Data Processing Agreement

This Data Processing Agreement with its Annexes (together, this/the "**DPA**") is incorporated into the LBC Services Agreement and the Master Services Agreement (both the "**MSA**") (or other electronic or mutually executed written agreement that references it), between Lobyco A/S (the "**Data Processor**") and the customer/client (the "**Data Controller**") stated in the MSA, each a "**party**"; together "**the parties**".

1. Application and scope

1.1 This Data Processing Agreement (the/this "DPA") applies as an incorporated part of the LBC Services Agreement and the Master Service Agreement (both the "MSA") between the parties (or other electronic or mutually executed written agreement that references it).

1.2 In the context of the provision of the MSA between the parties, the Data Processor will process personal data on behalf of the Data Controller in accordance with the DPA.

2. Definitions

2.1 The following definitions shall apply in this DPA:

- "GDPR" means Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and the free movement of such data (General Data Protection Regulation).
- "Data Protection Laws" means all applicable data protection and privacy laws and regulations, including where applicable the GDPR, and any national implementing legislation, regulations and secondary legislation, as amended or updated from time to time.
- "data controller", "data processor", "data subject", "personal data", "processing" (and "process") and "personal data breach" shall have the meaning given in article 4 of the GDPR.

3. Preamble

3.1 The DPA set out the rights and obligations of the Data Controller and the Data Processor, when processing personal data on behalf of the Data Controller.

3.2 The DPA is designed to meet the legal obligations stated in Article 28(3) of the GDPR.

3.3 In the context of the provision of the MSA between the parties, the Data Processor will process persona data on behalf of the Data Controller in accordance with the DPA.

3.4 The DPA replaces any previously signed data processing agreements, addendums or other similar terms between the parties.

3.5 Four annexes are attached to the DPA and form an integral part of the DPA:

- Annex A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.
- Annex B contains the Data Controller's conditions for the Data Processor's use of sub-processors and a list of sub-processors authorised by the Data Controller.
- Annex C contains the Data Controller's instructions with regards to the minimum security measures to be implemented by the Data Processor.
- Annex D contains provisions for other activities which are not covered by the DPA.

3.6 In case of discrepancies between the online text version and the pdf version of the DPA, the pdf version shall prevail.

4. The rights and obligations of the Data Controller

4.1 The Data Controller must ensure the DPA meets the legal requirements under the GDPR and additional requirements under applicable Data Protection Laws, has a lawful basis for processing and that the Data Processor's obligations are clearly outlined in the instructions under Clause 5.

4.2 The Data Controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

4.3 The Data Controller shall be responsible, among other, for ensuring that the processing of personal data, which the Data Processor is instructed to perform, has a legal basis.

4.4 The Data Controller shall refrain from any action that would prevent the Data Processor from fulfilling its obligations under any law to which the Data Processor is subject, including as regards cooperation with the competent supervisory authorities.

5. The Data Processor acts according to instructions

5.1 The Data Processor shall process personal data only on documented instructions from the Data Controller, unless required to do so by law to which the Data Processor is subject. The Data Processor shall inform the Data Controller in writing of that legal requirement before processing, unless that requirement prohibits such information on important grounds of public interest.

5.2 Such instructions shall be specified in the DPA. Subsequent instructions can also be given by the Data Controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the DPA.

5.3 The Data Processor shall inform the Data Controller if instructions given by the Data Controller, in the opinion of the Data Processor, contravene any law to which the Data Processor is subject.

6. Confidentiality

6.1 The Data Processor shall keep the personal data confidential.

6.2 The Data Processor shall only grant access to the personal data being processed on behalf of the Data Controller to persons under the Data Processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

6.3 The Data Processor shall at the request of the Data Controller demonstrate that the concerned persons under the Data Processor's authority are subject to the abovementioned confidentiality.

7. Security of processing

7.1 The Data Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, as set out in Annex C.

7.2 The Data Controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. The Data Processor shall assist the Data Controller in evaluating risks to the rights and freedoms of natural persons inherent in the processing, based on information provided by the Data Controller and the Data Processor's knowledge of the processing activities.

7.3 Furthermore, the Data Processor shall assist the Data Controller in ensuring compliance with the Data Controller's obligations, by inter alia providing the Data Controller with information concerning the technical and organisational measures already implemented by the Data Processor along with all other information necessary for the Data Controller to comply with the Data Controller's obligation under applicable Data Protection Laws.

7.4 If the Data Controller requires additional security measures beyond those specified in Annex C, such measures shall be agreed upon separately and may result in additional costs to be borne by the Data Controller. This includes any requirements following new Data Protections Laws, amendments to existing laws, changes in judicial interpretations, or decisions issued by competent supervisory authorities etc.

7.5 Notwithstanding Clause 7.4 above, the Data Controller may not require the Data Processor to implement measures which would bring the Data Processor in non-compliance with this DPA or Data Protection Laws.

8. Use of sub-processors

8.1 The Data Processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).

8.2 The Data Processor has the Data Controller's general authorisation for the engagement of sub-processors.

8.3 The list of sub-processors authorised by the Data Controller can be found in Annex B.

8.4 Data Processor shall update the sub-processor list, cf. Annex B, at least thirty (30) days before engaging new sub-processors or making material changes to existing sub-processors and will provide the Data Controller with a notification of changes to sub-processors (a "Change Notice"), thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s).

8.5 The Data Controller may object to a new sub-processor on reasonable grounds relating to data protection compliance, provided such objection is made in writing within fifteen (15)

days of receiving the Change Notice and includes specific, substantiated concerns regarding data protection.

8.6 Where the Data Processor engages a sub-processor for carrying out specific processing activities on behalf of the Data Controller, the same data protection obligations as set out in the DPA shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the DPA and applicable Data Protection Laws.

8.7 The Data Processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the Data Processor is subject pursuant to the DPA and applicable Data Protection Laws.

8.8 A copy of such a sub-processor agreement and subsequent amendments shall – at the Data Controller's request – be submitted to the Data Controller, thereby giving the Data Controller the opportunity to ensure that the same data protection obligations as set out in the DPA are imposed on the sub-processor. DPA on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the Data Controller.

8.9 If the sub-processor does not fulfil his data protection obligations, the Data Processor shall remain liable to the Data Controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under applicable Data Protection Laws against the Data Controller and the Data Processor, including the sub-processor.

9. Transfer to third countries

9.1 The Data Processor may transfer personal data to third countries or international organisations as necessary for the provision of the services, provided such transfers comply with applicable Data Protection Laws and any specific instructions from the Data Controller.

9.2 In case transfers to third countries or international organisations, which the Data Processor has not been instructed to perform by the Data Controller, is required under EU or Member State law to which the Data Processor is subject, the Data Processor shall inform the Data Controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

9.3 Without documented instructions from the Data Controller, the Data Processor therefore cannot within the framework of the DPA:

- transfer personal data to a Data Controller or a Data Processor in a third country or in an international organization
- transfer the processing of personal data to a sub-processor in a third country
- have the personal data processed in by the Data Processor in a third country

9.4 The Data Controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in Annex D.2.

9.5 The DPA shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the DPA cannot be relied upon by the parties as a transfer tool under Chapter V GDPR.

10. Assistance to the Data Controller

10.1 Taking into account the nature of the processing, the Data Processor shall assist the Data Controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the Data Controller's obligations to respond to requests for exercising the data subject's rights laid down in applicable Data Protection Laws, in particular Chapter III GDPR, if applicable. Such assistance may be subject to additional fees as specified in the MSA.

10.2 This entails that the Data Processor shall, insofar as this is possible, assist the Data Controller in the Data Controller's compliance with:

- the right to be informed when collecting personal data from the data subject
- the right to be informed when personal data have not been obtained from the data subject
- the right of access by the data subject
- the right to rectification
- the right to erasure ('the right to be forgotten')
- the right to restriction of processing
- notification obligation regarding rectification or erasure of personal data or restriction of processing
- the right to data portability
- the right to object
- the right not to be subject to a decision based solely on automated processing, including profiling

10.3 In addition to the Data Processor's obligation to assist the Data Controller pursuant to Clause 10.2, the Data Processor shall furthermore, taking into account the nature of the processing and the information available to the Data Processor, assist the Data Controller in ensuring compliance with:

- the Data Controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;
- the Data Controller's obligation to without undue delay communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;

- the Data Controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment), by gathering relevant information enabling the Data Controller to prepare and carry out the DPIA.
- the Data Controller's obligation to consult the competent supervisory authority, prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the Data Controller to mitigate the risk.

10.4 The Data Controller shall carry out the overall case management, including the initial registration of the inquiry, task management and follow-up. The Data Controller shall carry out all communication with the data subjects in connection with the request.

10.5 The Data Processor shall in cooperation with the Data Controller establish and maintain the channels and contact points necessary for the exchange of information between the parties in the context of requests from data subjects that concerns personal data covered by the DPA.

10.6 Where technically feasible, the Data Processor shall provide tools or interfaces to enable the Data Controller to handle data subject requests, including:

- deletion/anonymization
- access
- rectification

11. Notification of personal data breach

11.1 In case of any personal data breach, the Data Processor shall, without undue delay after having become aware of it, notify the Data Controller of the personal data breach.

11.2 Notification shall be sent to the Data Controller's contact point, cf. Clause 17.

11.3 The Data Processor's notification to the Data Controller shall, if possible, take place within 48 hours after the Data Processor has become aware of the personal data breach to enable the Data Controller to notify the personal data breach to the competent supervisory authority, if required under applicable Data Protection Laws.

11.4 In accordance with Clause 10.3, the Data Processor shall assist the Data Controller in notifying the personal data breach to the competent supervisory authority, meaning that the Data Processor is required to assist in obtaining the following information:

- The categories of personal data involved in the breach
- The number of personal data records concerned
- The categories of data subjects involved
- An assessment of the number of data subjects affected
- An assessment of the likely effect of the breach on the data subjects (loss of confidentiality, loss of integrity, loss of availability)

- An assessment of the mitigating/enhancing effect of existing controls on the likely consequences for the data subjects
- An assessment of the mitigating effect of the immediate measures taken by the Data Processor to address the possible adverse effects of the breach on the data subjects
- An assessment of the mitigating/enhancing effect of specific circumstances relating to the breach on the likely consequences for the data subject
- An assessment of the likely consequences of the breach for the data subject
- An assessment of further actions needed to reduce the likelihood of similar breaches occurring in the future

12. Erasure and return of data

12.1 Personal data shall be retained by the Data Processor for the duration necessary to provide the services under the MSA. Data in logs and back-ups may be retained for up to 1 year for information security and service provision purposes, unless longer retention is required by applicable law.

12.2 Personal data concerning the Data Controller's customers may be erased by the Data Controller, by erasure or anonymization of specific customer accounts via the admin tool provided by the Data Processor.

12.3 On termination of the provision of personal data processing services, the Data Processor shall be under obligation to delete all personal data processed on behalf of the Data Controller and certify to the Data Controller that it has done so unless applicable law requires storage of the personal data.

13. Audit and inspection

13.1 The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with the obligations laid down in the DPA and allow for and contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller.

13.2 The Data Processor shall annually obtain an auditor's report from an independent third party concerning:

1) the Data Processor's compliance with the DPA
2) the design and effectiveness of the Data Processors implemented IT controls.

13.3 The parties have agreed that the following types of auditor's report may be used to demonstrate compliance:

- ISAE 3000 report or similar

13.4 The auditor's report shall without undue delay be submitted to the Data Controller upon request.

13.5 Based on the results of such an audit, the Data Controller may request further measures to be taken to ensure compliance with the DPA.

13.6 The Data Controller or a representative appointed by the Data Controller shall have access to inspect, including physically inspect, the locations, where the processing activities under the DPA are carried out by the Data Processor. The right to inspect includes the physical facilities as well as systems used for and related to the processing. Such an inspection shall be performed when the Data Controller deems it necessary.

13.7 The Data Processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the Data Controller's and Data Processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the Data Processor's physical facilities on presentation of appropriate identification.

13.8 If the inspection reveals insufficient security measures or other breaches of the DPA on the part of the Data Processor, the Data Processor must take necessary steps to counter such breaches without undue delay.

14. The parties' agreement on other terms

14.1 The parties may agree other clauses concerning the provision of the personal data processing service specifying e.g. liability, as long as they do not contradict directly or indirectly the DPA or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by applicable Data Protection Laws.

14.2 Terms regarding liability is governed by the MSA between the parties.

14.3 Costs or hours used by the Data Processor due to technical or procedural changes requested by the Data Controller will be charged by the Data Processor to the Data Controller on a T/M basis (time used and external costs incurred by Data Processor will be charged to the Data Controller), including but not limited to changes to (i) instruction on use of personal data, (ii) security or (iii) other procedures applicable to personal data.

14.4 Other Data Controller specific actions related to the processing of personal data will be charged by Data Processor, if it is not explicitly stated in this DPA that Data Processor shall perform such actions free of charge. Requests for such actions, assistance, information or documentation made by the Data Controller, its auditors or customers under the data processing agreement or under applicable legislation regarding data protection shall thus be charged by Data Processor to the Data Controller on a T/M basis (time used and external costs incurred by Data Processor will be charged to the Data Controller).

15. Commencement and termination

15.1 This DPA is effective as of the effective date of the MSA.

15.2 Both parties shall be entitled to require the DPA renegotiated if changes to the law or inexpediency of the DPA should give rise to such renegotiation.

15.3 The DPA shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the DPA cannot be terminated unless other DPA governing the provision of personal data processing services have been agreed between the parties.

15.4 If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the Data Controller, the DPA may be terminated by written notice by either party.

16. Amendments

16.1 The Data Processor may amend this DPA from time to time to reflect changes in applicable Data Protection Laws, regulatory guidance, or to improve clarity, provided that such amendments do not materially reduce the data protection standards set forth herein.

16.2 Amendments that do not affect the core data protection obligations, rights of data subjects, or the scope of the processing — including but not limited to administrative, formatting, or clarification changes - shall be deemed non-material. Such amendments may enter into force at the end of a notice period of thirty (30) calendar days', unless the Data Controller objects in writing before the effective date.

16.3 Amendments that materially affect the Data Processor's obligations, the Data Controller's rights, or the scope, nature, or purpose of the processing shall be deemed material. Such amendments require the Data Controller's explicit written consent before entering into force. If the Data Controller does not consent, the parties shall engage in good faith negotiations to resolve the matter.

17. Contact point

17.1 The parties may contact each other using the contacts/contact points specified in the MSA.

17.2 The parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

Annex A: Information about the processing

A.1 The subject of/instruction on the data processing:

The Data Processor's services under the MSA are exposed through a mobile app that can be individually designed to fit the purposes of the Data Controller. The Data Processor's digital ecosystem communicates with the Data Controllers' back-end systems, and collects data from users of the mobile app.

A.2 The purpose of the Data Processor's processing of personal data on behalf of the Data Controller is:

The overall purpose of the processing activities is to deliver the agreed services under the MSA, to provide and support an ecosystem that enables the Data Controller to boost its customer loyalty, to create a frictionless shopping experience and to support the continuous optimization of the customer experience.

A.3 The Data Processor's processing of personal data on behalf of the Data Controller shall mainly pertain to (the nature of the processing):

The Data Processor performs the following processing activities:

- Facilitating the collection of personal data from the users of the mobile app
- Recording, organizing, structuring, and storing personal data to the support the service delivery
- Combining and using personal data to support the service delivery, including segmentation and profiling
- Facilitating the on-going transfer of personal data between the Data Controllers' customers and the digital ecosystem of the Data Processor services
- Facilitating the on-going transfer of personal data between the Data Processor and its sub-processors
- Deleting personal data according to the Data Controller's instruction
- Anonymizing personal data for continuous optimization of the customer experience

A.4 The processing includes the following categories and types of personal data:

Categories of personal data:

☒ Personal data (GDPR article 6)
☐ Regulated personal data (e.g., social security number)
☐ Sensitive personal data (GDPR article 9)
☐ Criminal offences (GDPR article 10)

Depending on the services delivered under the MSA, the Data Processor may process the relevant types of personal data.

A.5 Processing includes the following categories of data subject:

The Data Controllers' customers.

A.6 Processing has the following duration:

The Data Processor's processing of personal data on behalf of the Data Controller may be performed when the DPA commence.

Personal data related to the Data Controller's customers are processed until the termination of this DPA in accordance with Clause 15.

A.7 The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):

Personal data is transferred and processed on a continuous basis.

A.8 For transfers to (sub-) processors, also specify subject matter, nature, and duration of the processing:

The subject matter of personal data transferred to sub-processors is the Data Controller's customer data, which is transferred to sub-processors to provide, support, and improve the services, as outlined in the MSA.

A.9 Identify the competent supervisory authority/-ies:

Data Controller: The competent supervisory authority in accordance with applicable Data Protection Laws.

Data Processor: The Danish Data Protection Agency (Datatilsynet).

Annex B: Authorized sub-processors

B.1 Approved sub-processors

The full up-to-date list of approved sub-processors and affiliates is available here: lobyco.com/legal/subprocessors.

B.2 Prior notice for the authorisation of sub-processors

The Data Processor shall inform in writing the Data Controller of any intended changes concerning the addition or replacement of sub-processors at least thirty (30) days in advance, thereby giving the Data Controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s), in accordance with the procedure stated in Clause 8.

B.3 Processing locations

Processing of the personal data under the DPA shall be performed in the locations outlined in B.1 above.

Annex C: Security measures

The full, most up-to-date description of the Data Processor's technical and organizational security measures is available here: lobyco.com/legal/security

The Data Processor may enhance or expand its security measures at any time to reflect evolving best practices, emerging threats, or new regulatory requirements, without prior approval from the Data Controller.

Annex D: Terms of agreement on other subjects

D.1. Supplemental conditions regarding sub-processors

The Data Controller accepts the Data Processor's use of the following sub-processors on their standard terms and conditions, which may be updated by their discretion:

Sub-processor	Supplement conditions	Terms & Conditions	Use of sub-processors
Microsoft Ireland Operations Limited	Microsoft Azure services constitute an integrated part of the Data Processors services. Microsoft Azure services are delivered in a dynamic distributed ecosystem on Microsoft's standard Terms and Conditions.	https://azure.microsoft.com/en-us/support/legal	https://servicetrust.microsoft.com/DocumentPage/ea6e2b66-933b-4b11-aafb-2225f36bfd73
Atlassian Pty Ltd.	Services are delivered on Atlassian's standard terms and conditions.	https://www.atlassian.com/legal/atlassian-customer-agreement	https://www.atlassian.com/legal/sub-processors
Additionally for clients using the Firebase Analytics service			
Google LLC	Services are delivered on Google Firebase Analytics standard terms and conditions.	https://marketingplatform.google.com/about/analytics/terms/us	https://business.safety.google/adssub-processors

D.2. Authorized transfers to third countries

The Data Processor is authorized to transfer personal data to the sub-processors with processing locations in third countries, cf. Annex B.

The Data Processor shall be free to choose a valid legal basis for the transfer of personal data under applicable Data Protection Laws, including Chapter V of the GDPR.

Assignment of rights to sub-processors

The Data Processor is entitled to assign its rights under this clause to its sub-processors. Accordingly sub-processors may and shall establish a valid legal basis for transfer of personal data to third countries and organizations outside the EEA, which includes entering into appropriate transfer mechanisms under applicable Data Protection Laws, including Standard Contractual Clauses or other legally recognized transfer tools.

Documentation requests

Upon reasonable written request from the Data Controller, the Data Processor shall provide available documentation regarding the legal basis for transfers to third countries, in compliance with applicable Data Protection Laws.