Data processing in compliance with Art. 28 General Data Protection Regulation (GDPR)[1]

Agreement

between

– the person responsible, hereinafter referred to as the 'Client' –

and

The Team Enablers GmbH (Product Surwayne)

Baumwall 7

20459 Hamburg

– processor, hereinafter referred to as the 'Contractor' or 'TTE' –

The Client and Contractor each individually referred to as the 'Party' and jointly referred to as the 'Parties'.

1 Subject matter of the contract

Within the framework of the delivery and performance relationship that exists between the Parties (hereinafter referred to as the 'main contract'), Art. 4 (8) GDPR requires that the Contractor works as the processor with personal data for which the Client is acting as the person responsible within the meaning of Art. 4 (7) GDPR (hereinafter referred to as 'Client Data'). This contract sets out the Parties' rights and obligations that result from data protection law and that relate to the Contractor's handling of Client Data for the purposes of executing the main contract.

2. Type and purpose of processing

2.1 The Contractor will process Client Data on its behalf and only in accordance with the Client's instructions. Art. 5 (2) GDPR states that the Client will remain the person responsible ('data owner') within the meaning of data protection law.

2.2 Client Data will be processed within the framework of processing in accordance with the determinations regarding the type and purpose of processing as set out in **Appendix 1** to this contract. This refers to the type of Client Data as set out in **Appendix 1** and to the categories of persons concerned as defined there.

2.3 The contractually agreed data processing will be carried out exclusively in a member state of the European Union. The work may only be transferred to a third country if the special requirements set out in Art. 44 ff. GDPR have been fulfilled.

[1] Regulation (EU) 2016/679 of the European Parliament and the Council dated 27 April 2016 regarding the protection of natural persons in relation to the processing of personal data, the free movement of data and the repeal of Directive 95/46/EC (General Data Protection Regulation), OJ L 119, dated 04.05.2016, P. 1 to 88.

Contractor

3. Client's right to issue instructions

3.1 The Contractor will only use Client Data in accordance with the Client's instructions as finally expressed in the provisions of this contract. Individual instructions that deviate from the provisions of this contract or which impose additional requirements require the Contractor's prior consent and will be made in accordance with the amendment procedure set out in the main contract.

3.2 The Contractor will inform the client as soon as possible if he is of the opinion that an instruction violates the GDPR or other data privacy provisions within the EU or its Member States. The Contractor will also be entitled to suspend the execution of the instruction until the Client has confirmed the instruction.

3.3 To the extent that the law applicable within the European Union or its Member States to which the Contractor is subject obliges the Contractor to process the personal data without instructions from the Client, the Contractor will notify the Client of the relevant legal requirements prior to processing unless the law in question prohibits such communication due to an important public interest.

3.4 The Client's instructions must be issued at least in text form (e.g. email). The Client will immediately confirm oral instructions at least in text form (e.g. email).

3.5 The Client will upon first request release the Contractor from all claims if claims for payment of damages pursuant to Art. 82 GDPR are asserted against the Contractor due to a violation of the GDPR without the Contractor having violated any instructions issued by the Client. The Client will also assume the costs of the Contractor's necessary legal defence here, including all court and lawyer's fees. The indemnity obligation will not apply if an instruction was unlawful and this was apparent to the Contractor or if the claim for damages is based on the violation of a duty specifically imposed on the Contractor by the GDPR.

4. Duties of the Client

4.1 The Client will be responsible for the legality of the processing of Client Data as well as for the protection of the rights of the persons concerned. The Client will upon first request release the Contractor from any claims asserted by third parties against the Contractor as a result of Client Data being processed.

4.2 The Client is the owner of Client Data and the owner of all possible rights concerning Client Data.

4.3 The Client must inform the Contractor immediately and comprehensively if, while reviewing the results from the processing results, it discovers errors or irregularities in regard to data protection regulations or its instructions.

4.4 To the extent that the Contractor intends to defend itself by legal means against a claim for damages pursuant to Art. 82 GDPR, against an impending or already imposed fine pursuant to Art. 83 GDPR or other sanctions pursuant to Art. 84 GDPR, the Client authorises the Contractor to disclose details about processing, including instructions issued, for the purposes of defence.

4.5 The Client will support the Contractor in the event of audits by a supervisory authority, administrative or criminal proceedings, the assertion of liability claims by a person concerned or a third party or the assertion of other claims within the scope of what is reasonable and necessary to the extent that these actions are connected to this processing.

5. Duties of the Contractor

5.1 The Contractor may not make copies or duplicates of Client Data within the framework of processing without the Client's prior consent. Copies to the extent that they are required to guarantee proper data processing and the proper provision of performances in accordance with the main contract (including data backup) as well as copies required for compliance with statutory retention obligations are excluded from the above.

5.2 The Contractor will support the Client in the event of audits by the supervisory authority, administrative or criminal proceedings, the assertion of liability claims by a person concerned or a third party or the assertion of other claims within the scope of what is reasonable and necessary to the extent that these actions are connected to this processing.

5.4 The contractor must in accordance with Art. 28 (3) (2) (b) GDPR oblige in writing the persons employed in the processing of Client Data to maintain confidentiality and must first acquaint them with the data protection provisions that are relevant to them. This will not be necessary if the persons employed in the processing of Client Data are already subject to an appropriate legal obligation to maintain confidentiality.

5.5 To the extent and as long that the legal requirements for the duty to effect a corresponding appointment are given, the Contractor will be obliged to appoint in writing a company data protection officer who is an expert in the field of data protection law and data protection practice and who is reliable and capable of fulfilling the tasks that have been set out in Art. 39 GDPR and who will perform his or her activities in compliance with Art. 38, 39 GDPR and Art 38 (2) Bundesdatenschutzgesetz (BDSG – Federal Data Protection Act). This person's contact details will be provided to the Client for the purposes of establishing direct contact at least in text form (e.g. email). The Client will be informed immediately when a new data protection officer is appointed.

5.6 The Contractor is subject to official supervision in accordance with Art. 40 BDSG and to the regulations governing fines and penalties in Art. 42, 43 BDSG and in Art. 83 (4-6) GDPR in accordance with Art. 41 BDSG.

5.7 The Contractor must ensure that the Client is able to satisfy himself of the Contractor's compliance with the obligations pursuant to Art. 28 GDPR. The Contractor undertakes to provide the Client when requested to do so with the necessary information and, in particular, to provide proof of the implementation of the technical and organisational measures to be implemented in accordance with **Appendix 2** within the framework of the monitoring rights pursuant to Clause 8 of this contract.

6. Technical and organisational measures

6.1 The Contractor will implement and maintain the technical and organisational measures listed in **Appendix 2** to this contract pursuant to Art. 28 (3) (2) (c), Art. 32 GDPR prior to the commencement of the processing of the Client Data and will maintain them for the term of the contract. The measures to be taken are generally data security measures and measures that will ensure a level of protection appropriate to the risk in regard to the confidential nature, integrity, availability and resilience of the systems. The state of the art, the implementation costs and the type, scope and purposes of processing as well as the different probabilities of occurrence and significance of the risk to the rights and freedoms of natural persons within the meaning of Art. 32 (1) GDPR must be taken into account.

6.2 Due to the fact that the technical and organisational measures are subject to technical progress and technological development, the Contractor will be permitted to implement alternative adequate measures, provided that the safety level of the measures does not fall short of that set out in **Appendix 2**. The Contractor must document such changes. Essential changes to the measures require the Client's prior written consent and must be documented by the Contractor and made available to the Client on request.

7. Contractor support in the fulfilment of the Client's obligations in accordance with Art. 32 – 36 GDPR

The Contractor will, while taking into account the type of processing and the information available to the Contractor, assist the Client in its compliance with the obligations concerning the security of personal data, reporting obligations in the event of data leaks, data protection impact assessments and prior consultations that have been set out in Articles 32 to 36 of the GDPR. These include

a) ensuring an adequate level of protection through technical and organisational measures that take account of the circumstances and purposes of the processing as well as the predicted probability and severity of a possible infringement of rights as a result of security vulnerabilities and that enable an immediate determination of relevant infringement events,

b) support to the Client in the event of a breach in the protection of personal data pursuant to Art. 33 GDPR,

c) the obligation to support the Client within the framework of its duty to provide information pursuant to Art. 34 GDPR regarding a person concerned,

d) support to the Client for its data protection impact assessments within the meaning of Art. 35 GDPR,

e) support to the Client within the framework of prior consultations with the supervisory authority pursuant to Art. 36 GDPR.

8. Client's monitoring rights

8.1 The Client is entitled to enter the Contractor's business premises at which Client Data is being processed during normal business hours at its own expense, without interrupting the course of operations and under strict confidentiality of the Contractor's trade and business secrets, in order to ensure compliance with the obligations arising out of this agreement, in particular the technical and organisational measures as set out in **Appendix 2** to this contract. The Contractor will on request provide the Client with proof of the implementation of the technical and organisational measures.

8.2 The Contractor will grant the Client the rights of access, information and inspection required to carry out the checks pursuant to Clause 8.1.

8.3 The Client must inform the Contractor in good time (as a rule at least two weeks in advance) of all circumstances associated with the execution of the checks. The Client may as a rule carry out one check per calendar year. This does not affect the Client's right to carry out further checks in the event of special incidents.

8.4 If the Client commissions a third party with the execution of checks, the Client will oblige the third party in writing in the same way as the Client is obliged to the Contractor on the basis of this Clause 8 of this contract. The Client must further oblige the third party to confidentiality and secrecy unless the third party is subject to a professional obligation of maintain confidentiality. Upon the Contractor's request, the Client must immediately present the commitment agreements entered into with the third party to the Contractor. The Client may not commission any of the Contractor's competitors with the execution of checks.

8.5 At the Contractor's discretion, proof of compliance with the technical and organisational measures as set out in **Appendix 2** may, instead of on-site checks, also be provided on the basis of compliance with approved rules of conduct in accordance with Art. 40 GDPR, certification in accordance with an approved certification procedure in accordance with Art. 42 GDPR, submission of a suitable up-to-date certificate, reports or report extracts from independent bodies (e.g. auditors, audit, data protection officers, IT security departments, data protection auditors or quality auditors) or a suitable certification by IT security or data protection audit – e.g. in accordance with BSI-Grundschutz (Federal Office for Information Security – Basic Protection) (‘audit report’) if the audit report enables the Client to satisfy itself appropriately of compliance with the technical and organisational measures as set out in **Appendix 2** to this contract.

9. Subcontracting relationships

9.1 The Contractor may establish subcontracting relationships (subcontractors) in regard to the processing or use of Client Data. At present, the subcontractors specified in **Appendix 3** with name, address and content of the order are working for the Contractor. The Client declares that it consents to their employment. The Contractor must always inform the Client of any intended changes in relation to the involvement or replacement of subcontractors. If the Client does not object to new subcontractors within two weeks of receipt of the notice concerning the new subcontractor, this new subcontractor's involvement will be deemed to have been approved by the Client.

9.2 Services by third parties that the Contractor utilises as an ancillary service to support the execution of the order are not deemed to constitute subcontracting relationships within the meaning of this provision. These include, for example, telecommunications services, maintenance and user service, cleaning staff, auditors or the disposal of data carriers. The Contractor is, however, obliged to also conclude appropriate contractual agreements in accordance with the law and to implement monitoring measures for ancillary services provided by third parties in order to ensure the protection and security of Client Data.

9.3 The subcontractor's obligation must be effected in writing, which may also be in an electronic format (e.g. email). The Contractor must choose its subcontractors carefully and verify before they are commissioned that they are able to fulfil the agreements that the Client and the Contractor have entered into. The Contractor must for every subcontract ensure that the conditions specified in Art. 28 (2) and (4) GDPR are complied with.

9.4 The Contractor must ensure that the provisions agreed in this contract and any supplementary instructions by the Client also apply to the subcontractor. It must in principle be possible for the Client to exercise its monitoring rights as set out in Clause 8 towards the subcontractor. The Client will on written request be entitled to obtain from the Contractor information about the content of the contract essentially relating to data protection and the implementation of the subcontractor's obligations relevant to data protection, if necessary, also through inspection of the relevant contract documents.

9.5 The provisions of this Clause 9 will also apply if a subcontractor that is based in a third country is employed. The Contractor must in such cases ensure the admissibility under data protection law by means of suitable legal instruments, e.g. standard EU contract clauses.

9.6 Client Data may only be transferred to the subcontractor and the subcontractor may only become active for the first time if all the subcontracting requirements have been met.

10. Rights of the persons concerned

10.1 The rights of the persons affected by the data processing as set out in Chapter 3 GDPR (Art. 12-23 GDPR) while taking account of Part 2, Chapter 2 BDSG (Art. 32-37 BDSG), in particular to information, disclosure, correction, erasure, restriction of processing, data transferability or objection to the stored Client Data, must be asserted against the Client.

10.2 If a person concerned should contact the Contractor directly in regard to the rights listed in 10.1, the Contractor must immediately forward this request to the Client.

10.3 In the event that a person concerned asserts his or her rights within the meaning of Clause 10.1, the Contractor must support the Client in the fulfilment of these claims to an appropriate and for the Client necessary extent with suitable technical and organisational measures based on the type of processing. This presupposes that the Client has requested TTE to do so in writing or in text form and that the Client reimburses TTE for the costs it incurs as a result of complying with the request.

10.4 The Contractor must make it possible for the Client to correct, erase or block Client data or, at the Client's request, carry out the correction, blockage or erasure itself if and to the extent that it is impossible for the Client to do so itself.

11. Return and erasure of provided data and data carriers

11.1 The Contractor must erase all Client data in a manner appropriate to data protection subsequent to the conclusion of the provision of the contractual performance (in particular in the event of notice of termination or other termination of the main contract) or earlier at the Client's request and return to the Client data media received from the Client which still contain Client Data at this time. The same applies to test and scrap material. This will not apply where there is an obligation under EU law or the law of the member states to store personal data. Additional costs resulting from different information regarding the return or erasure must be borne by the Client.

11.2 The Contractor must draw up a report about the erasure or destruction of Client Data, which must be submitted to the Client on request.

11.3 Documentation that serves as proof that data was processed in accordance with the order and law or statutory retention periods must be retained by the Contractor beyond the end of the contract in accordance with the respective retention periods.

12. Duration of contract and notice of termination

The term and notice of termination of this contract is governed by the provisions regulating the term and notice of termination of the main contract. Notice of termination of the main contract automatically results in termination of this contract. Isolated termination of this contract is excluded.

13. Relationship to main contract

The provisions of the main contract will apply to the extent that no special regulations are contained in this contract. The regulations from this contract will take precedence in the event of contradictions between this contract and regulations from other agreements, in particular in regard to the main contract.

14. Term of validity

This contract will be valid from when it is signed. Due to the fact the provisions of Art. 28 GDPR will only apply from 25 May 2018, the contract must be interpreted until the end of 24 May 2018 in the light of Art. 11 Bundesdatenschutzgesetz (BDSG).

15. Written form clause

Amendments and supplements to this document and all its components – including any assertions – require a written agreement and the express note that they refer to an amendment or supplement to these conditions. This also applies to the waiver of this formal requirement.

________________________________ ________________________________
Place, date Place, date

________________________________ ________________________________
Client's signature Contractor's signature

Appendices:

Appendix 1: Purpose, type and scope of data processing, type of data and group of those concerned

Appendix 2: Technical and organisational measures

Appendix 3:	Subcontractors

Appendix 1: Type and purpose of data processing, type of data and categories of those concerned

Type and purpose of data processing:

The Contractor operates the Surwayne online application program. This program is used to facilitate anonymous internal company surveys and to stimulate methods for improving the rated projects and general teamwork. The Contractor uses Surwayne to enable the Client to analyse and rate the improvement methods implemented along with their direct effects, e.g. on team spirit and performance capacities, in order to optimise projects and teamwork individually and effectively. The use of Surwayne requires that personal data (e.g. the relevant email addresses used for the surveys) is forwarded by the Client to the Contractor. The Contractor transfers the Client's personal data to a data processing centre. The data processing centre processes and stores the Contractor's Client Data for the Contractor.

Type of personal data:

Names and email addresses of the employees (of the Client)

Categories of persons concerned:

Client employees, freelancers or third parties whose data is used jointly with the Contractor for the purpose of delivering the Surwayne performance.

Appendix 2: Technical and organisational measures

1. Confidentiality (Art. 32 (1) (b) GDPR) and encryption (Art. 32 (1) (a) GDPR)

Entrance control

Measures to prevent unauthorised persons from gaining entrance to the data processing facilities that are used to process personal data:

- All the Contractor's (and / or subcontractor's) locations where there is an information system in which personal data is used or stored are equipped with appropriate security systems. TTE reasonably limits physical access to such personal data.
- Entrance controls have been installed at all the processor's data centres. Unauthorised entrance to the data centres is prevented by 24x7 monitoring and entrance restrictions.
- Surveillance cameras have been installed at the entrance door to the data centres and security monitoring by the property management has been installed.
- Offices and workspaces where personal information is processed are protected by 'clear desk' and 'clear screen' requirements, office closing procedures and the use of secure cabinets and containers.
- Delivery and loading areas are monitored and separated from information processing systems to prevent unauthorised entrance.
- Security areas are protected by appropriate entrance controls to ensure that only authorised persons are able to gain entrance. Measures to protect these security areas include permit and identity-card checks, visitor registration and requirements for employees to interrogate anyone without an identity card and any unknown person.
- Technical checks have been implemented to ensure the physical security of information system components against security threats.
- Network and server equipment, including LAN servers, network bridges and routing selectors, have been physically protected from unauthorised physical access by having been installed in locked rooms or cabinets.
- Security policies have been drawn up to control the overall approach to securing systems and data

Access control / encryption

Measures to prevent unauthorised persons from using the data processing equipment and procedures:

- Equipment, information or software are not removed from the premises of TTE (and / or the subcontractor) without permission and / or logging.
- Procedures have been established for when data carriers are to be disposed of or reused to prevent the subsequent recovery of the information stored on them.
- Procedures have been established to prevent the unauthorised recovery of the information stored on data carriers containing files when they need to leave the premises for maintenance work.
- Processing in accordance with common procedures and instructions.
- Encryption procedures are being used to protect the confidentiality of information during transmission.
- Access to information has been restricted through the definition of procedures for handling, identifying, copying, distributing, storing, transporting, disposing of and printing information as hard copies.
- Storage devices that contain information are physically destroyed or securely overwritten and are not treated with a delete function before disposal or reuse.
- The Contractor (and / or the subcontractor) has designated and secured areas for the storage of collected data carriers.
- A password management system has been set up to check user authorisation for accessing information resources.

Access control

Measures to ensure that only those authorised to use the data processing procedures have access to the personal data subject to their access authorisation:

- Security policies have been set up to manage the overall approach to securing systems and data, classifying data assets, clarifying security tasks and raising employee awareness.
- Only authorised persons may grant, modify or revoke access to an information system in which personal data

is used or stored.

- User management procedures define user roles and their rights as to how access is granted, modified and terminated; ensure the appropriate separation of duties; and define logging / monitoring requirements and mechanisms.
- All the Contractor's (and / or the subcontractor's) employees are assigned a unique user ID.
- Access rights are implemented in accordance with the 'smallest rights' method. Users are granted the smallest number of rights required to perform their work tasks.
- A formal user registration procedure exists for granting and denying access to information resources.
- The systems perform configurations to encourage sound passwords and minimize the possibility of the unauthorised use of accounts.
- The Contractor's (and / or subcontractor's) employees have been clearly identified and undergo a rigorous registration procedure before they are granted access to information resources.
- System access will be suspended when the Contractor's (and / or the subcontractor's) employee leaves the workplace.
- Logging mechanisms are employed to ensure that it is possible to subsequently trace the person and the time of data access.
- Clearly separated production and verification areas are maintained by the Contractor (and / or the subcontractor).
- Data collation and treatment are carried out in accordance with the relevant procedures and instructions.
- Encryption methods are employed to protect the confidentiality of information during transfer.
- Access to information has been restricted through the definition of procedures for handling, identifying, copying, distributing, storing, transporting, disposing of and printing information as hard copies.
- All the Contractor's (and / or the subcontractor's) employees are assigned a unique user ID.
- Remote access to systems and data requires a two-stage access-authorisation verification.
- Periodic audits of user accounts are performed to ensure that appropriate minimum rights have been granted and accounts of unauthorised users have been removed.

Separation checks / purpose-binding checks

Measures to ensure that data that is collected for different purposes can be processed separately:

- Access rights are implemented in accordance with the 'smallest rights' method.
- Large networks are divided into individual logical areas to protect information.
- All material is logically separated at the application layer using separate containers with controls, including access and authorisation controls.
- All data is stored in separate logical database containers with access controls.
- All files are stored in separate logical access structures with access controls.

2. Integrity (Art. 32 (1) (b) GDPR)

Handover checks

Measures to ensure that personal data cannot be read, copied, altered or removed without authorisation during electronic transmission or during transport or storage on data carriers and that it is possible to verify and establish at which points it is intended to transfer personal data by data transfer devices:

- Data collation and treatment are carried out in accordance with the relevant procedures and instructions.
- Encryption methods are employed to protect the confidentiality of information during transfer.
- Access to information has been restricted through the definition of procedures for handling, identifying, copying, distributing, storing, transporting, disposing of and printing information as hard copies.
- Hard-copy media are distributed in a controlled manner.
- Storage devices that contain information are physically destroyed or securely overwritten and are not treated with a delete function before disposal or reuse.
- Equipment, information or software is not removed from the premises of the Contractor (and / or the subcontractor) without permission and / or logging.
- Procedures have been established to prevent the unauthorised recovery of the information stored on data carriers containing files when they need to leave the premises for maintenance work.
- The Contractor (and / or the subcontractor) has installed protection against viruses and malware to support the security and availability of the systems.
- Authorised routes between users and services are routed and restricted.
- An intrusion detection system has been installed to monitor and log security incidents.
- Remote access to systems and data requires a two-stage access-authorisation verification.
- Logging mechanisms are employed to ensure that it is possible to subsequently trace the person and the time

of data access.
- Secure data transfer methods have been set up.
- Encryption methods are employed to protect the confidentiality of information during transfer.
- Equipment, information or software is not removed from the premises of the Contractor (and / or the subcontractor) without permission and / or logging.

Input checks

Measures that ensure that it is possible to subsequently verify whether and by whom personal data can be input, modified or removed in data processing systems:

- Logging mechanisms are employed to ensure that it is possible to subsequently trace the person and the time of data access.
- Verification logs are protected against changes and are checked independently.
- Authorised routes between users and services are routed and restricted.
- Procedures have been established for when data carriers are to be disposed of or reused to prevent the subsequent recovery of the information stored on them.
- Procedures have been established to prevent the unauthorised recovery of the information stored on data carriers containing files when they need to leave the premises for maintenance work.
- The Contractor (and / or the subcontractor) has set up internal procedures that ensure that processing is effected in accordance with instructions.

3. Availability and resilience (Art. 32 (1) (b) GDPR), rapid recovery (Art. 32 (1) (c) GDPR

Availability monitoring

Measures to ensure that personal data is protected against accidental destruction or loss (the information relates to the Contractor's own IT systems):

- The contractor (and / or the subcontractor) has drawn up appropriate disaster recovery and business resumption plans. TTE (and / or the subcontractor) regularly reviews both the business continuity plan and the risk assessment. Business continuity plans are tested and regularly updated to ensure that they are up to date and effective.
- The Contractor (and / or the subcontractor) has drawn up data backup plans and uses automatic data backup systems for data management. Backup copies are kept secure.
- The Contractor's (and / or subcontractor's) data centre facilities maintain additional power and network systems and reasonable environmental controls to ensure the continuity of system availability.
- The Contractor (and / or the subcontractor) has installed protection against viruses and malware to support the security and availability of the systems.

4. Procedure for regular review, assessment and evaluation (Art. 32 (1) (d) GDPR, Art. 25 (1) GDPR)

Processing checks

Measures to ensure that personal data that is processed on a contracting basis can only be processed in accordance with the Client's instructions:

- Personal data is used for internal purposes and only insofar as such use is necessary to provide the performances specified in the agreement (and any changes) and this appendix in accordance with Art. 11 Bundesdatenschutzgesetz dated April 2015.
- The Contractor (and / or the subcontractor) operates in accordance with the conditions regarding processing as set out in the agreement and this appendix.
- The Contractor (and / or the subcontractor) has set up internal procedures that ensure that processing is effected in accordance with instructions.

Data protection management

Measures that enable data protection processes to be controlled and verifiably ensure compliance with data protection regulations:

- The Contractor (and / or the subcontractor) has appointed a data protection officer and has established rules for the protection of privacy.
- Monitoring systems are used to manage system capacity and usage.
- All incidents relating to personal data security are dealt with in accordance with the appropriate incident response procedures.
- The Contractor (and / or the subcontractor) has drawn up data backup plans and uses automatic data backup systems for data management. Backup copies are kept secure.
- The Contractor's (and / or subcontractor's) data centre facilities maintain additional power and network systems and reasonable environmental controls to ensure the continuity of system availability.
- The Contractor (and / or the subcontractor) has installed protection against viruses and malware to support the security and availability of the systems.
- The Contractor (and / or the subcontractor) has set up internal procedures that ensure that processing is effected in accordance with instructions.
- A password management system has been set up to check user authorisation for accessing information resources.
- The systems perform configurations to encourage sound passwords and minimize the possibility of the unauthorised use of accounts.
- Periodic audits of user accounts are performed to ensure that appropriate minimum rights have been granted and accounts of unauthorised users have been removed.
- The Contractor (and / or the subcontractor) has determined and assigned responsibility for compliance management and support functions.
- The Contractor (and/or the subcontractor) considers the separation of duties in the design of the organisational structures and the allocation of official duties.
- The Contractor (and / or the subcontractor) has established guidelines for the handling of software development and modification
- The Contractor (and / or the subcontractor) has centralised the management for the purchase of hardware and software.
- A documented data protection management system has been introduced to manage GDPR requirements.

Appendix 3:   Subcontractors

Name, address / country, order content

Mittwald CM Service GmbH & Co. KG / Germany, storage of data (hosting)
Artur Heinze (Agentejo) / Germany, IT development and support
Usersnap GmbH / Austria, customer feedback tool