DATA BREACH POLICY

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

NATEEO SRL
via dell'Innovazione 1
I – 36043 Camisano Vicentino (VI)
tel +390444419472
fax +390444419490
info@nateeo.it
www.nateeo.it

REGISTRO IMPRESE DI VICENZA CF/P.IVA 03804370249 – CODICE ISO IT03804370249 – R.E.A. VI 355429– CAP.SOC. 100.000 EURO INT.VERS.
Società soggetta a direzione e coordinamento da parte di Cereal Docks S.p.A. ex art.2497 C.C

INDEX

1. INTRODUCTION

Nateeo 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 undue delay in case of a personal data breach (including any notification to the competent Supervisory Authority and any communication to the data subject).

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 data subjects, 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 Supervisory Authority and/or the data subjects.

2. PURPOSE

The purpose of this procedure is to define the flow of activities for the management of infringements 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. DEFINITIONSERRORE. IL SEGNALIBRO NON È DEFINITO.

- *personal data* means any information relating to an identified or identifiable natural person ('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 (hereinafter referred to as "**Personal Data**");
- *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 (hereinafter referred to as "**Processing**);

- *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 Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law (hereinafter referred to as "**Controller**");
- *processor*, means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (hereinafter referred to as "**Processor**");
- *data subject*, means any identified or identifiable natural person (hereinafter referred to as "**Data Subject**");
- *data protection officer*, is a technical consultant appointed by the Controller, whose competencies are regulated by the GDPR (hereinafter referred to as "**DPO**" or "**RPD**");
- *team privacy*, is a group of persons appointed by the 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) (ii) managing the Organizational Model for the Protection of Personal Data adopted by the Controller;
  (iii) (iii) dealing with the DPO, where appointed;
  (hereinafter referred to as "**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 "Garante per la protezione dei dati personali") (hereinafter referred to as "**Supervisory 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** - " Modulo di comunicazione interna di Data Breach " 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 the following form of Annex **A** - " Modulo di comunicazione interna di Data Breach " 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 Data Subjects
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.);
- once these actions have been identified, who should act to contain the Breach;
- 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 data subject (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 data subjects, the Controller, assisted by the Privacy Team and the DPO, where appointed, will assess the seriousness of the breach by using Annex **B** - "Modulo di valutazione del rischio connesso al Data Breach" 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 Data Subjects 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 Data Subjects

Once the need to communicate the breach to the Data Subjects 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 Data Subjects 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 Data Subjects (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 Data Subject. 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 Data Subjects.

Step 5: Documentation of the Breach

Regardless of the need to notify the Authority (step 3) and/or the Data Subjects (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 "Schema di Registro delle violazioni dei dati personali" 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 processing	Period of retention
Internal and external Data Breach communication forms	(Art. 6, para. 1(c), GDPR) Processing necessary to fulfill a legal obligation to which the Controller is subject (Art. 6, para. 1(f), GDPR) Processing 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) Processing necessary to fulfill a legal obligation to which the Controller is subject (Art. 6, para. 1(f), GDPR) Processing 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) Processing necessary to fulfill a legal obligation to which the Controller is subject (Art. 6, para. 1(f), GDPR) Processing 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) Processing necessary to fulfill a legal obligation to which the Controller is subject (Art. 6, para. 1(f), GDPR) Processing 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 - Modulo di comunicazione interna di Data Breach" – *only Italian version*
- "B - Modulo di valutazione del rischio connesso al Data Breach" – *only Italian version*
- "C – Schema di Registro delle violazioni dei dati personali" – *only Italian version*

*Allegato "**A**" – Modulo di comunicazione di Data Breach*

Qualora sia rilevata una sospetta, presunta o effettiva violazione dei dati personali, è necessario darne immediata comunicazione al Titolare del trattamento mediante compilazione del modulo che segue da inviare a mezzo e-mail al seguente indirizzo: teamprivacy@cerealdocks.it

Comunicazione di Data Breach

Data di compilazione:	

□ **DESTINATARIO INTERNO ***

Dati della persona che fa la segnalazione:

Cognome e nome	
Incarico/Mansione	
Dati di contatto (indirizzo e-mail, numero di telefono)	

□ **DESTINATARIO ESTERNO ***

Dati del soggetto che fa la segnalazione:

Ditta\Ragione sociale	
Dati di contatto del DPO (ove nominato)	
Cognome e nome del soggetto segnalatore	
Dati di contatto (indirizzo e-mail, numero di telefono)	

* indicare, alternativamente, se il soggetto che fa la segnalazione è un Destinatario interno o un Destinatario esterno.

*****

DESCRIZIONE DELL'EVENTO

Data di scoperta della violazione (data, ora)	
Data e luogo della violazione (data, ora, luogo)	
Descrizione di cosa è successo	
Descrizione di come è successo	

*Allegato "**A**" – Modulo di comunicazione di Data Breach*

Categorie e numero approssimativo di interessati coinvolti nella violazione	
Altri dettagli rilevanti (eventuali azioni poste in essere al momento di scoperta della violazione ecc..)	

A cura del Titolare del trattamento (o del referente da esso incaricato)		**DATA E ORA RICEZIONE MODULO:**	
Modalità di ricezione:		N° Progressivo di segnalazione (da Registro Violazione Dati):	
Sistemi coinvolti:			
Vulnerabilità rilevate:			

*Allegato "**B**" – Modulo di valutazione del rischio connesso al Data Breach*

Assessment di gravità della violazione	Da compilare a cura del Titolare con l'ausilio del Team privacy, del DPO (ove nominato) ed eventualmente del Responsabile IT
Dispositivi oggetto del Data Breach (computer, rete dispositivo mobile, file o parte di un file, strumento di back up, documento cartaceo, altro).	
Modalità di esposizione al rischio (tipo di violazione): lettura (presumibilmente i dati non sono stati copiati), copia (i dati sono ancora presenti sui sistemi del titolare), alterazione (i dati sono presenti sui sistemi ma sono stati alterati), cancellazione (i dati non sono più presenti e non li ha neppure l'autore della violazione), furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione), altro.	
Breve descrizione dei sistemi di elaborazione o di memorizzazione dati coinvolti, con indicazione della loro ubicazione.	
Se il laptop o altro dispositivo mobile è stato perso/rubato: quando è stata l'ultima volta in cui il laptop è stato sincronizzato con il sistema IT centrale?	
Quante persone sono state colpite dalla violazione dei dati personali trattati nell'ambito della banca dati violata?	
Qual è la tipologia dei dati coinvolti nella violazione?	
La violazione può comportare pregiudizio alla reputazione, perdita di riservatezza di dati protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro dato economico o sociale significativo?	
Gli interessati rischiano di essere privati dell'esercizio del controllo sui dati personali che li riguardano?	
Quali misure tecniche e organizzative sono adottate ai dati oggetto di violazione? (i.e. pseudonimizzazione, cifratura dei dati personali ecc..)	
Il Titolare del trattamento ha adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati successivamente alla violazione?	
Classificazione della gravità della violazione (1-non grave, 2-grave o 3-molto grave) e motivazioni:	

*Allegato "**B**" – Modulo di valutazione del rischio connesso al Data Breach*

Notificazione del Data Breach all'Autorità Garante	Si/NO Se sì, notificato in data: Dettagli:
Comunicazione del Data Breach agli interessati	Si/NO Se sì, notificato in data: Dettagli:

NATEEO SRL
via dell'Innovazione 1
I – 36043 Camisano Vicentino (VI)
tel +390444419472
fax +390444419490
info@nateeo.it
www.nateeo.it

REGISTRO IMPRESE DI VICENZA CF/P.IVA 03804370249 – CODICE ISO IT03804370249 – R.E.A. VI 355429– CAP.SOC. 100.000 EURO INT.VERS.
Società soggetta a direzione e coordinamento da parte di Cereal Docks S.p.A. ex art.2497 C.C

*Allegato "**C**" – Schema di registro delle violazioni dei dati personali (cfr. file Excel)*

ID EVENTO	SEGNALAZIONE				VIOLAZIONE				
ID evento	data e ora	segnalante	unità organizzativa coinvolta	organi informati	luogo violazione	modalità violazione	sistemi/apparati/reti/ banche dati oggetto di data breach	natura della violazione dei dati personali	altri elementi utili alla descrizione violazione
eventuale codificazione interna per la rintracciabilità dell'evento	circostanze cronologiche della segnalazione	indicare se destinatari interni o esterni (cfr. all. A alla procedura di data breach)	indicare ufficio/unità organizzativa interessata dalla violazione	indicare ufficio/unità organizzativa destinataria della segnalazione	indicare, se ricorrenti, circostanze di luogo della violazione della sicurezza	descrivere il flusso delle azioni in cui è consistita la violazione	indicare le infrastrutture o gli applicativi coinvolti nelle violazioni	indicare se si tratta di violazione della riservatezza, delle integrità e/o della disponibilità dei dati	indicare ogni altra circostanza utile alla analisi della violazione
				indicare il livello superiore appropriato di gestione; la persona responsabile o alle persone incaricate di gestire gli incidenti, stabilire l'esistenza di una violazione e valutare il rischio				"**violazione della riservatezza**": divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali; "**violazione dell'integrità**": modifica non autorizzata o accidentale dei dati personali; "**violazione della disponibilità**": perdita, accesso o distruzione accidentali o non autorizzati di dati personali.	

INTERESSATI e DATI				CONSEGUENZE	RIMEDI		ATTENUAZIONE		TEMPI
categorie di interessati	numero approssimativo di interessati	categorie dei dati personali	numero approssimativo di registrazioni dei dati personali	conseguenze della violazione dei dati personali	misure adottate per porre rimedio alla violazione	misure di cui si propone l'adozione per porre rimedio alla violazione	misure adottate per per attenuare i possibili effetti negativi	misure di cui si propone l'adozione per attenuare i possibili effetti negativi	tempo ripristino
indicare in particolare se si tratta di soggetti vulnerabili	indicare un dato quantitativo, anche approssimato	indicare se si tratta di dati particolari, di dati relativi a condanne o reati, o altri tipi di dati	indicare un dato quantitativo, anche approssimato	indicare eventuali pregiudizi e danni materiali o immateriali-patrimoniali o reputazionali - patiti dagli interessati	indicare precauzioni già adottate che eliminano le conseguenze	indicare precauzioni in corso di adozione che eliminano le conseguenze	indicare precauzioni già adottate che riducono le conseguenze	indicare precauzioni in corso di adozione che riducono le conseguenze	indicare tempo della chiusura dell'espisodio della violazione
				ad esempio la perdita del controllo da parte degli interessati sui loro dati personali, la limitazione dei loro diritti, la discriminazione, il furto o l'usurpazione d'identità, perdite finanziarie, la decifratura non autorizzata della pseudonimizzazione, il pregiudizio alla reputazione e la perdita di riservatezza dei dati personali protetti da segreto professionale, nonché qualsiasi altro danno economico o sociale significativo					

NOTIFICA AL GARANTE				COMUNICAZIONE AGLI INTERESSATI				NOTE
rischio per i diritti e le libertà delle persone fisiche:	invio di notificazione all'Autorità	ragioni del ritardo della notificazione all'Autorità	ragioni di omessa notifica all'Autorità	indicare se ricorre rischio elevato per i diritti e le libertà delle persone fisiche	comunicazione agli interessati:	modalità della comunicazione agli interessati	ragioni della omessa comunicazione agli interessati	note
indicare improbabile/non improbabile	indicare si/no; in caso affermativo indicare data e ora; se totale o parziale; in tale caso, il numero ordinale della notifica (prima, seconda, ecc.) o se ultima	indicare circostanze relative all'accertamento della violazione che giustifichino il ritardo posteriore a 72 ore	indicare ragioni di improbabilità del rischio per glinteressati	indicare tipo di rischio e ragioni per cui tale rischio sia elevato	indicare si/no; in caso affermativo indicare data e ora; indicare se effettuata su ordine dell'Autorità	indicare mezzo di comunicazione utilizzato e modalità di assistenza agli interessati	(inserire una delle ipotesi di cui all'art. 34, par. 3, lett. a), b), c) Gdpr	note aggiuntive
considerare: 1) Tipo di violazione; 2) Natura, carattere sensibile e volume dei dati personali; 3) Facilità di identificazione delle persone fisiche; 4) Gravità delle conseguenze per le persone fisiche; 5) Caratteristiche particolari dell'interessato; 6) Caratteristiche particolari del titolare del trattamento di dati; 7) Numero di persone fisiche interessate; 8) Aspetti generali.		qualora non sia effettuata entro 72 ore, la notifica all'autorità di controllo deve essere corredata dei motivi del ritardo	ad esempio dati personali già disponibili pubblicamente, la cui divulgazione non costituirebbe un rischio probabile per la persona fisica; dati personali resi sostanzialmente incomprensibili ai soggetti non autorizzati e se esiste una copia o un backup; dati personali correttamente crittografati			La comunicazione agli Interessati dovrà essere scritta in un linguaggio chiaro e semplice e dovrà contenere: a) il nome e i dati di contatto del DPO (ove nominato) o di altro punto di contatto presso cui ottenere più informazioni; b) la descrizione delle probabili conseguenze della Violazione; c) la descrizione delle le misure adottate o di cui il Titolare propone l'adozione per porre rimedio alla Violazione e, se del caso, per attenuarne i possibili effetti negativi. Quanto alle modalità di comunicazione, caso per caso, il Titolare dovrà sempre privilegiare la modalità di comunicazione diretta con i soggetti interessati (quali email, SMS o messaggi diretti). Il messaggio dovrà essere comunicato in maniera semplice e trasparente, evitando quindi di inviare le informazioni nel contesto di newsletter, che potrebbero essere facilmente fraintese dagli Interessati. Nel caso in cui la segnalazione diretta richieda uno sforzo ritenuto sproporzionato, allora si potrà utilizzare una comunicazione pubblica, che dovrà essere ugualmente efficace nel contatto diretto con l'interessato.	ad esempio,a seconda dei casi: cifratura allo stato dell'arte oppure mediante tokenizzazione;immediata individuazione e avvio di un'azione contro il soggetto che ha avuto accesso ai dati personali prima dell'utilizzo; comunicazione pubblica o prevedere l'adozione di disposizioni tecniche per rendere le informazioni sulla violazione disponibili su richiesta	