b4 value.net GmbH
Trippstadter Straße 122
D-67663 Kaiserslautern
Tel. +49 6359 9379 0
Fax: +49 6359 9379 099
Commercial Register No. HRB 4024, Kaiserslautern District Court, Tax ID No. 19 673 0799 1,
VAT ID No. DE 813949895

Agreement
regarding the processing of personal data on behalf of a

controller pursuant to Article 28 of the EU GDPR

between

the customer

hereinafter referred to as **"controller"** -

and

b4 value.net GmbH
Trippstadter Straße 122
67663 Kaiserslautern

- hereinafter referred to as **"processor"**-

The processor has appointed the **following person as data protection officer** :

Bernd Alf Sittel
Dieselstrasse 1
67269 Grünstadt
Contact:
General inquiries : Datenschutz@b4value.net
Confidential : bernd.sittel@b4value.net
By telephone : +49 6359 9379 155

Content:

1 Preamble 3
2 Type and subject of the agreed service: 3
3 Types and categories of personal data, as well as categories of data subjects 3
4 Rights and obligations of the controller 3
5 Rights and obligations of the processor 3
6 Subcontracting relationships 5
7 Exercising the rights of data subjects 5
8 Disclosure, return and deletion of processed data 5
9 Term and termination of this agreement 6
10 Obligation of confidentiality 6
11 General Provisions and Final Provisions 6
Appendix A - Scope and subject matter of the agreed services, business purposes: 8
Appendix B - Scope and type of data collected and processed, categories of persons: 9
Appendix C - List of Subcontractors 13
Appendix D - Technical and organizational measures 14

1 Preamble

The processor provides a data processing service to the controller.
This agreement supplements existing contractual agreements as follows:

2 Type and subject of the agreed service:

The service includes the collection and processing of data, documents, records and information, hereinafter referred to as **"data"** , which are transmitted by the controller or by third parties authorized by the controller to the processor.
The type, scope, and purpose of the commissioned service are described in **Annex A** of this agreement. It is hereinafter referred to as **"data processing"** .

3 Types and categories of personal data, as well as categories of data subjects

The type of data and the group of affected parties are described in **Annex B** to this agreement.

4 Rights and obligations of the controller

4.1 The ***controller*** is entitled to verify the proper processing of data, in particular personal data, at any time, either personally or through a third party commissioned for this purpose. Such verification also includes ensuring compliance with confidentiality regulations beyond the legally protected content.

4.2 The ***controller*** has the right to conduct audits of compliance with this agreement at the ***processor***'s premises during normal business hours, with at least 10 days' notice. The audit must be conducted in such a way as to not unduly disrupt the business operations of the ***processor*** and its customers.

5 Rights and obligations of the processor

Personal data enjoys special protection during data processing by the processor. The processor undertakes to comply with the relevant regulations for handling personal data in accordance with the legislation applicable at the time of conclusion of the contract.
Data processing takes place at all times on the basis of the aforementioned legal grounds.

5.1 The ***processor*** undertakes to comply with all applicable data protection regulations, in particular those of the German Federal Data Protection Act (BDSG 2018) and the European General Data Protection Regulation (EU GDPR), within the scope of its activities for the controller , and to ensure compliance by its employees or the employees of any subcontractors or other third parties commissioned by it.

5.2 The ***processor*** undertakes to maintain a record of processing activities in accordance with Article 30 of the GDPR. It also undertakes to provide the ***controller*** with the best possible support in preparing its own processing documentation.

5.3 In accordance with Article 37 of the EU GDPR, the ***processor*** must appoint a data protection officer. The name and contact details of the data protection officer are shown on page 1 of this contract. The ***processor*** undertakes to inform the controller immediately of any changes to the appointment.

5.4 The contractually agreed data processing takes place exclusively in a member state of the European Union or in another contracting state of the Agreement on the European Economic Area. Any transfer to a third country requires prior consent of the controller and may only take place if the specific requirements of Articles 44 et seq. of the GDPR are met.

5.5 The ***processor*** undertakes to implement and maintain all technical and organizational measures (TOMs) in an appropriate manner that are necessary to comply with the obligations of this agreement. The TOMs must be designed to meet a current and appropriate level of protection and ensure compliance with the obligation. The TOM catalog, which is attached to this agreement as Annex D "Technical and Organizational Measures" in the version valid at the time of conclusion of the contract, serves as the definition of the minimum requirements for data protection and data security. Any further technical or organizational measures that go beyond those defined in Annex D are permissible, provided they do not hinder the ***processor*** in the performance of the contract and appear reasonable in relation to the effort required.

5.6 The **processor** shall ensure that the controller can verify the processor's compliance with its obligations under Article 28 of the GDPR. The processor undertakes to provide the controller with the necessary information upon request and, in particular, to demonstrate the implementation of the technical and organizational measures. Such measures, which may extend beyond the specific contract, can be demonstrated by***:***

- Compliance with approved codes of conduct pursuant to Art. 40 GDPR;
- Certification according to an approved certification procedure pursuant to Art. 42 GDPR;
- Current certificates, reports or excerpts from reports by independent bodies (e.g. auditors, internal audit, data protection officer, IT security department, data protection auditors, quality auditors);
- a suitable certification through an IT security or data protection audit.

5.7 The reproduction of the received data, documents, and information by the ***processor*** requires the express prior written consent of the ***controller***. This excludes reproductions necessary for the performance of the contract and routine reproductions for data backup purposes.

5.8 The ***processor*** shall carry out data processing exclusively in accordance with the documented instructions of the controller. If the controller issues instructions to the ***processor*** relating to the processing that constitute a breach of the legal provisions underlying this agreement or the content of this agreement, the ***processor*** is obligated to inform the controller of this immediately in writing. In this case, the ***processor*** may refuse to carry out the specific instruction.

5.9 The ***processor*** undertakes to inform the controller immediately of any infringement of rights or of any resulting or derived claims against the ***processor***, provided that these are based on the performance of the contract.

5.10 The ***processor*** undertakes to provide the controller with the best possible support in fulfilling its obligations in accordance with Articles 32-36 of the EU GDPR.

5.11 The ***processor*** undertakes to provide the controller with the best possible support in carrying out the controls.

5.12 The ***processor*** is entitled to establish subcontracting relationships and to commission the subcontractors to perform all or part of the services owed to the controller.
Further details are set out in Section 6.

5.13 The ***processor*** undertakes to inform the ***controller*** immediately of any attempt by third parties to gain unauthorized access to, or inspect, the data, documents, records, or information relating to the contract, as well as the contract results. The identity of the third parties ***shall*** be disclosed to the ***controller*** where possible.

This applies in particular if a violation of applicable laws or provisions of this agreement is threatened or has been caused by employees or agents of the processor.

6 Subcontracting relationships

6.1 According to Article 28, paragraph 2 of the GDPR, the ***processor*** has the right to establish new or different subcontracting relationships and to have the commissioned service performed in whole or in part by these subcontractors. The subcontractors to be engaged are subject to the general written approval of the controller. The ***processor*** must inform the controller in advance of any changes to the subcontracting relationships in order to grant the controller the opportunity to object as stipulated in the aforementioned article of the GDPR. If no objection is raised within a period of four weeks, the subcontracting is deemed approved.

6.2 At the time of conclusion of this data processing agreement, the subcontractors listed in Annex C, "Subcontracting Relationships," will be engaged by the ***controller*** to provide partial services. Upon conclusion of this agreement, the subcontractors listed in Annex C will be deemed approved by the ***controller***.

6.3 The ***processor*** is obliged to ensure the data protection and data security of the controller's data, even in the case of outsourced ancillary services, to take appropriate and legally compliant contractual agreements and control measures.

6.4 The ***processor*** is liable for damages caused by sub-processors in accordance with the provisions of Article 28 paragraph 4 sentence 2 EU-GDPR in conjunction with Article 82 EU-GDPR.

6.5 Notwithstanding the foregoing, the responsible party has the right to examine all existing and future subcontracting relationships in accordance with legal requirements before concluding the contract .

7 Exercising the rights of data subjects

7.1 The rights of individuals whose personal data is collected, processed, or used must be asserted by them against the ***controller***. The ***controller*** is responsible for safeguarding these rights in connection with the transfer of data, information, and documents to the ***processor***. The ***processor*** must support the data controller in safeguarding and enforcing the rights of data subjects, particularly with regard to notification, access, rectification, restriction of processing, and erasure. The direct response to requests from data subjects pursuant to Articles 15-19 of the GDPR is the sole responsibility of the ***controller***, unless a different legal or contractual provision obligates the ***processor*** to do so.

8 Disclosure, return and deletion of processed data

8.1 All data, documents and information that the ***processor*** receives from the controller and/or a third party commissioned by the controller are the exclusive property of the controller .

8.2 The ***controller*** has the right to demand the release and/or deletion of all data, documents, and information provided to the ***processor*** for the performance of the agreed services at any time and without stating reasons. This also applies during the term of the agreed services. The ***processor*** is responsible for carrying out the release and/or deletion to the extent that this is possible within the scope of fulfilling its contractual obligations. The right to release and/or deletion also applies to data that the ***processor*** itself created in connection with the execution of the contract, insofar as this is possible within the scope of fulfilling the ***processor***'s contractual obligations.

8.3 The processor expressly and without exception excludes any right to retain any data, documents, and information arising from the performance of the commissioned service. This exclusion does not apply to copies of data or documents required to comply with legal retention obligations or to protect the processor's own rights against the ***controller***. This exception ends upon expiry of any applicable statutory retention period or the cessation of other requirements.

The processor also undertakes to securely delete all unnecessary data, documents, and information, in particular personal data, unless the controller has requested their release. This also applies to all lists, proof prints, and similar documents received within the scope of the contract or created by the controller and relating to the controller .

8.4 The obligation to delete or return data to sub-processors arises from the provision in Article 28, paragraph 3, sentence 2, letter g of the EU GDPR. (see …)

9 Term and termination of this agreement

9.1 The term of this agreement is linked to the duration of use by the responsible party, or to the term of the contractual agreements underlying the service(s) described in ***Annex*** A.

9.2 In the event of termination of the cooperation, for whatever reason, the ***processor*** undertakes to immediately, unconditionally, and free of charge return to the data controller or to a third party designated by the ***controller*** all data, documents, records, and information, including data carriers, received from the data controller and/or from a third party commissioned by the ***controller*** within the scope of the cooperation. The data must be returned in a standard data format, such as that used by the ***processor*** for the contractual fulfillment of its obligations.

10 Obligation of confidentiality

10.1 All content of any kind and origin that becomes known to the ***processor*** in the course of fulfilling the service described in ***Annex*** A is subject to absolute confidentiality towards any third party. This applies in particular to all company data and content that is or could be identifiable or derived from the transmitted data, even if it is not personal data within the meaning of the data protection laws applicable at the time of conclusion of the contract.

10.2 All employees and/or agents of any kind deployed by the ***processor*** to carry out the contractual activities must be bound to data secrecy in accordance with Article 28, paragraph 3, letter b, of the EU GDPR, as well as to the maintenance of private secrets in accordance with Section 203 of the German Criminal Code (StGB), provided that the ***controller*** is a professional bound by confidentiality or has been bound accordingly by a professional bound by confidentiality. This obligation must be documented in writing and presented to the ***controller*** upon request .

11 General Provisions and Final Provisions

11.1 The aforementioned obligations regarding data protection, confidentiality, and disclosure are to be considered essential contractual obligations (primary obligations) of the contract concluded with the data controller . This hereby expressly supplements the underlying contract/contract.

11.2 Any amendments and/or additions to this agreement must be in writing to be effective. This also applies to any waiver of this written form requirement.

11.3 The place of jurisdiction for all disputes arising from or in connection with this agreement is the court with subject-matter and territorial jurisdiction for the controller. The controller is also free to assert any claims arising from this agreement before the court with subject-matter and territorial jurisdiction for the processor's registered office.

11.4 Statutory regulations concerning exclusive jurisdictions remain unaffected.

11.5 Liability arising from violations of data protection regulations or this data protection agreement is governed by statutory provisions.

11.6 Should any provision of this agreement be or become invalid or unlawful, this shall not invalidate the entire agreement. Both parties hereby agree to promptly reach an agreement on a valid provision that most closely approximates the intended purpose.

Attachments:

- Annex A - Scope and subject matter of the agreed services, business purposes
- Annex B - Scope and type of data collected and processed, categories of persons
- Annex C - List of subcontractors
- Annex D - Technical and organizational measures

b4 value.net GmbH
Trippstadter Strasse 122D-67663
Kaiserslautern
Tel. 0700 - 278258 - 3638
Fax. 0700 - 278258 - 3329HRB
4024 AG KaiserslauternSt
.Nr.19 673 0799 1
VAT ID DE 813949895

Annex A - Scope and subject matter of the agreed services, business purposes:

The processor performs the following service on behalf of the controller using the data provided to him:

1. **Document and data transfer using the transfer portal:**

- Receiving technical data for the creation of structured business documents such as invoices, credit notes, delivery notes, dunning letters, orders, contracts, billing documents and general documents as visual documents and/or data sets.
- Storage and management of user and company data in the portal, as well as transmission of business contact details between document senders and recipients in the course of normal business operations.
- Transmission of the aforementioned documents to the recipient, as indicated in the technical data, in electronic form or to third parties for the production of printed materials and their dispatch in paper form.
- Provision of a technical means of archiving business documents in the form of a short-term archive (duration by agreement) or a long-term archive to satisfy legal retention obligations as an ancillary service.
- Use of personal data in partially or non-anonymized form to create structuring elements (groups, case worker identifiers) in the customer interface.
- Creation of structured data sets (see figure in Appendix B) according to the type of raw data processed and the target document.
- Use of the data for billing purposes for services provided through the portal.
- The data necessary for processing within the scope of the agreed business purpose, including personal data, may also be used on a test system of the contractor intended for functional testing during the setup and configuration of the client's account to ensure the complete, agreed scope of services and, if necessary, to provide necessary functional tests in combination with the client's test systems to the extent required.

Scope of responsibility:

Depending on the delivery method (channel/format) specified by the controller, responsibility ends with successful delivery to the recipient's inbox for registered recipients and with the technically successful completion of the transmission for all other delivery methods. The controller assumes no further responsibility for the recipient's access, knowledge, processing, or use of the provided content.

2. **Partially or fully automated invitation process to business partners (customers or suppliers of the responsible party) for process optimization using the transfer portal:**

- Data is collected according to the data categories described in Appendix B via a separate website, which is promoted for the aforementioned purpose via email from the transfer portal. The data collected there is consolidated and transferred to the portal to create so-called "local business partners" who then complete the registration process automatically upon request.

Demarcation:

The sender's (controller's) responsibility ends with the successful dispatch of the invitation.

3. **Processing of service requests in the service management system:**

- A uniform service management system is used company-wide to process service requests, with the help of which the service tickets are processed.

4. **Documentation of customer support in the CRM system**

- A uniform CRM system is used company-wide to document customer service, in which contact details and content of incoming customer contacts such as emails or notes about telephone contacts are managed.

Annex B - Scope and type of data collected and processed, categories of persons:

1. **To fulfill the purpose: Acquire/connect portal participants, create new ones (see Appendix A, Nos. 1 and 2)**

Participant master data:

Participants in the portal are corporate bodies that register on the contractor's portal with the master data shown in the illustration and acquire the right to use the portal with this registration.

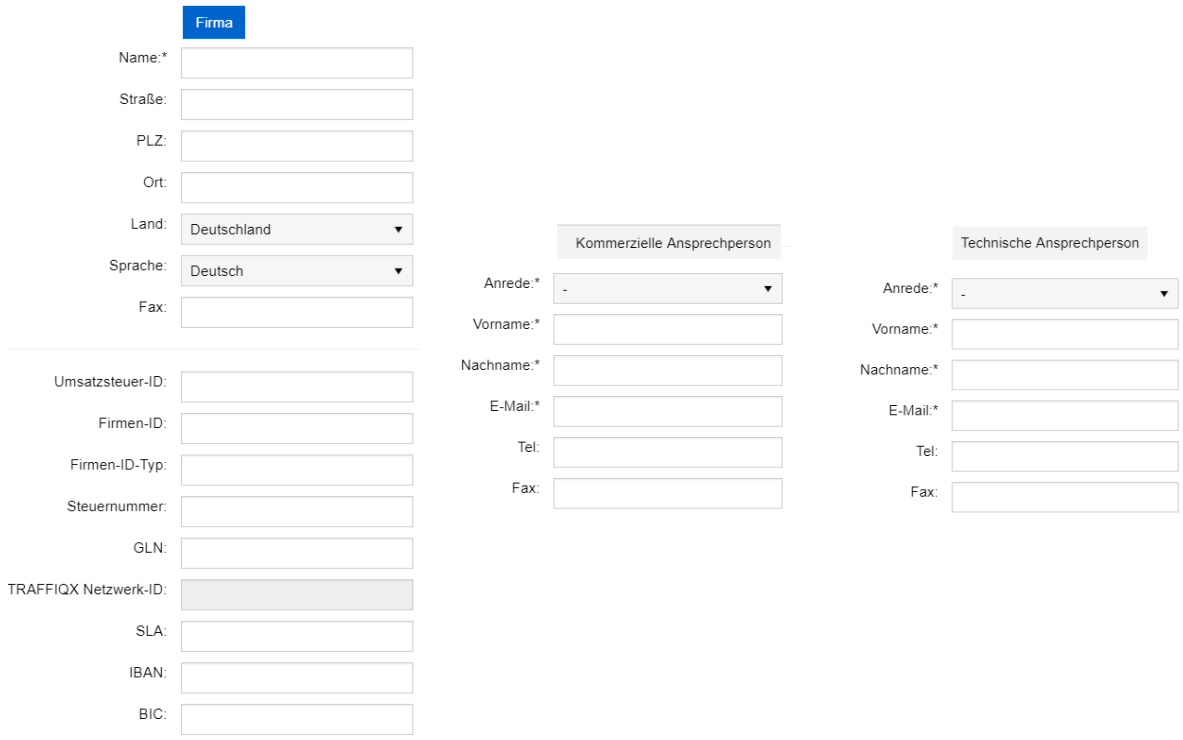


Figure 1Master data Participants on the TRAFFIQX®-System

The master data recorded here corresponds to that which identifies such a company in normal business transactions.

In the case of company names that concern a natural person, the protection of data in accordance with the Federal Data Protection Act applies without restriction.
When a corporation is registered as a legal entity, a comprehensive obligation of absolute confidentiality applies.

Personal data, user accounts:
Any number of users can be created per participant/organization in the form of a user account.
Each user account represents a person within the participant's company who is authorized to use the participant account with dedicated user data to fulfill defined tasks within the company structure.

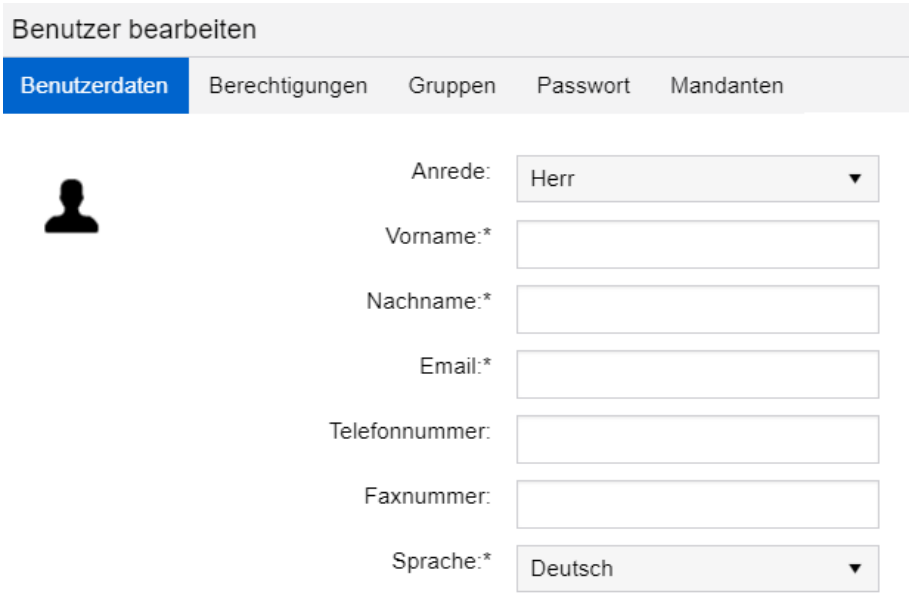


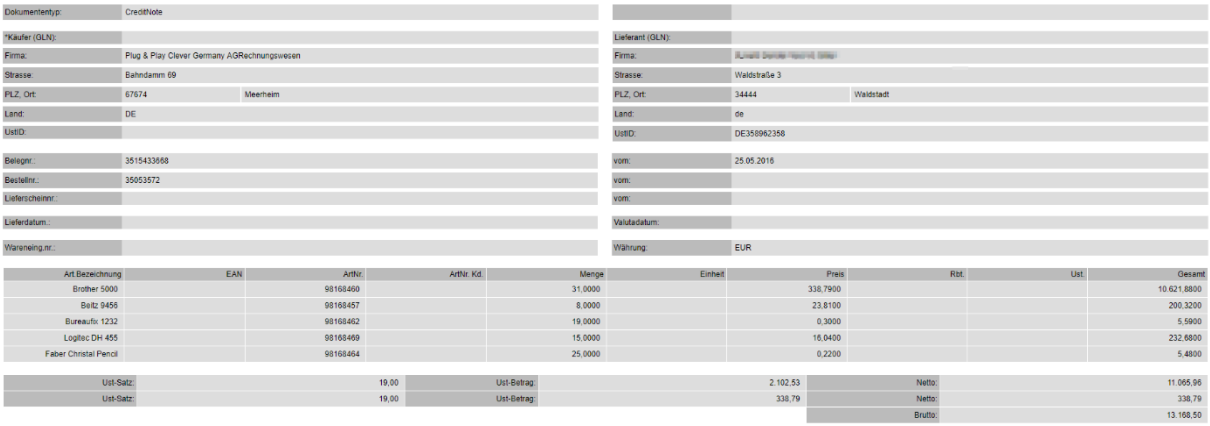
Figure 2Data example user account

The data collected in the user account is personal and as such worthy of protection in accordance with the German Federal Data Protection Act (BDSG2018) / equivalent GDPR.
Any use of the data for purposes other than the agreed business purpose relating to this order is fundamentally and without exception prohibited.
In particular, the transfer of personal data in any form, even in part, for purposes other than those agreed upon here is prohibited.

Document data:
To create the structured business documents mentioned above, data content from different categories is necessary:

- Address details of senders and recipients
- Key data for identifying and categorizing the documents
  (document number, document date, etc.)
- Data relating to the content of the business transaction
  (article data, prices, categories, etc.)

The image shows a typical example of the content of an invoice data record (excerpt from demo network):



Dokumententyp:	CreditNote		
*Kaufer (GLN):		Lieferant (GLN):	
Firma:	Plug & Play Clever Germany AGRechnungswesen	Firma:	[redacted]
Strasse:	Bahndamm 69	Strasse:	Waldstraße 3
PLZ, Ort:	67674 Meerheim	PLZ, Ort:	34444 Waldstadt
Land:	DE	Land:	de
UstID:		UstID:	DE358962358
Belegnr.:	3515433668	vom:	25.05.2016
Bestellnr.:	35053572	vom:	
Lieferscheinnr.:		vom:	
Lieferdatum.:		Valutadatum:	
Wareneing.nr.:		Währung:	EUR

Art.Bezeichnung	EAN	ArtNr.	ArtNr. Kd.	Menge	Einheit	Preis	Rbt.	Ust	Gesamt
Brother 5000		98168460		31,0000		338,7900			10.621,8800
Beltz 9456		98168457		8,0000		23,8100			200,3200
Bureaufix 1232		98168462		19,0000		0,3000			5,5900
Logitec DH 455		98168469		15,0000		16,6400			232,6800
Faber Christal Pencil		98168464		25,0000		0,2200			5,4800

Ust-Satz:	19,00	Ust-Betrag:	2.102,53	Netto:	11.065,96
Ust-Satz:	19,00	Ust-Betrag:	338,79	Netto:	338,79
				Brutto:	13.168,50

Figure 3Example invoice data record

2. To fulfill the purpose: data maintenance in the CRM system as well as in the service management system (see Appendix A, Nos. 3 and 4):

Address master data in the CRM system:

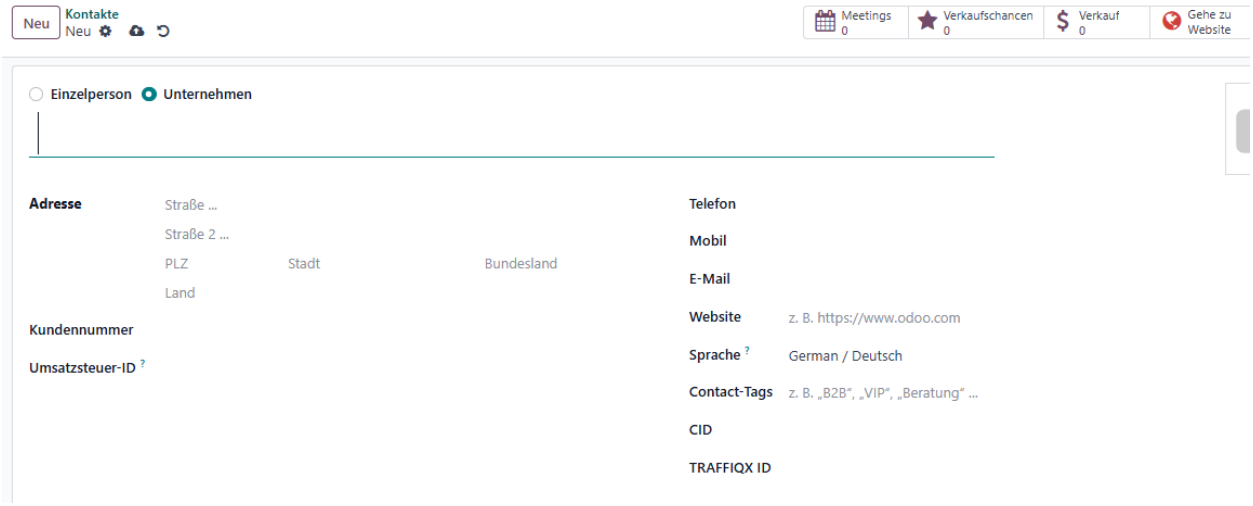


Figure 4Example address master record in the CRM system

Contact person for the address in the CRM system:

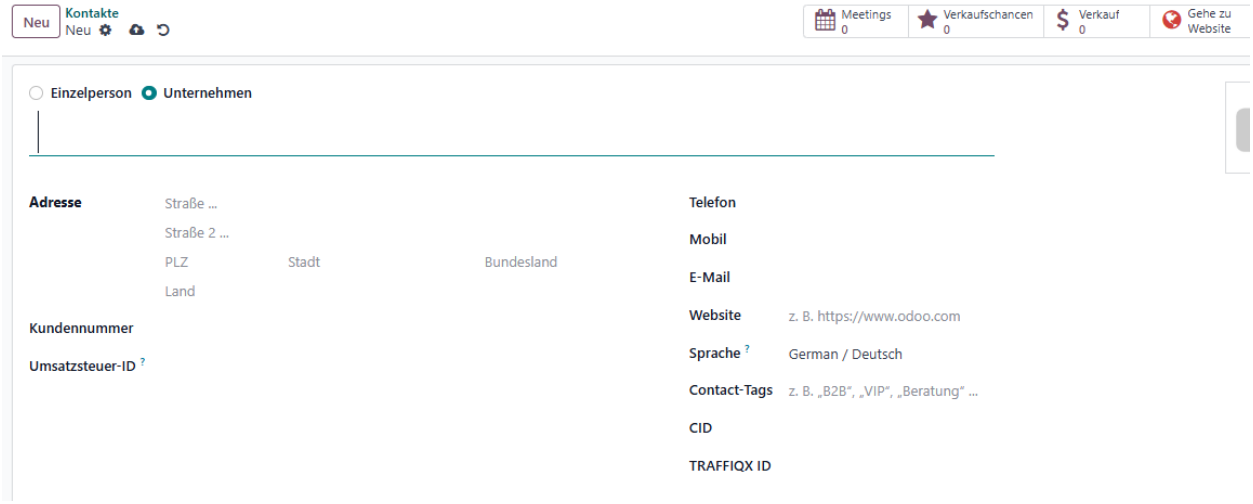


Figure 5Example contact person record in the CRM system

Contact tracing when contacting those affected directly (by phone / email):

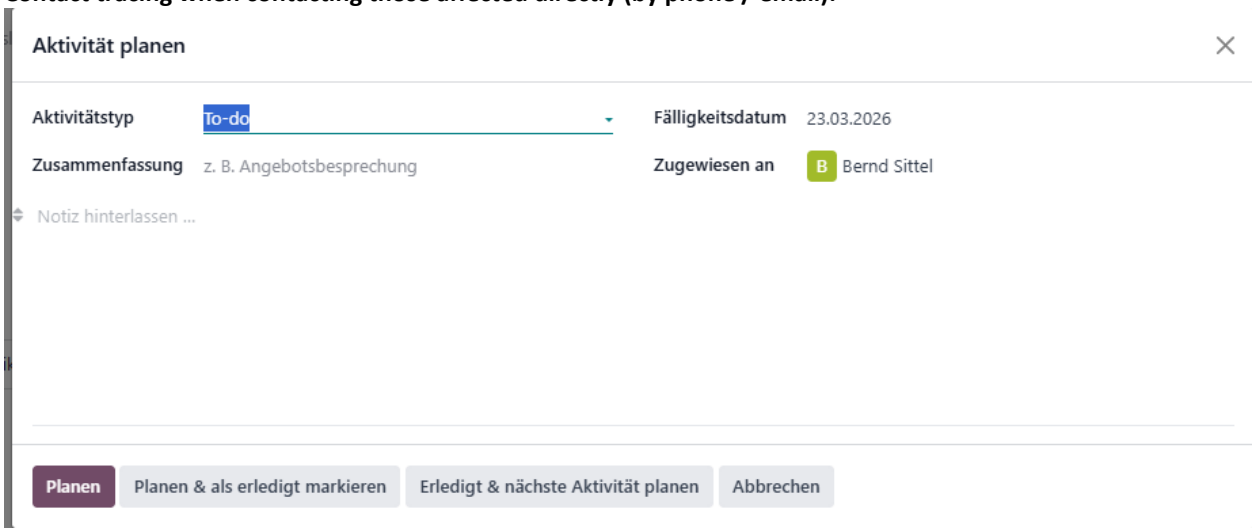


Figure 6Example contact record in the CRM system

The following categories of personal data are used:

- Interested parties
- Employees of the interested parties
- Customers
- Customer employees
- Service provider for customers
- Employees of the customers' service providers
- suppliers
- Suppliers' employees
- Service providers of the suppliers
- Employees of the service providers of the suppliers

Annex C - List of Subcontractors

Printing service provider:

- RICOH Deutschland GmbH
  Georg Kohl Document Center
  Georg-Kohl-Str. 4274336 Brackenheim
- DATEV eG
  Paumgartnerstraße 6-14
  90429 Nuremberg

Sales and consulting partners:

- Nils König
  Neukoppel 9a 25337 Elmshorn

Signature service provider:

- D-Trust GmbH
  Kommandantenstraße 1510969 Berlin
- Trust Weaver AB
  Wallingatan 12
  SE-SE-111 60 Stockholm

Hosting, maintenance and service of ITSM/CRM systems:

- Seiwert GmbH
  Solmsstr. 4160486 Frankfurt
- Odoo SA
  Chaussée de Namur 401367 Grand- Rosière (Ramillies)
  Belgium

Provider of other technical support services, maintenance and development of ITSM/CRM systems:

- OBS Solutions GmbH
  In der Wüste 72, 57462 Olpe

E-Invocing compliance service provider

- Generix Group GmbH
  Walter-Kolb-Straße 9-11
  60594 Frankfurt am Main

Annex D - Technical and organizational measures

In accordance with Article 32 GDPR, b4 will define the technical and organizational measures to ensure and comply with data protection within the meaning of the law.

Internal organization

b4 structures its internal organization in such a way as to meet the specific requirements of data protection. In particular, measures are provided that are suitable for achieving an adequate level of data protection, depending on the type of personal data or data categories to be protected.

Necessary control mechanisms that must be observed:

The measures taken by b4 were designed with a view to ensuring the levels of control enshrined in the applicable legal provisions.

Pseudonymization, encryption in accordance with Art. 32 paragraph 1 lit. a GDPR

- In the context of the business activities of b4value.net GmbH, there is no process that requires or makes pseudonymization seem necessary.
- All hard drives in all systems have hardware encryption.
- All access to b4 systems is exclusively via transport-encrypted channels and mechanisms. All data transfers to all systems that support encrypted transfer are encrypted.

Technical and organizational measures to ensure confidentiality, availability, resilience and integrity, in accordance with Article 32, paragraph 1. lit. b GDPR, serve:

- Data carriers are subject to a documented picking and depicking process. Only certified service providers are used for data carrier destruction.
- All service providers are subject to a strict selection process. A data protection agreement corresponding to the commissioned service is mandatory upon conclusion of the contract.
- All b4 employees are bound by confidentiality obligations. The legal basis for this confidentiality obligation is subject to a documented, regular awareness-raising process.
- All b4 employees receive ongoing training and awareness programs on data protection and information security. A regular, documented training and awareness program is implemented for handling data and data processing systems.
- All employees are subject to a documented process of regular security checks.
- Access to the b4 premises is subject to a documented access control process. All visits by external persons are documented.
- All network infrastructure components are subject to a documented update process and a documented inventory procedure.
- A comprehensive firewall appliance is in operation, securing all external access to the network infrastructure.
- There are separate Wi-Fi structures for guests and internal b4 resources (employees and devices).
- The logical separation of data sets for different purposes or environments is consistently ensured.
- Unnecessary connections or connections that are idle are always automatically disconnected.
- Process-related procedures are established for handling personal data. Data access rights in all systems follow the principles of "data minimization" and purposefulness, according to the tasks of the respective individuals and groups. These are implemented through a comprehensive role and rights concept.
- Subcontracted suppliers are obligated to maintain an appropriate level of data protection by means of a data protection agreement tailored to the processing (data processing agreement or joint controllership).
- All access to publicly accessible systems is exclusively via encrypted transfers.
- All computer systems are equipped with a multi-stage virus protection system.
- All browsers used in the corporate environment are hardened according to the respective manufacturer's specifications.
- All data is subject to a multi-stage backup and restore process, which is regularly tested for reliability.
- Changes and updates to systems or services are carried out and documented according to defined processes.

**Technical and organizational measures to ensure recoverability,
pursuant to Article 32 paragraph 1 lit. c GDPR serve:**

- All data is subject to a multi-stage backup and restore process, which is regularly tested for reliability.

Procedures for the regular review, assessment and evaluation of the effectiveness of the technical and organizational measures to ensure the security of processing pursuant to Article 32(1). lit. d GDPR serve:

- All technical and organizational measures are subject to regular review for compliance and effectiveness by qualified employees of the responsible party and, where necessary, by external auditors.
- The test results are documented.
- Information security incidents and potential data breaches are recorded, assessed, documented, and processed within a defined process as part of the Information Security Management System (ISMS) in accordance with ISO 27001. Defined reporting channels, responsibilities, and processes exist for root cause analysis and the implementation of corrective and preventive measures. Information security and data protection incidents can be reported, among other ways, via the email addresses Security@b4value.net or Datenschutz@b4value.net.

This document was created electronically and is valid without a signature.