Data Processing Agreement

Standard Contractual Clauses

Pursuant to Article 28(3) of Regulation (EU) 2016/679 (the General Data Protection Regulation) for the Processor's processing of personal data

between

THE CUSTOMER

hereinafter referred to as "the Data Controller"

and

Heyloyalty
CVR 29394458
Jens Baggesens Vej 47
8200 Aarhus N
Denmark

hereinafter referred to as "the Data Processor"

Each a "Party" and collectively referred to as "the Parties".

The Parties HAVE AGREED upon the following Standard Contractual Clauses (the "Clauses") with the purpose of complying with the General Data Protection Regulation and ensuring the protection of privacy and the fundamental rights and freedoms of natural persons.

1. Content

2. Preamble

1. These Clauses set out the rights and obligations of the Data Processor when processing personal data on behalf of the Data Controller.

2. The Clauses are designed to ensure the Parties' compliance with Article 28(3) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th of April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (the General Data Protection Regulation).

3. In connection with the provision of marketing automation services, the Data Processor processes personal data on behalf of the Data Controller in accordance with these Clauses.

4. The Clauses shall take precedence over any similar provisions contained in other agreements between the Parties.

5. Four appendices are attached to these Clauses, which form an integral part of them.

6. Appendix A contains specific information regarding the processing of personal data, including the purpose and nature of the processing, the type of personal data, categories of data subjects, and the duration of the processing.

7. Appendix B contains the Data Controller's conditions for the Data Processor's use of sub-processors and a list of the sub-processors approved by the Data Controller.

8. Appendix C contains the Data Controller's instructions regarding the Data Processor's processing of personal data, a description of the minimum requirements for security measures to be implemented by the Data Processor, and the procedures for supervision of the Data Processor and any sub-processors.

9. Appendix D contains provisions concerning other activities not covered by these Clauses.

10. The Clauses and their appendices shall be retained in written form, including in electronic form, by both Parties.

11. These Clauses do not exempt the Data Processor from obligations imposed upon it by the General Data Protection Regulation or any other applicable legislation.

3. The Data Controller's Rights and Obligations

1. The Data Controller is responsible for ensuring that the processing of personal data is carried out in accordance with the General Data Protection Regulation (see Article 24), with data protection provisions under other EU law or the national law of Member States with these Clauses.

2. The Data Controller has both the right and the duty to determine the purposes and the means of processing personal data.

3. The Data Controller is responsible for ensuring, among other things, that there is a legal basis for the processing of personal data that the Data Processor is instructed to perform.

4. The Data Processor Acts Only on Instructions

1. The Data Processor may process personal data only on documented instructions from the Data Controller, unless such processing is required under EU law or the national law of a Member State to which the Data Processor is subject. Such instructions shall be specified in Appendices A and C. Subsequent instructions may also be given by the Data Controller during the course of processing, but any such instructions must always be documented and retained in written form, including in electronic form, alongside these Clauses.

2. The Data Processor shall immediately inform the Data Controller if, in its opinion, an instruction infringes the Regulation or other data protection provisions under EU or Member State law.

5. Confidentiality

1. The Data Processor shall grant access to personal data processed on behalf of the Data Controller only to persons under the Data Processor's authority who are subject to a duty of confidentiality or an appropriate statutory obligation of secrecy, and only to the extent necessary. The list of authorized persons shall be reviewed regularly, and access shall be withdrawn where it is no longer required. Once access has been revoked, personal data shall no longer be accessible to those individuals.

2. Upon request from the Data Controller, the Data Processor shall demonstrate that the persons under its authority who have access to personal data are subject to the confidentiality obligation mentioned above.

6. Security of Processing

1. Article 32 of the General Data Protection Regulation requires that the Data Controller and the Data Processor, taking into account the state of the art, implementation costs, and the nature, scope, context, and purposes of processing, as well as the varying likelihood and severity of risk to the rights and freedoms of natural persons, implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

The Data Controller shall assess the risks to the rights and freedoms of natural persons posed by the processing and implement measures to mitigate those risks. Depending on relevance, such measures may include:

- Pseudonymization and encryption of personal data;
- The ability to ensure ongoing confidentiality, integrity, availability, and resilience of processing systems and services;
- The ability to restore the availability of and access to personal data in a timely manner in the event of a physical or technical incident;
- A process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures to ensure processing security.

2. Under Article 32, the Data Processor must also independently assess the risks to the rights and freedoms of natural persons arising from the processing and implement measures to mitigate those risks. To facilitate this assessment, the Data Controller shall provide the Data Processor with the necessary information to identify and evaluate such risks.

3. In addition, the Data Processor shall assist the Data Controller in complying with its obligations under Article 32 by providing information on the technical and organizational security measures the Data Processor has already implemented, as well as any other information necessary to demonstrate compliance.

If, in the opinion of the Data Controller, additional measures are required to address identified risks beyond those already implemented by the Data Processor, the Data Controller shall specify such additional measures in Appendix C.

7. Use of Sub-processors

1. The Data Processor shall comply with the conditions set out in Article 28(2) and (4) of the General Data Protection Regulation when engaging another data processor (a Sub-processor).

2. Accordingly, the Data Processor may not engage a Sub-processor for the fulfilment of these Clauses without the prior general written authorization of the Data Controller.

3. The Data Processor has the Data Controller's general authorization to use Sub-processors. The Data Processor shall notify the Data Controller in writing of any planned changes concerning the addition or replacement of Sub-processors at least 30 days in advance, thereby giving the Data Controller the opportunity to object to such changes before the Sub-processor(s) in question are engaged. A longer notice period for specific processing activities may be stated in Appendix B. The list of Sub-processors already approved by the Data Controller appears in Appendix B.

4. When the Data Processor engages a Sub-processor to carry out specific processing activities on behalf of the Data Controller, the Data Processor shall, through a contract or other legal act under EU or Member State law, impose on the Sub-processor the same data-protection obligations as those set out in these Clauses. This must ensure that the Sub-processor provides sufficient guarantees to implement appropriate technical and organizational measures in such a way that the processing will meet the requirements of these Clauses and of the Regulation.

The Data Processor shall therefore ensure that the Sub-processor, at a minimum, complies with the Data Processor's obligations under these Clauses and the Regulation.

5. Copies of Sub-processor agreements and any subsequent amendments shall be made available to the Data Controller upon request, thereby enabling the Data Controller to verify that equivalent data-protection obligations have been imposed on the Sub-processor. Commercial terms unrelated to data-protection content need not be disclosed.

6. The Data Processor shall include in its agreement with the Sub-processor a clause designating the Data Controller as a third-party beneficiary in the event of the Data Processor's bankruptcy, allowing the Data Controller to assume the Data Processor's rights and to instruct the Sub-processor to delete or return personal data.

7. If the Sub-processor fails to fulfil its data-protection obligations, the Data Processor shall remain fully liable to the Data Controller for the performance of the Sub-processor's obligations. This does not affect the rights of data subjects under the Regulation, in particular Articles 79 and 82, against both the Data Controller and the Data Processor, including the Sub-processor.

8. Transfer to Third Countries or International Organizations

1. Any transfer of personal data to a third country or an international organization may only be carried out by the Data Processor on documented instructions from the Data Controller and must always take place in accordance with Chapter V of the Regulation.

2. Where the Data Processor is required under EU or Member State law to transfer personal data to a third country or an international organization without instructions from the Data Controller, the Data Processor shall inform the Data Controller of that legal requirement before processing, unless such notification is prohibited by law for important reasons of public interest.

3. Without documented instructions from the Data Controller, the Data Processor shall not, within the scope of these Clauses:

- Transfer personal data to a controller or processor in a third country or an international organization;
- Entrust the processing of personal data to a Sub-processor in a third country; or
- Process personal data in a third country.

4. The Data Controller's instructions regarding the transfer of personal data to a third country, including the legal basis for the transfer under Chapter V of the Regulation, shall be specified in Appendix C.6.

5. These Clauses shall not be confused with the standard contractual clauses referred to in Article 46(2)(c) and (d) of the Regulation and do not in themselves constitute a legal basis for the transfer of personal data under Chapter V of the Regulation.

9. Assistance to the Data Controller

1. Considering the nature of the processing, the Data Processor shall assist the Data Controller, as far as possible and by appropriate technical and organizational measures, in fulfilling the Data Controller's obligation to respond to requests for the exercise of the data subjects' rights as set out in Chapter III of the Regulation.

This means that the Data Processor shall, as far as possible, assist the Data Controller in ensuring compliance with:

- The duty of information when collecting personal data from the data subject;
- The duty of information where personal data have not been obtained from the data subject;
- The right of access;
- The right to rectification;
- The right to erasure ("the right to be forgotten");
- The right to restriction of processing;
- The obligation of notification 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.

2. In addition to the Data Processor's obligation under Clause 6.3, the Data Processor shall, considering the nature of processing and the information available to it, further assist the Data Controller in:

- The Data Controller's obligation to notify, without undue delay and, where feasible, no later than 72 hours after becoming aware of it, any personal data breach to the competent supervisory authority, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons;
- The Data Controller's obligation to notify, without undue delay, the data subject of a personal data breach when it is likely to result in a high risk to the rights and freedoms of natural persons;
- The Data Controller's obligation to carry out, prior to processing, an assessment of the impact of the envisaged processing operations on the protection of personal data (a Data Protection Impact Assessment);
- 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.

3. The Parties shall specify in Appendix C the necessary technical and organizational measures by which the Data Processor shall assist the Data Controller and to what extent and in what scope. This applies to the obligations referred to in Clauses 9.1 and 9.2.

10. Notification of Personal Data Breach

1. The Data Processor shall, without undue delay, notify the Data Controller after becoming aware of a personal data breach.

2. The Data Processor's notification to the Data Controller shall, where possible, be made no later than 24 hours after the breach has been discovered, in order for the Data Controller to comply with its obligation to notify the competent supervisory authority under Article 33 of the Regulation.

3. In accordance with Clause 9.2(a), the Data Processor shall assist the Data Controller in notifying the breach to the competent supervisory authority. Such assistance shall include providing the following information, as required by Article 33(3):

- The nature of the personal data breach, including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- The likely consequences of the personal data breach;
- The measures taken or proposed by the Data Controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. The Parties shall specify in Appendix C the information that the Data Processor shall provide in assisting the Data Controller with its obligation to notify the competent supervisory authority of a personal data breach.

11. Deletion and Return of Data

1. Upon termination of the services relating to the processing of personal data, the Data Processor shall delete all personal data processed on behalf of the Data Controller and confirm to the Data Controller that the data has been deleted, unless EU or Member State law requires storage of personal data.

12. Audit and Inspection

1. The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with Article 28 of the Regulation and these Clauses and shall allow for

and contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller.

2. The procedures for audits and inspections of the Data Processor and its Sub-processors are set out in Appendices C.7 and C.8.

3. The Data Processor shall grant supervisory authorities, which under applicable law have access to the facilities of either the Data Controller or the Data Processor, access to the Data Processor's physical premises upon presentation of proper identification.

13. Agreement on Other Matters between the Parties

1. The Parties may agree on additional terms concerning the services involving the processing of personal data, such as provisions on liability, provided that such additional terms do not directly or indirectly contradict these Clauses or impair the fundamental rights and freedoms of data subjects as set out in the Regulation.

14. Commencement and Termination

1. These Clauses shall enter into force on the date of signature by both Parties.

2. Either Party may request renegotiation of the Clauses if legislative changes or practical issues give rise to the need for amendment.

3. The Clauses shall remain in force for as long as the service involving the processing of personal data continues. During this period, the Clauses may not be terminated unless other provisions governing the delivery of the service are agreed between the Parties.

4. If the delivery of the services involving the processing of personal data ceases, and the personal data has been deleted or returned to the Data Controller in accordance with Clause 11.1 and Appendix C.4, the Clauses may be terminated by either Party upon written notice.

5. Signatures

On behalf of the Data Controller

Name: _____

Telephone: _____

E-mail: _____

Signature: _____

On behalf of the Data Processor

Name: Nicolaj Balle Ladiges
Title: CEO
Telephone: 26 85 34 14
E-mail: nl@heyloyalty.com

Signature: _____

15. Contact Persons of the Data Controller and the Data Processor

1. The Parties may contact each other via the contact persons listed below.

2. The Parties are obliged to keep each other informed of any changes regarding contact persons.

Data Controller

Name: _____

Telephone: _____

E-mail: _____

Heyloyalty DPO

Telephone: 7027 1337

E-mail: dpo@heygroup.dk

Appendix A – Information about the Processing of Data

A.1 Purpose of the Data Processor's processing of personal data on behalf of the Data Controller

The purpose of data processing is to collect and store the subject's (hereinafter referred to as the contact's) data and interests, in order to personalize and distribute newsletters via text message (SMS), email or other electronic channels containing the contact's data and targeting their specific interests.

A.2 Nature of the Data Processor's processing of personal data on behalf of the Data Controller

- Development and support of the Heyloyalty system, which is a campaign and automation tool for e-commerce.
- The Data Processor provides the Heyloyalty system for the Data Controller's use, within which the Data Controller's contact lists are stored.
- The Heyloyalty system sends newsletters/emails on behalf of the Data Controller to the Data Controller's registered contacts and provides related support.
- Provision of support and consultancy services.
- When a Heycommerce license is purchased, behavioral data about the contact on the customer's website/webshop are collected for the purpose of tailoring newsletters and creating individually customized campaigns. This behavioral data includes "abandoned cart" actions—when a contact adds items to the basket without completing a purchase—and which products and categories the contact searches for or clicks on.
- When the Webpush module is purchased, data about the contact's activity on the customer's website is collected for the purpose of sending webpush notifications (using the Webpush service).
- When the Webpush module is purchased, it is possible to link a webpush permission (if granted) to the existing contact on the list via the Heyloyalty Tracking Script.

The combination of the customer's selected Heyloyalty services, and thereby the nature of the processing, is always visible on the customer's Heyloyalty account under Integration and List Integrations.

A.3 Types of personal data being processed

The data processed will consist of "ordinary personal data" as defined under Article 6 of the Regulation, provided by the contact upon subscribing to newsletters or when subsequently updating their own data. Examples include:

- Contact's first and last name;
- Contact's email address and phone number;
- Contact's interests and preferences;
- Gender;

- Date of birth;
- Address;
- Postal code, city, and country;
- Reference (origin of subscription).

The data collected will appear on the Data Controller's Heyloyalty account in details within the contact lists and, if purchased, within the Data Controller's Heycommerce database.

The Data Controller may request additional information from the contact (via custom-defined fields), including potentially sensitive personal data during registration or subsequent updates.

The Data Processor must be informed and given appropriate notice by the Data Controller if the Data Controller wishes Heyloyalty to process sensitive personal data.

A.4 Categories of data subjects

Contacts who have subscribed, or previously subscribed, to a contact list of the Data Controller and thereby provided consent to receive direct marketing communications.

A.5 Duration of processing

The processing of personal data may commence upon the entry into force of these Clauses and will continue for the duration of the collaboration agreement between the Parties. The processing is not time-limited and will continue until the termination of the agreement.

Appendix B – Sub-processors

B.1 Approved Sub-processors

Name	CVR No.	Address	Description of Processing
Team.Blue Denmark A/S	29412006	Højvangen 4, 8660 Skanderborg	Hosting of data
Ubivox Technologies ApS	27379494	Østre Stationsvej 43, 3rd floor, 5000 Odense C	E-mail services
InMobile	31426472	Axel Kiers Vej 18L, 8270 Højbjerg, Denmark	SMS services

At the time of entry into force of these Clauses, the Data Controller has approved the use of the abovementioned Sub-processors for the described processing activities.

The Data Processor may not—without the Data Controller's prior written consent—use a Sub-processor for any processing activity other than the one described and agreed upon or engage another Sub-processor for that activity.

B.2 Notice period for approval of Sub-processors

No further provisions.

Appendix C – Instructions on the Processing of Personal Data

C.1 Subject of Processing / Instruction

The Data Processor's processing of personal data on behalf of the Data Controller takes place in order to fulfil the cooperation agreement between the Parties and to deliver the services purchased by the Data Controller from Heyloyalty, as reflected on the Data Controller's Heyloyalty account. See further details in Appendix A.2 – Nature of the Processing.

C.2 Security of Processing

The level of security shall reflect the following:

- The Data Processor implements the necessary technical and organizational measures to ensure data protection in accordance with data-protection legislation and Articles 25 and 32 of the GDPR (privacy by design and by default).
- The Data Processor has mapped its personal data processing activities, including an assessment of sensitivity, and performed a security assessment of all data locations and transfer points, implementing appropriate measures according to the risk assessment for the classified personal data.
- The technical and organizational measures ensure protection against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data, and prevent any processing that violates the law.

General security measures:

- The Data Processor must implement encryption and pseudonymization of personal data as risk-reducing measures where it is deemed appropriate.
- Access to personal data must be restricted to persons necessary for the performance of obligations under the cooperation agreement.
- Systems must be implemented to detect, restore, counter and report incidents concerning personal data.
- Transfers of personal data to Sub-processors must be carried out securely.
- All access to personal data from the Data Controller or its representatives occurs through SSL encryption.
- The software delivered under the cooperation agreement includes a role-management system that enables the Data Controller to control its representatives' access to personal data.
- The Data Processor has established a hosting platform ensuring that all personal data are securely stored, protected from unauthorized access, and backed up to allow restoration of all data in case of incidents.
- The Data Processor has implemented software and procedures to maintain a high level of internal IT-security.

Further details on security can be found in Heyloyalty's Privacy Policy on its website.

Authorization and Access Control

Access to personal data occurs only through personal authorization with a unique username and password in the internal systems established by the Data Processor to fulfill its obligations under the collaboration and data-processing agreements.

The Data Processor has ensured that Sub-processors use personal authorization and access control when accessing the Heyloyalty system (where access is necessary for their service).

External Communication Connections

All access to the Heyloyalty system is via SSL encryption.

Outgoing emails are TLS-encrypted, where the contact's email client supports this.

Control of Failed Access Attempts

Unauthorized access attempts are prevented by firewalls, and repeated attempts to access servers are blocked.

Logging

- Logs are kept of the date, and which representative of the Data Processor accesses personal data as part of fulfilling the collaboration agreement.
- Random checks of these logs are carried out to ensure that access occurs only in accordance with authorized instructions.
- Random checks are also conducted to ensure that Sub-processors and their representatives access personal data only when relevant to the services provided or under the Data Processor's direct instruction.

Home and/or Remote Workstations

- Processing of personal data by the Data Processor may be performed from home or remote workstations.
- Access to personal data takes place via encrypted traffic (HTTPS) to and from the Heyloyalty system using industry-standard SSL certificates.
- All employees of the Data Processor authorized to process personal data are subject to a duty of confidentiality, have received appropriate training in data security, and may only use personal data as required to perform the Data Processor's obligations and rights under the collaboration agreement.

C.3 Assistance to the Data Controller

The Data Processor shall, to the extent possible and within the scope described below, assist the Data Controller in accordance with Clauses 9.1 and 9.2 by implementing the following technical and organizational measures:

The Data Processor assists the Data Controller in ensuring compliance with Articles 32–36 of the Regulation concerning security measures, breach notifications and, where relevant, consultation with supervisory authorities.

The Data Processor shall provide all necessary information to enable the Data Controller to document that processing performed by the Data Processor meets these obligations and shall allow and assist with control and audits. The Data Processor is obliged to inform the Data Controller if, in its opinion, an instruction is unlawful.

The Data Processor hereby informs the Data Controller that the collection of personal data must comply with applicable law, specifically noting that contacts must give informed, specific consent to the intended data use when such consent is required by law. The Data Processor also informs the Data Controller that emails and text messages (SMS) sent via the Heyloyalty system are transmitted in plain text and are therefore not suitable for sensitive personal data; access to personal data by contacts should be password-protected. Unencrypted emails and text messages (SMS) are considered inadequate media for ordinary personal data, such as names and addresses.

C.4 Retention Period / Deletion Procedure

Personal data is retained by the Data Processor for the duration of the collaboration or until the Data Controller requests deletion or return of the data.

At the Data Controller's request, the Data Processor shall delete or return all personal data to the Data Controller or a third party designated by the Data Controller and delete all copies, unless retention is required by law.

If no other instruction is provided, personal data shall be deleted 120 days after termination of the collaboration.

Where the Data Controller instructs that the data be returned or transferred, the Data Controller shall determine at that time the method and storage medium to be used. Any chosen medium must be standard for such data transfers.

C.5 Location of Processing

- Heyloyalty's office in Aarhus or at employees' addresses as part of remote work;
- The addresses of approved Sub-processors (as listed in Appendix B.1);
- Personal data received from the customer's contacts are stored by a third party. Data are hosted on servers in Denmark owned by Team.Blue Denmark A/S, with whom a data-processing agreement has been entered into, ensuring data security;
- If the customer chooses to use a third party not directly integrated with Heyloyalty, responsibility for this lies with the customer.

C.6 Instruction regarding Transfer of Personal Data to Third Countries

Unless the Data Controller has provided documented instruction within these Clauses or subsequently regarding transfer of personal data to a third country, the Data Processor is not authorized to perform such transfers under these Clauses.

C.7 Procedures for the Data Controller's Audits and Inspections

The Data Controller may supervise the Data Processor whenever deemed necessary.

The Data Controller or its representative has the right, at reasonable intervals and with prior notice, to conduct on-site audits concerning compliance with this Data Processing Agreement. The Data Controller may also conduct supervision by means of questionnaires, requests for documentation, or written statements.

The Data Controller shall bear its own costs of supervision. The Data Processor shall allocate the resources (mainly time) necessary for the Data Controller to conduct such supervision.

If the Data Processor spends more than the first four hours of the day assisting the Data Controller with supervision, they may be charged at the Data Processor's standard hourly rates, subject to prior agreement for each audit.

If the Data Controller prefers an alternative form of supervision (for example, an independent ISAE 3000 auditor's report on the Data Processor's GDPR compliance), the Data Processor may prepare such a report at the Data Controller's own expense.

C.8 Procedures for Audits and Inspections of Sub-processors

The Data Processor shall appropriately supervise its Sub-processors regarding compliance with the Regulation, other EU or Member State data-protection provisions, and these Clauses. The Data Processor may determine what constitutes appropriate supervision, considering the specific risk associated with the processing carried out by the Sub-processor.

In addition to planned audits, supervision of a Sub-processor may be conducted whenever the Data Processor (or the Data Controller) deems it necessary.

Documentation of such supervision shall be provided to the Data Controller without undue delay. The Data Controller may challenge the scope or method of the audit and may request that a new audit be performed under different terms or methods.

Based on the audit results, the Data Controller is entitled to request the implementation of additional measures to ensure compliance with the Regulation, EU or Member State law, and these Clauses.

Appendix D – Regulation of Other Matters between the Parties

No special conditions are currently noted.