Directive on the General Data Protection Regulation of the European Union (GDPR)

1. Introduction

1.1. Purpose of the Directive

This internal Directive shall set out the rules within the Company in order to comply with the GDPR and to prevent the introduction of a similar regulation in Switzerland.

1.2. Scopes of Application

This internal Directive shall apply to the whole company, except entities that have no commercial contacts with UE Member States or Switzerland, namely entities Rollomatic Inc., as well as the Company's Asian entities. This Directive shall also apply to processors processing and storing personal data in the exact same way.

1.3. Definitions

Data	Information relating to an identified or identifiable natural person. Any information relating to an identified or identifiable natural person are concerned, including data, which have been pseudonymised but could be attributed to a natural person by the use of additional information.
Processing	Any operation, which is performed on personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Active Processing	Any operation, which goes beyond the reception without request and preservation of a track generated automatically in a computer system.

2. Directives

First, the directive describes principles adopted by the Company to ensure compliance with the GDPR (below under figure 2.1.). Second, the Directive describes for each steps rules to meet GDPR's requirements (below under figure 2.2.).

2.1. Principles

In order to comply with the requirements of the GDPR, the Company's data processing is based on the following principles:

- Harvesting storage and data processing shall be strictly limited to keep business running smoothly to rely on legitimate interests ;
- The Company does not actively process personal data. In other words, it does not carry on any commercial activity with such data collection. Personal data are only collected to support business activity needs ;
- Data processed by the Company are divided into the following three categories. These categories are provided for conveniently implementing the guidelines set out below regarding the nature of data :
    - **Data Employee and other data that stored in a system such as software (hereinafter "Basic Data")**

      Personal Data related to employee records, payroll and social insurance processing and accounting (including ERP system). In accordance with the GDPR, processing of employees' personal data is based not on an express consent or performance of a contract but on the legitimate interest.

- **Data from other people collected in connection with human resources procedures (hereinafter "HR related Data")**

  Job applicants' personal data collected for recruitment purposes.

- **Data from other persons collected in connection with commercial activities (hereinafter "Miscellaneous data")**

  Personal data related to employees of a legal entity (customers) collected within the framework of commercial exchanges.

- **Data passively collected (hereinafter "Passive data")**

  Personal data collected by emails or phone calls by the Company and store without any processing (email addresses, phone number, etc.).

- We implement all necessary means to ensure data security and systems

2.2. Detailed Directives

The following guidelines help to ensure compliance with the principles enacted by the GDPR.

a. Principle of Transparency

According to the GDPR, information and communication relating to data processing must be easily accessible, easy to understand and formulated in clear and simple terms. In particular, the person must be informed of the risks, rules, guarantees and rights related to data processing. GDPR provides also to data subject the guarantee to be informed about the modalities to exercise his rights (identity of the data controller, purpose of the treatment, right to obtain the confirmation and the communication of personal data concerned etc.).

This principle finds application as follows:

- **Basic data** collected as part of a recruitment process that results in a commitment, the employment contract provides information given in that present Directive ;

- **HR related data** collected as part of an unsuccessful recruitment are kept for a period of five years and then automatically destroyed. The job applicant is informed when the decision on his postulation is communicated and he can oppose to it. In this case, his data are deleted without any delay. In addition, it is specified that job applicant's data are collected only in relation to the position and limited to the useful information to determine the candidate's level of competence. For further information, candidates can find out about the data processing policy on the Company's website ;

- **Miscellaneous data**, include data collected during the registration of a user to the "Newsletter" of the Company, for a request to Wi-Fi access of the Company (in case of visit), or the program "MyRollomatic". These miscellaneous data are only subject to storage to allow a contact with the data subject or information taken by these people (through a login) on a portal made available by the Company. For more information about miscellaneous data, data subjects can consult the data processing policy on the website of the Company. It may be also be noted, they are informed of the processes when they subscribe to these tools ;

- **Passive data** being not actively processed, no other measures except the general security principle are provided.

b. Deadlines

According to the GDPR, a data retention period must be fixed and limited to the strict minimum (deadlines must be set for deletion or periodic review).

This principle finds application as follows:

- Retention of **Basic data** is required by a number of legal provisions and also useful in the interest of employees (e.g. personal data required for social insurances after the employee left the Company). These data are kept without time limit ;

- **HR related data** are automatically deleted after 5 years ;

- As it is not possible for the Company to determine whether **Miscellaneous data** are still useful or relevant (does the person still work for the customer or not?), this type of data is only deleted upon request ;

- **Passive data** being not actively processed, no other measures except the general security principle are provided.

c. Right of Access, to Rectification and to be forgotten

The GDPR provides that reasonable steps must be taken to ensure that inaccurate personal data are rectified or deleted. Modalities must be provided to facilitate the exercise of the rights conferred: the right of access without any charge to data, to request their rectification or erasure.

This principle finds application as follows:

- Each employee has the right to request at no cost access to his **Basic data** and the right to ask a rectification about his data. For the reasons mentioned above, an employee cannot ask to have his personal data erased ;
- Each unsuccessful candidate has the right to access to his **HR related data** and to request their rectification and erasure, without any charge;
- Each natural person whose data are kept has the right to request at no charge access to his / her **Miscellaneous data** and to request their rectification, as well as their erasure;
- **Passive data** being not actively processed, no other measures except the general security principle are provided.

d. Data Portability

According to the GDPR, the data subject has a right to transfer for free his / her personal data in a commonly machine readable format to another data controller.

This principle finds application as follows:

- The company grants this right to all concerned, for **Basic data**, **HR related data** and **Miscellaneous data** ;
- **Passive data** being not actively processed, no other measures except the general security principle are provided.

For any request, relating to the rights provided by the GDPR for personal data storage and processing, you can contact the data controller at the following email address: privacy@rollomatic.ch

3. Data Controller

The Data controller can be defined as the person, service or other body that is responsible for the treatment and who, alone or jointly with others, determines the purposes and means of the treatment.

According to the GDPR, the data controller shall designate in writing a representative in the Union

The Data controller must keep a record of processing activities carried out, which must contain information relating to the data controller, processing and the persons and data concerned.

In any case, you have the right to lodge a claim with the Supervisory Authority of the country in which you live against the data controller in case of non-respect of your rights in the processing of your personal data. For Switzerland, the competent Supervisory Authority is the Federal Data Protection and Information Commissioner.

3.1. Main Data Controller

Within the Company, the Board of Directors is the main Data controller. Within this Board, Head of Human Resources is the contact person for the Directive.

3.2. Representative in the Union

The Company has designated BHK Datenschutz und Compliance GmbH in Lörrach (DE) to conduct this role.

3.3. Record of Processing activities

The Company has a record of processing activities, which contains information about new employees, job applications and requests for rectification or erasure of personal data. The record also contains this Directive relating to the data controller, processing and the persons and data concerned.

4. Implementation

4.1. Entry into Force

This Internal Directive enters into force on 22nd May, 2018. She was reviewed on 5th December, 2018.

4.2. Processors in the EU

For the Directive enforcement, processors based in the EU processing and storing data declare have been informed of the Directive and confirm (i) to be able to comply with it and (ii) have their own Directive in order to ensure compliance with GDPR.