Data processing agreement

2SafeYOU

Agreement version 1.1

Data processing agreement

§1 - Introduction

This agreement concerns the processing of personal data ("Data Processor Agreement"). It governs 2SafeYOU A/S, Herstedvang 12, 2620 Albertslund, CVR no. 25807766 (the "Data Processor") processing of personal data on behalf of the Customer (the "Data Controller") and is an annexe to the agreement on the use of 2SafeYOU.

("2SafeYOU Subscription Agreement"), in which the Parties have agreed on the detailed terms for the provision of services by the Data Processor ("Main Services").

§2 - Legislation

The purpose of the Data Processor Agreement is to ensure that the Data Processor complies with the personal data protection legislation ("Data Protection Legislation") applicable at all times, in particular:

i. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data as implemented in the Danish Act on the Processing of Personal Data (Act 2000-05-31 No. 429 as amended) and other applicable legislation,

ii. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, which entered into force on 24 May 2016 and became applicable in Denmark on 25 May 2018 ("GDPR"), including by the adoption of the Danish Data Protection Act.

§3 - Processing of personal data

In the context of the provision of the Main Services, the Data Processor processes personal data on behalf of the Data Controller.

"Personal data" includes "any information relating to an identified or identifiable natural person" as defined in GDPR Article 4(1)(1) ("Personal Data"). The personal data and the categories of data subjects covered by the Data Processor Agreement are listed in Sub-Annexe A, which is regularly updated in the Data Processor's list of processing operations, which the Data Processor shall provide to the Data Controller upon written request. The Data Processor's processing activities and the purpose of processing the Personal Data are only to provide the Main Services.

The Data Processor processes the personal data of the Data Controller and its employees only for the purpose of providing personal protection as part of the 2SafeYOU solution.

§4 - Instructions

The Data Processor may process personal data only upon documented instructions from the Data Controller ("the Instructions"). At the time of signing, the instruction is that the Data Processor may process the Personal Data for the purposes of providing the Main Services and otherwise in accordance with this Processor Agreement.

The Data Controller warrants that the Personal Data entrusted to the Data Processor will be processed and transferred by the Data Controller in accordance with the legislation in force at any given time, including the rules of the Danish Data Protection Act on the legal basis for processing and information obligations towards data subjects.

The Data Processor shall inform the Data Controller without undue delay if the Data Processor believes that the applicable Instruction violates Danish Data Protection Law.

§5 - Obligations of the Data Processor

Confidentiality:

The Data Processor shall treat the Personal Data as strictly confidential. Personal data may not be copied, transmitted or processed outside the Instruction without the express prior consent of the Data Controller.

The Data Processor's employees must have assumed a confidentiality obligation, which means that the employees are subject to confidentiality about all matters relating to the Personal Data.

Security:

The Data Processor implements the necessary technical and organisational measures to ensure data protection in accordance with the Danish Data Protection Legislation and in compliance with Article 32 of the GDPR.

The Data Processor shall ensure that access to the Personal Data is limited to those employees for whom it is necessary to process the Personal Data in order to fulfil the Data Processor's obligations to the Data Controller.

The Data Processor shall also ensure that employees who process Personal Data on behalf of the Data Processor only process such Personal Data in accordance with the Instructions.

Upon written request by the Data Controller, the Data Processor shall provide documentation of the Data Processor's security measures.

Impact assessments and prior consultation:

Where the assistance of the Data Processor is necessary and appropriate, the Data Processor shall assist the Data Controller in the preparation of any regulatory impact assessment in accordance with Article 35 of the GDPR, as well as any prior consultation in accordance with Article 36 of the GDPR.

Rights of data subjects:

If the Data Controller receives a request from an individual for the exercise of the individual's rights under the Data Protection Legislation and the proper response to the request requires the assistance of the Data Processor, the Data Processor shall provide the Data Controller with necessary and relevant information and documentation. The Data Processor must be given a reasonable time to provide this assistance in accordance with the time limits set out in the Data Protection Legislation.

If the Data Processor receives a request from a person for the exercise of the person's rights under Data Protection Law and the request relates to the Data Controller's Personal Data, the Data Processor shall, without undue delay, forward the request to the Data Controller.

Security breach:

The Data Processor shall notify the Data Controller of any personal data breach that could potentially lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the Personal Data processed on behalf of the Data Controller ("Security Breach").

Security breaches must be notified to the Data Controller without undue delay.

The Data Processor shall maintain a record of all Security Breaches. The record must document at least the following:

i. The facts surrounding the Security Breach,

ii. Effects of the Security Breach, and

iii. the remedial measures taken.

Upon written request, the Security Breach Record shall be made available to the Data Controller or the supervisory authorities.

Documentation of compliance with the Data Processor Agreement

The Data Processor shall, upon written request, provide evidence to the Data Controller that the Data Processor:

i. complies with its obligations under this Data Processing Agreement and the Instructions.

ii. complies with the provisions of the personal data protection legislation in force at any time,

in respect of personal data processed on behalf of the Data Controller.

The Data Processor shall provide evidence thereof within a reasonable time.

Location of the Personal Data

Personal data are processed only by the Data Processor at the Data Processor's address and its subsidiary in Poland. Personal data may be transferred to a Control Centre for the processing of alarms, but only on the instructions of the Data Controller. In this case, the Data Processing Agreement of the Control Centre applies.

The Data Processor does not transfer the Personal Data to third countries or international organisations.

Future transfers of Personal Data may, in any event, only take place to the extent permitted by Data Protection Legislation.

§6 - Sub-processors

The Data Processor may generally make use of third parties for the processing of the Personal Data on behalf of the Data Controller ("Sub-processor"), to the extent that the Data Processor notifies the Data Controller of each Sub-processor before the processing is started by the Sub-processor so that the Data Controller has the opportunity to object objectively to the Data Processor's choice of Sub-processor. If the Data Controller wishes to object to this, the Data Controller must give written notice within 7 calendar days of receipt of the notification of the addition or change of a Sub-processor by the Data Processor. Failure by the Data Controller to object will be deemed to constitute implied consent to the sub-processing.

The Data Processor shall enter into a written agreement with any Sub-processors imposing on the Sub-processors the same data protection obligations as are imposed on the Data Processor, including under this Data Processor Agreement. The Data Processor shall also keep under regular review its sub-processors and shall be able to provide evidence thereof to the Data Controller.

The Data Processor shall be directly responsible for the processing of personal data by the Sub-processor in the same way as if the processing had been carried out by the Data Processor itself.

At the time of the conclusion of the Data Processor Agreement, the Data Processor shall use the Sub-processors listed in Sub-Annexe B. When the Data Processor uses new Sub-processors, these must be added under the heading "New Sub-processors" in Sub-Annexe B.

§7 - Fees and costs

The Data Controller shall pay the Data Processor a fee according to the time taken to comply with the following points: "Impact assessments and prior consultation", "Rights of data subjects", "Security breach", and "Documentation of compliance with the Processor Agreement" in §5 of this Data Processor Agreement. For the calculation of the fee, the applicable hourly rates of the Data Processor shall be used.

If changes in Data Protection law, including its interpretations and guidance, result in significantly increased costs for the Data Processor, the Data Controller shall indemnify the Data Processor for any documented additional costs incurred as a result.

§8 - Default and liability

The default, liability, and limitations of liability provisions of the Main Agreement shall apply to this Data Processing Agreement as if this Data Processing Agreement were an integral part thereof.

The liability of the Parties for all cumulative claims under this Data Processing Agreement shall be limited to the total payments due under the Main Services for the 12-month period immediately preceding any event of default. If the Data Processor Agreement has not been in force for 12 months, the amount shall be calculated proportionally on the basis of the agreed payment during the period for which the Data Processor Agreement has been in force.

The limitation of liability does not include the following:

i. Loss resulting from the other Party's grossly negligent or intentional acts.

ii. Costs and resources incurred in fulfilling a Party's obligations to a supervisory authority.

§9 - Duration

The Data Processor Agreement shall remain in force until the Main Agreement terminates or the Data Processor Agreement is terminated.

§10 - Termination

The authority of the Data Processor to process the Personal Data on behalf of the Data Controller shall lapse upon termination of the Data Processor Agreement for any reason.

The Data Processor may continue to process the Personal Data for up to three months after the termination of the Data Processor Agreement, to the extent necessary to carry out necessary legal measures. During the same period, the Data Processor is entitled to include the personal data in the Data Processor's usual backup procedure. During this period, the Data Processor shall be deemed to continue processing in accordance with the Instructions.

The Data Processor and its Sub-processors shall return all Personal Data processed by the Data Processor under this Data Processor Agreement to the Data Controller upon the termination of the Data Processor Agreement, to the extent that the Data Controller is not already in possession of the Personal Data. The Data Processor is then obliged to delete all the Personal Data of the Data Controller. The Data Controller may request the necessary evidence that this has been done.

§11 - Contact

The Contact details for the Data Controller and the Data Processor are found in the Main Agreement.

Sub-Annexe A - Details of the Agreement

Personal data

The Data Processor processes the following types of Personal Data as part of the provision of the Main Service:

i. The general contact details of the persons who are contacts of the Data Controller.

ii. Registration of users to be protected by 2SafeYOU with: name, phone number, email.

iii. Collection of the users' location either via GPS and/or via indoor positioning, which is forwarded to the colleagues or security personnel who have to respond to a panic alarm or a lone-worker alarm.

iv. A time-limited alarm history so that any incidents can be investigated.

Registered

The Data Processor processes personal data of the following categories of data subjects on behalf of the Data Controller:

i. Staff of the Data Controller

Sub-Annexe B

Approved Sub-processors

The following Sub-processors are authorised at the time of the conclusion of the Data Processor Agreement under the conditions set out in the Data Processor Agreement and the Data Protection Legislation:

The 2SafeYOU solution is hosted by this company:

OVH Hosting Ltd.

Unit 12, The Courtyard Building, Carmanhall Road, Sandyford, Dublin 18

Registration number: 468585

The physical centres used are all located within the EU. The chosen solution is located in Frankfurt/Limburg:

Limburger Str. 45, 65555 Limburg an der Lahn, Germany

The hosting centre does not process personal data but only operates the server on which the solution is installed.

Backup data for 2SafeYOU is stored in the company's data centre:

Synology Inc.

9F., No.1, Yuandong Rd., Banqiao Dist., New Taipei City, Taiwan

The data centre where the backup is stored is in Europe:

Europe - Frankfurt

The data centre does not process personal data but only operates the storage on which the solution's backup is stored.

New Sub-processors

The following Sub-processors have been put into use and notified to the Data Controller after the entry into force of the Data Processor Agreement, after which this Annexe is updated:

NONE

--- END OF DOCUMENT ---