Registered Adress & Warehouse: Piedrujas iela 5a, Riga, LV1073, Latvia,
VAT Registration Nr LV40003989630
Tel +371 67138848 / Fax. +371 67138883 / info@ccfbaltija.com

PERSONAL DATA PROCESSING AND INFORMATION SECURITY POLICY

Riga, 02 May 2018

Table of contents

1. Definitions of terms used

Company	**Limited Liability Company "CCF Baltija"**, reg. No. 40003989630, reg. address: Piedrujas iela 22, Riga, LV-1073, hereinafter referred to as the Company, which is the employer of every employee employed on the basis of an Employment Contract.
Immediate superior	The representative of the Company, which is specified in the respective Employee's Employment Contract or appointed by a Company order as the Employee's immediate superior.
Employee	Any natural person employed by the Company.
Management	The Board, the Executive Director and/or any other person at the Company, which are assigned management functions and authorities.
Policy	This Personal Data Processing and Information Security Policy.
Third party	A natural person, legal person or other person, which is not linked to the Company.

2. Purpose and scope of the policy

2.1. The purpose of the Personal Data Processing and Information Security Policy is to protect employees, partners and customers of the Company from illegal or harmful direct or indirect, intentional or accidental actions of persons, when processing information and data that get at the disposal of respective persons, as well as using certain equipment for the needs of performance of their job duties.

2.2. The Policy provides the data subject with information about the basis, purpose, scope of processing, protection and period of processing of personal data.

2.3. The Policy regulates processing of information in any systems or on any media, which are involved in processing of data/information at the Company, regardless of whether processing of data/information is related to internal commercial operations of the Company or external relations of the Company with any third persons.

Registered Adress & Warehouse: Piedrujas iela 5a, Riga, LV1073, Latvia,
VAT Registration Nr LV40003989630
Tel +371 67138848 / Fax. +371 67138883 / info@ccfbaltija.com

2.4. This Policy also regulates how Employees of the Company use the equipment and tools available to them within the scope of performance of their job duties.

2.5. The Policy can be applicable jointly with any other policies, regulations, procedures and/or guidelines, which the Company periodically takes and introduces.

2.6. All the questions about the processing of personal data, the information security system and matters of security of information/data, which are not stipulated in the Policy, should be addressed to the Board of the Company.

3. Classification of information

3.1. Any information/data, which becomes available to Employees in the course of performance of their job duties, if such information/data are related to the Company and its operations, customers or cooperation partners, shall be deemed belonging to the Company and confidential, and therefore protected by relevant regulatory enactments on protection of confidential information, trade/commercial secrets and personal data.

3.2. In order to ensure proper protection of information and data, the Company shall classify internal information. Information/data shall be protected regardless of whether such information comes at the disposal of any Employee in the form of any printed materials, on any data storage devices, as audio/video materials or in any other way.

3.3. The Company shall use the following general classification of information:

Category	Description	Scope of applicability (including, but not limited to)
Public information	Information, which can be processed and distributed at and outside the Company without any negative effect on the Company, any of its partners, customers and/or related parties.	(a) Public financial statements submitted to state authorities; (b) Information, which is available in public resources or otherwise publicly known, unless it has become publicly known, because an Employee acted in violation of information/data security requirements.
Internal information	Any information, any use of which, if it happens in violation of requirements of applicable regulatory enactments, this Policy or any other regulation adopted by the Company, can harm interests of the Company and/or any of its Employees, partners, customers.	(a) Any documents drafted and/or prepared by an Employee, structural unit of the Company; (b) Any catalogues (of contacts, information, etc.) created for the purposes of commercial activity of the Company; (c) Any internal service reports, notices, statements, opinions drafted for the needs of commercial activity of the Company.
Confidential Information	Any information, which is so essential for the Company, any of its customers and/or partners or related parties, unauthorised disclosure of which may negatively affect commercial activity, operations, reputation, general status of the Company, its shareholders, customers and/or cooperation partners, and serious harm can	(a) Policy, procedural, internal regulations, management decisions; (b) Information, which is labelled as a trade secret of the Company for the Employee; (c) Other financial, human resources, legal, marketing information, sales procedures, plans and operations; (d) Business, production plans; (e) Personal identification data;

Registered Adress & Warehouse: Piedrujas iela 5a, Riga, LV1073, Latvia,
VAT Registration Nr LV40003989630
Tel +371 67138848 / Fax. +371 67138883 / info@ccfbaltija.com

	be inflicted on any such persons as a result of such disclosure.	(f) Information protected by the confidentiality agreement signed by each Employee; (g) Information protected by confidentiality agreements or cooperation contracts, which the Company concluded in the course of its commercial activity.

4. Systems involved in processing of data/information

4.1. Any information systems, including, but not limited to computer equipment, any software, operating systems, any storage media, network accounts, e-mail accounts, browser systems and any other technical base and tools, used in the operation of the Company, are considered property of the Company.

4.2. Any Employee shall be liable to use such technical equipment and tools with due care and attention, and only for the purposes related to commercial activity of the Company. The only exceptions are the cases, when the Company grants technical equipment to an Employee (for example, a mobile device), giving an explicit consent to its use for personal means.

5. Legal basis of processing of personal data

5.1. The Company processes personal data based on the following legal bases:

5.1.1. for conclusion and fulfilment of a contract;

5.1.2. for fulfilment of laws and regulations;

5.1.3. in accordance with data subject's consent;

5.1.4. in order to implement the liabilities existing between the Company and the customer or legitimate interests of the Company arising from the concluded contract or law.

6. Personal data processing purposes

6.1. The Company processes personal data:

6.1.1. for identification of customers;

6.1.2. for preparation, conclusion, supplementing, reconclusion and termination of contracts;

6.1.3. for customer service;

6.1.4. for fulfilment of liabilities under concluded contracts;

6.1.5. for administration of settlements;

6.1.6. for debt recovery;

6.1.7. for promotion of use and distribution of services;

6.1.8. for customer surveys;

6.1.9. for preparation of reports;

6.1.10. for accounting, planning and statistics;

6.1.11. for provision of information to state administration authorities and subjects of operational activities in the cases and in the amount defined in laws and regulations in force in the Republic of Latvia.

Registered Adress & Warehouse: Piedrujas iela 5a, Riga, LV1073, Latvia,
VAT Registration Nr LV40003989630
Tel +371 67138848 / Fax. +371 67138883 / info@ccfbaltija.com

7. Categories of recipients of personal data

7.1. The Company does not disclose to third persons any personal data or any information of customers obtained during the provision of services and during the effective period of the contract, including on services received, unless:

7.1.1. data should be transferred to the respective third person under a concluded contract to perform any function necessary for the fulfilment of the contract or delegated by the law, for example, within the scope of bank settlements;

7.1.2. preparation and delivery of invoices to the customer;

7.1.3. sending of parcels to the customer;

7.1.4. based on a clear and unambiguous consent of the customer;

7.1.5. to the persons defined in the laws and regulations in force in the Republic of Latvia upon their justified request in accordance with the procedure and scope defined in laws and regulations in force in the Republic of Latvia;

7.1.6. in the cases defined in laws and regulations in force in the Republic of Latvia for the protection of legitimate interests of the Company, for example, by appealing to a court or other state authorities against a person who has infringed these legitimate interests of the Company.

8. Duration of storage of personal data

8.1. The Company shall store and process personal data of customers, while at least one of these criteria exists:

8.1.1. the contract concluded with the customer is in force;

8.1.2. while in accordance with the procedure defined in the laws and regulations in force in the Republic of Latvia the Company or the customer may implement its legitimate interests, for example, bring a claim to a court;

8.1.3. while any of the parties has a legal basis for storage of the data;

8.1.4. while the customer's consent to the processing of the personal data is in force, if there is no other legal basis for the processing of the data.

8.2. When the conditions listed in Paragraph 8.1 of the Policy cease to exist, the customer's personal data will be erased.

9. Customer's consent to processing of data and rights to withdraw it

9.1. The customer may provide its consent to the processing of his/her personal data, the basis for the processing of which is consent, in person in the office of the Company at Piedrujas iela 22, Riga, LV-1073, Latvia, or by writing to e-mail:contacts@ccfbaltija.com

9.2. The customer may withdraw its consent to the processing of his/her personal data in the same way as it was provided – in the office of the Company at Piedrujas iela 22, Riga, LV-1073, Latvia, or by writing to e-mail: contacts@ccfbaltija.com. The withdrawal of consent shall not affect the processing of data that was carried out at the time when the customer's consent was in force.

9.3. No customer's consent is necessary, and its withdrawal shall not affect the processing of fata carried out based on other legal bases, for example, on the basis of a concluded agreement.

10. Duties of Employees of the Company

10.1. Any information/data, which get at the disposal of the Employee, when they perform their job duties, shall be deemed confidential and should be used as confidential, observing their protection according to this Policy, and shall not be disclosed to any third parties, unless the Management informs that such information has become public or was otherwise reclassified into information, which is no longer protected according to the procedure laid down in this Policy.

Registered Adress & Warehouse: Piedrujas iela 5a, Riga, LV1073, Latvia,
VAT Registration Nr LV40003989630
Tel +371 67138848 / Fax. +371 67138883 / info@ccfbaltija.com

10.2. All the personal data and other information, using which a natural person can be identified, shall be collected and processed only, when needed and to the extent it is needed for the purposes of performance of Employee's job duties, provided that such actions are carried out within the limits of the authority granted to the Employee and according to the data protection requirements envisaged in the law (in particular, according to **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)**).

10.3. Any requests of data and/or requests for processing of data, which any Employees received from data owners – natural persons in the course of performance of his/her job duties, shall be sent immediately for further review by the Board.

10.4. Any Employee shall be liable to observe this Policy, as well as fulfil the requirements of applicable local, regional or international regulatory enactments envisaging information/data processing and protection conditions. Failure to observe this Policy shall be considered a serious violation of the work procedures and may result, at the discretion of the Company, in disciplinary penalty or firing of the Employee. The Employee in violation may also be held administratively or criminally liable.

11. Access and protection management

11.1. Employees may access any devices available to Employees, if it is necessary for the needs of performance of job duties of respective Employees to the extent, they need them for the performance of their job duties and within the scope of their responsibility. Access rights to any systems do not mean that the Employee is authorised to view or use all the information available in the respective system.

11.2. User IDs used are unique and identify each specific Employee. Any Employee is responsible for all the actions related to his/her personal ID account, therefore, the primary duty is to ensure that the Employee's ID is not available to any third persons and even other Employees, unless the Company has established other procedure.

11.3. System safety passwords shall be created with due care, in such a way that they cannot be guessed, they do not include personal data and are changed on a regular basis (at least once in 3 (three) months). Any Employee is personally responsible for the compliance of his/her password with this Policy and other regulations of the Company.

11.4. The Employee shall access confidential information / data only, if such authorisations are envisaged in the Employment Contract of the respective Employee, and/or if the Company has granted such authorisation to the Employee.

12. Security measures

12.1. All the data and information collected and processed in any form (printed, electronic, etc.) are subject to the requirements of this Policy and any regulatory framework with regard to collection, processing, protection and storage of such data/information, and such documents should be stored in a safe place specified by the Company with such a period of storage as envisaged by applicable laws and/or specified by the Company.

12.2. Employees are prohibited to store any confidential information in their devices, with the exception of information, which is temporarily necessary for any specified job-related activity. All the necessary confidential and personally identifiable information should be stored only in the cloud storage approved by IT staff of the Company and in the intranet of the Company. Any downloading of such data to local devices should be avoided and should be done only, when it is reasonably necessary due to processing of information for working needs.

12.3. A properly authorised IT staff of the company shall be entitled to filter and supervise access of Employees to internet and activities of Employees on the internet according to the requirements of applicable regulatory enactments.

12.4. Any mobile, portable devices (including laptops, tablets, smartphones and other palmtop devices), as well as any cloud information storages should be approved by the IT staff of the Company and properly protected to prevent any unauthorised access.

Registered Adress & Warehouse: Piedrujas iela 5a, Riga, LV1073, Latvia,
VAT Registration Nr LV40003989630
Tel +371 67138848 / Fax. +371 67138883 / info@ccfbaltija.com

12.5. Only licensed systems and software authorised by the Company can be installed in equipment and tools used at the Company. A permission of the IT staff should be received before downloading and installation of any software in the devices owned by Employees and used for the purposes described in this Policy.

12.6. In the cases, when Employees use personal (home) devices to access corporate resources of the Company (for example, customer relationship management (CRM) programme, e-mail, online/cloud databases) Employees shall be liable to observe the requirements of this Policy in the same way, as if they use the equipment provided by the Company. Therefore, it is prohibited to store in the device any Company-related data and information; processing of any data is permissible only using the cloud and online storages used by the Company.

12.7. In any case, it is strictly prohibited to use public access devices (for example, internet cafés, libraries, etc.) unless critically and urgently necessary for job purposes and the Employee's Immediate Superior has given an explicit written consent to such actions.

12.8. If the Employee is granted the right to access the file storage system of any Company's customer or cooperation partner, the Employee should be liable to use the access tools assigned by the customer or the partner and to observe the provided instructions about secure information/data processing requirements (including the encryption system, use of passwords, data usage restrictions, use of specifically intended places, etc.).

12.9. As soon as at the Company's discretion protected data/information are no longer necessary for Company's operations, such data/information shall be deleted, all its copies shall be destroyed, the Employees involved in processing of respective information/data about their duty to delete/destroy and transfer back to the Company information/data, which they no longer need for the performance of their job duties, and, in particular, return to the Company, delete and destroy copies, if the legal employment relationship with the respective Employee is terminated.

12.10. No information/data specified in this policy should be sent, forwarded or submitted in any other ways to a Third party, unless it is necessary for the performance of Employee's job duties, and to the extent it is necessary for the performance of such job duties. If data are forwarded or submitted to Third parties, protection of the data must be ensured, and all relevant security measures should be taken.

12.11. The Company shall audit the systems used in processing of information/data to control their constant compliance with this Policy and applicable regulatory requirements.

13. Prohibited actions

13.1. Unless specifically indicated otherwise, no equipment, systems or tools belonging to the Company, its customers or cooperation partners should ever or in any conditions be used for any purposes not related to the Employee's job duties or Company operations.

13.2. The activities listed below are strictly forbidden, without any exceptions:

13.2.1. infringement of rights protected by intellectual property rights of any person or company, including, but not limited to use, installation, copying, distribution or storage of any illegal software, online platforms, any other electronic content, for which the Company has no license, in any systems or equipment of the Company;

13.2.2. unauthorised copying of may copyright-protected materials;

13.2.3. infringement of rights of any person excessively and unnecessarily collecting and processing personal data of the subject;

13.2.4. access to data, server or account for such purposes, which are not related to the Company's commercial activity or performance of Employee's job duties;

13.2.5. exporting of software, technical information, decryption software or technology in violation of applicable international or national regulatory enactments and/or instructions of the Company;

Registered Adress & Warehouse: Piedrujas iela 5a, Riga, LV1073, Latvia,
VAT Registration Nr LV40003989630
Tel +371 67138848 / Fax. +371 67138883 / info@ccfbaltija.com

13.2.6. exporting of any data or information, which has the value of property and/or confidential value at the Company, if such exporting is not necessary in the course of Company's commercial activity or performance of Employee's job duties, and/or, if this violates internal rules of the Company, applicable regulatory enactments;

13.2.7. Disclosing of the password of the Employee's account and providing other persons access to such an account (including, but not limited to Employee's family members);

13.2.8. creation of fraudulent offers of products or services using the Company account;

13.2.9. commitment of network communication security breaches or breaks. Such security breaches include, but are not limited to access to data, if the Employee is not their intended recipient, or login to a server or account, which the Employee was not explicitly authorised to access, unless such rights are granted to the Employee due to participation of the respective Employee in the specific project of the Company;

13.2.10. use of any programme/script/command or sending of any message for the purposes of disturbing or disabling a work session of any user with any means.

14. Reporting security incidents

14.1. All information/data processing security incidents or potential incidents should be immediately reported to the Management, which should, respectively, take all measures to prevent potential harm, eliminate consequences of the inflicted harm and restore the previously existing security status.

14.2. When applicable, the Management shall ensure further reporting of breaches of data/information security to authorities and natural persons involved as envisaged by applicable regulatory enactments and/or European Union laws.

_____

SIA "CCF Baltija"
Member of the Board Igors Pankevičs