessed in relation to applicable local regulations.

IV.4 Management of privacy in projects

IV.4.1 Data minimisation

Only personal data necessary for the proper functioning of processing is collected, stored, used, transmitted and accessed (in case of exception DPO must be notified).

For any change to the purposes of the processing of personal data, the need for the personal data collected must be verified.

*N.B.: Personal data **cannot be sold to third parties,** unless required by law or if the consent of the data subject has been obtained.*

IV.4.2 Access management

Access to personal data must be controlled so that only people required to handle this data as part of their duties are able so to do.

In particular, access to personal data in information systems requires user authentication and authorisation.

Access management is controlled, particularly via management of arrivals/departures/mobility, as well as by regularly reviewing access.

Any existing paper documentation including personal data must be stored in secure spaces, in order to be able to access it when required by legitimate persons.

IV.4.3 Privacy by Design/by Default & DPIA

Privacy by Design/by Default

Appropriate technical and organisational measures are implemented to guarantee, by default, that only personal data necessary for processing is processed.

Such measures are implemented from design of processing/products/services, and offer a sufficient level of data protection enabling respect of the rights of data subjects.

These personal data security and protection measures are integrated as early as possible into project management. These measures must be appropriate and proportional to the impact on the privacy of the data subjects assessed.

A simplified impact assessment is conducted prior to the personal data processing, to identify whether the processing is likely to create a high risk to the fundamental rights and freedoms of data subjects and therefore must be subjected to a DPIA.

DPIA (Data Protection Impact Assessment)

When processing of personal data is likely to create a risk to the fundamental rights and freedoms of data subjects, a privacy impact assessment of this processing is performed. The criteria intended to determine the need for an impact assessment are those listed in the introduction of the impact assessment procedure

This impact assessment is a process with the aim of assessing the impacts on the privacy of data subjects and defining appropriate measures to reduce the impact.

A DPIA methodology has been defined and formalised.

IV.5 Management of relations with third parties and/or subcontractors

When processing activities are delegated to third parties, the processing **must be governed by a contract or another judicial deed** including at least the following provisions:

- Compliance with GDPR requirements
- Assistance, particularly regarding reports of data breaches, impact assessments, applicable formalities and requests for the exercise of rights of data subjects
- Respect of data security and confidentiality
- Conditions of subcontracting (Sidetrade must at least be able to be informed and be able to object to it)
- Conditions of control by Sidetrade of compliance with the subcontractor's obligations
- Conditions of return or deletion of data following the service
- Description of actions expected from the service provider in connection with the service (instructions)

The legal contract or another judicial deed must stipulate that the subcontractor makes available to the data controller all information necessary to demonstrate compliance with the obligations stipulated by the GDPR and to enable the performance of audits, including inspections, by the data controller or another auditor that it appointed, and contribute to these audits.

The "third party and/or subcontractors" must inform the data controller if, in its opinion, an instruction infringes upon this regulation or other provisions of the Union or Member States in terms of data protection.

Any subcontractor must be able to guarantee and justify data protection measures appropriate to the processing performed on behalf of the data controller. This also applies to processing of personal data where Sidetrade is "subcontractor". Sidetrade must guarantee that subcontractors propose this appropriate level of protection of personal data.

When Sidetrade subcontracts, it is required to guarantee that the data subject of the subcontracted data processing is informed and, as applicable, has consented to this subcontracting.

The legal contract or another judicial deed must guarantee that the subcontractor uses data for other purposes, transmits it or uses it in a manner non-compliant with the terms of the contract, it shall be considered as data controller and **shall be personally liable for offences** committed.

The legal contract or another judicial deed must stipulate that the "third party and/or subcontractors" cannot subcontract to a third party data processing that was ordered from it by the data controller, unless it has been authorised so to do.

IV.6 Management of personal data transfers (Sidetrade internal and outside the EU)

The transfer of personal data to countries outside the European Union is prohibited as a general rule. For it to be authorised, it **must** meet certain conditions, particularly including:

- The recipient country offers an appropriate level of data protection according to the European Commission, or
- The European Commission's standard contract clauses are included in the contract, or
- The recipient company has Binding Company Rules approved by the European Commission, or
- In case of transfer of data to the United States, the recipient company has signed up to "Privacy Shield"
- The data subject is informed and aware of the transfer and that this complies with applicable local regulations. Information supplied to data subjects regarding any transfer of their data must include the purpose of the transfer, the identity of the recipient and the rights of the data subject.

Transfer of personal data outside the European Union must be authorised by the DPO and the legal department after having obtained confirmation that it is transferred in accordance with this policy and applicable procedures and legal requirements.

IV.7 Personal data breach management

Sidetrade is required to anticipate and put in place necessary measures to detect and react in case of breach of personal data.

In case of breach, the supervisory authority may be informed of the breach within 72 hrs of learning of the breach. In the case that the breach is likely to create a high risk for data subject, the data subject must be informed.

The terms and conditions for the management of breaches of personal data are specified in an Incident response procedure.

IV.8 Training/Awareness

It is important for all Sidetrade employees and third parties to fully understand their responsibilities in respect of all personal data protection policies and procedures. Employees responsible for any form of processing of personal data must be fully aware of their obligations not to collect, process or use personal data without appropriate authorisation, maintain the required levels of confidentiality and detect and sound the alarm in case of data breach.

Sidetrade employees must commit to respect confidentiality when they accept their responsibilities and be aware that the obligation of confidentiality continues after the end of their duties.

Sidetrade entities are required to add personal data protection training for all employees to their existing training requirements to make staff aware of related policies and procedures.

Furthermore, specific training/awareness sessions must be organised to train the employees who will process, not only specific categories of personal data such as human resources, but also all operational departments that perform specific personal data processing.

End of document