DATA BREACH POLICY

under Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 concerning the protection of natural persons with regard to the processing of personal data and the free movement of such data

INDEX

1. INTRODUCTION

Cereal Docks Organic S.r.l. (hereinafter also referred to as the "**Controller**" or "**Company**") is required, pursuant to:

(i) the General Regulation on Data Protection - 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 (hereinafter "**GDPR**") and

(ii) the Legislative Decree no. 196/2003 containing the "Personal Data Protection Code" and the amendments introduced by the Legislative Decree. no. 101/2018 (hereinafter the "**Code**"),

hereinafter jointly referred to as the "**Personal Data Protection Legislation**",

to maintain the security of personal data processed within the scope of its activities and to act without unjustifiable delay in case of data breach (including any notification to the competent Guarantor Authority and any communication to the interested parties).

It is of paramount importance to provide for action to be taken in the event of potential or actual infringements of personal data, in order to avoid any risk to the rights and freedoms of the affected recipients, as well as economic damage to the Company and to be able to report the event in the time and manner provided by the GDPR to the Guarantor Authority and/or the persons concerned.

2. PURPOSE OF THE MODEL

The purpose of this procedure is to define the flow of activities for the management of violations of personal data processed by the Controller.

3. RECIPIENTS

This procedure is addressed to all persons who, for any reason, process personal data falling within the competence of the Controller including:

- the employees, as well as those who in any capacity - and therefore regardless of the type of relationship - have access to the personal data processed in the course of their employment on behalf of the Controller (hereinafter referred to as "**Internal Recipients**");
- any person (natural person or legal entity) other than the Internal Recipients who, by reason of the existing contractual relationship with the Controller, has access to the above mentioned data and acts as Data Processor pursuant to art. 28 of the GDPR or autonomous Data Controller (hereinafter referred to as the "**External Recipients**"),

hereinafter generically referred to as "**Recipients**".

All Recipients must be duly informed of the existence of this procedure by methods and means that ensure their understanding.

4. DEFINITIONS

- *Personal Data* means any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, by reference in particular to an identifier such as a name, an identification number, location data, an online identifier or to one or more characteristics of his or her physical, physiological, genetic, mental, economic, cultural or social identity (hereinafter referred to as '**Personal Data**');
- *Processing* means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automatic 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 of data, restriction, erasure or destruction (hereinafter referred to as "**Processing**");

- *Data Controller* means the natural or legal person, public authority, agency or other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by the European Union or Member State law, the Controller or the specific criteria applicable to its designation may be determined by Union or Member State law (hereinafter referred to as '**the Controller**');
- *Data Processor* means the natural or legal person, public authority, service or other body processing personal data on behalf of the Controller (hereinafter referred to as the '**Processor**');
- *Data Subject* means any identified or identifiable natural person (hereinafter referred to as the '**Data Subject**');
- *Data Protection Officer* is a technical consultant appointed by the Data Controller, whose competencies are regulated by the GDPR (hereinafter "**DPO**");
- *Privacy Team*, is a group of persons appointed by the Data Controller with the function of
  (i) carrying out, also with the help of external consultants appointed by the Company, all activities related to and necessary for *compliance* with data protection legislation;
  (ii) managing the Organizational Model for the Protection of Personal Data adopted by the Controller;
  (iii) dealing with the DPO, where appointed;
  (hereinafter "**Privacy Team**");
- *Supervisory Authority* means the independent public authority set up by a Member State in accordance with Article 51 of the GDPR (in Italy this authority is identified with the Data Protection Authority') (hereinafter referred to as the "**Authority"**);
- *Breach of Personal Data*, the breach of security that involves accidentally or illegally destruction, loss, modification, unauthorized disclosure or access to personal data transmitted, stored or otherwise processed (hereinafter '**Infringement**' or '**Data Breach**').

Infringements can occur for various reasons which may include, but are not limited to:

- disclosure of confidential data to unauthorized persons;
- loss or theft of data or instruments in which the data is stored;
- loss or theft of paper documents;
- corporate infidelity (e.g.: data breach caused by an internal person who has permission to access the data shall produce a copy distributed in a public environment);
- abusive access (e.g. data breach caused by unauthorised access to systems information with subsequent disclosure of the information acquired);
- cases of computer piracy;
- databases altered or destroyed without authorisation issued by their Owner;
- viruses or other attacks on the computer system or company network;
- violation of physical security measures (e.g.: forcing doors or windows of security rooms or archives containing confidential information);
- loss of laptops, devices or company computer equipment;
- sending e-mails containing personal and/or particular data to the wrong recipient.

5. BREACH NOTIFICATION PROCEDURE

Infringements are handled by the Controller with the help of the Privacy Team and under the supervision of the DPO, where appointed.
Specifically, the Privacy Team and the DPO have the task of assisting the Controller in the resolution of issues relating to a suspected, alleged or actual Data Breach event by addressing the following aspects (by way of example but not limited to) where applicable:

1. determine whether or not the infringement in question is to be considered an infringement;
2. assign a level of severity to the infringement;
3. ensure that a proper and impartial investigation is initiated, conducted, documented and concluded;

4. identify the requirements for resolution of the infringement and monitor the resolution;
5. coordinate with the Authority;
6. coordinate internal and external communication;
7. ensure that those concerned are adequately informed.

If deemed appropriate and necessary, following the outcome of the initial analyses carried out with regard to the potential degree of seriousness as well as specificity of the Breach, the Controller, in consultation with the Privacy Team and the DPO, if appointed, may also involve additional external experts in the management activities of Data Breach (by way of example, a computer security expert or an external communication agency to assist the Controller in case of need for communication to third parties).

In case of suspected, alleged or actual Breach, it is of utmost importance to ensure that the Breach is addressed immediately and correctly in order to minimize the impact of the Breach and prevent its possible repetition.

In the event that one of the Recipients becomes aware of a suspected, presumed or actual Breach, he/she must give immediate communication as follows:
(i) if he or she is an Internal Recipient, to his or her area/function manager who will deal with the support of the recipients themselves, to inform the Controller through the compilation of Annex **A** - "Internal Data Breach Communication Form" to be sent by email to teamprivacy@cerealdocks.it;
(ii) if he is an External Recipient, he/she shall inform the Controller without undue delay by filling out Annex **A** - "Internal Data Breach Communication Form" to be sent by email to the address teamprivacy@cerealdocks.it.

6. BREACH MANAGEMENT PROCEDURE

To handle a personal data breach the following steps shall be followed:
Step 1: Identification and preliminary investigation
Step 2: Containment, data recovery and risk assessment
Step 3: Possible notification to the Authority
Step 4: Possible communication to interested parties
Step 5: Documentation of the breach event

Step 1: Identification and preliminary investigation
Annex A, duly completed, will allow the Controller, with the help of the Privacy Team and with the support of the DPO, if appointed, to conduct an initial assessment of the communication received, in order to determine whether a Data Breach event has actually occurred and whether a more in-depth investigation is necessary, proceeding in this case with step 2.
In the event of a breach of data contained in a computer system, the Controller must also involve the IT Manager or his delegate in the whole procedure indicated in this document in case of absence.

Step 2: Containment, data recovery and risk assessment
Once it has been established that a Data Breach incident has occurred, the Controller together with the Privacy Team and the DPO, if appointed, will have to establish:

- whether there are actions that could limit the damage that the breach could cause (i.e. physical repair of instrumentation; use of back up files to recover lost or damaged data; isolation/closure of a compromised sector of the network; change of access codes, etc.);
- who should act to contain the breach, once these actions have been identified;
- whether it is necessary to notify the breach to the Authority (where the infringement is likely to present

a risk to the rights and freedoms of physical persons);
- whether it is necessary to notify the breach to the persons concerned (where the breach presents a high risk for the rights and freedoms of natural persons).

In order to identify the need for notification to the Authority and communication to the parties concerned, the Controller, assisted by the Privacy Team and the DPO, where appointed, will assess the seriousness of the breach by using Annex **B** - "Data Breach Risk Assessment Form" which must be examined together with Annex A, also taking due account of the principles and indications set out in Articles 33 and 34 of the GDPR.

Step 3: Possible notification to the Authority
Once it has been assessed the need to notify the Authority of the infringement suffered on the basis of the procedure described in step 2, as prescribed by the GDPR, the Controller must do so without undue delay and, where possible, within 72 hours from the time it has become aware of it.
If notification to the Authority is not made within 72 hours, the notification shall be accompanied by the reasons for the delay.

The notification shall at least:
(a) describe the nature of the breach including, where possible, the categories and approximate number of Interested parties concerned and the categories and approximate number of personal data records in question;
(b) communicate the name and contact details of the DPO, if appointed, or of another contact person who can provide with further information;
(c) describe the likely consequences of the breach;
(d) describe the measures taken or proposed to be taken by the Controller to remedy the breach; and, where appropriate, to mitigate its possible negative effects.

If and to the extent that it is not possible to provide the information at the same time, the information may be provided to the Authority at a later stage without further undue delay.

Step 4: Possible communication to interested parties
Once the need to communicate the breach to the Interested Parties has been assessed on the basis of the procedure referred to in step 2, as prescribed by the GDPR, the Controller must do so, without undue delay.
Communication to the interested parties must be in clear and simple language and must contain:
a) the name and contact details of the DPO or of another contact person who can provide further information;
(b) a description of the likely consequences of the breach;
(c) a description of the measures taken or proposed by the Controller to remedy the infringement; and, where appropriate, to mitigate its possible negative effects.

With regard to the methods of communication, on a case-by-case basis, the Controller must always give priority to a direct method of communication with interested parties (such as emails, SMS or direct messages). The message shall be communicated in a simple and transparent way, thus avoiding sending information through newsletters, which could easily be misinterpreted by the interested person. In case the direct notification requires a disproportionate effort, then public communication may be used. It will have to be as effective as addressing directly the person concerned.

Step 5: Documentation of the Breach
Regardless of the need to notify the Authority (step 3) and/or the Interested Parties (step 4) of the

breach, whenever a potential Data Breach is communicated by the Recipients through Annex A, the Controller is required to document it.
This documentation activity will be carried out by the Controller, with the help of the Privacy Team, of a special "Personal Data Breach Record Table" shown in Annex **C**.
The Personal Data Breach Record Table must be continually updated and made available to the Authority if he requests access.

7. ACCOUNTABILITY

Compliance with this procedure is mandatory for all Recipients and its non-compliance may lead to disciplinary measures against employees in default or the termination of existing contracts with defaulting third parties, in accordance with the applicable legislations.

8. RECORD RETENTION PERIOD BASED ON THIS DOCUMENT

Document	Legal basis for the treatment	Period of retention
Internal and external Data Breach communication forms	(Art. 6, para. 1(c), GDPR) Treatment necessary to fulfill a legal obligation to which the Controller is subject (Art. 6, para. 1(f), GDPR) Treatment necessary for the pursuit of the legitimate interest of the Controller as part of the management of its organization	Permanent
Documented decisions of the Controller regarding the Breach	(Art. 6, para. 1(c), GDPR) Treatment necessary to fulfill a legal obligation to which the Controller is subject (Art. 6, para. 1(f), GDPR) Treatment necessary for the pursuit of the legitimate interest of the Controller as part of the management of its organization	5 years
Communication of a Breach	(Art. 6, para. 1(c), GDPR) Treatment necessary to fulfill a legal obligation to which the Controller is subject (Art. 6, para. 1(f), GDPR) Treatment necessary for the pursuit of the legitimate interest of the Controller as part of the management of its organization	5 years
Inventory of personal data breaches	(Art. 6, para. 1(c), GDPR) Treatment necessary to fulfill a legal obligation to which the Controller is subject (Art. 6, para. 1(f), GDPR) Treatment necessary for the pursuit of the legitimate interest of the Controller as part of the management of its organization	Permanent

9. USE OF THE PRESENT DOCUMENT

The person responsible for this document is the Controller, who must check the document at least once a year and, if necessary, make any amendments/updates.

Annexes

- "A - Internal Data Breach Communication Form"
- "B - Data Breach Risk Assessment Form"
- "C – Personal Data Breach Record Table"

*Annex "**A**" – Internal Data Breach Communication Form*

If a suspected, presumed or actual personal data breach is detected, immediate notice shall be given to the Data Controller by filling out the form below to be sent by e-mail to following address: teamprivacy@cerealdocks.it

Data Breach Communication

Document filled out on (date):

□ **INTERNAL RECIPIENT ***

Data of the person reporting the breach:

Surname and name	
Task/Job	
Contact Data (address e-mail, telephone number)	

□ **EXTERNAL RECIPIENT ***

Data of the subject reporting the breach:

Firm\Company name	
Contact data of the DPO (if appointed)	
Surname and name of the reporter	
Contact Data (e-mail address, telephonenumber)	

* indicate, alternatively, whether the reporting entity is an Internal Recipient or an External Recipient.

*****

DESCRIPTION OF THE EVENT

Date of discovery of the breach (date, time)	
Date and place of the breach (date, time, place)	
Description of what happened	
Description of how it happened	
Categories and approximate number of interested parties involved in the breach	
Other relevant details (any actions taken at the moment of discovery of the breach, etc.)	

*Annex "**A**" – Internal Data Breach Communication Form*

To be filled out by the Data Controller (or the contact person appointed by it)	**DATE AND TIME THE FORM HAS BEEN RECEIVED:**	
Please indicate how the form has been received:	Sequential number of the reported event (from the Data Breach Record)	
Systems being involved:		
Detected vulnerabilities:		

*Annex "**B**" – Data Breach Risk Assessment Form*

Assessment of the seriousness of the breach	To be filled out by the Controller with the help of the Privacy Team, DPO (where appointed) and possibly of the IT Manager
Devices affected by Data Breach (computer, mobile device network, file or part of a file, back up tool, paper document, other).	
Modes of exposure to risk (type of breach): reading (presumably the data has not been copied), copy (the data is still present on the systems of the Controller), alteration (the data are present on the systems but have been altered), deletion (the data are no longer present and even the breacher does not have them), theft (the data are no longer on the Controller's systems and are owned by the breacher), other.	
Brief description of the processing systems or data storage involved, with indication of their location.	
If your laptop or other mobile device has been lost / stolen: when was the last time that the laptop has been synchronized with the central IT system?	
How many people have been affected by the breach of the personal data being processed within the database breach?	
What is the type of data involved in the breach?	
May the breach result in damage to the reputation, loss of confidentiality of data protected by professional secrecy, unauthorized decryption of pseudonymisation, or any other crucial economic or social data?	
Do those concerned risk being deprived of the control over their personal data?	
What technical and organisational measures are taken regarding the data breach? (i.e. pseudonymisation, encryption of personal data, etc.)	
Has the Data Controller taken measures to prevent the occurrence of a high risk for the rights and freedoms of the persons concerned after the breach?	
Classification of the severity of the breach (1-low, 2-critical or 3-high) and reasons:	
Has the Data Breach been reported to the Data Protection Authority?	YES/NO If yes, please indicate the date: Details:
Has the Data Breach been reported to the Data Subjects concerned?	YES/NO If yes, please indicate the date: Details:

*Annex "**C**" – Personal Data Breach Record Table (see Excel file)*

DATA CONTROLLER	**Cereal Docks Organic S.r.l.** Via Ca' Marzare, n. 3 36043 – Camisano Vicentino (VI) Tel. +390444 419411 email: info@cerealdocks.it Posta Elettronica Certificata: cerealdocksorganic@pec.resinova.it P. IVA e Codice Fiscale: 04063200242
DATA PROTECTION OFFICER	**TD&A Studio Associato** (hereinafter referred to as "DPO") E-mail: dpo@cerealdocks.it

EVENT ID	NOTIFICATION				BREACH EVENT					DATA and DATA SUBJECTS				CONSEQUENCES	REMEDY		MITIGATION OF ADVERSE EFFECTS		TIME	NOTIFICATION TO THE GUARANTOR				NOTIFICATION TO THE INTERESTED PARTIES				NOTE
Event ID	**Date and Time**	**Reporting person**	**organisational unit affected by the breach**	**addressees of the notification**	**place of the breach event**	**methods of committing the breach event**	**systems/equipments/ networks/data banks subject to data breach**	**nature of the personal data breach**	**other elements useful to the description of the breach event**	**data subjects affected**	**approximate number of affected data subjects**	**categories of personal data**	**approximate number of personal data records**	**consequences of personal data breach**	**measures taken to remedy the breach event**	**measures intended to remedy the infringement**	**measures proposed to remedy the breach event**	**measures proposed to mitigate possible adverse effects**	**restore time**	**risk to the rights and freedoms of natural persons**	**sending notification to the Authority**	**reasons for the delay in notifying the Authority**	**reasons for failure to notify the Authority**	**indicate whether there is a high risk to the rights and freedoms of natural persons**	**notification to the interested parties**	**methods of notification to interested parties**	**reasons for failure to inform interested parties**	**notes**
Provide a code, if necessary, for the traceability of the breach event	Indicate circumstances of the notification in chronological order	Indicate whether internal or external recipients are involved (see Annex 4, data breach communication form)	Indicate the office/organisational unit affected by the breach event	Indicate the office/organisational unit to which the request is addressed	Describe, if applicable, the place of the breach event	Describe how the breach event took place and its impact	Indicate the infrastructure or the applications involved in the breach event	Indicate whether there is a breach of confidentiality, integrity and/or availability of data	Indicate any other circumstances relevant to the analysis of the breach event	Indicate in particular whether they are vulnerable	Indicate a given quantity, even if approximate	Indicate whether the breach event concerns particular data, data relating to convictions and offences, or other types of data	Indicate a given quantity, even if approximate	Indicate any prejudices and material or non-material damage (financial or reputational - suffered by the persons concerned	Indicate precautions already taken which eliminate the consequences	Indicate precautions being taken intended to eliminate the consequences	Indicate precautions already taken which reduce the consequences	Indicate precautions being taken that reduce the consequences	Indicate the time needed to resolve the breach event	Indicate whether improbable or not improbable	Indicate yes/no, if yes, indicate date and time, and if late or partial; in this case, assign an ID to the notification (first, second, etc.)	Indicate in which circumstances the breach event has to be notified with reasons for the delay of more than 72 hours	Explain why the risk to the parties concerned is unlikely	Indicate the type of risk and the reasons why their risk is high	Indicate yes/no; if yes, indicate date and time, and if late or partial; in this case, assign an ID to the notification (first, second, etc.)	Indicate the means of notification used and how the persons concerned will be assisted	Document one of the hypotheses referred to in Article 34(3)(a), (b), (c) of the GDPR	Additional notes
				Indicate the appropriate higher level of management and the persons responsible or persons in charge of managing incidents, establish the existence of a breach and assess the risk.				**"breach of confidentiality"** means unauthorised or accidental disclosure of or access to personal data; **"breach of integrity"** means unauthorised or accidental modification of personal data; **"breach of availability"** accidental or unauthorised loss, access or disposal of personal data.											Consider (1) Type of breach, (2) Nature, sensitive nature and volume of personal data, (3) Ease of identification of natural persons, (4) Severity of consequences for natural persons, (5) Special characteristics of the data subject, (6) Special characteristics of the data controller, (7) Number of natural persons concerned, (8) General aspects.		If it is not made within 72 hours, the notification to the supervisory authority must be accompanied by the reasons for the delay.	e.g. personal data already publicly available, the disclosure of which would not pose a likely risk to the natural person's rights and freedoms or personal data rendered by noncomprehensible to unauthorised persons and whether there is a copy or backup, personal data properly encrypted			The notification to the Interested Parties shall be written in clear and simple language and shall contain: a) the name and contact details of the data protection officer or other contact person who can provide more information; b) a description of the likely consequences of the breach event; c) a description of the measures taken or proposed by the Data Controller to address the personal data breach, where appropriate, to mitigate its possible negative effects. With regard to the methods of notification, on a case-by-case basis, the Controller shall always give priority to direct communication with the parties concerned (such as emails, SMS or direct messages). The message must be communicated in a clear and transparent manner, thus avoiding sending information through newsletters, which could be easily misunderstood by the Interested Parties. In the event that direct reporting requires a disproportionate effort, there will be a public notice or similar measure, which must be equally effective in notifying directly the interested party.	For example, as appropriate: state of the art encryption or tokenization; immediate identification and initiation of a password change; identification of fraud events in the personal data prior to use; public disclosure or provision of technical arrangements to make information on the breach available upon request.	