Agreement on Contract Data Processing
according to Article 28 Regulation (EU) 2016/679 EU GDPR

as well as

Information regarding the transfer of personal data to third countries

by and between

Messe Düsseldorf GmbH, Stockumer Kirchstr. 61, Messeplatz, 40474 Düsseldorf, represented by its Management,

– hereinafter referred to as “Contractor” or as “Data Exporter” –

and

Contractual Partner ((company) name and address see Application forms),

– hereinafter referred to as “Principal” or as “Data Importer” –

CHAPTER A – PREFACE

Preamble

Contractor is the operator of the trade show premises in Düsseldorf, Germany. Here and elsewhere in the world it holds trade shows, exhibitions and congresses. In the scope of the aforementioned field of activity, Contractor offers different digital services. These services may involve the processing of personal data.

Principal is the exhibitor at one of the events held by Contractor.

NOW THEREFORE the Parties conclude the following Agreement. It applies if and as far as a corresponding service agreement has been concluded between the Parties.

Clause 1
General provisions

(1) The present Agreement regulates the rights and duties of the parties in connection with the processing of personal data.

(2) Contractor shall process personal data at Principal’s request in accordance with EU Regulation 2016/679 Article 4 (8) and Article 28 – General Data Protection Regulation (GDPR). As far as the respective service has been ordered per separate agreement, this request refers to the services:

- Matchmaking,
- exhibitor-staff registration,
- visitor invitation and / or
- invitation to use the Online Ordering System (OOS) and invitation into the function of a further contact person in the scope of the organization of the trade fair participation.

Chapter B of the present Agreements holds an agreement in the sense of GDPR Article 28 GDPR. For Chapter B the definitions as set out in GDPR Article 4 shall apply.

(3) Under the condition that the services

- Entrance Ticket Coupon Redemption and / or
- Scan2Lead

has / have been ordered by separate agreement – depending on where the data importer is based – a data transfer to third countries takes place. Chapter C regulates the details in this regard.

CHAPTER B - Contract Data Processing

Clause 2
Object of the Agreement

The subject matter of processing, the type and purpose of processing, the type of personal data and the categories of data subjects comprise the following:

(a) Matchmaking:

(aa) Purpose of data processing: Contractor offers a digital networking-platform by the name of "Grip", on which demanders and providers of services and products are able to find each other by aid of their personal data provided upon individual sign-up. Based on matches between the aforementioned criteria or because of similarities with other persons within the networking-platform contacts that may potentially be interesting for them are suggested to the users. Each user may subsequently get in touch with such contacts by using an app or a desktop-version thereof. Principal submits personal data to Contractor, in order for the Contractor to invite the data subject to become a member of the networking-platform.

(bb) Types of personal data subject to processing: last name, first (given) name, photo (if available), e-mail address, profession, industry membership information, fields of interest, information on product and service portfolio.

(cc) Categories of data subjects: data of visitors and exhibitors including their staff members, (executive) officers, and other representatives as well as staff members, (executive) officers, and other representatives of other companies involved in the trade show participation of Principal.

(b) Exhibitor-staff registration:

(aa) Purpose of data processing: Contractor registers persons working at Principal's trade show booth during the runtime of a trade show. Principal submits to Contractor personal data of said persons, in order for Contractor to invite the data subjects to be registered as an exhibitor-staff member. To optimize procedures of Principal's trade show participation Contractor will address registered persons with regard to services and topic related follow-up events as well as with regard to communicational services such as matchmaking (§ 2 letter a)) and Scan2Lead (§ 15 paragraph 2 letter b)).

(bb) Types of personal data subject to processing: last name, first (given) name, photo (if available), e-mail address, profession, industry membership information, fields of interest.

(cc) Categories of data subjects: data of visitors and exhibitors including their staff members, (executive) officers, and other representatives as well as staff members, (executive) officers,

and other representatives of other companies involved in the trade show participation of Principal.

(c) Visitor invitation:

(aa) Purpose of data processing: Contractor offers a service, in the scope of which Principal submits to Contractor lists with e-mail addresses of its (Principal's) clients, who are eligible as potential visitors of a trade show held by Contractor and attended by Principal as exhibitor. Subsequently Contractor submits entrance ticket vouchers to Principal's clients using the e-mail addresses provided inviting them to the trade show. This service pursues the purpose of facilitating Principal the process of inviting its clients by virtue of sending them an entrance ticket voucher, instead of beforehand having to purchase these vouchers from Contractor and subsequently forward them to its clients.

(bb) Types of personal data subject to processing: last name, first (given) name, and e-mail address.

(cc) Categories of data subjects: From Principal's point of view potential trade show visitors as well as staff members, (executive) officers, and other representatives of other companies involved in the trade show participation of Principal.

(d) Invitation to use the Online Ordering System (OOS) and invitation into the function of a further contact person in the scope of the organization of the trade fair participation:

(aa) Purpose of data processing: Contractor offers an Online Ordering System (OOS), within which Principal may order additional services for its participation in a trade show. Within its OOS-account and within its general booth order the person designated in the application form as contact person for Principal's participation has the option to invite other persons as additional users. In order for other users to be invited in such way, the inviting person must enter the e-mail address of the person to be invited into the OOS. On behalf of Principal Contractor will subsequently invite the person to be invited by using the e-mail address provided. In the same way the designated contact person may have further persons invited into the function as additional contact person in the scope of the organization of the trade fair participation (without access to OOS).

(bb) Types of personal data subject to processing: last name, first (given) name, sex, e-mail address, profession, telephone number, fax number.

(cc) Categories of data subjects: From Principal's point of view potential trade show visitors as well as staff members, (executive) officers, and other representatives of other companies involved in the trade show participation of Principal (e.g. in the fields of press releases, controlling construction and dismantling, technical support, booth construction, booth management during runtime, internet and marketing).

Clause 3
Rights and duties of the Principal

(1) The Principal is the data controller as defined in GDPR Article 4 (7) in respect of the data processed by the Contractor at its request. Under clause 4 (3), the Contractor is entitled to inform the Principal if it believes that a contract and/or instruction given by the Principal leads to illegitimate data processing.

(2) The Principal as the data controller is responsible for safeguarding the rights of data subjects. The Contractor shall notify the Principal without undue delay if data subjects are asserting their rights as data subjects towards the Contractor.

(3) The Principal shall inform the Contractor without undue delay upon noticing errors or irregularities occurring in connection with the processing of personal data by the Contractor.

(4) The Principal is responsible for compliance if it is subject to a notification duty towards third parties under GDPR Article 33 or 34 or if it is under any other notification duty applicable to the Principal.

(5) Upon request the Principal will inform the Contractor about the contacts of its data protection officer in textform.

Clause 4
Contractor's general duties

(1) The Contractor shall process personal data exclusively within the parameters of agreements concluded and/or in observance of any supplementary instructions issued by the Principal. This provision applies with the exception of statutory regulations placing the Contractor under an obligation to undertake other processing. In such a case the Contractor shall notify the Principal of those legal requirements prior to processing, unless the relevant legal provision prohibits such notification on the grounds of important public interest. The purpose, type and scope of data processing shall otherwise be based exclusively on this Agreement and/or the Principal's instructions. The Contractor may not undertake any data processing in derogation of this provision unless such processing has the Principal's express written consent

(2) The Contractor undertakes to arrange its organisation and operations in such a way that the data it processes for the Principal shall be adequately secured against unauthorised third-party access to the extent required in each instance. The Contractor shall coordinate with the Principal in advance regarding any changes in the organisation of its contract data processing where this is important to data security.

(3) The Contractor shall inform the Principal without undue delay of any instances where it considers that an instruction issued by the Principal violates legal requirements. The Contractor is authorised to suspend implementation of such an instruction until it has been either confirmed or modified by the Principal. If the Contractor can demonstrate that data processing as instructed by the Principal may lead to the Contractor's liability under GDPR Article 82, the Contractor is entitled to suspend further processing until the liability situation between the parties has been clarified.

Clause 5
Contractor's data protection officer

Upon request the Contractor will inform the Principal about the contacts of its data protection officer in textform. The contacts of the external data protection officer is also available on its internet page at www.messe-duesseldorf.de/privacy .

Clause 6
Contractor's notification duties

The Contractor understands that the Principal may be under a reporting duty according to GDPR Articles 33 or 34, whereby it must report any personal data breach to the supervisory authority within 72 hours of becoming aware of it. The Contractor shall support the Principal in the implementation of reporting duties.

Clause 7
Principal's collaboration duties

(1) The Contractor shall support the Principal in its duty to respond to requests of persons wishing to exercise their rights as data subjects under GDPR Articles 12-23. The provisions of clause 11 of this Agreement are also applicable.

(2) The Contractor shall participate in creating a directory of processing activities undertaken by the Principal. The Contractor shall provide the Principal with any details that may be required for this purpose in an appropriate form.

(3) The Contractor shall support the Principal in complying with the duties specified in GDPR Articles 32-36 with due regard to the type of processing and the information that is available to the Contractor.

Clause 8
Inspection authorities

(1) The Principal is entitled to ascertain compliance with statutory data protection provisions and/or compliance with the provisions agreed between the parties and/or compliance with the Principal's instructions. It may do so by conducting inspections and other checks at any time and to the required extent or by having such inspections conducted by auditors who shall be specified from case to case. The Principal may, at its discretion, choose to conduct inspections by obtaining self-disclosure information from the Contractor. On request, the Contractor undertakes to provide the Principal with information required by the latter to meet its contract monitoring duties by making the relevant documentation available.

(2) The Contractor shall ensure that the Principal can ascertain compliance with the relevant technical and organisational measures specified in EU GDPR Article 32, thus enabling the Principal to meet its obligation to conduct impact assessments prior to data processing and during the term of the contract. For this purpose, the Contractor shall prove to the Principal, upon request, that it has implemented the technical and organisational measures required in EU GDPR Article 32 and **Annex 1**. Proof of the implementation of such measures, which do not just affect the specific contract, may, at the Principal's discretion, also take the form of submitting a recent audit certificate, reports or report excerpts from independent bodies (e.g. a chartered accountant, auditor, data protection officer, IT security department, data protection auditors, quality auditors) or appropriate certification arising from an IT security and data protection audit.

(3) The Principal may request an inspection of the data processed by the Contractor for the Principal as well as insofar of the data processing systems and programs used by the Contractor.

(4) If the supervisory authority takes measures towards the Principal under GDPR Article 58, especially concerning information and inspection duties, the Contractor shall provide the Principal with the required information and shall enable the relevant supervisory authority to conduct an on-site inspection. The Contractor shall notify the Principal if such measures are planned.

Clause 9
Subcontracting

(1) Principal is aware of the commitment of the following subcontractors by Contractor:

(a) for Matchmaking:

- Intros.at Ltd., 82 Rivington Street, Unit 5, 2nd Floor, EC2A 3AZ, London, England
- Dimedis GmbH, Dillenburger Str. 83, 51105 Cologne, Germany

(b) for exhibitor-staff registration:

- Dimedis GmbH, Dillenburger Str. 83, 51105 Cologne, Germany

(c) for visitor inviation:

- Dimedis GmbH, Dillenburger Str. 83, 51105 Cologne, Germany

(2) The Contractor shall select the subcontractor with care and shall ascertain prior to subcontracting that the subcontractor is able to comply with the arrangements made between the Contractor and the Principal.

(3) The Contractor shall ensure that the provisions agreed in this Agreement and, if applicable, any supplementary instructions provided by the Principal also apply to the subcontractor.

(4) The Contractor shall conclude with its subcontractor a contract data processing agreement that meets the requirements of GDPR Article 28. In addition, the Contractor shall place the subcontractor under the same personal data protection duties that have been specified between the Principal and the Contractor.

(5) Subcontracting as detailed above (subclauses 1 to 6) does not cover third-party services used by the Contractor merely as ancillary services in the performance of its business activities. This includes, for example, cleaning services, telecommunications services without specific reference to services provided by the Contractor to the Principal, postal and courier services, transport services and security services. However, even in the case of third-party ancillary services, the Contractor shall ensure that appropriate arrangements and technical and organisational measures are taken to ensure the protection of personal data. The servicing and updating of IT systems and applications is a form of subcontracting which is subject to approval and contract processing as specified in GDPR Article 28 if servicing and testing concerns IT systems which are also used for the performance of services for the Principal and if servicing may involve accessing personal data processed by the Contractor on behalf of the Principal.

Clause 10
Non-disclosure commitment

(1) When processing data for the Principal, the Contractor undertakes to ensure the non-disclosure of data which it obtains under the contract or of which it becomes aware. The Contractor undertakes to observe the same confidentiality provisions incumbent upon the Principal. The Principal undertakes to notify the Contractor of any special confidentiality regulations that may be applicable.

(2) The Contractor shall ensure that it is familiar with the applicable data protection regulations and their use. The Contractor also gives its assurance that it will familiarise its employees with the data protection regulations that are relevant to them and that it has placed the same under a non-disclosure commitment. The Contractor further gives its assurance, in particular, that it has placed employees under a non-disclosure commitment if they are involved in conducting the relevant work and that such employees have been informed of the Principal’s instructions.

(3) On request, the Contractor shall provide documentary evidence to the Principal that its employees have been placed under the commitment detailed in subclause 2.

Clause 11
Duties of confidentiality

(1) Both parties agree that all information obtained in the course of executing this Agreement shall be treated as confidential for an indefinite period and shall be used exclusively for the execution of this Agreement.

Neither party is entitled to use this information either wholly or in part for any purposes other than those mentioned herein or to disclose the same to third parties.

(2) This duty does not apply to information which one of the parties has demonstrably received from a third party without being under a confidentiality commitment or which is in the public domain.

Clause 12
Fee

The Contractor's fee shall be agreed separately.

Clause 13
Technical and organisational data security measures

(1) The contractor warrants to the principal that it will undertake all technical and organisational measures that may be required to comply with the applicable data protection legislation. This includes, in particular, the specifications of GDPR Article 32.

(2) The status of technical and organisational measures available at the conclusion of this Agreement has been appended to this Agreement as Annex 1. The parties agree that modifications to the technical and organisational measures may be necessary in order to satisfy technical and legal requirements. Any major changes which may affect the integrity, confidentiality or availability of the personal data shall be coordinated by the Contractor with the Principal in advance. Measures which only involve minor technical or organisational changes and do not adversely affect the integrity, confidentiality or availability of personal data can be implemented by the Contractor without coordination with the Principal. The Principal may at any time request an updated version of the technical and organisational measures taken by the Contractor.

(3) The Contractor shall regularly inspect the technical and organisational measures it has taken, and shall also check their effectiveness as appropriate. The Contractor shall notify the Principal if there is a need to improve and/or modify those measures.

Clause 14
Termination

After the termination of this Agreement, any documents, data and deliverables in the Contractor's possession, which were created through the processing or use of data arising from their contractual relationship and in the Contractor's possession, shall either be returned to the Principal or shall be erased as instructed by the Principal. This provision does not impact any statutory retention duties or other duties to store data.

CHAPTER C – Data transfer into a third country

Clause 15
Definitions

(1) For the purposes of the present CHAPTER C:

(a) "personal data", "special categories of data/sensitive data", "process/processing", "controller", "processor", "data subject" and "supervisory authority/authority" shall have the same meaning as in Directive

95/46/EC of 24 October 1995 (whereby “the authority” shall mean the competent data protection authority in the territory in which the data exporter is established);

(b) “the data exporter” shall mean the controller who transfers the personal data;

(c) “the data importer” shall mean the controller who agrees to receive from the data exporter personal data for further processing in accordance with the terms of these clauses and who is not subject to a third country’s system ensuring adequate protection;

(2) The details of the transfer (as well as the personal data covered) are specified hereinafter.

(a) Entrance Ticket Coupon Redemption

(i) Data subjects – The personal data transferred concern the following categories of data subjects:

- Professional exhibition visitors (including journalists) (representatives of companies visiting trade exhibitions).
- Exhibition visitors (public events without status as professional visitor).
- Club members.

(ii) Purposes of the transfer(s) – Any transfer is carried out for the following purposes:

Companies/Entrepreneurs (data importers) who have issued vouchers for visitors will receive the visitor data (name, address, communication data, calendar day of voucher redemption) for the vouchers redeemed, provided this has been agreed by contract. This allows the aforementioned companies/entrepreneurs to determine to which extent vouchers issued by them have actually been used.

(iii) Categories of data – The personal data transferred concern the following categories of data:

With professional exhibition visitors: Registration data such as company data with addresses, contact persons and communication data, calendar day of voucher redemption, information on branch of industry, product interests as well as contract and settlement data.

With Exhibition visitors: Name, address, communication data, exhibitors of interest, payment data, calendar day of voucher redemption.

With Club Members: Name, address, communication data, exhibitors of interest, personal data (date of birth, household income, purchasing behaviour, calendar day of voucher redemption).

(iv) Recipients – The personal data may be discloses only to the following recipients of categories of recipients:

None.

(b) Scan2Lead

(i) Data subjects – The personal data transferred concern the following categories of data subjects:

- Professional exhibition visitors (including journalists) (representatives of companies visiting trade exhibitions).
- Club members.

(ii) Purposes of the transfer(s) – Any transfer is carried out for the following purposes:

The data exporter offers exhibitors (data importers) upon the conclusion of a separate agreement the option of accessing data on trade visitors and Club Members electronically (so called Scan2Lead service). This service is subject to the visitor allowing the exhibitor to scan the barcode on their admission ticket. This means visitors themselves decide whether exhibitors have access to their electronic "visiting card". Data transfer does not occur if the visitor objects to having their data passed on to the exhibitor. The exhibitor may by aid of Scan2Lead contact the respective visitor upon ending of the respective trade show, in order to intensify the business relationship initiated at the trade show.

(iii) Categories of data – The personal data transferred concern the following categories of data:

- With professional exhibition visitors: Registration data such as company data with addresses, contact persons and communication data, calendar day of voucher redemption, information on branch of industry, product interests as well as contract and settlement data.
- With Club Members: Name, address, communication data, exhibitors of interest, personal data (date of birth, household income, purchasing behaviour, calendar day of voucher redemption).
- With all data subjects: Additions and / or amendments of the dataset as well as notes discretely added by the user to the dataset submitted upon scanning.

(iv) Recipients – The personal data may be discloses only to the following recipients of categories of recipients:

None.

Clause 16
Legal bases for the transfer of personal data to a third country

(1) Depending on the location of the data importer, the personal data listed above may be transferred to a third country. Any third country of our exhibitors can be considered as a recipient country. The specific recipient as well as the specific recipient country can be taken from the respective sender of the voucher or the exhibitor badge. In the third country, there is no level of data protection equivalent to that level of data protection of the European Union, so that there is a certain risk in the transfer of personal data. This includes, for example, the risk that the personal data is processed beyond the required purpose or that government authorities have access to personal data. Furthermore, no specific guarantees are provided to compensate for this deficit, such as the establishment of a data protection supervisory authority.

(2) The lawfulness of the transfer of personal data to a third country is governed by the following principles:

(a) **Entrance Ticket Coupon Redemption**

(i) The data processing is based on Art. 49 para. 1 lit. b) GDPR. In the absence of an adequacy decision pursuant to Article 45 para. 3, or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions: the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request. The transmission of personal data is necessary to achieve the purpose of the contract. In return for the transmission of personal data, the visitor receives an admission ticket for a specific event of the data exporter. With this ticket, the visitor can visit the event and use the services offered there. In this case, payment of the ticket price in a monetary amount is not required.

(b) Scan2Lead

(i) The data processing is based on Art. 49 para. 1 lit. b) GDPR. In the absence of an adequacy decision pursuant to Article 45 para. 3, or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions: the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards (see clause 16 para. 1). In principle, i.e. subject to legal restrictions, the exhibitor may at any time object to the processing of your personal data either via e-mail to privacy@messe-duesseldorf.de or via postal mail to Messe Düsseldorf GmbH, G2-RV, PF 101006, 40001 Düsseldorf, Germany.

ANNEX 1

Contractor's Technical and Organisational Data Security Measures

The Contractor shall take the following technical and organisational measures for data security within the meaning of Art. 32 GDPR.

1. Confidentiality (Art. 32 para. 1 lit. b GDPR)

- **Access Control**

  Measures to prevent unauthorised persons from gaining access to data processing equipment processing or using personal data

Technical Measures	Organisational Measures
Chip Cards / Transponder Systems	Key Regulation / List
Manual Locking System	Reception / Doorman
Security Locks	Visitor Book / Protocol of Visitors
Protection of Building Shafts	Employee Badges / Visitor Badges
Doors with External Knobs	Visitors accompanied by employees
Video Surveillance of Entrances	Care in the selection of security personnel
	Care in the selection of cleaning staff

- **Data Access Control**

  Measures to prevent data processing systems (computers) from being used by unauthorised persons. Access control refers to the prevention of the unauthorised use of equipment

Technical Measures	Organisational Measures
Login with User Name + Password	Managing user authorisations
Anti-Virus software server	Generation of user profiles
Anti-Virus software clients	Central password management
Firewall	Guideline for "Safe Password"
Intrusion detection systems	Guideline for "Deletion / Destruction"
Mobile device management	General Data Protection Guideline and/or Security
Use of VPN in the event of remote access	Mobile device policy
Smartphone encryption	Instructions for "Manual Desktop Lock"
BIOS protection (separate password)	
Automatic desktop lock	
Notebook / Tablet encryption	

- **Data Access Control**

  Measures to ensure that persons authorised to use a data processing system have access only to data subject to their right of access and that personal data cannot be read, copied, altered or removed without authorisation during processing, use and after storage.

Technical Measures	Organisational Measures
External document shredder (DIN 66399)	Use of authorisation concepts
Logging of access to applications, specifically when entering, changing and deleting data	Minimum number of administrators

	Management of user authorisations by administrators

- **Separation Control**

  Measures to ensure that data collected for different purposes can be processed separately. This may be ensured, for example, by logical and physical separation of data

Technical Measures	Organisational Measures
Separation of Productive and Test Environment	Control via authorisation concept
Logical separation (Systems / Databases / Data Carriers) in virtual systems	Definition of database rights
Multi-client capability of relevant applications	

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

Transfer Control

Measures to ensure that personal data cannot be read, copied, altered or removed without authorisation during its electronic transmission or during transport or storage on data carriers and that it is possible to verify and establish the points to which personal data are to be transmitted by data transmission facilities

Technical Measures	Organisational Measures
Use of VPN	Documentation of the data recipients as well as the duration of the planned transfer and/or the deletion
Deployment over encrypted connections like sftp, https	Overview of regular retrieval and transmission processes

- **Input Control**

  Measures to ensure that it can be subsequently verified and established whether and by whom personal data have been entered, modified or removed in data processing systems

Technical Measures	Organisational Measures
Technical logging of the input, modification and deletion of data	Overview of programs which can be used to enter, change or delete which data
Manual or automated control of logs	Traceability of input, modification and deletion of data by individual user names (not user groups)
	Allocation of rights to enter, change and delete data on the basis of an authorisation concept
	Clear responsibilities for deletions

3. Availability and Resilience (Art. 32 Abs. 1 lit. b GDPR)

- **Availability Control**

  Measures to ensure that personal data are protected against accidental destruction or loss.

Technical Measures	Organisational Measures
Fire and smoke detection systems	Backup & Recovery concept (worded in full)

Fire extinguisher in the server room / Sprinkler system	Checking the back-up process
Temperature and humidity monitoring in the server room	Regular data recovery tests and result logging
Air-conditioned server room	Storage of backup media in a secure location outside the server room
UPS	Existence of an emergency plan (e.g. BSI IT basic protection 100-4)
Protective socket strips in server room	Separate partitions for operating system and data
RAID System / Hard disk mirroring	
Video surveillance of server room entrances	

- **Rapid Recoverability (Art. 32 para. 1 lit. c GDPR)**

  Measures that ensure that systems and data can be recovered quickly after a malfunction

Technical Measures	Organisational Measures
Second data centre at the Messe Düsseldorf exhibition centre	
Data mirroring (Metrocluster)	
Half-hour snapshots for recovery of deleted or modified data	

4. Processes for regular testing, assessing and evaluating (Art. 32 para. 1 lit. d GDPR; Art. 25 para. 1 GDPR)

- **Data Protection Management;**

Technical Measures	Organisational Measures
Central documentation of all procedures and regulations on data protection with access for employees as required / authorisation (Intra-net)	Appointment of an internal company Data Protection Officer (DPO)
Other documented safety concept	Employees trained and obliged to confidentiali-ty / data
A review of the effectiveness of the technical protective measures is carried out at least once a year	Regular awareness-raising of employees at least once a year
	Appointment of an external Information Securi-ty Officer (ISO)
	The Data Protection Impact Assessment (DPIA) will be carried out as necessary
	The organisation complies with the information obligations under Articles 13 and 14 of the GDPR

- **Incident Response Management**

  Lists all measures that support the response to security breaches

Technical Measures	Organisational Measures
Use of Firewall and regular updates	Documented procedure for detection and reporting of security incidents / data breaches (also with regard to reporting obligations to supervisory authorities)
Use of spam filters and regular updates	Documented procedure for dealing with security incidents
Use of virus scanners and regular updates	Involvement of DPO and ISO in security incidents and data breaches
Intrusion Detection System (IDS)	Documentation of security incidents and data breaches via e-mail / ticket system under planning
Intrusion Prevention System (IPS)	Formal procedure and responsibilities for following up security incidences and data breaches

- **Default Privacy Settings (Art. 25 para. 2 GDPR)**

Privacy by design / Privacy by Default

Technical Measures	Organisational Measures
No more personal data is collected than is necessary for the purpose in question	
Simple exercise of the data subject's right of withdrawal through technical measures	

- **Order Control**

Measures to ensure that personal data processed on behalf of the customer can only be processed in accordance with the instructions of the customer. In addition to data processing on behalf of the client, this point also includes the performance of maintenance and system support work both on site and by remote maintenance

Technical Measures	Organisational Measures
	Prior examination of the safety measures taken by the contractor and their documentation
	Selection of the contractor under due diligence considerations (especially with regard to data protection and data security)
	Conclusion of the necessary agreement for order processing or EU standard contract clauses
	Written instructions to the contractor
	Obligation of the Contractor's employees to maintain data secrecy
	Agreement on effective control rights vis-à-vis the contractor
	Regulation on the use of further subcontractors
	Ensuring the destruction of data after completion of the order
	In the case of prolonged cooperation: ongoing review of the contractor and their level of pro-

	tection

ANNEX 2

DATA PROCESSING PRINCIPLES

1. Purpose limitation: Personal data may be processed and subsequently used or further communicated only for purposes described in clause 15 paragraph 2 or subsequently authorised by the data subject.
2. Data quality and proportionality: Personal data must be accurate and, where necessary, kept up to date. The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.
3. Transparency: Data subjects must be provided with information necessary to ensure fair processing (such as information about the purposes of processing and about the transfer), unless such information has already been given by the data exporter.
4. Security and confidentiality: Technical and organisational security measures must be taken by the data controller that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the data controller.
5. Rights of access, rectification, deletion and objection: As provided in Article 12 of Directive 95/46/EC, data subjects must, whether directly or via a third party, be provided with the personal information about them that an organisation holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the data exporter. Provided that the authority has given its prior approval, access need also not be granted when doing so would be likely to seriously harm the interests of the data importer or other organisations dealing with the data importer and such interests are not overridden by the interests for fundamental rights and freedoms of the data subject. The sources of the personal data need not be identified when this is not possible by reasonable efforts, or where the rights of persons other than the individual would be violated. Data subjects must be able to have the personal information about them rectified, amended, or deleted where it is inaccurate or processed against these principles. If there are compelling grounds to doubt the legitimacy of the request, the organisation may require further justifications before proceeding to rectification, amendment or deletion. Notification of any rectification, amendment or deletion to third parties to whom the data have been disclosed need not be made when this involves a disproportionate effort. A data subject must also be able to object to the processing of the personal data relating to him if there are compelling legitimate grounds relating to his particular situation. The burden of proof for any refusal rests on the data importer, and the data subject may always challenge a refusal before the authority.
6. Sensitive data: The data importer shall take such additional measures (e.g. relating to security) as are necessary to protect such sensitive data in accordance with its obligations under clause 17.
7. Data used for marketing purposes: Where data are processed for the purposes of direct marketing, effective procedures should exist allowing the data subject at any time to “opt-out” from having his data used for such purposes.
8. Automated decisions: For purposes hereof “automated decision” shall mean a decision by the data exporter or the data importer which produces legal effects concerning a data subject or significantly affects a data subject and which is based solely on automated processing of personal data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. The data importer shall not make any automated decisions concerning data subjects, except when:
   (a) (i) such decisions are made by the data importer in entering into or performing a contract with the data subject, and
   (ii) (the data subject is given an opportunity to discuss the results of a relevant automated decision with a representative of the parties making such decision or otherwise to make representations to that parties.

   or

   (b) where otherwise provided by the law of the data exporter.