Data Processor Agreement

ver.28.01.2022

Between

the data controller:

Company:

CRN (CVR)

Address

and

Data processor

WOBA ApS

CRN (CVR no.): 37609641

Langebrogade 4

DK-1411

Copenhagen

Denmark

1. Contents

2. Background for the data processor agreement

1. This agreement sets out the rights and obligations that apply when the data processor processes personal data on behalf of the data controller.

2. The agreement is designed for the purposes of the parties' compliance with Article 28(3) *of 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 regarding the free movement of such data

   and repealing Directive 95/46/EC (General Data Protection Regulation),
   which sets specific requirements for the content of a data processor agreement.

3. The data processor's processing of personal data takes place with a view to fulfilling the parties' main agreement/contract.

4. The data processor agreement and the Subscription Agreement are interdependent and cannot be terminated separately. However, without terminating the Subscription Agreement, the data processor agreement may be replaced by another valid data processor agreement.

5. This data processor agreement takes precedence over any similar provisions in other agreements between the parties, including in the Subscription Agreement.

6. There are three annexes to this agreement. The annexes function as an integral part of the data processor agreement.

7. Annex A of the data processor agreement contains further information about the processing, including the purpose and nature of the processing, the type of personal data processed, the categories of data subjects processed and the duration of the processing.

8. Annex B to the data processor agreement contains the data controller's conditions for the data processor to make use of any data sub-processors, as well as a list of any data sub-processors that the data controller has approved.

9. Annex C of the data processor agreement contains further instructions on what processing the data processor shall carry out on behalf of the data controller (the object of the processing), which security measures must be observed as a minimum, and how the data processor and any data sub-processors are supervised.

10. The data processing agreement and its annexes shall be maintained in writing, including electronic copies to be kept by both parties.

11. This data processor agreement does not release the data processor from obligations which, under the General Data Protection Regulation or any other legislation, are directly imposed on the data processor.

3. Rights and obligations of the data controller

1. The data controller is responsible to the outside world (including the data subject) for ensuring that the processing of personal data takes place within the framework of the General Data Protection Regulation and the Danish Data Protection Act.

2. The data controller therefore has both the right and the obligation to make decisions about the purposes for which processing may be carried out and which aids may be used.

3. Among other things, the data controller is responsible for ensuring that there is a legal basis for the processing that the data processor is instructed to carry out.

4. The data processor acts on instructions

1. The data processor may only process personal data in accordance with documented instructions from the data controller, unless required otherwise by EU law or the national law of the Member States to which the data processor is subject. In such cases, the data processor shall notify the data controller of this legal requirement before processing, unless the legislation in question prohibits such notification for reasons of important societal interests, cf. Article 28(3) schedule a of the Regulation mentioned in section 2.2.

2. The data processor shall immediately inform the data controller if, in the data processor's opinion, an instruction is in breach of the General Data Protection Regulation or data protection provisions of other Union or national law of the Member States.

5. Confidentiality

1. The data processor shall ensure that only persons currently authorised for this have access to personal data processed on behalf of the data controller. Access to the information must therefore be stopped immediately if the authorisation is revoked or expires.

2. Only persons for whom it is necessary to have access to the personal data in order to be able to fulfil the data processor's obligations to the data controller may be authorised.

3. The data processor ensures that the persons authorised to process personal data on behalf of the data controller have committed themselves to confidentiality or are subject to an appropriate statutory duty of confidentiality.

4. The data processor must, at the request of the data controller, be able to demonstrate that the relevant employees are subject to the above-mentioned duty of confidentiality.

6. Authorisation and access control

1. Login security: The data processor's digital survey system ("Woba") is delivered as a SaaS platform and any authorised user can access it via Woba's application (for mobile, tablet and computer) and online analysis tools. Login access to Woba is managed through unique user rights (all users are assigned a unique login) on the data processor's platform, which are assigned to the data processor's employees according to a principle of least privilege (PoLP) for them to be able to solve their tasks. All information at login is encrypted, as are the responses when the user is logged in. The data processor bases the user rights management on Woba on the customer's instructions (mailing list), which the data controller sends to the data processor before starting the survey. In this way, the data processor ensures that only authorised respondents (employees) and administrators (HR/ managers) have access to the data processor's platform to be able to answer and see results for the survey. The data processor uses both MFA (multi-factor authentication) and temporary access tokens to ensure that only authorised persons have access to the personal information processed.
2. Data security: All personal data is located on servers of the data processor's hosting provider, Amazon Web Services (AWS), in Frankfurt, EU. AWS is compliant with GDPR standards, including ISO 27001 for physical safety and accessibility. AWS has more than 500 GDPR features and services that focus on technical security (such as blocking unauthorised traffic – firewalls) and compliance, and AWS develops new features on an ongoing basis. In addition, AWS conducts ongoing penetration tests to improve its security features and processes.
   Access directly to the database is only available to the data processor's CTO as well as one trusted technical key employee, who acts as a deputy for the data processor's CTO in the event of illness or accident.

7. Processing security

1. The data processor shall take all necessary measures in accordance with Article 32 of the General Data Protection Regulation. It is clear that, taking into account the current level, implementation costs and the nature, scope, coherence and purpose of the processing in question, as well as risks of varying probability and seriousness to the rights and freedoms of natural persons, appropriate technical and organisational measures must be taken to ensure a level of security appropriate to these risks.

2. The above obligation implies that the data processor must conduct a risk assessment and then implement measures to address identified risks.

8. Securing data

As the data is not physically stored with the data processor but only exists on external, managed servers, the data processor's fulfilment of their obligations regarding security in Woba is described in the preceding provisions of this agreement. This includes storing data in Frankfurt (within the EU and in accordance with the GDPR), encrypting data both over network and "at rest", having backups on external servers (also in Frankfurt) and ensuring that subcontractors comply with the guidelines for secure disposal of obsolete hardware etc.

Access to the system is granted to the data processor's employees according to a principle of least privilege and is thus always restricted as much as possible.

The data processor requires ISO 27001 certification of its subcontractors' handling of e.g. the data processor's database and system hosting, thereby ensuring proper, physical security of the data processor's data, with access control to hosting centres, firefighting and monitoring as well as fail-over systems.

The data processor's employees are instructed and trained in the employment of the provisions of this agreement and the data processor's internal guidelines in this regard. If the data processor's guidelines are updated or expanded, the data processor's employees will be informed as soon as possible and no later than one month thereafter. Annual refresher courses in the overall guidelines are held for all employees, just as employees are subsequently tested in their understanding of the guidelines.

9. Security flaws

There are internal processes for handling breaches of data security, which indicate which persons are responsible for which tasks, including technical, communicative and organisational tasks. Within the first 24 hours, the main tasks are to stop the breach, to secure information for subsequent investigations, to determine the extent of the breach and to contact all affected customers and authorities. The data processor cooperates fully with all of the data processor's customers and ensures that everyone has access to all information necessary to comply with their legal obligations in the event of a breach of data security.

The data processor's employees are responsible for reporting any suspicion of a breach of data security, whether this suspicion is due to contact from a customer, a supplier or own experience. As soon as a breach is confirmed, it is assessed whether the flaw is still present (physically or technically), and if this is the case, access via the flaw is blocked immediately, ultimately by taking the system offline until the flaw has been removed.

10. Violation of safety regulations

The data processor prioritises data security and compliance with the General Data Protection Regulation, which is why all employees are obligated, without delay, to make the data processor's customers aware of both breaches and the risk of breaches as soon as these are identified.

If the data processor becomes aware of breaches, the customer is immediately made aware of this, either by contacting the person who is engaging in inappropriate behaviour or by directly contacting the data processor's contact person at the customer.

In the event of an identified breach, the data necessary for subsequent investigation of events is secured, the breach is stopped if it remains active and the extent of the breach is uncovered. If the breach of the security regulations has affected customers, they will be informed without undue delay and with sufficient speed for them to be able to comply with any legal obligations regarding reporting.

11. Anonymisation, pseudonymisation and encryption of personal information

All data interaction (data collection, viewing of results, etc.) between the data processor's users and the digital platform is encrypted by default by the data processor's system, and all individual responses are anonymised as a rule.

Data is retained in the system as long as the contract with the customer stipulates that there is a need for this. Thereafter, data will be deleted and any extracts, reports and the like generated on the basis of this data will no longer be available.

If a survey has been set up as anonymous, the analysis tool only allows you to see results when the data base exceeds the set, lower limit for anonymity (currently 5 responses).

All individual answers are assigned an encrypted ID number, which is why individual answers and thus name, surname and work email are anonymous and cannot be recognised. Free-text comments are only displayed with an indication of the month of the answer, the department (if more than 5 answers in the department) and the corresponding numerical answer (0 to 4).

Open surveys are not pseudonymised.

All data interaction (data collection, result display, etc.) between the data processor's users and the digital platform is encrypted by default by the data processor's system. There are a number of security measures for this, but fundamentally all communication takes place between the data processor's individual systems and with the user over encrypted connections (SSL). Data is encrypted "at rest" to prevent unwanted access in the event of a breach of database security. If personal data is to be transmitted digitally, this must currently be done by storing data e.g. on a USB key and physically transferring this to us, as the data processor can thus ensure that data is not compromised.

12. Backup

The data processor's systems and database all have encrypted PITR backups on external servers within the EU. Systems can be restored to any stage back in time without limitation. The database can be restored at any time, 14 days back in time.

If the purpose of the survey is no longer valid or a user gets in touch and wants their data and user deleted from the data processor's system, data is stored via backup for up to 30 days, if the customer wishes to re-establish the agreement. If not, the deletion process will be completed automatically thereafter. In addition, the data processor is covered by Tryg's cyber insurance ("eProtect"), which helps us prevent attacks in the form of e.g. viruses or DDoS attacks. As part of this insurance, the data processor has access to professional assistance 365 days a year to ward off attacks or get back on track quickly.

13. Rights of the data subject

1. Correction of information

   If the data processor receives a request (by telephone or by email to the data processor's support department) from a registered user who suspects or has become aware that the data processor has received wrong or false personal information about them, the data processor corrects the information “without unnecessary delay” and within 48 hours at the latest. The data processor's support team can only access an end user's account and information if the data subject has consented to granting them access.
   In the case of the data processor, “incorrect information” is often about correcting e.g. factual information such as name, email address, department, etc., which can be corrected directly from the data processor's content management system. Before the data processor corrects the incorrect information, the data processor must have confirmation from the customer's administrator (the person who passed on the incorrect information) that the correction is right. Here, the data processor informs the customer’s administrator about which previously submitted information is incorrect and provides the correct information.

2. Erasure of information

   The individual user who uses Woba owns all their own data uploaded to the data processor's digital platform and, as a rule, is entitled to have all information about themselves deleted *without undue delay* with a deletion period of 48 hours. I.e. all information about the user (name, surname, work email, workplace and department) and their responses to Woba's questionnaire, as well as results, can be deleted at any time. Data is deleted upon request from the database, logs, and backups, and data in physical form is also destroyed, after verification of the enquiry (verification that the enquiry comes from the person who is requesting that all information about them is deleted). This way, the data processor deletes personal data in such a way that it cannot be recovered. In other words, the data processor deletes the registered user's personal data if: 1) It is no longer necessary to have information about the data subject for the data processor's processing purpose. 2) The processing is based on the data subject's consent and the user in question withdraws this consent. 3) The user's data are processed in violation of the General Data Protection Regulation in any way (for more on this see WBI's data processor agreement, clause 11). In addition to notifying the enquiring user of the deletion, the data processor also notifies the person at the customer who provided the information about the deleted user.

3. Right of access

   By enquiry to support (by telephone and email), information is provided on all registered data from the data processor's systems after verification of the enquiry (verification that the enquiry comes from a person who has the right to enquire). When the user contacts us and makes a request, they always have the right to see the personal data that the data processor processes about them in the data processor's system, based on which the user assesses whether the information is correct, needs to be rectified or erased, etc. The data processor then sends the data subject a copy of the information itself to their email address free of charge. Before sending the email with the information, the data processor sends a security approval to the person's email address (the employee's work email, provided to the data processor by the customer), which must be verified via the person’s inbox before the information can be received. In this way, the data processor ensures that the information is sent to the correct person. ONLY information about the data subject themself is sent as a copy.

4. Data portability

   Data from the data processor's database is exported in an easy-to-read and clear CSV format. Data that can be exported includes the users' historical answers, including an indication of the time they were provided, as well as the required personal information that the data processor has on the data subject (name, email, workplace and department/ team). The data subject will thus be able to easily access and control the information that the data processor has registered in the system and will also be able to easily transfer their personal data to another IT environment.

   All users of Woba have the right to receive their own personal information, the answers they have uploaded to the system, as well as analysis results which include their answers – and may at any time receive these in an easy and clear format. The data processor's procedure for receipt follows the same standard as in point 3 under right of access in this document.

5. Giving consent

   By logging in, the terms and conditions of the data processor are accepted and agreed to (*active position* must be taken – it is not possible to log in without acceptance). By accepting the data processor's terms and conditions, the individual user accepts that the system collects, archives and uses their answers for the purpose of the survey and makes them available to the user's employer.

6. Withdrawal of consent

   Every Woba user owns all their data uploaded to the data processor's digital system. When the user first logs into Woba, the data processor therefore also states in its terms and conditions that it is possible for any user to revoke their consent. If the user contacts us via the data processor's support department regarding the revocation of consent for Woba to process their personal data, the data processor will delete their data without undue delay and no later than 48 hours after the revocation of consent.

   The data processor then sends the user a free electronic copy of the deletion information via their email. Before sending the email with the deletion information, the data processor sends a security approval to the person's email address (the employee's work email, which the data processor has been provided by the customer), which must be verified via the person’s inbox to receive the deletion information. The user must confirm via their email before the data processor starts deleting their data.

7. Profiling (automatic individual decisions)

   Every user of Woba has the opportunity not to be subjected to automatic processing of their personal data in the data processor's analysis surveys at the workplace. If the customer so chooses, the customer's employees have the opportunity to have an individual profiling based on their answers to the survey. Profiling in the data processor's systems is a mathematical calculation based on the employee's responses. These profiles (“results”) are only available to the individual respondent and thus neither the employer nor other companies have access to these. If the customer has decided that employees will receive their individual results, this is described in the data processor's terms and conditions, which the individual actively accepts before answering.

14. External communication connections

All communication with the data processor's platform takes place via encrypted connections, regardless of whether this concerns general use of the platform, synchronisation of code, or work with a database.

15. Input and output material

1. Input: Only technically and professionally knowledgeable personnel who work with data entry in WOBA have access to input data material. The data processor secures this access through authorised access control. In addition, all company computers have personal, security-approved passwords, so the data processor ensures that employees who do not work with data entry do not have access to the material. Input data (in the data processor's context, e.g. employee lists and organisational structures sent digitally) is deleted from email and hard drive within 4 weeks after processing has been completed. The 4 weeks ensure that input data is available in case errors are detected or a different processing is required.

If input data is provided in physical form, this will also be shredded within 4 weeks after the processing has ended.

2. 2. Output data: Output data material (including reports, presentations and data extracts) is generated digitally by the data processor's platform at the customer's request and can be downloaded by the employees to whom the customer gives authorised access. All data interaction (data collection, result display, etc.) between the data processor's users and the digital platform is encrypted by default by the data processor's system.

Only technically and professionally knowledgeable personnel may work with output material in WOBA. Output generated by the selected staff (e.g. penetration test or paper-based reports) is deleted and/or shredded within 4 weeks when the need to use the results ceases. The data processor has implemented clear security standards – e.g. if a WOBA employee has a folder with customer-related reports stolen – where the customer is notified of any incidents and where these are reported without undue delay.

16. Logging

All interaction with the data processor's digital platform is logged in the data processor's database, which means that the data processor can track the individual user's operations and interactions at any time. Each log contains information about who did what (user, type of application, etc.) and at what time the application was exercised. Each log is established via queries to the data processor's database and stored for at least 6 months. In addition to the registration in the database, server logs are stored on separate servers.

17. User administration

The data processor's platform is used by two types of users – people who provide information (employees) and people who analyse this information (managers/HR and top management). A person may well belong to both categories at the same time. In connection with the submission of information (answering the survey), the user has login access to see their own previous answers and company totals (if the company has provided access to these).

Persons who analyse data (managers) are assigned login access to one or more organisational units (departments). At the same time, the user's rights are limited based on role (administrator or manager), where the administrator has access to all information and settings, including user lists, but cannot correct, create or delete individual answers. A department manager has read-only access to answers from own departments to selected surveys and can be assigned read-only rights to all surveys in addition to those (though still only for own departments), administrator rights (correct, create and delete) regarding employees, and administrator rights regarding administrators or regarding the launch of surveys.

Encryption: All employees and managers are thus granted unique rights via an encrypted ID number so that they only have access to answer, view, archive and delete the information that is relevant to them. All data interaction (data collection, results display, etc.) between the data processor's users and digital platform is encrypted by default by the data processor's system.

In other words, no employees have access to information that they do not need when answering Woba's surveys.

18. The use of data sub-processors

1. The data processor must meet the conditions set out in Article 28(2) and (4) of the General Data Protection Regulation to make use of another data processor (data sub-processor).

2. Thus, the data processor may not use another data processor (data sub-processor) to fulfil the data processor agreement without prior specific or general written approval from the data controller, which, however, cannot be denied unless the data processor has serious and factual objections to it. By signing this data processor agreement, the data controller gives their written consent that the data processor may use the data sub-processors listed in Annex 2.2 to this data processor agreement.

3. In the event of general written approval, the data processor must notify the data controller of any planned changes regarding the addition or replacement of other data processors and thereby give the data controller the opportunity to object to such changes, cf. Annex B.

4. When the data processor has the data controller's consent to use a data sub-processor, the data processor ensures that the same data protection obligations as those stipulated in this data processor agreement are imposed on the data sub-processes, through a contract or other legal document in accordance with EU law or the national law of the Member States, in particular providing the necessary guarantees that

the data sub-processor will implement the appropriate technical and organisational measures in such a way that the processing meets the requirements of the General Data Protection Regulation.

5. If the data sub-processor does not fulfil its data protection obligations, the data processor remains fully liable to the data controller for the fulfilment of the data sub-processor's obligations

6. The data controller's detailed conditions for the data processor's use of data sub-processors are set out in Annex B to this agreement.

19. Transfer of information to third countries or international organisations

1. The data processor may only process personal data in accordance with documented instructions from the data controller, including with regard to the transfer (transfer, disclosure and internal use) of personal data to third countries or international organisations, unless required otherwise by EU or national law to which the data processor is subject. In such cases, the data processor shall notify the data controller of this legal requirement before processing, unless the legislation in question prohibits such notification for reasons of important societal interests, cf. Article 28(3), schedule a.

2. Without the data controller's instructions or approval, the data processor may – within the framework of the data processor agreement – therefore not e.g.:

    a. disclose the personal data to a data controller in a third country or in an international organisation,
    b. leave the processing of personal data to a sub-processor in a third country,
    c. have the data processed in another division of the data processor which is located in a third country.

20. Assistance to the data controller

1. Taking into account the nature of the processing, the data processor shall assist the data controller as best possible using appropriate technical and organisational measures in fulfilling the data controller's obligation to respond to requests for the exercise of data subjects' rights as set out in Chapter 3 of the General Data Protection Regulation. This means that the data processor must, to the extent possible, assist the data controller in ensuring compliance with:

    a. the duty to provide information when collecting personal data from the data subject
    b. the duty to provide information if personal data has not been collected from the data subject

c. the data subject's right of access
d. the right to rectification
e. the right to erasure ('the right to be forgotten')
f. the right to restrict processing
g. the duty to notify in connection with the correction or deletion of personal data or restriction of processing
h. the right to data portability
i. the right to object
j. the right to object to the results of automated individual decision-making, including profiling.

2. The data processor shall assist the data controller in ensuring compliance with the data controller's obligations under Articles 32 to 36 of the General Data Protection Regulation, taking into account the nature of the processing and the information available to the data processor, cf. Article 28(3), schedule f.

This means that, taking into account the nature of the processing, the data processor must assist the data controller in complying with:

a. the obligation to take appropriate technical and organisational measures to ensure a level of safety appropriate to the risks associated with the processing;
b. the obligation to report breaches of personal data security to the supervisory authority (The Danish Data Protection Agency) without undue delay and, if possible, no later than 72 hours after the data controller has become aware of the breach, unless it is unlikely that the breach of personal data security poses a risk to natural persons' rights or freedoms.
c. the obligation to communicate the personal data breach to the data subject without undue delay when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;
d. the obligation to carry out an impact assessment on data protection if a type of processing is likely to involve a high risk to the rights and freedoms of natural persons;
e. the obligation to consult the supervisory authority (The Danish Data Protection Agency) before processing, provided that an impact assessment concerning data protection shows that the processing will lead to a high risk in the absence of measures taken by the data controller to limit the risk;

21. Notification of breach of personal data security

1. The data processor shall inform the data controller without undue delay after becoming aware that there has been a breach of personal data security involving data held by the data processor or a data sub-processor.

The data processor's notification to the data controller must, if possible, take place no later than 24 hours after the data processor becomes aware of the breach so that the data controller has the opportunity to comply with any obligation to report the breach to the supervisory authority within 72 hours.

2. In accordance with clause 9.2(b) of this Agreement, the data controller shall – taking into account the nature of the processing and the information available for it – assist the data controller in notifying the supervisory authority of the breach. This may mean that the data processor must help to provide the following information required by Article 33(3) of the GDPR to be specified in the data controller's notification to the supervisory authority:

    a. The nature of the breach of personal data security including, if possible, the categories and approximate number of data subjects impacted, as well as the categories and approximate numbers of personal data records concerned;
    b. Likely consequences of the breach of personal data security
    c. Measures taken or proposed to be taken to deal with the breach of personal data security, including, where appropriate, measures to limit its potential harmful effects

22. Deletion and return of information

1. Upon termination of the processing services, the data processor is obligated, at the discretion of the data controller, to delete or return all personal data to the data controller, as well as to delete existing copies, unless EU law or national law prescribes the storage of personal data. For further specification of this point see Annex C, C.3.

23. Supervision and auditing

1. The data processor shall make available to the data controller all information necessary to demonstrate the data processor's compliance with this agreement and shall enable and contribute to audits, including inspections, carried out by the data controller or another auditor authorised by the data controller.

2. The data processor is obligated to give authorities who, under applicable legislation, have access to the data controller's and data processor's facilities, or representatives acting on behalf of said authority, access to the data processor's physical facilities against proper identification.

24. Entry into force and termination

1. This agreement is considered to have been entered into and signed at the same time as the Subscription Agreement and enters into force at the same time and terminates at the same time as the Subscription Agreement.

2. This agreement may need to be renegotiated by both parties if changes in the law or inconveniences in the agreement or changes in the Subscription Agreement give rise to this.

3. Termination of the data processor agreement can take place in accordance with the termination terms, incl. notice of termination, that apply for the Subscription Agreement, and the data processor agreement is to be considered automatically terminated at the same time as the termination of the Subscription Agreement

4. The agreement shall remain in force for as long as the processing continues. Regardless of the termination of the Subscription Agreement and/or the data processor agreement, the data processor agreement will remain in force until the end of the processing and the deletion of the information by the data processor and any data sub-processors.

25. Contact persons/contact points at the data controller and the data processor

1. The parties can contact each other via the contact persons specified in the Subscription Agreement

.

Annex A Information on the processing

The purpose of the data processor's processing of personal data on behalf of the data controller:

The primary purpose of the processing is to map the working environment of the data controller and the well-being of the data controller's employees/users. Thus, data, including processing, is to be used to *prevent* physical and mental work-related injuries as a result of the work environment and to promote the well-being of employees.

What the data processor's processing of personal data on behalf of the data controller primarily concerns:

The processing is done automatically by Woba – including the app and dashboard – which automatically generates analyses based on the responses that the data controllers' employees/ users report in the app.

The processing includes the following types of personal information about the data subjects:

Name, email address and unit in the organisation (e.g. department, team or area). These three types of information are standard and a prerequisite for data controllers to use Woba. No information beyond the above is requested by the data processor.

Which categories of data subjects the processing includes:

The data subjects are employees who work at the data controllers' company and who have entered into an agreement with the data processor, WOBA ApS. The term "employees" refers to both non-managerial and managerial staff.

The data processor's processing of personal data on behalf of the data controller may commence after the entry into force of this agreement. The processing has the following duration:

Until the purpose of the processing ceases, cf. the section 'Rights to Data' in the 'Subscription Agreement', or until the data controller wants the processing to cease, whichever comes first.

Annex B Conditions for the data processor's use of data sub-processors and list of approved data sub-processors

1. **Terms for the data processor's use of any data sub-processors** The data processor has the data controller's general approval to make use of data sub-processors. However, the data processor shall notify the data controller of any planned changes regarding the addition or replacement of other data processors and thereby give the data controller the opportunity to object to such changes. Such notification must be received by the data controller at least 1 month before the application or change is to take effect. If the data controller has objections to the changes, the data controller must notify the data processor within 2 weeks of receiving the notification. The data controller can only object if the data controller has reasonable, concrete grounds for this.

2. **Approved data sub-processors**

Upon the entry into force of the data processor agreement, the data controller has approved the use of the following data sub-processors:

Name	Address	Description of processing
Aiven Oy	Helsinki, Finland	Aiven hosts the data processor's database. The company is Finnish, and the data is located on a server at UpCloud, another Finnish company, and is physically located in Frankfurt, Germany.
Heroku (a salesforce company)	The Landmark @ 1 Market St. Suite 300 San Francisco, CA 94105, USA	Heroku hosts the actual systems (which process data). The company is American, but data is in “Region: EU” in Frankfurt, Germany. Heroku is hosted by Amazon Web Services on EU-central-1 and is subject to EU law. No data *is* passed through Heroku, and reference can be made to Salesforces' statement on mechanisms covering Schrems II: https://www.sales-force.com/content/dam/web/en_us/www/documents/legal/Agreements/EU-Data-Trans- fer-Mechanisms-FAQ.pdf
Postmark (a Wildbit company)	2400 Market Street, No. 200, Suite 235B, Phil-adelphia, PA 19103, USA	Postmark is used as an email service to send out emails with invitations to sign up or log in to Woba. Postmark does not store a full address book, but acts as a relay. Re. Postmark's handling of Schrems II, please see https://postmarkapp.com/blog/postmarks-response-to-the-schrems-ii-judgment-privacy-shield-invalidation
Google	1600 Amphithe-atre Parkway,	The data processor uses Gmail for support or other communication via email. Data is physically located in

	Mountain View, CA 94043, USA	EU – https://www.google.com/about/data-centers/inside/locations/index.html. Gmail is *not* used by the solution itself.
Amazon Web Services (AWS)	Seattle, Washington, USA	AWS stores the data processor files (icons and PDFs) on a server at eu-central-1, which is physically located in Frankfurt in Germany and is subject to EU law. *No* personally identifiable data is stored with AWS.

Upon the entry into force of the data processor agreement, the data controller has specifically approved the use of the above-mentioned data sub-processors for precisely the processing described above. The data processor may not – without the data controller's specific and written approval – use the individual data sub-processor for “other” processing than agreed or let another data sub-processor carry out the described processing.

Annex C Instructions for processing personal information

1. The object of the processing

The data processor's processing of personal data on behalf of the data controller shall take place as follows:

Data is analysed and processed automatically by Woba as well as manually by internal employees permanently employed by WOBA. For manual processing, only Excel is used.

2. Processing security

The level of security must reflect:

That this concerns collection of personal data of a *non*-sensitive nature. As described above, the data processor collects email, name and unit in the organisation (e.g. department, team or area) from the data controllers' employees/users as a prerequisite for being able to use the data processor's platform, Woba. However, as a data processor, the data processor is entitled and obligated to establish the necessary and appropriate organisational and technical security measures regarding the data collected.

Reference is also made to the data processor agreement's clauses 5–17.

3. Storage period/deletion routine

The personal information, including raw data, is stored with the data processor for up to 5 years after the collaboration with the data controller has ceased, unless the data controller requests that the information be deleted or returned. This is done because the data processor (WOBA) uses raw data for research and development purposes.

4. Location of processing

The processing of the personal data covered by the agreement may not take place at locations other than the following without the data controller's prior written consent :

Langebrogade 4, DK-1411 Copenhagen (address of the processer, WOBA ApS).

In addition, by signing this agreement, permission is granted for the above-mentioned data sub-processors to store data at the listed addresses.

5. Detailed procedures for the data controller's supervision of the processing carried out by the data processor

Any expenses of the data controller in connection with a physical inspection are borne by the data controller. However, the data processor is obligated to set aside the resources (mainly the time) necessary for the data controller to carry out their inspection.