Nebu B.V.
Pakhuisplein 42 V
1531 MZ Wormer
The Netherlands
T: + 31 251 311 413
E: nebu@nebu.com
W: www.nebu.com

Nebu Data Protection Policy

Reference	:	Nebu - ISO - 2018 - 0075
Version	:	1.0
Date	:	May 14, 2018
Owner	:	Zoltan Szuhai
Validation:	:	Otto van Linden
Status	:	Final

CONTENTS

Version Control			
Version	Status	Date	Change Log
V1.0	Final	May 14, 2018	-

1 Introduction

In order to fulfill its business purpose, Nebu needs to gather and use certain information about individuals.

Individuals can include customers, suppliers, business contacts, employees and other people the organization has a relationship with or may need to contact.

This policy describes how information on these individuals, i.e. personal data[1], is collected, handled and stored to meet the company's data protection standards and to comply with the law.

This data protection policy ensures Nebu:

- Complies with GDPR and follows good practice
- Protects the rights of employees, customers and partners
- Is open about how it stores and processes individuals' personal data
- Protects itself from the risks of a data breach

2 The General Data Protection Regulation (May 25th 2018)

Nebu adheres to the principles of the European General Data Protection Regulation. In accordance with these principles personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed
- Accurate and, where necessary, kept up to date.
- Kept no longer than is necessary for the purposes for which the personal data is processed.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures
- Not transferred outside the countries of the European Economic Area without adequate protection.

Read the full policy :
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG

[1] ***Personal Data*** *- all the information collected from an individual that can be used to identify him or her (for instance a credit card number, a telephone number, physical information or simply a name.)*

3 Policy Scope

This policy applies to:

- The head office of Nebu B.V
- All branches of Nebu B.V.: Nebu Hungary KFT, Nebu United Kingdom B.V.
- All employees of Nebu B.V. and its branches
- All resellers, contractors, suppliers and other people working on behalf of Nebu B.V and its branches.

It applies to all data that the company holds relating to identifiable individuals, even if that information was collected before the GDPR came into effect.

4 Responsibilities

Everyone who works for or with Nebu has the responsibility to ensure data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, the following people have key responsibilities:

1. The company board is ultimately responsible for ensuring that Nebu meets its legal obligations.

2. The data protection/compliance officer is responsible for:
   - Keeping the company circle updated about data protection responsibilities, risks and issues.
   - Reviewing all data protection procedures and related policies
   - Arranging data protection training and advice for the people covered by this policy.
   - Handling data protection questions from staff and anyone else covered by this policy.
   - Dealing with requests from individuals about the data Nebu holds on them, also referred to as ‘Subject Access Requests (SAR)’).
   - Checking and approving any contracts or agreements with third parties that may handle the company’s sensitive data.

3. The Director Research & Development, is responsible for:
    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
    - Performing regular checks and scans to ensure security hardware and software is functioning properly.
    - Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.

4. The Head of Marketing, is responsible for:
    - Reviewing all data protection statements attached to communications such as forms, emails and letters.
    - Addressing any data protection queries from journalists or media outlets
    - Where necessary, working with other member of staff to ensure marketing and business initiatives abide by data protection principles.

5 Data audit and register

Regular data audits to manage and mitigate risks will be conducted and documented in the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

6 Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to Compliance Officer.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot access it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people could access them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees.

- If data is stored on removable media, these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.

All servers and computers containing data should be protected by approved security software and a firewall.

7 Data Use

It is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft, therefore organizational measures should be taken to ensure protection of the data:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally
- Personal data must be encrypted before being transferred electronically. The Compliance Officer can explain how to send data to authorized external contacts.
- Personal data should never be transferred outside of the European Economic Area, if not previously agreed and authorized to do so.
- Employees should not save copies of personal data to their own computers.

8 Data Accuracy

The law requires Nebu to take reasonable steps to ensure data is kept accurate and up to date.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Employees should not create any unnecessary additional data sets.
- Employees should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
- Nebu will make it simple for data subjects to update their information.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

9 Subject Access Policy

All individuals who are the subject of personal data held by Nebu are entitled to:

- Ask what information the company holds about them and why.
- Ask for the suppression or modification of their data.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.

If an individual contacts the company requesting this information, this is called a subject access request (SAR).

10 Disclosing Data for Other Reasons

In certain circumstances, the GDPR allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Nebu will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the Data Protection/Compliance Officer and from the company's circle where necessary.

11 Providing Information

Nebu aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the company has a privacy statement, setting out how data relating to individuals is used by the company.

A version of this statement is also available on the company's website.

12 Glossary: Terms and Definitions used in relation to the GDPR

Consent- explicit approval from the data subject to the collection and processing of his/her data.

Data Controller - any entity, public authority, company or person who decides why, how and what data needs to be collected and processed.

Data Portability - the requirement for controllers to provide the data subject with a copy of his or her data in a format that allows for easy use with another controller.

Data Processor - the entity that processes data on behalf of the Data Controller

Data Protection Authority - national authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the EU.

Data Protection Officer - an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR.

Data Subject - a natural person (yourself for instance) whose personal data is processed by a controller or processor

Encrypted Data - personal data that is protected through technological measures to ensure that the data is only accessible/readable by those with specified access

Personal Data - all the information collected from an individual that can be used to identify him or her (for instance a credit card number, a telephone number, physical information or simply a name)

Personal Data Breach - a breach of security leading to the accidental or unlawful access to, destruction, misuse, etc. of personal data

Privacy by Design - a principle that calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition

Privacy Impact Assessment - process of evaluation of the risks and the level of protection of your personal data.

Processing - any operation performed on personal data, whether or not by automated means, including collection, use, recording, storage etc.

Profiling - automated processing of personal data in order to evaluate, analyse or predict the future behavior of a person.

Pseudonymisation - way of processing data so that it cannot be attributed to its owner without additional information, separated from the pseudonymised data.

Right to be Forgotten - also known as **Data Erasure**, it entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties cease processing of the data

Right to Access - also known as **Subject Access Right**, it entitles the data subject to have access to and information about the personal data that a controller has concerning them

Sensitive personal data - the GDPR refers to sensitive personal data as “special categories of personal data.” The special categories of data include racial or ethnic origin, political opinions, religious or philosophical views, trade union membership, sexual orientation, and health, genetic and biometric data where processed to uniquely identify an individual. Personal data relating to criminal convictions and offenses are not included, but similar extra safeguards apply to its processing.

Supervisory Authority - a public authority which is established by a member state in accordance with article 46

Third party - any entity, person, company or country who is involved in the handling of the data outside the data subject, the controller, the processor or an EU entity.