Personal Data Protection Compliance Policy

HEIDI CHOCOLAT SA

~ May 2018 ~

TABLE OF CONTENTS

1. INTRODUCTION

This Personal Data Protection Compliance Policy (a) applies to personal data processing by electronic means and paper-based storage systems, (b) excludes any processing of personal data of employees, applicants for positions within the Company, and (c) does not apply to the Company's obligations under national regulations in its specific field of activity.

This Personal Data Protection Compliance Policy shall be effective as of 25 May 2018. Until this date, all personnel of the Company shall take all necessary measures to ensure compliance with this Personal Data Protection Compliance Policy.

CORRECT IMPLEMENTATION AND APPLICATION OF THIS PERSONAL DATA PROTECTION COMPLIANCE POLICY SHALL BE STRICTLY MONITORED BY THE COMPANY. WILFUL, NEGLIGENT OR ACCIDENTAL NONCOMPLIANCE WITH THIS PERSONAL DATA PROTECTION COMPLIANCE POLICY MAY RESULT IN SIGNIFICANT FINANCIAL LOSSES AND REPUTATIONAL DAMAGE FOR THE COMPANY AND POSSIBLY DISCIPLINARY ACTIONS AGAINST LIABLE EMPLOYEES OF THE COMPANY.

(1) EU laws on personal data protection require the Company to fully comply with the following principles:

Lawfulness, fairness and transparency	Personal data shall be processed in accordance with law, fairly and transparently in relation to the data subject.
Limitation of purpose	Personal data shall be collected for determined, explicit, and legitimate purposes and shall not be processed in a manner incompatible with those purposes.
Data minimization	Personal data shall be appropriate, relevant, and limited to what is required by the purposes for which it is processed.
Accuracy	Personal data shall be accurate and updated, where necessary.
Time-limited storage	Personal data shall be kept in a form that allows identification of the Data subjects for as long as it is necessary to achieve the purpose for which Personal Data is processed.
Integrity and confidentiality	Personal data shall be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing, and accidental loss, destruction or damage, by using appropriate technical or organizational measures.
Liability	The company, as an operator, shall be responsible for and shall have to demonstrate compliance with the EU Personal Data Protection Laws.

(2) Personal Data Protection starts with each person who is part of HEIDI CHOCOLAT S.A. ("**HEIDI**" or "**Company**").

(3) Company personnel are required to carefully manage the Personal Data. This Personal Data Protection Compliance Policy explains how the protection of Personal Data must be ensured in the entire Company. The following main guidelines are mandatory and should be explained in this document:

- we only process Personal Data for specified processing purposes, and we are aware that the purpose of processing has a valid legal ground;
- we are transparent with the Data subjects; We always inform individuals about how the Company uses Personal Data (whether the individual is an employee, client, vendor, or any other business partner); the fact that we receive personal data of an individual who is representative of company or who acts as an employee of a company does not make the Personal Data less important or place it outside the scope of personal data protection;
- we use Sensitive Data only if necessary and only where expressly permitted;
- we ensure that Personal Data is up to date, complete and accurate;
- we answer promptly any personal data request, we allow the Data subjects to correct, delete or restrict the processing of their personal data;
- we protect Personal Data from loss, modification, disclosure, or unauthorized access.

(4) This Personal Data Protection Compliance Policy was drafted under the GDPR as at the time of its drafting there was no national law in this respect. Any regulation (either European or national) may require the modification or supplementation of this policy.

2. TERMINOLOGY

(5) In this Personal Data Protection Compliance Policy, the following terms shall have the meaning described below:

"Affiliate"	Means any of the following companies: Kex Confectionery S.A., Kandia Dulce S.A, Kex Confectionery Limited, Heidi Chocolat Suisse AG-Switzerland, Heidi Chocolat Group SA, Heidi Chocolat Schwermer GmbH, Heidi Chocolat AG Niemetz Schwedenbomber Niederlassung Österreich, Schokothek Handels GmbH
"Automated decision-making"	Means a process where the inputs are evaluated solely by IT devices, without the involvement of individuals, for example, according to pre-defined criteria / algorithms, the last decision taken having significant consequences for the Data subject.
"Controller"	Means HEIDI CHOCOLAT S.A., the entity that determines the purposes and means of processing Personal Data.
"Processor"	Means an entity that processes Personal Data on behalf of the controller.
"Data protection officer"/"DPO"	Means a natural or legal person which may be designated by the Company pursuant to an obligation imposed by EU Data Protection Laws. The role of the DPO is to: (a) inform and advise the Company and its employees about their obligations to comply with EU Data Protection Laws, (b) monitor compliance with EU Data Protection Laws, (c) be the first contact point for the supervisory authority and for individuals whose data is processed. Details of the DPO's rights and responsibilities are provided in this document.
"Data subject"	Means the identified or identifiable natural person to whom Personal Data refers. For reasons related to this policy, Data subjects may be employees, customers, or representatives of suppliers and business partners.
"EU laws on personal data protection"	Means all laws and regulations applicable in Romania, whether primary legislation (such as national laws and / or GDPR, defined below), or secondary legislation (such as the Working Group Guidelines or other guidelines issued by the Supervisory Authority) applicable to personal data processing.
"GDPR"	Means 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.
"Internal regulations"	Means all internal documents (irrespective of their name or subject), and not limited to the internal regulation, policies and procedures, that constitutes the documented statutory and compliance framework of the Company.
"Personal data"	Means any information relating to an identified or identifiable natural person protected under the EU Data Protection Laws and Regulations. For the purpose of this Personal Data Protection Compliance Policy, Personal Data

	includes Personal Data relating to criminal convictions and offenses (as defined below) and Special Categories of Personal Data (as defined below).
"Personal data concerning criminal convictions and offenses"	Means Personal Data relating to criminal convictions, offenses and / or pardons.
"Processing"	Means any operation or set of operations which is performed on Personal Data, whether or not by automated means, such as collection, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data.
"Profiling"	Any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.
"Company's records concerning data processing"	Means mandatory records held at Company level that provide an overview of all processing activities within the organization (e.g. what kind of data categories are processed, by whom (which departments or business units) and the purpose of the processing).
"Special categories of personal data"	Means personal data revealing ethnic origin, political, religious or philosophical beliefs, or membership in trade unions, while the processing of genetic and biometric data in order to uniquely identify a natural person as well as data on health, life or sexual orientation of an individual.
"Sub-processor"	Means any person designated by or on behalf of the processor or an Affiliate to process Personal Data on behalf of the Company;
"Supervisory authority"	Means the National Supervisory Authority for Personal Data Processing or any other authority to which data protection responsibilities are assigned under the EU laws and regulations on the protection of personal data of any Member State.
„Transfer"	Means disclosing or otherwise making available to third parties (including Affiliates or Sub-processor) personal data either by physically transmitting Personal Data to that third party or by allowing access to the Data by other means. In order to avoid any misunderstanding, storage and backup copying shall be considered transfer within the meaning of this Personal Data Protection Compliance Policy.

3. PURPOSES OF DATA PROCESSING BY THE COMPANY

- The Company holds an inventory of the processing purposes currently applicable to it,
- The purposes of data processing are comprehensively stated in the Company's Processing Registers (kept by the Data Protection Officer),
- Each data processing purpose has legal grounds and is directly linked to the Company's business activities,
- The purposes for data processing are the red line for each processing activity, the Data Protection Officer being immediately informed of any deviation from, or modification of them,
- Personal data shall be processed (collection, use, storage, etc.) in strict compliance with the purposes of processing.

3.1. Company identified the specific purposes of data processing

(6) Generally, the Company collects, uses, stores or otherwise processes Personal Data in the following circumstances:

a. When a Data subject submits any form or document, concludes a formal agreement or provides other documentation or information about its interactions and transactions with the Company;

b. When a Data subject interacts with Company personnel, including the employees responsible with customer/client relations, or other representatives, for example by telephone, letters, fax, in-person meetings or e-mail;

c. When images with a Data subject are captured by the Company through surveillance cameras while the Data subject is within the Company's premises;

d. When a Data subject requests to be contacted by the Company, be included in an email or other mailing lists, or when the Data subject responds to the Company's request for the provision of additional personal data;

e. When a Data subject interacts with the Company through Company Websites;

f. When the Company acts to prevent or investigate suspicion of fraud, illegal activities, omissions, or misconduct in connection with or likely to arise from the relationship of a Data subject with the Company;

g. When the Company complies or acts on a request or instructions of any public authority or responds to requests for information from regulatory agencies, ministries, statutory boards or other similar authorities;

h. When the Company performs tax, financial, regulatory, management, risk management (including risk exposure monitoring) statements and auditing,

i. When the Company seeks information about an Data subject and receives the Personal Data of the Person in question about his/her relationship with the Company, including insurance policies, for example from business partners, public agencies, current employer and relevant authorities; and / or

j. When a Data subject sends to the Company his/her personal data or the personal data of a third person (for example, information about the spouse, relatives or inflows, children, parents and / or employees, etc.) for any reason.

(7) All of the above mentioned activities are declared as the purposes of the data processing and are listed in the Company's Data Processing Records.

3.2. Purposes of data processing by the Company have a legal and valid ground

(8) Data processing purposes by the Company are grounded on one of the following:

(CONSENT)	The Data subject who has given his / her consent to the Processing.
(CONTRACT PERFORMANCE)	Processing is required: a. for a contract that the Data subject concluded; or b. as a result of a request by the Data subject for a detail in order to be able to conclude a contract.
(COMPLIANCE WITH LEGAL OBLIGATIONS)	Processing is required because there is a legal obligation on the part of the Company.
(LEGITIMATE INTERESTS)	Processing complies with the "legitimate interests".

(9) The grounds for each of the data processing purposes by the Company are mentioned in the Company's data processing records.

3.3. Data processing is limited to data required to achieve the purpose of data processing

3.3.1. Purposes of data processing by the Company are limited to certain categories of Data subjects and certain categories of Personal Data (data minimization)

(10) The Internal Regulations/policies mention the documents and/or what Personal Data are requested specifically from Data subject to be processed for that particular Person. On one hand, the Annexes to the Internal Regulations may include forms and contracts to be filled in and / or by the Data subject. On the other hand, the Internal Regulations allow Personal Data to be collected directly from the Data subject and entered directly into the IT system of the Company.

(11) Data processing involving "Special personal data categories and / or" Personal data relating to criminal convictions and offenses " should be dealt with as an exception and should be avoided as far as possible (unless requested specifically by the Internal Regulation and required by law).

(12) Any Additional Personal Data other than Personal Data expressly mentioned in the Company's Records and other than the Personal Data provided in the Internal Regulations may be requested from the Data subjects only with prior authorization from the Department Manager, from the Legal Department and / or the Data Protection Officer.

(13) All additional personal data other than Personal Data expressly mentioned in the Company Data Processing Records and other than those referred to in the Internal Regulations, received by the Company (either intentionally or by accident) from another source than from the Data subjects (except for those mentioned in article 3.1.j), must be considered as a breach of security of personal data and

must be brought to the attention of the Department Manager., of the Legal Department and / or the Data Protection Officer.

3.3.2. Personal data collected by the Company is accurate, complete and confidential (accuracy and confidentiality)

(14) All Personal Data collected by the Company in connection with any of the purposes of the data processing must be accurate. Internal Regulations require that Company personnel ensure that Personal Data obtained directly or indirectly from the Data subjects is verified by comparison with the relevant documentation.

(15) The integrity and confidentiality of all Personal Data collected by the Company with regard to the data processing purposes is mandatory. Internal Regulations require that Company personnel ensure that Personal Data obtained directly or indirectly from the Data subjects is safely stored and accessed for information purposes only.

3.3.3. Personal Data is processed at the Company until the purpose of data processing is achieved (time-limited storage)

(16) Depending on the purpose of data processing, Personal Data collected by the Company shall be kept either in physical form or in electronic format (or both):

a. for the period required to achieve the purpose of data processing, or
b. to the extent necessary to comply with the applicable legal requirements for a specified period, by a provision of a law, or
c. as appropriate, taking into account the applicable limitation period.

3.3.4. Data processing outside the processing purpose is generally prohibited (change of purpose)

(17) In general, Personal Data shall only be used for processing purposes for which it was initially collected (original purpose). Personal Data may be processed for the legitimate purposes of the Company in a manner different from the original purpose (secondary purpose) only if the original and secondary purposes are closely interrelated.

(18) It is generally permitted to use personal data for the following secondary purposes:

a. Identifying the risk profile of the Data subject or Company that the Data subject represents, or
b. Internal audits or investigations; or
c. Solving disputes; or
d. Regulatory reports.

(19) Any processing of Personal Data other than the processing purposes specifically set forth in the Company's Data Processing Records shall be immediately suspended and the Legal Department and the Data Protection Officer shall be notified of the situation as soon as possible.

(20) Any change of Original Data Processing Purposes shall be carefully assessed and, in case of doubt, the Company's personnel shall bring the matter to the Legal Department and the Data Protection Officer before proceeding with any further Processing.

3.3.5. Transfer of Personal Data

(21) During the operation and provision of its services, the Company may transfer the Data to another country or to international / foreign organizations only if the data security is duly guaranteed in that country or international / foreign organization.

(22) When transferring personal data to a state outside the European Economic Area, the Company grants appropriate guarantees for data protection on the basis of a contract concluded with that natural or legal person or international organization.

3.3.6. Profiling and automated decision-making

(23) Data processing within the Company does not involve the profiling or automated decision-making

4. COMPANY RESPECTS THE RIGHTS OF DATA SUBJECTS

Pursuant to the laws on personal data protection, Data subjects enjoy guaranteed rights:

- **Right to be informed,**
- **Right of access,**
- **Right to rectification,**
- **Right to erasure (right to be forgotten)**
- **Right to restriction of processing,**
- **Right to data portability,**
- **Right to object,**
- **Rights related to decision-making and profiling.**

All the Company's staff has been informed and knows how to act to any exercise of rights by the Data subjects.

4.1. Company informs the Data subjects about the processing of Personal Data

(24) As a rule, all documents handed over to the Data subjects (forms or contracts) contain all the information required for the Company to comply with the Company's obligation to properly inform the Data subjects about the data processing.

(25) Without prejudice to the content of the documents transmitted to the Data subjects, the Company's staff will, upon request, explain in detail – including orally - the business activity for which the data processing is performed, what kind of Personal Data is required from the Data subjects and the fact that the Company has taken appropriate technical and organizational measures to ensure that Personal Data is stored in secure and confidential conditions.

(26) If the Data subjects are not required to complete individual forms because they are required to submit only certain documentation or to communicate Personal Data verbally, the Company's personnel is obliged to inform the Data subjects about all the coordinates of the data processing activity. Here below is a list of issues to be brought to the attention of the Data subjects:

What information must be communicated?	At the time of receiving the Personal Data:

Name and contact data of the Company and DPO	✓
Purpose of data processing and legal grounds for data processing	✓
Company's legitimate interests	✓
Categories of Personal Data	
Recipients or categories of recipients of Personal Data	✓
Details of the transfer of Personal Data to third countries and security measures	✓
The period for which Personal Data shall be stored and the criteria used to determine this period	✓
Observance of each right of the Data subject	✓
Source of Personal Data and whether it comes from public sources	
If the provision of Personal Data is a legal or contractual requirement or obligation, as well as the possible consequences of non-compliance with this obligation	✓
Whether an automated decision-making process is in place or not, if profiles are created and information on the decision-making process, importance and consequences	✓

4.2. Company's staff acknowledges and knows how to answer a request by the Data subject

(27) EU laws on the protection of personal data require that any request by a Data subject is answered as soon as possible but no later than 31 days (term which, in particular situations can reasonably extend to up to 60 days) after receipt.

(28) Company's staff shall solve with priority all inquiries received from the Data subjects about the processing activity.

(29) In all cases, the Company's employees shall inform the Data subject that they may submit a formal request and / or complaint to the address designated by the Company to respond/deal with request related to Personal Data (such address may also represent the Company's DPO contact details).

5. DATA PROTECTION COMPLIANCE WITHIN THE COMPANY

5.1. Data Protection Officer appointed by Company

(30) Company may appoint a Data Protection Officer – either a natural person or a legal entity - with the qualifications required by EU Data Protection Laws:

a. The position of Data Protection Officer is established as directly subordinated and directly reporting to the General Manager of the company or to the Company's Board of Directors;
b. Data Protection Officer is not subject to conflict of interest;
c. Company involves the Data Protection Officer in due time and in an appropriate manner in all matters involving the protection of Personal Data;

(31) In case of appointing a DPO, the Company shall:

a. Disclose the contact details of Data Protection Officer to the Data subjects and publish them internally on the Company's intranet, internal telephone directory and organizational chart to ensure that his/her activity and tasks are known within the Company.
b. Submit the contact details to the relevant supervisory authority;
c. Ensure that the Data Protection Officer is invited to regularly attend meetings with middle and top management of the Company.
d. Always value the opinion of the DPO. In case of misunderstanding, it is important to state the reasons for not taking into consideration the DPO's opinion.
e. Immediately and without undue delay consult the Data Protection Officer in connection with a breach of data security or other incident.
f. In case the DPO is a natural persona and an employee of the Company, the Company shall support the DPO by "providing the necessary resources to carry out his/her tasks, accessing personal data and processing operations, and maintaining his/her specialist knowledge"
g. In case the DPO is a natural persona and an employee of the Company, the Company shall ensure regular training of the DPO, who should be given the opportunity to keep abreast of developments in the field of Personal Data protection. The aim should be to permanently increase the DPO's level of expertise; therefore, the Data Protection Officer should be encouraged to participate in training courses on Personal Data protection, as well as other forms of personal development.
h. Ensure that DPO "shall not receive instructions as to the performance of his/her duties."

(32) DPO is required to maintain the secrecy or confidentiality of the information concerning the performance of his/her tasks.

5.2. Internal tasks for ensuring the Data Protection compliance by trading departments

(33) Compliance with the protection of personal data is a continuous independent responsibility for each employee of the Company, and non-compliance with this policy may lead to professional liability.

(34) Notwithstanding the foregoing, the Company assigned certain tasks to assist the Company's personnel in the achievement and maintenance of compliance with the protection of personal data.

(35) Persons are designated for each department of the Company to be **responsible for the protection of Personal Data** and for the compliance and implementation of the Personal Data Protection Compliance Policy, from the commercial/functional point of view. The persons responsible for the protection of

personal data shall decide on, provide the means and facilitate the management of all data protection issues in the appropriate direction.

(36) The person within each department who is responsible for the protection of personal data must:

a. Ensure that his/her department shall process Personal Data in accordance with this Policy;
b. Work with the DPO and implement the requested changes in his/her department to be brought in line with EU Personal Data Protection Laws;
c. Duly complete and sign the audit questionnaires and other forms requested by the DPO;
d. Perform the impact assessment on data protection based on the model provided by the DPO;
e. Have the DPO's opinion on the risks or incidents of data protection, compliance issues, as well as answers to all questions in the department where he/she acts as the person responsible for the protection of personal data;
f. Submit to DPO reports on data protection risks and compliance issues at least once a year and more frequently when required by the DPO;
g. Coordinate with the DPO for performing formal investigations or assist in investigations by a governmental authority on the processing of data related to his/her department.

5.3. Internal regulations

(37) As a general statement, this Policy sets out the basic principles to be addressed in more detailed policies.

(38) Company shall develop and implement such policies, minimum standards and procedures in order to comply with this Personal Data Protection Compliance Policy.

(39) In the event of discrepancies between this Policy and EU Personal Data Protection Laws, the latter will prevail.