**Framework Agreement on**

**Electronic Data Interchange (EDI)**

**V 3.1**

between the business parties below:

|  |  |
| --- | --- |
|  | «Company»«Additional title»«Street»«ZIP» «CITY»«GLN»«VAT ID Nr.» |

and

|  |  |
| --- | --- |
|  | «Company»«Additional title»«Street»«ZIP» «City»«GLN»«VAT ID Nr.» |

who may act as the sender as well as the recipient of invoice data and are hereinafter referred to as “Parties” or individually as “Party”.

Contents

[1. Preamble - 3 -](#_Toc498520002)

[2. Subject Matter and Purpose - 3 -](#_Toc498520003)

[3. Definitions - 3 -](#_Toc498520004)

[4. Scope of Validity - 4 -](#_Toc498520005)

[5. Admissibility of Evidence and Legal Effect of EDI Messages - 5 -](#_Toc498520006)

[6. EDI Systems and Applications - 5 -](#_Toc498520007)

[7. Responsibility of the Parties Related to EDI - 6 -](#_Toc498520008)

[8. Storage, Inspection and Release - 7 -](#_Toc498520009)

[9. Data Protection and Data Security - 8 -](#_Toc498520010)

[10. Liability - 9 -](#_Toc498520011)

[11. Enforcement, Amendments, Term and Partial Invalidity - 9 -](#_Toc498520012)

[12. Technical Specifications and Requirements - 10 -](#_Toc498520013)

[13. Place of Jurisdiction, Applicable Law - 10 -](#_Toc498520014)

[Annex ./1 12](#_Toc498520015)

[Annex ./2 13](#_Toc498520016)

[Anhang ./3 19](#_Toc498520017)

# Preamble

The Parties have agreed to communicate their invoice data via electronic data interchange (EDI). All former EDI agreements between the parties (INVOIC) will become void upon enforcement of the present framework agreement.

This overall framework agreement is primarily for the purpose of compliance with requirements concerning value added tax, in particular the provisions of the Austrian Value Added Tax Act regarding the genuineness of origin and integrity of the data as well as of the Value Added Tax Ordinance (E-invoice VAT tax, BGBl. II Nr. 516/2012). The framework agreement is based on the recommendation 94/820/EG by the European Commission of October 19, 1994 on the legal aspects of electronic data interchange. Through the use of the recommended European EDI INVOIC agreement legal certainty is to be granted for both Parties and negotiations avoided in the individual case.

The present framework agreement is based on the GS1 Austria/ECR-application recommendation as specified in Annex 1 under “Data Format and Message Types”.

# Subject Matter and Purpose

The present EDI framework agreement regulates the electronic interchange of business data for the processing and invoicing of goods and services within the scope of the basic transaction.

Its purpose is

* determination of the techniques and processes for the exchange of EDI messages between the Parties involved in the EDI in compliance with tax law provisions;
* determination of the legal effect of the exchanged EDI messages; and
* regulation of the other terms between the Parties applicable to the EDI process.

# Definitions

In the present framework agreement the following terms have the following definitions:

* 1. "Sender" is the party who sends the other party an EDI message within the scope of the process described in the framework agreement.
	2. "Operation Time" is the time during which the IT system of a Party is available for receiving EDI messages.
	3. "Designated Data Storage" is the storage device (“Mailbox”) designated by each Party for the recording, storage and retrieval of EDI messages.
	4. "EDI" ('Electronic Data Interchange') is the electronic exchange of EDI messages ard between information systems according to an agreed stand.
	5. "EDI Messages" are structured data, messages and declarations of intent prepared according to the standards and formats set out ECR/. GS1 for electronic communication and processing.
	6. "Recipient" is the party receiving the EDI message within the scope of the process specified in the present framework agreement.
	7. “Basic Transaction” is the contract on goods and services which are prepared, concluded and/or processed underlying the present framework contract.
	8. “UN/EDIFACT” In accordance with the definition by the UN/ECE (United Nations Economic Commission for Europe) the regulations of the United Nations on Electronic Data Interchange in Administration, Trade, Transport and Traffic comprise a number of internationally agreed norms, indexes and guidelines for the electronic interchange of structured data, in particular for the exchange between independent, computer-based information systems in conjunction with the exchange of goods and services.
	9. "Transaction Journal" is the chronological record kept by each party containing all EDI notifications as sent/received.
	10. “Work Days”: Unless otherwise agreed on in the contact data (see Annex ./1), work days are Monday through Friday with the exception of public holidays
	11. “General Office Hours”, unless otherwise agreed on in the contact data (see Annex ./1) are from 9 a.m. until 3 p.m. on work days.

# Scope of Validity

* 1. **EDI Parties**
		1. Party to the EDI processed in the present framework agreement are the parties to the present framework agreement at their business domicile as specified on the title page.
		2. With the written approval of the respective other party works, company sites or branches of a party’s company may accede to the present framework agreement through a written declaration.
	2. **Scope of application, basic transaction**
		1. The Parties will determine the scope of application of the EDI for the rendering of goods, services or the interchange of information in Annex ./1 or a separate agreement.
		2. The contracts agreed on between the parties or General Business Terms will apply to the execution of the basic transaction.
		3. In accordance with the purpose of the present framework agreement the present terms will take precedence over any deviating terms of the basic transaction regarding the form and delivery of declarations of intent and/or the formation of contracts.
	3. **Third party services**

Regarding the performance of the EDI process the Parties have the right to hire a third party to perform their duties provided that the other party is informed of this beforehand. This will not release the Parties from their duties. Each party is responsible vis à vis the other party for actions, errors or omissions of third parties being hired in the same way they are responsible for their own actions unless a party hired the services of a third party at the instructions of the other party.

# Admissibility of Evidence and Legal Effect of EDI Messages

The Parties agree that electronic messages which comply with the norms defined in Annex./1 and are sent in accordance with the regulations of the present framework agreement have the same binding and legal effect as written messages and in the case of a dispute the recording of EDI messages stored by them in accordance with the terms of the present framework agreement is admissible before court and constitutes evidence of the facts contained therein unless contrary evidence is produced.

Every recipient of a message has the right and duty to process these messages as they were received in his IT system except in the case of obvious abuse. Delays by the network operator or operator of an intermediary message transmission service provider as well as transmission errors will be borne by the sender. The recipient of messages must however provide the sender with a printout of the record file in the case of disputes and also a printout of the receipt record where the storage period has not lapsed.

# EDI Systems and Applications

* 1. **Set-up, activation and maintenance of the EDI connection**

The time and type of set-up of the EDI connection as well as the parameters which must be complied with here are agreed on between the parties. EDI providers involved ensure that the data transmitted by the party issuing the invoice are forwarded to the recipient unfalsified and intact.

Agreements with EDI providers are not the subject matter of the present framework agreement and must be regulated with separate contracts, complying with the terms of the present framework agreement in the process.

After the set-up of the EDI connection the parties will agree on a test phase. The parties will jointly decide on the termination of the test phases as well as whether the EDI connection runs flawlessly and can be used in everyday business (“Activation”).

Each party will bear the costs of set-up, any future changes, operation and maintenance of the EDI connection incurred to him.

* 1. **Processing of the messages**

The EDI transmission files will be processed immediately (without culpable delay) after receipt.

EDI messages will be regarded as having been received by the recipient where they are stored within the operation time-resp. where no agreement has been concluded in this regard for the duration of one work day, complying with the agreed formats and standards in the designated data storage (“Mailbox”) of the recipient in such a way that they can be retrieved at his initiative.

* 1. **Maintenance of operational readiness**

Each party will ensure the provision of machines, programs and services necessary for the processing of the EDI in accordance with the specifications of the EDI manual and will make every effort to keep these in a condition appropriate for the operation of the EDI during the term of the present framework agreement.

* 1. **Adjustment to norms and standard**

Both parties intend to adapt the EDI processed under the present framework agreements to the respective latest norms, standards and engineering regulations in the area of EDI on the basis of mutual consent.

* 1. **Operation times and changes to them**

The IT systems of the parties are available for receiving messages on all work days. Extended support can be accessed during the general office hours.

Absences for longer periods planned due to company vacation, maintenance or adjustment work will be reported to the other party by the latest 2 work days before cancelation by telephone or e-mail. In other respects the parties will make every effort to keep disturbances as brief as possible.

The Parties will inform each other of any general restrictions of access for the systems and applications being used for the EDI (on certain days or times) as well as any changes thereof; they will ensure that such restricted operating times are recorded in the EDI manual.

# Responsibility of the Parties Related to EDI

* 1. **General**

The parties involved in the EDI will take suitable measures to ensure that only authorized persons gain access for the operation of the EDI in accordance with the present framework agreement. They will treat the identification and authentication features for the interchange of EDI messages with strict confidentiality and only make them accessible to authorized persons.

* 1. **Liability and risks of the sender**

The sender will ensure that the address of the EDI message being transmitted is correct as well as the designated identification and authentication features. Moreover it is incumbent on him to inspect the EDI messages with regard to subject-matter-related and formal accuracy and completeness in accordance with the prescribed standards and specifications.

The sender will bear the risk of loss or changes of an EDI message sent until receipt in the designated data storage (“Mailbox”) of the recipient.

* 1. **Liability and risks of the recipient**

The recipient is liable for the retrieval and transmission of the EDI messages from the designated data storage (“Mailbox”) as well as for their further processing.

* 1. **Interruptions and disturbances**

Where there is an interruption or error notification during the transmission of an EDI message to the designated data storage (“Mailbox”) of the recipient the sender will be liable for repeating the transmission until receiving feedback on the proper completion or storage.

Where there is no error log by the recipient EDI messages will be regarded as delivered in the form and with the content recorded in the sender’s transaction journal.

Where a party detects an error in data transmission via EDI or discovers that the EDI message he received was not intended for him he will inform the sender immediately, where the latter can be identified, but by the latest within 14 work days and will not process the EDI message any further before he has received the respective instructions from the sender. Messages sent to the wrong/mistaken recipient are to be deleted in agreement with the sender with the exception of recording in the transaction journal.

# Storage, Inspection and Release

* 1. **Keeping of a transaction journal**

During the term of the framework agreement each party will keep a transaction journal on all EDI messages sent/received by him.

* 1. **Inspection and guarantee of genuineness of origin**

The recipient must compare the data sent to him with the information in his master database and only proceed with the processing of an EDI transmission file in the case of a complete match with regard to content and form. Failing this, he is to proceed pursuant to Art. 9.3.

The sender/the party hired by him will be obligated to use the prescribed identification labels in order to guarantee genuineness of the origin of the data and the recipient will be obligated to check these in the corresponding segments of the UN/EDIFACT standards. The sender must cumulatively always use the following identification features:

− the GLN in the UNB segment allocated to the sender/the third party hired by him by GS1

− the GLN in the NAD segment allocated to the sender by GS1;

− the VAT ID number (VAT ID Nr.) allocated to the sender by the Internal Revenue Service in the RFF+VA segment.

Where the identification features (GLN and/or VAT ID/tax number) or personal key data of the sender change the sender must ensure that the recipient is immediately informed (precise advance notice time is to be defined in Annex./1).

The recipient will confirm the change of his key data to the sender (notice of change). The changed identification features may only be used after receipt of the change notification. The use of any previous identification features as from this time will entail an error log to the sender and non-processing (cf. Art. 9.3).

The Parties agree exclusively on a UN/EDIFACT standard for transmission of the EDI messages. The recipient guarantees that he is able to receive and process all EANCOM® versions specified in Annex ./1. The sender will be obligated to specify the EANCOM® version used in every EDI message.

* 1. **Inspection and guarantee of the integrity of the content**

Before the parties commence the EDI process in the production operations and the data being transmitted become binding (productive phase) the parties will first thoroughly test the transmission of EDI messages (test phase). Even during the test phase the parties will use real data but label them in the UNB segment as test data. The sender is responsible for ensuring that the real data being used in the test phase are labeled as test data. The recipient will ensure from the aspect of the system and at the organizational level that the data being transmitted for test purposes are processed but are not treated in any way like real data in the productive phase.

The sender/the third party hired by him is obligated to fill out the core data boxes in the respective UN/EDIFACT standard and as stipulated in Annex ./1. The recipient will check this. Moreover, the recipient will check the plausibility of the individual bits of information to each other in the core data boxes and with regard to the master data (plausibility check).

A component of the plausibility check is the inspection of the EDI message with regard to calculational accuracy, correct VAT tax at the VAT tax rate and the compulsory information for invoices as prescribed by law.

* 1. **Storage duties**

During the storage period applicable at their business domicile the parties will store the EDI messages recorded in the transaction journal on a data carrier according to the applicable regulations for proper recording and storage of business correspondence and accounting records.

* 1. **Release of records**

Each party will provide the other party upon request with a copy of the records on the exchanged EDI messages recorded in their transaction journal at their own expense.

* 1. **Access and Inspection**

The parties agree that the designated EDI coordinator or a designated trustee may access, inspect and make excerpts of the EDI messages exchanged between the parties recorded in the transaction journal of the other party or copies thereof after prior notice, maintaining confidentiality.

# Data Protection and Data Security

* 1. **Data protection**

The data protection regulations are explicitly settled in the “Agreement on the Provision of Data for the Purpose of Processing as a Service and Contract Processing Agreement » and apply as a binding component of the present framework agreement (see Annex ./2).

* 1. **Data security**

The parties will introduce and maintain the necessary and recommended inspection and safety measures and procedures in order to protect the EDI messages against access by unauthorized parties as well as unintentional changes, loss or destruction. Standard data security procedures going beyond this will be stipulated in Annex ./1 of the present framework agreement.

Each party will store a complete, chronological record of all EDI messages in their original form as exchanged between the parties during the business transaction in a secure form in accordance with the deadlines and specifications prescribed by national law.

Unless otherwise prescribed by national laws the messages will be stored by the sender in the format they were transmitted and stored by the recipient in the format they were received.

Where a party detects indications of access/use, change or suppression of declarations of intent, messages and documents exchanged via EDI by unauthorized parties he will make every effort to secure evidence of such an incident, inform the other party immediately and take suitable measures to prevent future incidents.

* 1. **Procedure in the case of error**

To the extent that an error is detected in the process of ensuring genuineness of origin and integrity of the data the entire EDI transmission file will not be processed.

Where an error concerns individual invoice records (EDI messages) in the EDI transmission file detection of an error will entail at least non-processing of the invoice records with the errors; invoice records without errors in contrast may be processed according to the recipient’s instructions.

The errors detected will be documented by the recipient in an error record. The sender will be informed immediately of the errors that were detected and of the non-processing of the data through the transmission or an error log.

* 1. **Confidentiality**

The confidentiality terms are regulated explicitly in the “Confidentiality Agreement” and apply as a binding component of this framework agreement (see Annex ./3).

# Liability

Each party involved in the EDI will assume liability for direct damage and loss incurred to the other party due to disturbances, interruptions, and errors in the exchange of EDI messages to the extent that he himself or a third party hired by him culpably breached the duties and responsibilities imposed on him by the present framework agreement.

To the extent permitted by law the liability amount will be limited to the value of the business transactions executed using EDI affected by the disturbance.

The parties will not be liable for the effect of technical disturbances outside of their scope of responsibility, in particular due to disturbances or interruptions of duly operated and maintained IT systems or data transmission services, or for the involvement of unauthorized third parties in spite of adequate data security precautions.

The exclusion of liability will not refer to damage to life, limb or health incurred on the basis of negligent breach of duty by a party.

Every case of liability for indirect or consequential damage in connection with the use of EDI is explicitly excluded to the extent permitted by law.

Guarantee and liability for the goods and services procured by EDI will be determined according to the terms of the basic transactions.

# Enforcement, Amendments, Term and Partial Invalidity

* 1. **Enforcement**

The present framework agreement will take force upon the date of signing (date of the last party to sign) by the parties for an indefinite period.

* 1. **Amendments**

Where necessary the parties will regard additional or alternative terms to the framework agreement concluded in writing as part of the framework agreement as from the time of their signing.

Should there be a legitimate need for an amendment due to an amendment of the law, Supreme Court order, changed opinions by the fiscal authorities or a deviation from the previous recommendation by the European Commission either party may demand an adjustment of the framework agreement. There is a legitimate need for an amendment where the amendment of the law, Supreme Court order, changed opinion of the fiscal authorities or deviation from the previous recommendation by the European Commission objectively entails a (partial) invalidity of regulations in the EDI agreement or a legal gap results from this. The principle of whether it is acceptable or not to one of the parties is irrelevant. This will apply in particular where input tax return by the recipient could be jeopardized by the aforementioned amendments.

Unilateral amendment of Annex ./1 integrated into the present agreement is admissible where

− a new EANCOM® version is being processed by the recipient or an EANCOM® version previously specified in Annex./1 can no longer be processed or

− the recipients specified in Annex ./1 change or

− the core data boxes specified in Annex ./1 are changed by the recipient.

The amendment will be enforced on the date of the notification of the amendment and will then as part of the present framework agreement replace Annex ./1 which has been valid up until this date (date of amendment) provided that the sender does not object to the amendment in text form within two weeks after receipt of the notification of the amendment. Where an objection is made against the amendment the parties will jointly inspect continuation of the framework agreement. Where no agreement is reached in this context either party will have the right to exceptional termination.

* 1. **Term**

Either party may terminate the framework agreement concluded for an indefinite term with 4 weeks’ notice.

In the case of a relevant ground either party may terminate the framework agreement exceptionally. There is a relevant ground in particular where the other party breaches cardinal terms of the present framework agreement or breaches terms repeatedly.

Termination of the framework agreement will only have an effect on transactions after this date.

* 1. **Contestability, Partial Invalidity**

The invalidity or contestability of one or several of its terms will not render the present framework agreement invalid. In such a case the parties will make every effort to replace the invalid or contested term with a valid and feasible term which comes as close as possible to the legal and economic substance of the invalid term. This will apply accordingly to legal gaps.

* 1. **Prescribed formalities**

Any amendments of the present framework agreement must be in writing; this will also apply to the waiver of the writing requirement; in contrast, textual form is sufficient for addenda or amendments of Annex ./1.

# Technical Specifications and Requirements

Annex ./1 contains the technical, organizational and procedural specifications (e.g. ECR message profiles) and requirements for the operation of EDI in accordance with the terms of the present framework agreement, which include e.g. the following terms:

* Contact data and contact partners
* Message types

# Place of Jurisdiction, Applicable Law

The Commercial Court in Vienna is the agreed place of jurisdiction for any disputes arising from the present framework agreement.

The present framework agreement is subject to Austrian law excluding the UN Sales Convention, international private law and its provisions on the conflict of laws.

**Annexes:**

 Annex ./1 Message Types and Formats

Annex ./2 Agreement on the Provision of Data for the Purpose of Processing as a Service and Contract Processing Agreement

Annex ./3 Confidentiality Agreement

|  |  |  |
| --- | --- | --- |
|  |  |  |
| Place, date |  | Place, date |
|  |  |  |
| Signature |  | Signature |
|  |  |  |
| Company |  | Company |

## Annex ./1

**to the**

**Framework Agreement on Electronic Data Interchange**

 **(EDI)**

***Example:***

**Contact data and contact partners**

* Technical issues
* Contract-related issues
* Mailing address
* Fax address
* E-mail address

**The parties communicate via the following method of transmission:**

* Communication methods and platforms (e.g. eXite, FTP, WEB EDI etc.)

**Bilateral agreements to be specified in further detail regarding run-up times, etc. may be concluded, such as:**

In the case of disturbances which temporarily prevent a Party from participating in the EDI, the other party must be informed immediately, if possible in writing (e-mail) or over the telephone. The parties will then exchange the corresponding data, messages and declarations of intent with the means and processes in the annex intended as provisional substitutes in such situations.

Should the possibilities to send EDI messages foreseeably not be available for a longer period of time the Parties will agree to temporarily or permanently suspend the EDI.

The recipient will inform the sender at least two weeks before the change in the text form and send him the entire new Annex 1./ at the same time (Notification of amendment).

**Data Format and Message Types**

The present framework agreement is based on the GS1 Austria/ECR application recommendation of the corresponding EDI message types published on GS1 homepage (<http://www.gs1.at>) in the download area. At the time of conclusion of the contract the following message types are active: ……………………………… .

##  Annex ./2

**Agreement on the Provision of Data for the Purpose of Processing as a Service and Contract Processor Agreement**

Preamble

As from May 25, 2018 the Guideline(EU) 2016/679 by the European Parliament and Council of April 27, 2006 on the protection of natural entities in the processing of personal data, free data traffic and for the rescission of Guideline 95/467EG (abbreviated: Data Protection Basic Ordinance, DSGVO) will apply in Austria. According to this it is indispensable to incorporate the following regulations on the DSGVO even before the DSGVO takes effect and to declare them binding together with the relevant agreement as from May 25, 2018.

Currently, the 2000 Data Protection Act 2000, BGBl. I Nr. 165/1999 (DSG 2000) is applicable in Austria and will continue to be in force even after May 25, 2018 outside of the scope of application of the DSGVO.

In consideration of these premises, pursuant to § 10 DSG 2000 the following agreement is being concluded between the parties which will be binding until May 24, 2018 with regard to Items 1-8 of the relevant agreement. As from May 25, 2018 Items 1-6 will be replaced by Item I. –VII of the relevant agreement and will continue to apply without restrictions together with Items 7-8 after May 25, 2018.

|  |  |  |
| --- | --- | --- |
| Hereinafter referred to as Client/resp. after May 25, 2018 the Responsible Party |  | Hereinafter referred to as Service Provider/resp. after May 25, 2018 Contractor Processor |
| REWE International AGIndustriezentrum Niederösterreich Süd, Straße 3, Objekt 162355 Wiener Neudorf  |  |  |

|  |
| --- |
| **Work being carried out/applications:** (in particular:Purpose and duration, type and nature of processing, type of personal data) |

The Service Provider will be obligated to use the data and processing results exclusively within the scope of the Client’s orders and to return them to the Client or to only communicate them after his written order. Likewise, use of the data provided for the Service Provider’s own purposes require such a written order. Use of data by the Service Provider for his own purposes is prohibited without the prior written consent of the Client. The Service Provider declares that there are no legal obstacles to the agreed contract data processing. Should the legal situation change and the agreed contract data processing no longer be able to be carried out in the agreed form the Service Provider will immediately inform the Client of this. In such a case the Client may suspend provision of the data and dissolve the present contract on a relevant ground.

The Service Provider declares in a legally binding manner that he imposed the duty of confidentiality as defined by §15 DSG 2000 on all persons hired for data processing before start of the work. In particular the duty of confidentiality by the persons hired for handling the data traffic will continue to apply after termination of their work and departure from the Service Provider. The duty of confidentiality also applies to data of legal entities and partnerships under Commercial Law.

The Service Provider declares in a legally binding manner that he has taken adequate safety measures as defined by § 14 DSG 2000 in order to prevent the data from being improperly used or accessed without authorization by third parties, being unintentionally or accidentally modified, lost or disclosed or otherwise used in breach of the applicable statutory provisions or terms of the present contract or the terms of the confidentiality agreement concluded between the Client and the Service Provider. In addition, the technical and organizational measures of the Service Provider as set out in Annex 1 to the present agreement will apply.

The Service Provider may hire another company (the "Subcontractor") with the written consent of the Client for the processing, storage and/or handling of the Client’s data. However, he will be obligated to conclude a contract as defined by § 10 DSG 2000 with the Subcontractor. In this contract the Service Provider must ensure that the Subcontractor assumes the same duties incumbent on the Service Provider on the basis of the present agreement.

The Service Provider will ensure for the technical and organizational prerequisites that the Client complies with the terms set out in § 26 (Information Right), § 27 (Right to Data Correction or Deletion) and § 28 (Right to Objection) DSG 2000 vis à vis the parties concerned within the statutory periods and can fulfill them to the extent stipulated by law and will provide the Client with all information and data necessary for this. The Service Provider will be obligated to immediately inform the Client of any such requests received by the Service Provider and forward them without delay to the Client. Likewise, any declarations of revocation by the parties concerned received by the Service Provider regarding any declarations of consent made by them must be forwarded immediately to the Client. The Service Provider will not respond to any such enquiries or obey them without having been instructed beforehand by the Client. In particular the Service Provider will not obey any request for deletion of data without having been instructed beforehand by the Client. The Service Provider will further take technical and organizational precautions to ensure that the Client is able to comply with the “data breach notification duty” set out in § 24 Sect. 2a DSG 2000 to the extent prescribed by law and within the periods prescribed by law. In particular the Service Provider will immediately inform the Client of any type of illegal use or loss of the personal data provided by the Client.

After completion of the service the Service Provider is obligated to return to the Client all processing results containing data provided by the Client as well as all copies thereof in a format specified by the Client/ resp. to continue to store them secured against unauthorized access at his instructions or to delete them at his instructions. Any type of deletion of data or processing results will require prior written instructions by the Client.

The Client has the right to access the systems used by the Service Provider for the relevant contract data processing and to enter the premises provided by the Service Provider for this purpose for inspection of the safety measures taken by the Service Provider. Such access or entry must take place with an advance announcement three days beforehand by the Client or a third party assigned by him accompanied by an informed representative of the Service Provider. In the case of suspicion or indication of major breaches of safety precautions by the Service Provider or third parties the Client is to be immediately granted access to the system/entry to the premises being used.

The present agreement is subject to Austrian substantive law under exclusion of the provisions on the conflict of laws.

Amendments of and addenda to the present contract as well as legally significant declarations on the basis of the agreement, must be in writing. The writing requirement must also be complied with when waiving the writing requirement itself. There are no verbal ancillary agreements to the present agreement. The invalidity of individual terms will not affect the validity of the remaining terms. The invalid or infeasible terms will be replaced by valid and feasible terms which come as close as possible to the intended economic purpose. The contractual parties will be obligated to transfer the duties from the present agreement passing ex lege explicitly and in writing to the respective legal successor (s) and to subject the latter in turn to transfer to the next legal successors. Unless the contractual parties stated otherwise the business addresses specified in the present contract are the delivery points for deliveries. The present agreement is being drawn up in duplicate and each party will receive one copy.

**Contract Processor Agreement in accordance with Art 28 Sect. 3 DSGVO**

As already stated in the Preamble of the relevant agreement, as from May 25, 2018, Items 1-6 of the relevant agreement will be replaced by Items I. -VII. Items 7. - 8. will continue to be in force even after May 25, 2018 and will continue to apply jointly with the following Items of I. – VII. of the relevant agreements without restrictions.

The Contract Processor will be obligated to use personal data and processing results exclusively at the documented instructions of the Responsible Party and to process them for the Responsible Party-even with regard to provision of personal data to a third party country or international organization unless the Contract Processor is obligated by law to perform the questionable processing (e.g. disclosure to an authority). In such a case the Contract Processor must inform the Responsible Party in accordance with Art 28 Sect 3 lit a DSGVO where permitted. Moreover, use of the data for his own purposes and the return of data provided is only to be carried out at the written instructions of the Responsible Party. Use of the data by the Contract Processor for his own purposes is not permitted without the prior written consent of the Responsible Party. Moreover, the Contractor Processor declares that there are no legal impediments to the contract processing. Should the legal situation change and the agreed contract processing no longer be able to be carried out in the agreed form the Contractor Processor will immediately inform the Responsible Party. In such a case the Responsible Party may suspend provision of the data and prematurely dissolve the present contract on a relevant ground. Furthermore, the Contract Processor is obligated pursuant to Art 28 Sect. 3 lit a DSGVO to immediately inform the Responsible Party should an instruction breach the DSGVO or other norms of applicable law.

The Contract Processor declares in a legally binding manner that he has imposed the duty of confidentiality on all persons hired prior to start of the work in accordance with Art 28 Sect. 3 lit b and Art 90 DSGVO. In particular, the duty of confidentiality of the persons hired to handle the data traffic will continue to apply after termination of their work and departure from the Contract Processor. The duty of confidentiality must also be complied with for data of legal entities and partnerships.

The Contract Processor declares in a legally binding manner that he has taken an adequate level of protection as defined by Art 28 Sect. 3 lit c DSGVO (Data Security Measures) and of Art 32 DSGVO in order to prevent unintentional or illegal destruction, loss, modification or unauthorized disclosure of personal data or that the data are otherwise used in breach of the applicable statutory provisions and the terms of the present contract or the terms of the confidentiality agreement concluded between the Responsible Party and the Contract Processor. Moreover, the technical and organizational measures of the Contract Processor as set out in Annex 1 to the present agreement will apply.

The Contract Processor can hire another company (the “Subcontractor”) with prior written consent by the Responsible Party for the processing, storage and/or handling of the Responsible Party’s data. However, he must impose a contract as defined in Art 28 ff. DSGVO (Subcontract processing agreement) on the subcontractor. In this contract the Contract Processor must ensure that the Subcontractor enters into the same duties the Contract Processor is entering into on the basis of the present agreement. The Contract Processor further declares in accordance with Art 28 Sect. 4 DSGVO that he concludes agreements with the Subcontract Processor which have a content equivalent to the relevant contract processing agreement. The Contract Processor will be liable for the fault of a subcontract processor in the same way as for his own fault. The Contract Processor will be liable pursuant to Art 82 DSGVO vis à vis every person to whom material or intangible damage was incurred by the breach of the statutory duties.

The Contract Processor as well as a Subcontract Processor hired by the Contractor Processor will ensure with regard to the technical and organizational requirements that the Responsible Party complies in particular with the provisions of Art 15 DSGVO (Information Right), Art 16 DSGVO (Right to Correction), Art 17 DSGVO (Right to Deletion), as well as Art 21 DSGVO (Right to Objection) vis à vis the parties concerned within the statutory periods to the extent required by law and will provide the Responsible Party with the necessary information and data for this. The Contract Processor will be obligated to immediately inform the Responsible Party of any such requests received by the Contract Processor and to forward them to the Responsible Party without delay. Likewise, any declarations of revocation by the parties concerned received by the Service Provider regarding any declarations of consent made by them must be forwarded immediately to the Client. The Service Provider will not respond to any such requests or obey them without having been instructed beforehand by the Client. The Service Provider will further take technical and organizational precautions to ensure that the Responsible Party is able to comply with the duty to report the breach of protection of personal data of the persons concerned as set out in Art. 33 DSGVO to the extent prescribed by law and within the periods prescribed by law (“data breach notification duty”) and furthermore is able to implement the privacy impact assessments and prior consultations. In particular the Contract Processor will report any illegal use or loss of personal data provided by the Responsible Party immediately to the Responsible Party.

V.

After completion of the service the Contract Processor is obligated to return to the Responsible Party all processing results and documents containing data provided by the Responsible Party as well as all copies hereof in a format specified by the Responsible Party/to continue to store them secured against unauthorized access or to have them destroyed according to instructions. Any form of destruction of data or processing results will require prior written instructions by the Responsible Party.

VI.

The Contract Processor is obligated pursuant to Art 30 DSGVO to keep an adequate record of processing work for each responsible party in compliance with the legal requirements.

VII.

The Responsible Party has the right to access the systems used by the Contract Processor in the relevant contract data processing for the purpose of inspection and to the premises used by the Contract Processor for this purpose. Such access or entry will require prior advance notice of three days by the Responsible Party or a third party hired by him accompanied by an informed representative of the Contract Processor. In the case of suspicion or indication of major breaches of security precautions by the Contract Processor or third parties the Responsible Party must be immediately granted access to the system or entry to the premises being used.

|  |  |  |
| --- | --- | --- |
| Company signing for the Client/”Responsible Party” after May 25, 2018 |  | Company signing for the Service Provider/”Contract Processor” after May 25, 2018 |
| REWE International AG |  |  |
| Date:  |  | Date: |

##  Anhang ./3

**NON DISCLOSURE AGREEMENT**

concluded between

**REWE International Dienstleistungsgesellschaft m. b. H.**

Industriezentrum Niederösterreich Süd, Straße 3, Objekt 16

2355 Wiener Neudorf

and

|  |
| --- |
|  |
|  |
|  |

The "Service Provider":

**Preamble**

The non-disclosure of confidential information to third parties is of utmost importance to RIAG-IT and the other affiliates of REWE to whom this information might relate, especially that this confidential information may not be divulged in any form, or be used or published for purposes other than those listed in this preamble.

In view of the foregoing, the parties agree to the following:

1. **Duty of Confidentiality**
	1. The Service Provider shall maintain strict confidentiality and not disclose confidential information as defined in clause 2 and shall ensure that third parties other than those named under clause 1.2 do not gain access to confidential information. In particular, this duty of confidentiality includes an obligation not to use or disclose confidential information within the meaning of clause 2 for one's own or for third-party purposes other than those named in the preamble.
	2. The Service Provider shall only disclose confidential information to those employees and employees of a legal entity controlled by the Service Provider, or which the Service Provider is (individually or jointly) controlled by ("control" means directly or indirectly holding or controlling over 50 percent of voting rights) and selected external parties mentioned by name, such as lawyers and other advisors and board members, who must be granted access for the purposes listed in the preamble. The Service Provider shall impose this duty of confidentiality upon all persons who have legitimate access to confidential information.
	3. RIAG-IT shall not disclose any concepts and offers created by the Service Provider or other confidential information that has been identified as such or that has been described as confidential when communicated orally, to any third parties and shall only use such information for the purposes described in the preamble.
	4. Furthermore, in the event that they are legally obliged to disclose the received information, both parties shall undertake to inform the other party of this immediately so that the other party may take the necessary measures to maintain information confidentiality to the maximum extent possible.
	5. Both parties shall undertake to comply with the provisions of the Austrian Data Protection Act (Datenschutzgesetz).
2. **Confidential information**
3. 1. Confidential information for the purposes of this agreement shall include this agreement as well as all addenda and appendices to it, as well as the fact that the parties are holding or aim to hold talks and negotiations regarding the project described in more detail in the preamble, including the contents of these talks and negotiations.
	2. Confidential information for the purposes of this agreement shall also include any information described or identified as confidential about RIAG-IT and other REWE affiliates, all information described or identified as confidential, especially information regarding the description of systems operations, RIAG-IT in-house developments, other software, drafts and plans, licensing information, which is disclosed to the Service Provider, whether orally or in writing, including data storage devices. In the event that the information is disclosed orally, its confidential nature must be indicated.
	3. Any information which (i) is generally known or publicly available at the time of signing this agreement, (ii) or becomes generally known or publicly available at a later point but not due to a breach of this non-disclosure agreement, (iii) or which was demonstrably legitimately known to one of the parties before conclusion of this agreement, (iv) or which was developed by the receiving party independently from the disclosing party, shall not be considered confidential.
4. **Written documents**
5. 1. Insofar as written documents containing confidential information or confidential information in any other tangible form are conveyed, copies shall be permitted exclusively for implementing the purposes described in the preamble. Both parties shall undertake to ensure that only those employees, selected external parties such as lawyers, accountants and auditors, other advisors and/or board members who must be granted authorized access to confidential information in accordance with point 1, shall have been granted access to the aforementioned documents including copies and other tangible materials.
	2. Both parties shall immediately return or destroy all documents, data storage devices, and copies submitted to them as well as their own notes regarding confidential information in the event that
		* 1. one of the parties is no longer interested in pursuing the purposes described in the preamble;
			2. the agreed time period for talks and negotiations has elapsed;
			3. they have been requested to do so by the other party in writing.
	3. Each party explicitly acknowledges that they have no right of retention - with the exception of statutory storage periods - to such documents and that all documentation is to be returned without reimbursement of expenses.
6. **Intellectual Property**

Neither party shall acquire any form of ownership rights or rights of use to information, documents, know-how, property rights etc. received from the other party. All intellectual property rights or copyrights shall remain with the disclosing party.

1. **Liability**

The parties exclude any liability and warranty for the completeness and accuracy of the disclosed information. This does not apply to cases of intent or gross negligence.

1. **Contractual penalty**

In the event of any breach of the contractual obligations provided for under this agreement, RIAG-IT may charge a contractual penalty of EUR XX,XXX (in words XXXXXX) without delay, which shall be payable irrespective of loss or culpability‑ and the Service Provider undertakes to pay the respective sum. RIAG-IT may assert a claim for damages going beyond the contractual penalty.

1. **Term of the non-disclosure agreement**

All duties of confidentiality are valid for a period of 5 years following the disclosure of the respective confidential information.

1. **Miscellaneous provisions**
2.
3.
4.
5.
6. 1. This agreement does not oblige either of the parties to disclose or receive confidential information.
	2. Neither party shall have the right to assign or to otherwise transfer or delegate the rights or obligations under this agreement without prior written permission from the other party.
	3. The receipt of confidential information under this agreement shall not impose any limitations on the receiving party with regard to the following activities:
7. the provision of competing products or services to those of the disclosing party to third parties;
8. the provision of products or services to competitors of the disclosing party; or
9. deployment of their employees at their own discretion.
	1. The receiving party shall 1) comply with all applicable import/export provisions, as well as any associated embargo provisions and provisions regarding trade restrictions and sanctions and 2) in the absence of an applicable administrative order as stipulated in the applicable export/import provisions, not export or re-export, whether directly or indirectly, technical data or software within the framework of this agreement (including products that result from this technical data or software) to a country prohibited according to the provisions stated above or into a prohibited country (this also applies to the disclosure to a citizen of one of these countries, irrespective of location). The provisions of this clause shall continue to have effect after termination or expiry of this agreement as well as for the abovementioned term of the duty of confidentiality and shall be maintained at least until they are fulfilled.
	2. The exclusive court of jurisdiction for any disputes arising under and in connection with this agreement, as well as for its existence and following its termination, is the competent court of jurisdiction for commercial matters in Vienna.
	3. This agreement shall be governed by Austrian law to the exclusion of the conflict of laws rules.
	4. Should any provision of this agreement be or become invalid, this shall have no effect on the validity of the other provisions of this agreement. The invalid provision(s) shall be replaced by a provision that, within the boundaries of law, comes closest to the will of the parties and most closely approximates the commercial effect of the invalid provision(s).
	5. Any changes or additions to this agreement must be made in writing in order to be valid. This also applies to any departure from the written form requirement. No collateral agreements have been made.

Wiener Neudorf, dated 15/11/17

 REWE International Dienstleistungsgesellschaft m. b. H**.**

\_\_\_\_\_\_\_\_\_\_\_\_\_, dated 15/11/17

 The service provider