

# Data Processing Agreement

## The Undersigned:

1 ..... , having its registered office and place of business in..... , for the purposes hereof duly represented by Mr/Ms ..... , in the capacity of ..... , hereinafter referred to as: **“the Principal”** or **“the Controller”**,

and

2. the private company with limited liability **IT&Care B.V.**, registered at Eindhoven, the Netherlands, and having its registered office at Science Park 5127, 5692 ED Son, the Netherlands, for the purposes hereof duly represented by Mr F. Torqué, in his capacity of Managing Director, also referred to hereinafter as: **“IT&Care”** or **“the Processor”**,

hereinafter individually referred to as **“Party”** and jointly as **“the Parties”**.

## whereas:

- in the context of being a good employer, the Principal wishes to monitor and promote the health, competences and motivation of its employees in order to keep its employees permanently employable during their employment at the Principal;
- the Principal in that receives support from ArboNed B.V., a certified services and healthcare provider that focuses on the sustainable employability of employees during their working lives (hereinafter: **“ArboNed”**);
- the Principal and ArboNed have entered into an agreement for the provision and execution of the aforementioned services (hereinafter: **“the ArboNed Agreement”**), and in that make use of the ICT infrastructure of IT&Care, a party that develops and provides integral web-based software applications to employers, employees and healthcare providers, in which confidentiality, integrity and availability of data are optimally guaranteed;
- the Principal more specifically makes use of the employer portal that is only accessible for himself (hereinafter: **“the Employer Portal”**), in which data of employees of the Principal are processed, including personal data of those employees (hereinafter: **“Personal Data of Employees”**);
- IT&Care on behalf of the Principal acts as Processor of the Personal Data of Employees that are processed via the Employer Portal;
- IT&Care on instruction of the Principal looks after the provision to ArboNed of the Personal Data of Employees required for the execution of the ArboNed Agreement;
- the Parties are held to comply with the provisions of the General Data Protection Regulation, in particular the Articles 28 and 32 of the General Data Protection Regulation, and in that context conclude the present Data Processing Agreement to record the agreements they have made regarding the processing of Personal Data of Employees (hereinafter: **“the Data Processing Agreement”**);

## agree the following:

### **Article 1. Definitions**

1.1 The terms “Personal Data”, “Processing”, “Controller”, “Processor”, “Data Subject” and “Third Party” as included in article 4 of the General Data Protection Regulation (hereinafter: **“GDPR”**) have the meaning given thereto in the GDPR. These are written with a capital letter in this Data Processing Agreement. Other terms written with a capital letter have the meaning given thereto in this Data Processing Agreement.

- 1.2 Personal Data of Employees means: all information about an identified or identifiable employee, as referred to in article 4 sub 1 of the Data Protection Regulation, that the Principal processes in the Employer Portal.
- 1.3 'Principal' shall also mean the affiliated companies of Principal where ArboNed also provides services to such affiliated companies in accordance with the ArboNed Agreement.

#### **Article 2. Purpose and necessity of the Processing**

- 2.1 Via the Employer portal, the Client performs comprehensive, up-to-date employee administration that allows it to execute its legal obligations concerning reintegration, absenteeism and sustainable employability, as well as ensure occupational health care for its employees, which includes providing associated health management, administration and reports. Employees' essential personal data must also be communicated to ArboNed for the execution of the contract in accordance with the applicable laws and regulations. These legal obligations arise inter alia from the Dutch Working Conditions Act and the Eligibility for Permanent Invalidation Benefit Restrictions Act.
- 2.2 IT&Care shall process Personal Data of Employees only for the purpose as described in Article 2.1 and only to the extent that the processing is necessary to meet that purpose.
- 2.3 The Parties acknowledge and confirm that the GDPR is applicable to the Processing of Personal Data of Employees via the Employer Portal, and that they are both aware of the obligations laid down in the GDPR. The Parties are each individually and independently held to ensure that the aforementioned obligations will be complied with.
- 2.4 The Parties will in good time provide each other with all necessary cooperation to enable proper compliance with the GDPR and the other applicable privacy laws and regulations.

#### **Article 3. Processing of Personal Data of Employees by IT&Care**

- 3.1 IT&Care is to be regarded as "Processor" and Principal as "Controller" as defined in the GDPR.
- 3.2 IT&Care shall process Personal Data of Employees only on instruction of the Principal, in accordance with its instructions and under its responsibility, and with due observance of the provisions of the End User License Agreement that the Principal concludes with ArboNed as part of the ArboNed Agreement for the use of the Employer Portal. IT&Care shall have no control over the purpose of and the means for the processing of the Personal Data.
- 3.3 The Personal Data of Employees shall only be stored and processed in the Netherlands.
- 3.4 The Processing of Personal Data of Employees by IT&Care is further elaborated in the Privacy Statement of IT&Care, which can be consulted via the website [www.itandcare.nl](http://www.itandcare.nl).

#### **Article 4. Categories of Personal Data and Data Subjects**

- 4.1 IT&Care can process the following categories of Personal Data of Employees for the Principal:
  - Personal Data, including:
    - a. Name and address;
    - b. E-mail address;
    - c. Phone number;
    - d. Date of birth;
    - e. Gender;
    - f. Nursing address of the sick employee;
    - g. Employee ID<sup>1</sup>;

---

<sup>1</sup> This means the Employee ID or any other coding specifically belonging to an employee that replaces the Citizen Service Number as a key value, as described in the National Absenteeism Standard ("NVS") 2017. This standard is endorsed by health and safety services affiliated with the branch association OVAL and is managed by Stichting Sivi.

- Specific Personal Data, including:
  - a. Health data, such as the date that the employee was reported sick, the date of the recovery notification, the probable duration of the absenteeism, whether one of the fall-back provisions of the Sickness Benefits Act ('Ziektewet') applies, whether the employee falls under the Work and Income according to Labour Capacity Act ('Wet Werk en Inkomen naar Arbeidsvermogen') or whether a sick employee was involved in a traffic accident;
  - b. Uniquely identifying personal data
- 4.2 The Data Subjects to which the Personal Data of Employees relate are in any case:
  - a. Employees;
  - b. Former employees.

#### **Article 5. Provision of Personal Data of Employees from the Employer Portal to ArboNed**

- 5.1 For the implementation of the ArboNed Agreement, IT&Care will at the Principal's request provide Personal Data of Employees to ArboNed, if and insofar as this is necessary and if there is a legal basis for doing so.
- 5.2 As a healthcare provider, ArboNed provides occupational health care to employees of the Principal, depending on the agreed services in the ArboNed Agreement, in order to keep them permanently employable during their working life. In the context of the medical monitoring and supervision of employees, ArboNed makes files of those employees to which it provides healthcare. In order to be able to comply with this statutory file requirement, ArboNed via the Employer Portal obtains the necessary Personal Data of Employees at the time that it provides or starts providing healthcare to employees of the Principal.
- 5.3 From the moment that Personal Data of Employees have been made available to ArboNed, ArboNed will be the Controller with regard to these Personal Data of Employees. The way in which ArboNed processes the Personal Data of Employees is described in the privacy regulations of ArboNed, which is available via the website [www.arboned.nl](http://www.arboned.nl).

#### **Article 6. Secrecy**

- 6.1 IT&Care shall be held to keep the Personal Data of Employees secret, except insofar as:
  - a. IT&Care is permitted to provide the Personal Data of Employees to ArboNed pursuant to the provisions of the Processor Agreement, or
  - b. a legal provision requires IT&Care to disclose Personal Data of Employees, or
  - c. the provision of Personal Data of Employees takes place on instruction of the Principal;
  - d. the provision of Personal Data of Employees is logically necessary in view of the nature of the services provided by IT&Care to the Principal.
- 6.2 IT&Care will impose on its employees who in the context of the Processing of Personal Data of Employees work with the Personal Data of Employees the same secrecy obligation as stated in this article.
- 6.3 The obligation of confidentiality included in this article shall apply independently from the duration of this Data Processing Agreement as specified in article 13, and will continue to exist after the termination of the Data Processing Agreement. The obligation of confidentiality shall not apply to Personal Data of Employees that have already become publicly known, other than as a result of a violation of the aforementioned obligation of confidentiality.

#### **Article 7. Security Measures**

- 7.1 In accordance with article 28 of the GDPR, the parties are responsible for the protection of Personal Data and the privacy of the Data Subject(s) concerned. IT&Care shall take appropriate technical and organizational protection measures to safeguard the confidentiality, integrity and availability of the Personal Data of Employees, as well as to guarantee the rights of the Data Subject(s). In the measures to be taken, IT&Care shall take into account the state of the technology, the implementation costs, the nature, scope, context and processing objectives and the risks for the rights and freedoms of the Data Subject(s) concerned.

- 7.2 IT&Care is ISO 27001 and NEN 7510 certified. The organizational and protection measures that it takes to implement the provisions of article 7.1 have been included in the Declaration of Applicability. These include the following measures:
- a. of Personal Data of Employees a real-time backup will be made, so that loss of Personal Data of Employees is prevented;
  - b. the backups mentioned under a. will be stored at a physically separated (fire) safe location;
  - c. the Employer Portal is placed in a twin data centre concept in order to be able to guarantee high availability;
  - d. IT&Care makes provisions for adequate access security so that the Personal Data of Employees are only accessible for authorized personnel;
  - e. IT&Care has an adequate and up-to-date mechanism to detect and deter malicious software, including but not limited to computer viruses;
  - f. penetration tests will regularly be carried out by external parties to test the systems for possible vulnerabilities;
  - g. IT&Care will use secure network connections.

#### **Article 8. Cooperation with Sub-Processors**

- 8.1 IT&Care uses Sub-Processors, listed in the Annex to the Data Processing Agreement. Principal agrees to the use of these Sub-Processors. If IT&Care uses other Sub-Processors, it will notify the Principal thereof. IT&Care will as Processor of the Principal remain fully responsible for the Processing of Personal Data of Employees by Sub-Processors.
- 8.2 If Sub-Processors are called in, IT&Care will enter into a Sub-Processor Data Processing Agreement in which these Sub-Processors will be given the same responsibilities and obligations regarding data processing and protection as those included in the Data Processing Agreement.

#### **Article 9. Data Breach Procedure**

- 9.1 Despite the technical and organizational measures taken on the part of IT&Care, a breach in connection with the Personal Data of Employees may occur by which the Personal Data of Employees have actually been destroyed or lost, have been changed, provided or have been made accessible in a way that is unlawful (hereinafter: **"Data Breach"**).
- 9.2 A Data Breach will be reported to the Principal in writing by IT&Care as soon as possible and in any case within 24 hours after discovery thereof.
- 9.3 After prior consultation with IT&Care, the Principal shall assess whether the Data Breach has to be reported to the Dutch Data Protection Authority, and possibly to the Data Subject(s). The responsibility for the (correct, timely and complete) report to the Dutch Data Protection Authority and possibly to the Data Subject(s) within the applicable legal time period lies with the Principal. If the Principal intends to report a Data breach to the Dutch Data Protection Authority and/or Data Subject(s), it will inform IT&Care thereof.
- 9.4 IT&Care shall at all times have the right to weigh independently whether it should report the Data Breach to the Dutch Data Protection Authority and possibly to the Data Subject(s).
- 9.5 IT&Care shall in any case provide the information about the Data Breach that the Principal needs in order to be able to comply with the aforementioned notification obligation(s), including:
- a. the nature of the breach, where possible stating the categories of Data Subjects and personal data registers and an estimate of the number of Data Subjects and personal data registers concerned;
  - b. if this is clear to IT&Care, the likely consequences of the Data Breach, such as loss of control of the Personal Data of Employees by Data Subjects, and the inability of Data Subjects to exercise their rights;
  - c. measures taken by IT&Care to limit the possible adverse consequences of the Data Breach.
- 9.6 IT&Care will keep the Principal informed of any new developments concerning the Data Breach and of the measures that IT&Care will take to limit the consequences of the Data Breach and to prevent repetition.

#### **Article 10. Audit**

- 10.1 IT&Care is ISO 27001 and NEN 7510 certified, and is audited annually in this context. If the Principal nevertheless wishes to have the compliance with this Processor Agreement checked by means of an audit, it is entitled to do so after consultation with IT&Care. An audit will only be carried out by an independent competent authority that is authorized for that purpose.
- 10.2 An audit takes place after the Principal has reached an agreement in writing with IT&Care about the time and scope of the audit, as well as about the competent authority that will perform the audit. The costs of the audit will be borne by the Principal.
- 10.3 With due observance of the provisions of this Article, IT&Care will provide its cooperation to an audit and make all information relevant to the audit available in a timely manner at the location where the audit is carried out.
- 10.4 The competent authority that carries out the audit will conform to the security procedures in force at IT&Care.
- 10.5 An audit must not unnecessarily disrupt the business activities of IT&Care.

#### **Article 11. Requests from Data Subjects**

- 11.1 IT&Care shall provide to the Principal all reasonable cooperation to ensure that the Principal can comply with the obligations under Chapter III of the GDPR within the statutory time limits. IT&Care can request a reasonable cost reimbursement for this, which will be reimbursed by the Principal.

#### **Article 12. Liability**

- 12.1 If a Party imputably fails to fulfil its obligations under this Data Processing Agreement, the GDPR and/or any other laws and regulations in the field of Processing of Personal Data, that Party shall be liable for the damage suffered by the other Party as a result thereof.
- 12.2 The liability of the Parties is limited to direct damage and to the maximum amount paid by the insurer of the Party that has been made liable.

#### **Article 13. Duration and termination of the Data Processing Agreement**

- 13.1 The Data Processing Agreement will be in force and effect during the term of the ArboNed Agreement. If the abovementioned ArboNed Agreement ends, this Data Processing Agreement also ends automatically.
- 13.2 Neither Party can terminate the Data Processing Agreement in the prematurely.
- 13.3 After termination of the Data Processing Agreement, IT&Care shall within a reasonable period of time ensure the removal of Personal Data in its systems, or return of the Personal Data of Employees to the Principal in a manner to be agreed by the Parties, unless there is a legal obligation for IT&Care to keep Personal Data of Employees in its possession.

#### **Article 14. Applicable Law and Disputes**

- 14.1 This Data Processing Agreement shall only be governed by Dutch law.
- 14.2 All disputes (including disputes that are only considered to be a dispute by one of the Parties) arising from the Processor Agreement will be submitted to the competent court in the court district of Oost-Brabant.

Thus agreed and drawn up in duplicate on \_\_\_\_\_

PRINCIPAL

IT&Care B.V.

\_\_\_\_\_



\_\_\_\_\_

F. Torqué  
Managing Director

**Annex to the Data Processing Agreement**

IT&Care is currently working with three sub-processors, regarding supporting IT processes for ArboNed BV, Fiqas Software B.V. (Fiqas) Byelex B.V (Byelex) and DataManagement Professionals B.V. (DMP). Fiqas and Byelex are used for the development of new applications To ensure the safe storage of (personal) data, backups of IT&Care are stored at DMP. DMP is ISO27001 certified and has conformed to high (security) requirements so that careful storage of backups is guaranteed. The backups received by DMP contain only encrypted data. Therefore, the data is not visible for DMP.