PROCEDURE IN CASE OF A PERSONAL DATA BREACH OR DATA LEAK

1. INTRODUCTION

Arthur Vandendorpe NV gives great importance to the protection of personal data and the protection of confidential information. The Company takes seriously its obligations with respect to the General Data Protection Regulation.

The Company insists that all its collaborators who come into contact with personal data and confidential information process it with the utmost care.

This policy applies to any person who, in any manner whatsoever, enters into contact, due to the performance of their duties, with confidential information (business secrets, professional information) or with data which may be considered as personal data within the meaning of the General Data Protection Regulation (e.g. the personal data of clients, suppliers and third parties). This Policy applies to all collaborators of the Company, including members of the Board of Directors, management members, independent employees, temporary workers, student job seekers and trainees (hereinafter: the “Collaborator”).

Through this Policy, the Company intends to inform Collaborators of the manner in which personal data and confidential information must be managed, in order to minimise as far as possible the risk of possible breaches. The Collaborator is bound to respect scrupulously the instructions below.

2. ACCESS

In performing its duties, the Collaborator has access to confidential information and personal data. Such confidential information and personal data may only be used to the extent necessary for the exercise of its duties. The Collaborator will ensure that confidential information and personal data are not shared with unauthorised persons (including unauthorised colleagues).

The Collaborator further agrees not to take cognisance of confidential information and personal data which it knows or should know it does not have the right to access.

The Collaborator will never use confidential information and personal data to the detriment of the Company.

3. OBLIGATIONS AND RESPONSIBILITIES

The Collaborator will always process confidential information and personal data with care and diligence. In particular, the following obligations and responsibilities apply:

Professional documents or filing systems may only be stored on systems provided for this purpose;

Professional documents or filing systems shall never be forwarded to a private mailbox or to a third party, unless this is essential for the performance of the activities of the Company;

All collaborators are responsible for the correct and careful management of passwords: passwords must be sufficiently complex, they should not be obvious and must be changed regularly (at least every six months);

Their PC/laptop must be locked with a password when the Collaborator plans to be absent for at least two hours. The computer must be completely turned off at the end of the workday;

We strive to apply a “clean desk policy”. Files containing confidential information or personal data must be removed from the office desk at the end of the work day and properly stored;

In the context of the “clean desk policy”, laptops, tablets, smartphones, USB sticks or other equipment must be stored and locked up in case of non-use and at the end of the day;

The printing of documents is processed confidentially, which means, among other things, that the Collaborator intending to print documents must use its follow me badge (the user cannot execute the print job without being physically present at the printer), that the printed documents cannot remain on the printer, and the Collaborator will only read documents that he himself sent to the printer; Confidential information and personal data will never be thrown away with ordinary paper waste; instead, the paper shredder provided for this purpose must be used;

Confidential information and personal data will be transported outside the Company as little as possible. The transport of documents must be strictly limited to the needs of the duties, such as meetings;

Collaborators will take all necessary steps to ensure that confidential information and personal data are not stolen or misplaced. No possible media, such as paper files, laptop, tablet, smartphone, USB stick, etc. shall be left unattended or in unsafe conditions outside the workplace (e.g., in the car). Should a Collaborator nevertheless be confronted with the loss or theft of one of these media, he will inform his manager or the data protection officer within six hours after becoming aware of this fact;

When using a Wi-Fi connection, the Collaborator will make sure that it is secure. Unsecured networks should never be used;

Any security issue or data leak, as well as the loss or theft of a laptop, tablet, USB stick, smartphone, etc., should be reported immediately and at most within six hours of its discovery, in accordance with the data leak procedure described in this Policy;

4. PROCEDURE IN CASE OF A PERSONAL DATA BREACH OR DATA LEAK

This procedure applies to any Collaborator who finds or suspects a breach of a personal data.

For the purposes of the General Data Protection Regulation (GDPR), a breach of personal data or a data leak is “a breach of security resulting in accidental or unlawful destruction, loss, tampering, unauthorised disclosure of personal data transmitted, stored or otherwise processed”.

The concept is to be taken broadly and includes the following data leaks:

- hacking / phishing / ransomware;
- offline data leak (paper tray, printer...);
- e-mail sent to an incorrect e-mail address;
- theft or loss of a USB stick;
- theft or loss of a paper file;
- theft or loss of a mobile phone, laptop, tablet;
- decrease or disappearance of accessibility (e.g. server failure).

The concept of personal data is to be understood in accordance with the General Data Protection Regulation (e.g. personal data of customers, suppliers, workers, third parties). In case of doubt as to whether or not an item constitutes personal data, the Collaborator will immediately contact the person or persons within the Company) who is responsible for data protection (currently: Natalie Verheyden, nve@vanlaere.be)
In the event of a data leak, the following procedure must be followed:

Phase 1 – Internal notification

The Collaborator observing a (possible) data leak informs immediately and at the latest within six hours of its discovery, Private Data Officer.

This notification will be made by telephone if possible, and in any case (also) by e-mail. In his e-mail, the Collaborator will mention at least: 1) the nature of the data leak (e.g., loss, no more access, breach of confidentiality); 2) the personal data involved; 3) the possible cause (e.g., hacking, loss, theft).

Phase 2 – Evaluation, consultation and recording in an internal register

The Private Data Officer reviews the notification upon receipt and makes an assessment based on the nature of the leak and the personal data concerned, as well as the cause and consequences of the data leak. This procedure is also applicable if a person performing the processing informs the Company of a data leak.

- **First case**: no data leak/no personal data/no risks

  If the notification does not involve a data breach, if no personal data has been leaked or if the data leak poses no risk to the rights and freedoms of the data subject, the Private Data Officer will report the internal notification to a member of the Company's management, will save the data leak in the internal register of the Company and inform the Collaborator. In this case, the process ends here.

- **Second case**: risks to data subjects or to the Company

  If the data leak includes personal data and poses a risk to the rights and freedoms of the data subject, or if the data leak creates risks or considerable impact on the Company (e.g. Impact on IT infrastructure, acts of malice, leakage of sensitive data or in large volumes), the Private Data Officer will immediately contact a member of the Company's management to discuss and assess the data leak (e.g. consequences for individuals and the Company, measures to restrict the consequences thereof and to avoid them in the future). If necessary, the Private Data Officer will bring together a crisis team, composed of: a member of the Company's management and, if applicable, others who may be useful to the consultation (e.g. Head of IT, CISO, external, etc.). A report on this consultation will be established, and the data leak will also be recorded in the internal register of the Company. If no risk is noted for the rights and freedoms of the data subject, the process ends here. Otherwise, Phase 3 begins.

Phase 3 – Notification to the Data Protection Authority (APD)

If a risk is noted for the rights and freedoms of the data subject, the Private Data Officer will communicate, after consulting with a member of the Company's management, the data leak to the Data Protection Authority. This communication is done using the form provided on the website of the Data Protection Authority.

The notification shall be made without delay and no later than 72 hours after discovery of the leak. If notification occurs later or only partially, it is necessary to provide a justification.

The notification will include the required data provided for in Article 33 of the General Data Protection Regulation: the nature of the data leak, the categories and number of data subjects; the categories and the volume of personal data (if possible); the possible consequences of the data leak, and the measures implemented to remedy the data leak and to avoid or reduce the effects of the data leak.

If the data leak does not lead to a major risk to the rights and freedoms of the data subject, the process ends here. Otherwise, Phase 4 begins.

Phase 4 – Notification to the data subjects

In the event of an increased risk to the rights and freedoms of the data subject(s), the data leak is in principle promptly disclosed to the data subject(s) concerned. In accordance with Article 34 of the General Data Protection Regulation, this communication sets out, in clear and simple terms, the nature of the data leak, its probable consequences and the measures implemented to remedy the data leak and to avoid or reduce the consequences.

However, this notification will not be necessary if technical and organisational measures have been taken to render the data unreadable (e.g. encryption, cryptography) or if steps have been taken to ensure that the high risk to the rights and freedoms of the data subject(s) no longer occurs.

Every time data is leaked, every effort is made to carry out the necessary measures and any necessary technical and organisational measures (e.g. vigilance points for the future, reducing the causes, repairing breakdowns and systems, eliminating infections). The Private Data Officer ensures their correct execution and the subsequent follow-up. All this is assessed and documented.

If a data leak is to be reported to the Data Protection Authority, the Private Data Officer prepares a report that reflects the nature of the data leak, the procedures implemented, the actions taken, the data subjects and the vigilance points for the future. Following approval by a member of the Company’s management, the Private Data Officer sends this report to the person or body responsible for the management of the Company.