Data Protection Statement

GDPR

Author	Nobby Vanheyst
Approval (Needed?: ☐Yes/☐No)	---
Version	V1.0
Classification	☐Intern, ☐Beperkt, ☒Extern, ☐Vertrouwelijk
Date Last change	26/11/2020
Document reference	---
Pages	5

Date	Version	Created By	Description	Approved?
26/11/2020	V1.0	Nobby Vanheyst	Document created	

INDEX

1 INTRODUCTION 4
2 ORGANISATIONAL MEASURES 4
3 LEGAL MEASURES 5
4 TECHNICAL MEASURES 5

1 Introduction

On 25 May 2018, the General Data Protection Regulation (GDPR) came into force. This European Regulation imposes a number of strict obligations and rules in the context of the protection of personal data and must be seen as a deepening of the existing data protection regulations.

In the meantime, this regulation has also been converted into a law at the national level, namely the Act of 30 July 2018 on the protection of natural persons with regard to the processing of their personal data (Wet betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van hun persoonsgegevens van 30 juli 2018).

In accordance with the applicable regulations in the context of privacy and the protection of personal data, Fabry International Network guarantees a qualitative level of data and data security by taking all necessary and reasonable technical and organizational measures.

Fabry International Network wants to inform its customers, contacts, suppliers or any other interested party in this respect to the maximum extent possible.

One year after the date of application, it is therefore appropriate to look back at the measures taken by the Fabry International Network.

2 Organisational measures

1. Fabry International Network has drawn up an extensive privacy policy, in which both external and internal explanations are provided regarding the personal data processed by Fabry International Network. In these privacy policies, the rights of the persons involved, the security and the retention policy were extensively put forward.

2. All employees were informed and made aware by Fabry International Network during a roadshow and training sessions. The finger is kept on the pulse by drawing up policies and procedures and employees must take part in internal information sessions and periodic training courses.

3. An internal/external Data Protection Officer has been appointed, ADDITIONS of Intigio BV, in Fabry International Network and an internal privacy team has been set up, to be reached via privacy@fabrynetwork.org.

4. Fabry International Network undertakes to give due consideration to the rights of data subjects when implementing or developing any new project and, if necessary, to carry out a Data Protection Impact Assessment (DPIA).

3 Legal measures

1. The employment contracts, the employment regulations and other internal policies for our internal employees contain provisions with regard to the confidentiality and protection of privacy with regard to data entrusted to us in the context of our assignment. These documents have been updated where necessary to comply with GDPR requirements;

2. Processing agreements have been drawn up in order to correctly encapsulate the transfer of data to our suppliers who are processors within the meaning of GDPR.

3. Clauses relating to privacy, security and protection of personal data in contracts and other documents exchanged with customers have been and will be strictly adhered to and evaluated at all times.

4. Fabry International Network insists that any other parties who are also data controllers also submit a GDPR statement, so that there too guarantees are offered in connection with the GDPR in accordance with the processing of personal data.

4 Technical measures

1. Multiple backups per day that are written encrypted to physically separated locations. This also includes writing to a cloud backup storage that has also been duplicated.

2. Access to internal systems is protected by a personal password that is changed on a regular basis and has to meet a certain complexity. Access to data is determined in terms of function and what is effectively needed to be able to perform the function.

3. On a frequent basis, all software and systems are updated for security and performance reasons.

4. Each device is equipped with an anti-virus that retrieves current threats and information from a global database.

5. E-mail passes through an anti-spam filter before it is delivered to the user. Here, too, a global database is used.