Contract for order processing according to GDPR (Art. 28 DS-GVO)

[as of May 2018]

Agreement

between

company:

Customer No.:

- Responsible person - hereinafter called client -

and

Clarity & Success Software GmbH, Bokeler Str. 28, 33790 Halle/Westf

- processor, hereinafter referred to as contractor -

Please read, fill in all fields highlighted and sign on page 9

For specific cases, an agreement is required under data protection law, which formally states that:

a) you are willing to provide us with your data for processing and if necessary

b) we treat this data with absolute confidentiality and delete it on our systems after completion of the order, if the data are no longer needed.

Therefore, it is necessary to complete the following order processing agreement so that you and we will comply with data protection and you have the assurance that your information is protected.

The individual stipulations of this agreement apply in each case to the aforementioned parties as well as to the companies affiliated with the parties, insofar as these are processed for or by this data on behalf of the customer. The list of included branches for the client is attached as Annex 2 to this contract.

1. Subject and duration of the contract

(1) Subject

The subject matter of the contract is based on the performance agreement **Hotline Agreement (support contract), Software Maintenance Agreement (update contract) and Licence Contract** (up to version 2.84) or **General Contractual Conditions for Software, Hotline and Updates** (from version 3.0 [Evolution])

of _____ *(date of signature of the contracts)*

to which reference is made here (hereinafter the performance agreement). In particular, order processing also includes the following measures:

☐ Access to databases of the Clarity & Success POS and merchandise system which is currently in use and all kind of data

☐ Access to customer data and sales data (day-end closings, stock movement etc.)

☐ Remote maintenance to data processing units of the client, incl. screenshots of permanent needed program settings without any personal related data.

☐ Data collection is carried out by sending by the client to the contractor or by download via remote maintenance with knowledge and permission of the client. Processing will be done only in case of support queries, to update the software or the database or for correction of the database. The data collected won't be used for other purposes and won't be passed on to third parties. Once the task is finished, the data will be deleted on the Clarity & Success-System if they won't be needed any longer.

(2) Duration

The duration of this contract (term) is the duration of the service level agreement.

2. Specification of the content of the order

(1) Nature and purpose of the intended processing of data

The nature and purpose of the processing of personal data by the contractor for the client are described in detail in the service agreement referred to in point 1.1.

The provision of the contractually agreed data processing takes place exclusively in a member state of the European Union or in another Contracting State to the Agreement on the European Economic Area. Any transfer to a third country requires the prior consent of the client and may only take place if the special requirements of Artt. 44 ff. DS-GVO(GDPR) are met.

The adequate level of protection in

- ☐ has been confirmed by an adequacy decision of the Commission (Article 45 (3) of the GDPR);
- ☐ is produced by binding internal data protection regulations (Art. 46 para. 2 lit. b i.V.m. 47 DS-GVO)(GDPR)
- ☐ is produced by standard data protection clauses (Article 46 (2) (c) and (d) DS-GVO)(GDPR)
- ☑ is produced by approved codes of conduct (Art. 46 para. 2 lit. e in conjunction with DS-GVO)(GDPR)
- ☑ is produced by an approved certification mechanism (Article 46 (2) (f) of the 42DS-GVO(GDPR))
- ☑ Is made and produced by an approved certification mechanism (Article 46 (2) (f) lit. e in conjunction with of the 42 GDPR
- ☑ Is made my other mechanisms: Audit (Article 46 para 2 litt a and b DS-GVO)

(2) Type of data

- ☑ The subject of the processing of personal data are the following data types / categories (enumeration / description of data categories)
- ☑ Personal master data
- ☑ customer data, customer history
- ☑ sales data (contractual relationship, product or contract interest)
- ☑ Product data
- ☑ inventory data
- ☑ Supplier data
- ☑ Purchasing data
- ☑ Repair data
- ☑ Employee data
- ☑ Communication data (eg. telephone, email)
- ☑ Contract Master data
- ☑ Contract settlement and payment data
- ☑ Planning and control data

(3) Categories of data subjects

The categories of persons affected by processing include:

- ☑ customers
- ☑ prospects
- ☑ subscribers (for example newsletter, customer magazine)
- ☑ employees
- ☑ suppliers
- ☑ sales representatives
- ☑ contact

3. Technical-organisational measures

(1) The contractor must document the implementation of the technical and organisational measures set out prior to the award of the contract and prior to processing, in particular with regard to the specific execution of the order, and hand them over to the client for review. If accepted by the client, the documented measures become the basis of the contract. Insofar as the inspection / audit of the client results in a need for adjustment, this must be implemented by mutual agreement.

(2) The contractor has the security gem. Arts. 28 para. 3 lit. c, 32 DS-GVO(GDPR), in particular in conjunction with Article 5 (1) (2) DS-GVO(GDPR). Overall, the actions to be taken are data security measures and to ensure a level of protection appropriate to the level of risk with regard to the confidentiality, integrity, availability and resilience of the systems. The state of the art, the implementation costs and the nature, scope and purpose of the processing as well as the different probability and severity of the risk for the rights and freedoms of natural persons within the meaning of Art. 32 para. 1 DS-BER must be taken into account. Details in Appendix 1].

(3) The technical and organisational measures are subject to technical progress and further development. In that regard, the contractor is permitted to implement alternative adequate measures. In doing so, the safety level of the specified measures must not be underset. Significant changes must be documented.

4. Correction, restriction and deletion of data

(1) The contractor may not correct, delete or restrict the processing of the data processed on behalf of the contract, but only according to the client's documented instructions. Insofar as an affected person directly addresses the contractor in this regard, the contractor will immediately forward this request to the client.

(2) Insofar as included in the scope of services, the cancellation concept, the right to be forgotten, rectification, data portability and information according to the client's documented instructions are to be ensured by the contractor directly.

5. Quality assurance and other obligations of the contractor

In addition to compliance with the provisions of this order, the contractor has statutory obligations under Art. 28 to 33 DS-GMOs(GDPR); In particular, it ensures compliance with the following requirements:

a) Written order of a data protection officer who carries out his activity in accordance with Art. 38 and 39 DS-GVO(GDPR).

Its contact details are communicated to the client for the purpose of direct contact. A change of the data protection officer will be communicated to the client immediately.

As data protection officer (s), the contractor currently has Mr / Ms [entry: first name, name, organizational unit, telephone, e-mail].

b) The preservation of confidentiality under Art. 28 para. 3 sentence 2 lit. b, 29, 32 para. 4 DS-GVO. The contractor will use only employees who are committed to confidentiality and who have been previously familiarized with the data protection regulations that are relevant to them. The Contractor and any person subordinated to the Contractor who has access to personal data may process such data only in accordance with the instructions of the Client, including the powers granted in this Contract, unless they are legally obliged to process.

c) c) The implementation and adherence to all technical and organizational measures required for this contract in accordance with art. 28 para. 3 sentence 2 lit. c, 32 DS-GMO
[Details in Appendix 1].

d) The client and the contractor cooperate with the supervisory authority on request to fulfill their duties.

e) Immediate information to the client about control actions and measures of the supervisory authority, in that as they relate to this order. This also applies insofar as a competent authority has determined in the context of an administrative or criminal procedure with regard to the processing of personal data in the processing of orders by the contractor.

f) Insofar as the client himself is subject to inspection by the supervisory authority, an administrative offense or criminal proceeding, the liability claim of a data subject or a third party or any other claim in connection with order processing by the contractor, the contractor shall support him to the best of his ability.

g) The contractor shall regularly review the internal processes as well as the technical and organizational measures to ensure that the processing in its area of responsibility complies with the requirements of applicable data protection law and that the protection of the data subject's rights is ensured.

h) verifiability of the technical and organizational measures taken towards the client within the scope of his control powers according to section 7 of this contract.

6. Subcontracting

(1) For the purposes of this regulation, subcontracting means such services which directly relate to the provision of the main service. This does not include ancillary services provided by the contractor, e.g. as a telecommunications services, postal / transport services, maintenance and user service or the disposal of data carriers and other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing facilities. However, the contractor is obliged to take appropriate and legally compliant contractual agreements and control measures in order to ensure data protection and data security of the client's data, even with outsourced ancillary services.
(2) The contractor may only commission subcontractors (other processors) after prior express written consent from the client.

a) The client agrees to the assignment of the following subcontractors under the condition of a contractual agreement in accordance with Art. 28 para. 2-4 DS-GVO (GDPR):

Company	Address/country	Trade/Business
byteprojects	Adelbyer Kirchenweg 36, 24943 Flensburg, Germany	Data transfer via server
Rapidmail GmbH	Augustinerplatz 2, 79098 Freiburg i.Br., Germany	Mail dispatch (e.g. newsletter)
Reisswolf GmbH	In der Heide 2, 33428 Harsewinkel, Germany	Document destruction in compliance with data protection
itao GmbH & Co. KG	Carl-Bertelsmann-Str. 81, 33332 Gütersloh, Germany	Creating and maintaining of the contratctor’s homepage (incl. the password protected customer area))

a) The change of the existing subcontractor is permissible insofar as:

- the contractor such outsourcing to subcontractors to the client a reasonable time in advance in writing or in writing and displays

- the client does not object to the planned outsourcing in writing or in text form until the date of transfer of the data to the contractor and

- a contractual agreement in accordance with Art. 28 para. 2-4 DS-GVO(GDPR) is used.

(3) The transfer of personal data of the client to the subcontractor and its initial action shall only be permitted upon submission of all conditions for subcontracting.

(4) If the subcontractor provides the agreed service outside the EU / EEA, the contractor shall ensure that the data protection law is admissible by taking appropriate measures. The same applies if service providers within the meaning of para. 1 sentence 2 are to be used.

(5) Further outsourcing by the subcontractor requires the express consent of the main client (at least in text form); All contractual arrangements in the chain of contract are also to be imposed on the additional subcontractor.

7. Control rights of the client

(1) The client has the right to carry out inspections in consultation with the contractor or to have them carried out by examiners to be named in individual cases. He has the right to satisfy himself of the compliance of this agreement by the contractor in his business through spot checks, which are usually timely to register.

(2) The contractor shall ensure that the client can satisfy himself of the compliance with the obligations of the contractor in accordance with Art. 28 DS-GVO(GDPR). The contractor undertakes to provide the client with the necessary information upon request and, in particular, to prove the implementation of the technical and organizational measures.

(3) The proof of such measures, which do not concern only the concrete order, can be carried out for example bydie Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO(GDPR);

- the certification according to an approved certification procedure according to Art. 42 DS-GVO;
- up-to-date certificates, reports or statements of independent bodies (for example: auditors, auditors, data protection officers, IT security departments, privacy auditors, quality auditors);
- appropriate certification by IT security or privacy audit (for example, Baseline protection).

(4) The contractor may assert a claim for compensation in order to enable controls by the client.

8. Notification in case of violations of the contractor

1. The contractor shall assist the contracting authority in complying with the obligations on security of personal data, reporting of data breaches, data protection impact assessments and prior consultations, as referred to in Articles 32 to 36 of the GDPR. These include u.a.

(a) ensuring an adequate level of protection through technical and organisational measures that take into account the circumstances and purposes of the processing and the predicted likelihood and severity of a possible breach of rights through vulnerabilities, and enable the immediate detection of relevant injury events

b) the obligation to report violations of personal data immediately to the client

(c) the obligation to assist the contracting entity in providing information to the person concerned, and to provide him with all relevant information without delay in that connection

d) the support of the client for its data protection impact assessment

(e) the assistance of the contracting authority in the context of prior consultations with the supervisory authority

(2) For services that are not included in the terms of reference or that are not the result of a wrongdoing by the contractor, the contractor may claim a fee.

9. Authorization of the client

(1) The client confirms oral instructions immediately (at least in text form).

(2) The contractor must inform the client immediately if he believes that an instruction violates data protection regulations. The contractor is entitled to suspend the execution of the corresponding instruction until it has been confirmed or changed by the client.

10. Deletion and return of personal data

(1) Copies or duplicates of the data are not created without the knowledge of the client. This does not include backup copies, to the extent necessary to ensure proper data processing, and data required to comply with statutory retention requirements.

(2) After the conclusion of the contractually agreed work or sooner upon request by the client - at the latest upon termination of the service agreement - the contractor shall have all the documents, processing and utilization results as well as data stocks which have come into his possession To hand over client or to destroy it after prior consent in accordance with data protection. The same applies to test and reject material. The log of the deletion must be submitted on request.

(3) Documentation serving as proof of orderly and proper data processing shall be kept by the contractor according to the respective retention periods beyond the end of the contract. He can hand them over to the client for his discharge at the end of the contract.

place, date | signature of Clarity & Success Software GmbH

Dipl.-Ing. Florian Henkel, Managing Director (contractor)

sign here please

place, date | signature of the client

Appendix 1 - Technical and organisational measures

1. Confidentiality (Article 32 (1) (b) DS-BER)

• Access control

Access control system (via scanning and recognition of the fingerprint), key / key assignment, monitoring device (alarm system, surveillance cameras, object protection)

• Access control,

Protection by server service providers, firewall protection, antivirus protection, no unauthorized system usage, for example: (secure) passwords, automatic locking mechanisms, two-factor authentication, data encryption;

• Access Control

Differentiated authorizations (profiles, roles, transactions and objects), password protection for all areas, password protection of the database, evaluation, acknowledgment, logging of accesses;

• Separation Control

Separate processing of data collected for different purposes, e.g. Multi-client capability, sandboxing;

• Pseudonymisation (Article 32 (1) (a) of the GDPR, Article 25 (1) of the GDPR)

The processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the need for additional information, provided that such additional information is kept separate and subject to appropriate technical and organizational measures;

2. Integrity (Article 32 (1) (b) of the GDPR)

• relay control

No unauthorized reading, copying, modification or removal in the case of electronic transmission or transport using a virtual private network (VPN) connection and logging, encryption, electronic signature;

• Entry Control

Determining if and by whom personal data has been entered, modified or removed from data processing systems by logging;

3. Availability and resilience (Article 32 (1) (b) DS-BER)

• Availability Control

Backup procedures, mirroring of hard disks, e.g. RAID procedure, uninterruptible power supply (UPS), separate storage, antivirus / firewall, emergency plan;

• Rapid recoverability (Article 32 (1) (c) DS-BER);

4. Procedure for regular review, evaluation and evaluation (Article 32 (1) (d) of the GDPR, Article 25 (1) of the GDPR)

• Data protection management;

• Incident response management;

• Privacy-friendly default settings (Article 25 (2) DS-GVO);

• Order control

No order data processing within the meaning of Art. 28 DS-GVO without corresponding instructions of the client, for example: Clear contract design, formalized order management, strict selection of the service provider, compulsory pre-compilation, follow-up checks.

The technical and organizational measures are subject to technical progress and further development. In that regard, the contractor is permitted to implement alternative adequate measures. In doing so, the safety level of the specified measures must not be undershot.

Annex 2 - included branches of the client

Fill in the fields on this page only if you have branches.

Date:

The order data agreement is to apply in addition to the head office for all existing and future branches in the following countries:

◯ worldwide ◯ only in the following countries:

Only in the following branches:

Customer No.	Branch name	Country