SPECIAL CONDITIONS FOR DISH PAY

TABLE OF CONTENTS

SPECIAL CONDITIONS FOR DISH PAY

PART I SPECIAL CONDITIONS FOR THE USE OF DISH PAY

1 SCOPE OF APPLICATION

1.1 These Special Conditions for DISH Pay ("**Special Conditions**") of DISH Digital Solutions GmbH, Metro Straße 1, 40235 Düsseldorf, Germany ("**DISH**") apply in addition to the General Business Terms and Conditions of Use of DISH ("**Terms of Use**") for the use of the payment function "DISH Pay" of the DISH Platform (as defined in the Terms of Use).

1.2 DISH provides all services of DISH Pay to the contractual partner of DISH ("**Client**"; the Client and DISH together referred to as the "**Parties**" and individually also as a "**Party**") solely on the basis of these Terms of Use. Deviating terms and conditions of the Client shall not apply even if DISH does not expressly reject them and/or provides services and/or performances without reservation despite knowledge of the Client's conflicting and/or deviating terms and conditions.

1.3 The processing of payments within the framework of DISH Pay is carried out by partners of DISH that are authorised as payment institutions, banks or other payment service providers in the European Union ("**Payment Service Partners**"). DISH does not itself provide payment services within the meaning of § (1) of the Zahlungsdiensteaufsichtsgesetz (Payment Services Supervision Act, *ZAG*) and Article 4 No. 3 of Directive (EU) 2015/2366 (PSD2), but contributes to them as a technical service provider without taking possession of the funds to be transferred to the Client.

2 CONCLUSION OF CONTRACT

2.1 DISH Pay is only open to entrepreneurs (§ 14 German Civil Code, *BGB*), in particular those who are active in the catering and food industry. Natural persons (individual enterprises) must be of full age and have unlimited legal capacity. The enterprise must not be active in excluded sectors in accordance with the conditions set out in Section 3.2.

2.2 The contract for the use of DISH Pay on the basis of these Special Conditions between the Client and DISH ("**User Contract**") is generally concluded by way of the Client and DISH (electronically) signing a contract with reference to these Special Conditions, the price list and the General Terms and Conditions of the Payment Service Partner(s). The Client assures to provide correct and complete information during the conclusion of the contract.

2.3 The contract for the purchase of payment terminals and/or other terminal equipment between the Client and DISH ("**Purchase Contract**") may be concluded together with the User Contract and/or separately at a later date. The same applies to maintenance contracts for the purchased terminals or rental contracts for terminals. For these contracts, the corresponding regulations contained in Part II apply in addition.

3 REGISTRATION WITH THE PAYMENT SERVICE PARTNER

3.1 The use of DISH Pay requires that the Client enters into and maintains a payment processing contract with one or more Payment Service Partners (each a "**Payment Contract**") arranged by DISH.

3.2 The available Payment Service Partners as well as the respective General Terms and Conditions of the Payment Service Partners and other terms and agreements of the Payment Service Partners can be accessed by the Client at the following address:

www.dish.co/dish-pay-list-of-payment-service-partners

3.3 Each Payment Service Partner is legally obliged to verify the identity of the Client and to collect further information about the Client before concluding a Payment Contract in order to prevent money laundering and terrorist financing (AML[1]/CFT[2]). In addition, the Payment Service Partner collects further information about the Client's economic situation in order to prevent payment defaults and misuse. In this context, the Client warrants to provide correct and complete information and not to be active in the industries excluded by the Payment Service Partner in accordance with the conditions set out in Section 3.2.

3.4 After the Client has provided DISH with the information pursuant to Section 3.3, its bank details and other information required by the Payment Service Partner and has confirmed the opportunity to take note of the conditions pursuant to Section 3.2, DISH will forward this information and (a) this information and (b) the application to conclude the Payment Contract(s) with the Payment Service Partner(s)on behalf of the Client to the Payment Service Partner(s). For the avoidance of doubt: The Payment Service Partner has the right to accept or reject the application. In the event of acceptance of the application, the Payment Contract(s) are concluded directly between the Client and the Payment Service Partner.

3.5 If the Payment Contract with a Payment Service Partner is terminated (or if no Payment Contract is concluded pursuant to Section 3.4), the Client may not (or no longer) use DISH Pay with this Payment Service Partner. If it was the only or the last Payment Service Partner, the use of DISH Pay as a whole is no longer possible until DISH can provide the Client with at least one new Payment Service Partner. If the Payment Contract with a Payment Service Partner is ultimately not concluded, DISH and the Client may rescind Purchase Contracts, maintenance contracts and rental contracts for terminal equipment concluded at the same time as the User Contract, insofar as the terminal equipment that is the subject of the contract cannot be used without the Payment Contract that has not been concluded; the statutory provisions apply regarding the rescission.

3.6 If the User Contract is terminated (as described in Section 14) or if the cooperation between DISH and the Payment Service Partner ends (as described in Section 4.2), DISH will terminate the Payment Contract(s) on behalf of the Client. Deviating agreements between the Client and the Payment Service Partner remain unaffected by this.

3.7 The Client hereby authorises DISH to receive notices from the Payment Service Partner and to terminate Payment Contracts on its behalf in accordance with Section 3.6.

[1] Anti-Money Laundering
[2] Countering the Financing of Terrorism

4 CHANGES TO THE PAYMENT SERVICE PARTNERS

4.1 DISH may, at its sole discretion, add additional Payment Service Partners to DISH Pay and to the overview pursuant to Section 3.2. The Sections 2.2 and 3.2 to 3.4 as well as Section 3.5 sentence 3 apply mutatis mutandis to the extension of the User Contract to include further Payment Service Partners.

4.2 If the partnership between DISH and a Payment Service Partner ends, DISH will generally notify the Client of this at least 14 days in advance. The time limit may be shortened if there is a good cause for doing so. Good cause exists in particular if DISH, taking into account all circumstances of the individual case and weighing the interests of all parties involved, cannot reasonably be expected to continue the contractual relationship between DISH and the respective Payment Service Partner until the expiry of the period pursuant to sentence 1.

5 DISH SERVICES

5.1 DISH Pay enables Clients to receive payments from their end customers (e.g. guests):

(a) if the end customer is present in the Client's establishment ("**POS**"[1]) via a suitable and/or digital POS system, which, depending on the payment methods offered by the Payment Service Partner, that may in particular be payments with debit cards, credit cards and similar payment instruments, direct debit payments (also card-**based**) or payments processed online via an app/QR code; and/or

(b) online in connection with orders placed via digital tools from DISH, insofar as reference is made to these Special Conditions in the Client's terms and conditions;

whereby the payment is processed in each case by a Payment Service Partner of DISH.

5.2 The acceptance of payments with debit cards, credit cards and similar payment instruments at the POS requires the purchase or rental of a DISH payment terminal approved by the Payment Service Partner and, if applicable, the conclusion of a maintenance contract for the payment terminal provided for by the Payment Service Partner.

5.3 The Client is aware that the Client bears the risk of non-payment for certain types of payments under the Payment Contract, in particular for payments without presentation of the debit card, credit card and similar payment instruments ("card not present" transactions), payments with a manual entry of the card data ("key-entered" transactions) and direct debit payments by the end customer.

5.4 The Payment Service Partner forwards the payments received on behalf of the Client directly to the Client after deducting the remuneration payable to DISH pursuant to Section 7.1. Onward transfers to the Client will be made by the Payment Service Partner in accordance with the terms and on the dates set out in the Payment Contract, provided that the Payment Service Partner may withhold individual payments received on behalf of the Client where there is a particularly high risk of fraud or non-payment in accordance with the terms set out in the Payment Contract. The Payment Service Partner may, if necessary, offset claims against the Client arising from direct debits chargebacks, credit card chargebacks, the remuneration for DISH pursuant to Section 6.1 and/or other claims; details are set out in the General Terms and Conditions of the Payment Service Partner.

[1] Point of Sale

5.5 DISH may adapt DISH Pay and other services to the state of the art and technical developments or needs. Insofar as the agreed scope of Services changes as a result, the provisions on the amendment of these Special Conditions apply in accordance with Section 16.

6 REMUNERATION

6.1 For the use of DISH Pay, remuneration is due in accordance with the respective valid price list. The amount of the remuneration may vary depending on the selected Payment Service Partner and the payment methods, as well as the chosen device. The Client can call up the current price list at any time at the following address:

www.dish.co/dish-pay-list-of-prices-of-services
www.dish.co/dish-pay-now-price-list

6.2 The remuneration payable to DISH for the use of DISH Pay also includes all fees and costs for the Payment Service Partner, unless otherwise stated. In this respect, the Client is not obliged to pay a fee directly to the Payment Service Partner.

6.3 Unless stated otherwise, all prices stated in the price list according to Section 6.1 and elsewhere are exclusive of statutory value added tax.

7 PAYMENT AND INVOICING

7.1 Generally, the Payment Service Partner is going to deduct the remuneration payable to DISH pursuant to Section 6 directly from the payments received for the Client (cf. Section 5.3) and settle them with DISH. DISH instructs the Payment Service Partner on behalf of the Client to proceed as described in sentence 1. DISH issues a monthly invoice to the Client for the remuneration paid in accordance with sentence 1.

7.2 Remuneration for the purchase of payment terminals and/or other terminal equipment will be invoiced by DISH to the Client upon conclusion of the corresponding Purchase Contract.

7.3 Other remunerations which are not retained pursuant to Section 7.1, such as in particular remunerations for maintenance services or the rental of terminal equipment, will be invoiced by DISH to the Client on a monthly basis, with fixed monthly fees being due at the beginning of a calendar month and variable fees being due after the end of the respective calendar month and invoiced to the Client.

8 DUTIES AND OBLIGATIONS OF THE CLIENT

8.1 The Client is obliged to continuously update and, if necessary, correct the data provided by it upon conclusion of the contract. The Client further has to ensure that messages sent to the e-mail address provided to DISH are regularly retrieved in order to receive information relevant to the contract.

8.2 Upon request by DISH or the Payment Service Partner, the Client has to complete a Self-Assessment Questionnaire (SAQ) truthfully and return it to DISH or the Payment Service Partner.

8.3 **The Client has to ensure that, when making payments with debit cards, credit cards and similar payment instruments, the security precautions specified by the payment system (in particular in accordance with the Payment Card Industry Data Security Standard, PCI-DSS, if agreed in the payment contract) are complied with and that the card data are not noted or otherwise recorded.** DISH has the right to verify compliance with the requirements pursuant to sentence 1 by means of inspections (audits) once per calendar year. The Client has to provide DISH (or a DISH agent subject to confidentiality obligations at least as strict as those set forth in Section 11) with access to its premises and all systems used to process payment data and related documentation for this purpose upon request in text form, whereby the request must be made at least two weeks in advance, and has to provide DISH (or the agent) with reasonable assistance. The audits have to take place during normal business hours, unless the Parties agree otherwise. DISH will endeavour to cause as little disruption as reasonably possible to the Client's ordinary business operations when carrying out the audits. In case of specific indications of a violation of the requirements according to sentence 1 by the Client, DISH may also perform the audit more frequently than annually and/or with a shorter lead time than two weeks. If significant errors are identified during the audit, the Client has to bear the costs of the audit.

8.4 Access data that the Client receives from DISH or selects itself will not be disclosed by the Client to unauthorised third parties and will be protected from access by unauthorised third parties. The same applies to end devices on which the access data are stored. The Client will inform DISH immediately if the Client has reasonable suspicion or is aware of a possible misuse of the access data provided. In this case, DISH is entitled to temporarily block the Client's access data until the suspicion of misuse has been cleared or new access data has been assigned by DISH and, if an unauthorised change to the Client's payout account cannot be ruled out, to arrange for the Payment Service Partner to suspend the payouts until clarification.

8.5 To the extent that DISH or the Payment Service Partner provides SIM cards (or profiles for eSIM cards; referred to only as **"SIM Cards"** in the following) as part of the services to the Client, such SIM Cards and the mobile services associated therewith are intended exclusively for use in connection with the respective service at the respective location of the Client. The Client may not use the SIM Cards and mobile services for any other purpose, in particular for setting up connections to connections chosen by the Client or for communicating with destinations chosen by the Client via the Internet. For any other use, DISH may charge the Client a fee of EUR 2.50 per MB or part thereof, unless the Client proves a lower damage.

8.6 It is the Client's responsibility to meet the system requirements necessary to use DISH Pay. In particular, DISH is not responsible for providing an Internet browser, an Internet connection or any other infrastructure that enables the Client to access DISH Pay.

8.7 Depending on the end device, it may be necessary to download and/or install the App in order to use DISH Pay. The Customer shall always use the latest version of the App. This includes downloading and installing updates that are made available. This may require an active Google user account.

8.8 DISH will make its best efforts to adapt the services promptly to legal provisions in the respective country or territory and any changes thereto. However, it is the Client's responsibility to check whether the services meet the requirements of the regulations applicable to him and, if necessary, to take supplementary measures.

9 PERMITTED USE

9.1 **The Client may only use DISH Pay for its own business purposes.** The Client is not entitled to grant a third party rights of use to DISH or to transfer its user account to third parties. The Client may not use DISH Pay in an unlawful manner or for unlawful purposes.

9.2 **In particular, the Client may not accept payments for third parties or provide other payment services.** In this context, the Client is advised that the provision of payment services without permission from the competent supervisory authority may constitute a criminal offence or an administrative offence.

9.3 The Client is also obliged vis-à-vis DISH to comply with its obligations under the Payment Contract with the Payment Service Partner and in particular to observe any restrictions regulated therein. **In particular, the Client may not use DISH Pay for goods and services that are excluded by the respective Payment Service Partner under the Payment Contract**.

9.4 In the event of credit card chargebacks, direct debit chargebacks or cases of fraud, the Client has to cooperate in the clarification process and to provide DISH and the Payment Service Partner with all relevant available information and evidence upon request.

9.5 In the event of a breach by the Client of its contractual obligations, in particular under this Section 9, the Client is liable to DISH to the full extent of the law. The Client's attention is drawn to the fact that this liability may also include contractual penalties imposed by the Payment Service Partners or payment system operators (e.g. credit card enterprises) for non-compliance with the terms and conditions of the payment system.

10 DATA PROTECTION

10.1 In providing DISH Pay and the services, DISH processes personal data of the Client, its employees and third parties for its own purposes. The Client's attention is drawn to DISH's separate privacy policy; this serves exclusively to inform the Client and the data subjects in accordance with the provisions of Regulation (EU) 2016/679 ("**GDPR**") and is not part of the contract.

10.2 The same applies to the Payment Service Partner, in particular when providing services as part of the acquisition business. For this purpose, the Client's attention is drawn to the privacy policy and the general terms and conditions of the respective Payment Service Partners, which the Client can access at the address given in Section 3.2.

10.3 In the context of the provision of technical services for payment processing by DISH Pay, DISH further processes personal data on behalf of the Client on the basis of the Order Processing Agreement contained in the Special Conditions. Within the scope of the technical processing, the respective Payment Service Partner will also act as a sub-processor of the Client. It is hereby clarified that this only includes processing activities where DISH or the Payment Service Partner itself does not determine the purposes and means of the processing of the personal data.

11 CONFIDENTIALITY

11.1 The Parties are obliged not to make confidential information available to third parties and not to use it for other purposes not serving the performance of the User Contract ("**Confidentiality Obligation**"). The Confidentiality Obligation also applies after the end of the contract term. All technical and contractual information and know-how made available to the Client as well as other information marked as confidential by one of the two Parties and having economic value is be deemed to be confidential. This expressly includes trade and business secrets.

11.2 The Confidentiality Obligation does not apply to the use of data by DISH under Section 12.

11.3 The Confidentiality Obligation also does not apply to information which has become or is already known to a Party or to the public without a breach of this Section 11, or which must be made accessible to third parties due to statutory provisions, judicial or official orders, or which is inspected by third parties bound to secrecy in the context of an intended acquisition.

12 DATA USE

12.1 The Client grants DISH the right to store, analyse and use for evaluation purposes all data generated during the use of DISH Pay. The Client also grants DISH the power to supplement the data obtained with data from affiliated companies (within the meaning of §§ 15 et seq. German Stock Corporation Law (*AktG*) of DISH sourced from possible business relationships of the Client with those (that DISH is going to request from such affiliated company), as well as other sources (for example from publicly accessible third-party sources (such as e.g. rating portals and social media) or other data sources accessible to DISH) to combine it and to evaluate it at DISH's discretion for its own purposes as well as to pass on these evaluations to third parties (in particular, but not exclusively, those involved in the (further) development and operation of DISH Pay as sub-service providers, as well as affiliated enterprises of DISH that offer digital solutions or other services for Client's business operations) and to make them accessible to them. This power shall remain valid even after termination of the User Agreement.

12.2 Special categories of personal data within the meaning of Article 9 (1) GDPR, data on criminal convictions and offences within the meaning of Article 10 GDPR, sensitive payment data within the meaning of § 1 (26) of the Payment Services Supervision Act (*ZAG*) as well as information, sourced through a control in accordance with Section 8.3 sentence 2 through 7 are in any case excluded from use pursuant to Section 12.1. Other personal data that DISH processes on behalf of Client pursuant to Section 10.3 will be anonymised by DISH on behalf of Client prior to use pursuant to Section 12.1.

12.3 The provisions of the GDPR, Directive 2002/58/EC, the German Telecommunications Telemedia Data Protection Act (*TTDSG*), and other provisions on data protection or privacy remain unaffected.

13 RESTRICTIONS ON USE

13.1 DISH is entitled to block or restrict the Client's access to DISH Pay if and to the extent that

(a) the Client has provided incorrect or incomplete information or has not corrected the information without delay, in breach of Section 2.2, 3.3 or 8.1;

(b) there are indications that the Client is using DISH Pay for money laundering, financing terrorism or other criminal acts;

(c) the Client's transactions have a number of credit card chargebacks, direct debit chargebacks or other non-payments that is significantly higher than the average for comparable payees;

(d) the Client uses SIM Cards in breach of Section 8.5;

(e) the Client processes payments for third parties in breach of Section 9.2; or

(f) the Client otherwise materially or repeatedly breaches any other obligation of the Client under these Special Conditions.

13.2 DISH will notify the Client of the restriction of use in text form before or at the same time as the restriction of use takes effect.

14 CONTRACT TERM AND TERMINATION

14.1 DISH and the Client enter into the User Agreement for an indefinite period of time, unless a specific contract term has been agreed upon.

14.2 The Client or DISH may terminate the User Agreement with one month's notice. If DISH and the Client have agreed on a specific contract term, the User Contract will be extended automatically in each case by the contractually agreed term, unless the Client or DISH terminates the contract as described in sentence 1 above before the expiration of the contract term. The Client may terminate the User Agreement and the rental agreement for terminal equipment if special circumstances result from the current price list. In this case, the Client may withdraw from the User Agreement and the rental agreement for terminal equipment against payment of a certain fee.

14.3 The right of the Parties to extraordinary termination of the User Agreement for good cause remains unaffected.

14.4 Good cause within the meaning of Section 14.3 for DISH exists in particular if:

(a) DISH is subject to statutory or regulatory obligations that require a complete termination of the provision of the services to the Client and thereby do not allow the Client to comply with the time limit under Section 14.2;

(b) (i) the Client is in default for two (2) consecutive months in the payment of the remuneration or of a not insignificant part thereof, or (ii) is in default for a period of more than two (2) months in the payment of the agreed remuneration in an amount equal to the agreed remuneration for two (2) months; or

(c) the Client has provided false or incomplete information in breach of Section 2.2, 3.3 or 8.1 and (i) the Client has not corrected or supplemented the information within a period of at least thirty (30) days set by DISH in text form, or (ii) DISH is unable to contact the Client because the email address provided by the Client is invalid or no longer valid;

(d) the Client, in breach of Section 8.2, fails to complete or return a questionnaire referred to therein after DISH has previously threatened the Client with terminating the User Agreement by setting a reasonable deadline, or the Client has not provided truthful information in such questionnaire;

(e) facts justify the assumption that the Client is using DISH Pay for money laundering, the financing of terrorism or otherwise for criminal acts;

(f) the Client's transactions have a number of credit card chargebacks, direct debit chargebacks or other non-payments that is significantly higher than the average for comparable payees, unless the Client can demonstrate special circumstances that would lead it to expect a higher number in the normal course of business;

(g) the Client has used SIM Cards in breach of Section 8.5 and the additional data traffic caused thereby exceeds 10 MB; or

(h) the Client otherwise materially or repeatedly breaches any of its obligations under these Special Conditions after DISH has threatened the Client with termination of the User Agreement before that.

14.5 The Client may ordinarily terminate the Agreement through a function provided for this purpose on the DISH Pay platform or in text form. Any other termination of the User Contract by one of the Parties requires text form. A notice of termination (in particular in the case of Section 14.4(c)(ii)) shall also be deemed to have been received if the Client has frustrated receipt of the e-mail by providing or failing to update an invalid e-mail address or one that has become invalid.

15 DISH'S LIABILITY

15.1 DISH's liability for all damages of the Client, regardless of the legal reason, is excluded, unless otherwise stated in the following Sections 15.2 - 15.5.

15.2 DISH shall be liable within the scope of the statutory provisions for:

(a) damage resulting from injury to life, body or health caused by an intentional or negligent breach of duty by DISH or one of its legal representatives or vicarious agents;

(b) damage resulting from an intentional or grossly negligent breach of duty by DISH or one of its legal representatives or vicarious agents; and

(c) other damage resulting from a (simple) negligent breach of obligations the fulfilment of which is a prerequisite for the proper performance of the Agreement with the Client and the observance of which the Client may regularly rely on, whereby, except in the cases of letters (a) and (b), DISH's liability shall be limited to typical and foreseeable damages.

15.3 Any liability on the part of DISH under the German Product Liability Act (*PHG*) (to the extent applicable) remains unaffected. The same applies to any liability on the part of DISH under other statutory provisions which expressly establish that liability cannot be excluded or limited in advance.

15.4 If DISH has given a guarantee as to quality or otherwise assumed strict liability, the liability arising therefrom shall be governed exclusively by the terms and conditions of the respective guarantee or assumption and this Section 15 does not apply.

15.5 The limitations of liability pursuant to this Section 15 apply to the liability of DISH's corporate bodies, vicarious agents, employees and other staff as well as affiliated enterprises (within the meaning of §§ 15 et seq. of the German Stock Corporation Act, *AktG*) of DISH and its corporate bodies, vicarious agents, employees and other staff accordingly.

16 AMENDMENTS TO THESE SPECIAL CONDITIONS

16.1 DISH reserves the right to make changes or additions to these Special Conditions (hereinafter only referred to as "**Amendments**"). DISH will notify the Client in text form of any proposed Amendments to the Special Conditions.

16.2 The proposed Amendments will only be implemented after the expiry of a reasonable and proportionate period of time with regard to the nature and scope of the planned Amendments and their consequences for the Client. This period is at least thirty (30) days from the date DISH notifies the affected Clients of the proposed amendments. DISH must grant longer periods if this is necessary to enable the Client to make the technical and/or business adjustments required due to the Amendments requested by DISH.

The aforementioned time limit does not apply if DISH

(a) due to statutory or regulatory obligations, must make Amendments to the Special Conditions in a manner that does not allow DISH to meet the time limit set forth in Section 16.2;

(b) in exceptional circumstances, must amend the Special Conditions in order to address an unforeseen and imminent threat to protect the DISH platform, consumers, the Client or other users from fraud, malware, spam, privacy breaches or other cybersecurity risks.

16.3 To the extent that the proposed amendments do not (i) affect the service description of already agreed service components, the remuneration or other main service obligations, (ii) are reasonable for the Client and (iii) do not place the Client in a worse position overall, the following applies:

(a) The amendments are deemed to have been approved if the Client does not object in text form within the time limit set out in Section 16.2. If the Client objects to the Amendment, DISH may terminate the User Agreement, according to Section 14.2.

(b) The Client has the right to extraordinary termination of the affected User Agreement before the expiry of the period according to Section 16.2.

(c) DISH has to inform the Client of the consequences of a failure to object and of the right to extraordinary termination when informing the Client of Amendments to the Special Conditions.

(d) The Client may waive compliance with the time limit in accordance with Section 16.2 and thus waive its right to object or right to extraordinary termination in accordance with lit. (b) by means of an unambiguous confirmatory act.

16.4 In the case of other changes to the Special Conditions for which the conditions set forth in Sections 16.3(i) to 16.3(iii) are not met or for which DISH, in its sole discretion, does not wish to proceed in accordance with Section 16.3, DISH will request the Client in text form to expressly consent to the amendment of the Special Conditions within the period set by DISH in accordance with Section 16.2. If the Client does not grant the consent within a period of time set by DISH, DISH is free to make use of the option to terminate the User Contract in accordance with Section 14.2.

16.5 The Amendments do not apply to Purchase Contracts. The Special Conditions in the version included in the respective Purchase Contract apply exclusively to these.

17 ASSIGNMENTS OF RIGHTS AND OBLIGATIONS

17.1 The Client is not entitled to assign rights and obligations under this User Contract or a Purchase Contract without DISH's prior written consent. § 354a of the German Commercial Code (*HGB*) remains unaffected.

17.2 DISH is entitled to transfer the User Contract to affiliated enterprises (as defined in §§ 15 et seq. of the German Stock Corporation Act, *AktG*) of DISH, provided that this does not represent an unreasonable hardship to the Client. In this context, a division of rights and/or obligations among the affiliated enterprise (within the meaning of §§ 15 et seq. of the German Stock Corporation Act, *AktG*) and DISH is possible, provided that the Client is not placed in a worse position as a result. In the case of a Client who is entitled to deduct input tax, it is not considered to be undue hardship or a worse position if VAT is incurred in the Client's country of domicile for the first time as a result of the transfer.

18 APPLICABLE LAW AND JURISDICTION

18.1 The contract and all claims and rights arising out of or in connection with the User Contract are governed exclusively by and construed and enforced in accordance with the laws of Germany, excluding its conflict of laws rules. The application of the United Nations Convention on Contracts for the International Sale of Goods (CISG) is excluded. The place of performance is Düsseldorf.

18.2 If the Client is a merchant, a legal entity under public law or a special fund under public law, the exclusive place of jurisdiction for all disputes arising from or in connection with this agreement, its execution or its performance shall be Düsseldorf. If the Client is domiciled abroad, DISH may, however, also bring an action there.

PART II CONDITIONS FOR THE PROVISION OF TERMINAL EQUIPMENT (IN PARTICULAR PAYMENT TERMINALS)

CHAPTER A PURCHASE OF TERMINAL EQUIPMENT

These terms and conditions apply to the purchase of terminal equipment, in particular payment terminals for the use with DISH Pay's Payment Service Partners, and accessories.

1 GENERAL PROVISIONS

1.1 When purchasing terminal equipment (in particular payment terminals) and accessories, the Client acquires the object of purchase against payment of a one-off remuneration.

1.2 Unless otherwise expressly agreed, consumables such as batteries, rolls of sales slips, ink or toner, cables and accessories as well as software on separate data carriers are not part of the purchase.

1.3 The use of a payment terminal for certain payment services may be dependent on the conclusion and existence of an effective maintenance contract according to Chapter B.

1.4 SIM Cards are not part of the object of purchase and remain the property of DISH or the network operator. Reference is made to Part I, Section 8.3. The use of the mobile phone function may also depend on the existence of an effective maintenance contract according to Chapter B.

1.5 The Client will return to DISH for proper disposal any payment terminals that have been discarded or are no longer required. The Client will also impose this obligation on the respective purchasers in the event of resale.

2 RETENTION OF TITLE

2.1 The terminal equipment remain the property of DISH until the purchase price has been paid in full.

2.2 In the event of a resale of the terminal equipment, the buyer hereby assigns to DISH, which accepts, by way of security the claim(s) against the purchaser arising therefrom. The same applies to other claims which take the place of the goods or otherwise arise in respect of the goods. DISH authorises the Client to collect the claims assigned to the seller as collateral in its own name; DISH may revoke this collection authorisation only in the event of enforcement.

3 WARRANTY

3.1 The warranty (limitation of claims due to defects) is limited to one year from handover for new terminal equipment, otherwise excluded. This does not apply if DISH has fraudulently concealed a defect.

3.2 In deviation from Section 3.1, claims for damages due to defects are governed exclusively by Part I, Section 15.

CHAPTER B MAINTENANCE SERVICES (TERMINAL REPLACEMENT SERVICE)

These terms and conditions apply to maintenance contracts for purchased terminal equipment that are concluded in addition to the Purchase Contract according to Chapter A. The maintenance of rented property is part of the rental contract; with regard to this Chapter C, Section 4 applies.

1 SCOPE OF MAINTENANCE SERVICES

1.1 The maintenance service for terminal equipment includes the elimination of defects and other faults of the terminal equipment that occur outside the warranty. If defects occur on a terminal equipment during the agreed period, DISH will remedy them by repair or exchange for a terminal equipment of at least equal value.

1.2 If the maintenance service is performed at the Client's location on an island, the Client will be invoiced separately by DISH for the waiting and travel times incurred as a result of this maintenance service as well as the costs of the crossing.

2 EXCLUSIONS

2.1 Unless otherwise agreed, the maintenance services do not include the provision of a rental device during the repair of the terminal equipment. In the event of a replacement, the Client will receive a replacement device and is obliged to return the defective terminal equipment properly packaged within two weeks to the address specified by DISH (or DISH's supplier).

2.2 The maintenance services do not include the removal of defects caused by improper use of the terminal equipment, wilful destruction, mechanical damages as well as other external influences such as falling, loss, burglary, lightning, overvoltage, fire or water damage or fire or normal wear and tear (in particular regarding the batteries). In such cases, DISH may offer a separately remunerated (i) repair or (ii) replacement of the terminal equipment to the Client. If the defect is due to the terminal equipment's opening, changing, repairing, modifying or adding to, which is carried out by a party other than DISH, the maintenance services are excluded.

2.3 Maintenance services do not include consumables such as batteries, rolls of sales slips, ink or toner, cables and accessories, unless otherwise agreed.

3 OBLIGATIONS OF THE CLIENT

3.1 The Client shall immediately report any defects or malfunctions of the terminal equipment and answer any queries to a reasonable extent.

3.2 It is the Client's responsibility to cooperate to a reasonable extent in the rectification of defects and other defaults, such as by temporarily shutting down or restarting the terminal equipment. The Client has to grant DISH access to the terminal equipment during normal business hours.

3.3 The Client will assist DISH with the maintenance services at its premises by providing knowledgeable personnel who can provide information about the specifics of its environment, as well as other terminal equipment and software used with the Devices for testing purposes. It shall also provide any test material required for the maintenance services, unless this test material is part of DISH's normal equipment.

3.4 DISH is entitled, but not obliged, to carry out preventive maintenance services. The Client will grant DISH access to the terminal equipment for this purpose during normal business hours by arrangement.

CHAPTER C RENTAL OF TERMINAL EQUIPMENT

These terms and conditions apply to the rental of terminal equipment, in particular payment terminals for use with DISH Pay's Payment Service Partners, and accessories.

1 GENERAL PROVISIONS

1.1 In the case of a rental, DISH provides the Client with the agreed terminal equipment (in particular payment terminals), including the associated user documentation and the agreed accessories (hereinafter the "**Rental Items**") for the duration of the rental period.

1.2 Unless otherwise agreed, consumables such as batteries, rolls of sales slips, ink or toner, cables and accessories as well as software on separate data carriers are not part of the Rental Items.

1.3 The rental period in accordance with Section 1.1 commences on the day on which the Rental Items are made available to the Client.

2 HANDOVER AND COMMISSIONING OF THE RENTAL ITEMS

2.1 The Client will install the Rental Items and make them ready for use, unless otherwise agreed.

2.2 Insofar as installation or handover of the Rental Items at the Client's location has been agreed, the condition of the rented items will be inspected in the presence of the Client and any defects will be recorded in a handover report to be countersigned by the Client. The Parties will also record in this handover protocol whether and which defects are to be remedied by DISH.

3 USE OF THE RENTAL ITEMS

3.1 The Client has to handle the Rental Items with care and protect them adequately against damage or loss. In the event of damage or loss, the Client has to notify DISH thereof without undue delay in text form.

3.2 The Client may use the Rental Items exclusively for the processing of payments at the agreed location for its own purposes. It may not sublet the Rental Items or otherwise make them available to third parties (employees of the Client are deemed to be no third parties).

3.3 The Client may not modify the Rental Items without DISH's written consent or unless the modifications are updates provided by DISH. If the Client nevertheless makes changes to the Rental Items, it must reverse these before returning the Rental Items.

3.4 The Client may not sell or pledge the Rental Items or deposit them as a collateral. In the event of a seizure by a third party, the Client has to inform DISH thereof without undue delay in text form.

4 MAINTENANCE OF THE RENTAL ITEMS

4.1 The Client has to notify DISH immediately in text form of any defects occurring in the Rental Items so that DISH can remedy them. DISH may remedy defects in the Rental Items in particular by repairing the Rental Items or by replacing them with a device equivalent to the Rental Items. Claims for damages due to defects are governed exclusively by Part I, Section 15.

4.2 If the Client receives a replacement device, the Client is obliged to return the defective or exchanged terminal equipment within two weeks properly packaged to the address specified by DISH (or DISH's supplier).

4.3 DISH is entitled to perform preventive maintenance services on the Rental Items. The Client will grant DISH access to the Rental Items for this purpose during normal business hours by arrangement.

4.4 The Client may not maintain the Rental Items itself or have them maintained by third parties.

5 INSURANCE; RISK

5.1 For a rental period of more than one year, DISH will insure the Rental Items against fire and theft at its own expense. Should such damage occur, DISH may charge the Client a deterrent fee in the amount of EUR 100.00, unless the Client is not responsible for the damage.

5.2 In the event of damage to or loss of the Rental Items for which the Client is responsible, DISH will invoice the Client for the repair costs or the replacement value.

6 END OF THE RENTAL PERIOD; RETURN

6.1 The Client has to return the Rental Items after the expiry of the rental period within ten (10) days in its original condition, insofar as deviations from the original condition are not due to normal wear and tear of the Rental Items, modifications to the Rental Items permitted by DISH or maintenance measures by DISH.

6.2 If collection of the Rental Items at the Client's location has been agreed, the condition of the rented items will be examined in the presence of the Client and any defects will be recorded in a handover protocol to be countersigned by the Client upon return.

Otherwise, the Client has to return the Rental Items properly packaged to DISH; the Client has to bear the transport costs for the return shipment, unless otherwise agreed.

6.3 Section 14.2, sentence 3 remains unaffected in the event of rental agreement's termination.

PART III ORDER PROCESSING AGREEMENT

For Clients who have their registered office or their respective branch office in a country of the European Union (EU) or another contracting party to the Agreement on the European Economic Area (EEA), the order processing agreement set out in the following applies Chapter A exclusively to the processing of personal data for the Client by DISH.

For Clients who have their registered office or their respective branch in a country outside the EU / EEA ("**Third Country**"), Chapter A that agreement also applies if and to the extent that an adequacy decision within the meaning of Article 45 GDPR applicable to the Client exists for the respective Third Country. If there is no adequacy decision for the Third Country or it is not applicable to the Client, Chapter B applies instead.

CHAPTER A CLIENTS IN THE EU OR EEA AND IN THIRD COUNTRIES WITH ADEQUACY DECISIONS

Section I

CLAUSE 1 PURPOSE AND SCOPE OF APPLICATION

a) The purpose of these Standard Contractual Clauses (the "**Clauses**") is to ensure compliance with Article 28 (3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

b) The controllers and processors listed in **Annex I.A** have agreed to these Clauses in order to ensure compliance with Article 28 (3) and (4) of Regulation (EU) 2016/679 and/or Article 29 (3) and (4) of Regulation (EU) 2018/1725.

c) These Clauses apply to the processing of personal data in accordance with **Annex I.B**.

d) **Annexes I** and **II** form an integral part of the Clauses.

e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

CLAUSE 2 INVARIABILITY OF THE CLAUSES

a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

CLAUSE 3 INTERPRETATION

a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

CLAUSE 4 HIERARCHY

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Section II OBLIGATIONS OF THE PARTIES

CLAUSE 5 DESCRIPTION OF THE PROCESSING

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in **Annex I.B**.

CLAUSE 6 OBLIGATIONS OF THE PARTIES

6.1 Instructions

a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

6.2 Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in **Annex I.B**, unless it receives further instructions from the controller.

6.3 Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in **Annex I.B**.

6.4 Security of processing

a) The processor shall at least implement the technical and organisational measures specified in **Annex II** to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (hereinafter "**Personal Data Breach**). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

6.5 Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "**Sensitive Data**"), the processor shall apply specific restrictions and/or additional safeguards.

6.6 Documentation and compliance

a) The Parties shall be able to demonstrate compliance with these Clauses.

b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

6.7 Use of sub-processors

a) The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 14 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

c) At the controller's request, the processor shall provide a copy of such a sub-processor order processing agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

6.8 International transfers

Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

The controller agrees that where the processor engages a sub-processor in accordance with Clause 6.7 for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

CLAUSE 7 ASSISTANCE TO THE CONTROLLER

a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions.

c) In addition to the processor's obligation to assist the controller pursuant to Clause 7(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

   i) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (hereinafter "**Data Protection Impact Assessment"**) where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

   ii) the obligation to consult the competent supervisory authority/ies prior to processing where a Data Protection Impact Assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

   iii) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

   iv) the obligations under Article 32 of Regulation (EU) 2016/679.

d) The Parties shall set out in **Annex II** the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

CLAUSE 8 NOTIFICATION OF PERSONAL DATA BREACH

In the event of a Personal Data Breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 of Regulation (EU) 2016/679 or under Articles 34 and 35 of Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

8.1 Data Breach concerning data processed by the controller

In the event of a Personal Data Breach concerning data processed by the controller, the processor shall assist the controller:

a) in notifying the Personal Data Breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the Personal Data Breach is unlikely to result in a risk to the rights and freedoms of natural persons);

b) in obtaining the following information which, pursuant to Article 33(3) of Regulation (EU) 2016/679, shall be stated in the controller's notification, and must at least include:

   i) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;

   ii) the likely consequences of the Personal Data Breach;

   iii) the measures taken or proposed to be taken by the controller to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

   Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay;

c) in complying, pursuant to Article 34 of Regulation (EU) 2016/679, with the obligation to communicate without undue delay the Personal Data Breach to the data subject, when the Personal Data Breach is likely to result in a high risk to the rights and freedoms of natural persons.

8.2 Data Breach concerning data processed by the processor

In the event of a Personal Data Breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

b) the details of a contact point where more information concerning the Personal Data Breach can be obtained;

c) its likely consequences and the measures taken or proposed to be taken to address the Personal Data Breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in **Annex II** all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

Section III FINAL PROVISIONS

CLAUSE 9 CONTRACT VIOLATION AND TERMINATION

a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

   i) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

   ii) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

   iii) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 6.1(b), the controller insists on compliance with the instructions.

d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

CHAPTER B STANDARD CONTRACTUAL CLAUSES FOR CLIENTS IN THIRD COUNTRIES WITHOUT AN ADEQUACY DECISION

Section I

CLAUSE 1 PURPOSE AND SCOPE OF APPLICATION

a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (the General Data Protection Regulation) when transferring personal data to a third country.

b) The Parties:

i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in **Annex I.A** (hereinafter each '**Data Exporter**'), and

ii) the entity/ies in a third country receiving the personal data from the Data Exporter, directly or indirectly via another entity also Party to these Clauses, as listed in **Annex I.A** (hereinafter each '**Data Importer**')

have agreed to these standard contractual clauses (hereinafter: '**Clauses**').

c) These Clauses apply with respect to the transfer of personal data as specified in **Annex I.B.**

d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

CLAUSE 2 EFFECT AND INVARIABILITY OF THE CLAUSES

a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

b) These Clauses are without prejudice to obligations to which the Data Exporter is subject by virtue of Regulation (EU) 2016/679.

CLAUSE 3 THIRD-PARTY BENEFICIARIES

a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the Data Exporter and/or Data Importer, with the following exceptions:

i) Clause 1, Clause 2, Clause 3, Clause 6

ii) Clause 7 — Clause 7.1(b) and Clause 7.3(b)

iii) Clause 12.1(c), (d) and (e)

iv) Clause 13(e)

v) Clause 15

b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

CLAUSE 4 INTERPRETATION

a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

CLAUSE 5 HIERARCHY

In the event of a conflict between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

CLAUSE 6 DESCRIPTION OF THE TRANSFER(S)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in **Annex I.B**.

Section II OBLIGATIONS OF THE PARTIES

CLAUSE 7 DATA PROTECTION SAFEGUARDS

The Data Exporter warrants that it has used reasonable efforts to determine that the Data Importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

7.1 Instructions

a) The Data Exporter shall process the personal data only on documented instructions from the Data Importer acting as its controller.

b) The Data Exporter shall immediately inform the Data Importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

c) The Data Importer shall refrain from any action that would prevent the Data Exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

d) After the end of the provision of the processing services, the Data Exporter shall, at the choice of the Data Importer, delete all personal data processed on behalf of the Data Importer and certify to the Data Importer that it has done so, or return to the Data Importer all personal data processed on its behalf and delete existing copies.

7.2 Security of processing

a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transfer, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter "**Personal Data Breach**"). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data (7), the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transfer, where the purpose of processing can be fulfilled in that manner.

b) The Data Exporter shall assist the Data Importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a Personal Data Breach concerning the personal data processed by the Data Exporter under these Clauses, the Data Exporter shall notify the Data Importer without undue delay after becoming aware of it and assist the Data Importer in addressing the breach.

c) The Data Exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.3 Documentation and compliance

a) The Parties shall be able to demonstrate compliance with these Clauses.

b) The Data Exporter shall make available to the Data Importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

CLAUSE 8 RIGHTS OF DATA SUBJECTS

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the Data Importer or, for data processing by the Data Exporter in the EU, under Regulation (EU) 2016/679.

CLAUSE 9 EXCLUSIVE REMEDY

a) The Data Importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

CLAUSE 10 LIABILITY

a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the Data Exporter under Regulation (EU) 2016/679.

c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

e) The Data Importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

Section III LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

CLAUSE 11 LOCAL LAWS AND PRACTICES AFFECTING COMPLIANCE WITH THE CLAUSES

a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the Data Importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the Data Importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved, and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

c) The Data Importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the Data Exporter with relevant information and agrees that it will continue to cooperate with the Data Exporter in ensuring compliance with these Clauses.

d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

e) The Data Importer agrees to promptly notify the Data Exporter if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

f) Following a notification pursuant to paragraph (e), or if the Data Exporter otherwise has reason to believe that the Data Importer can no longer fulfil its obligations under these Clauses, the Data Exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the Data Exporter and/or Data Importer to address the situation. The Data Exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the Data Exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the Data Exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

CLAUSE 12 OBLIGATIONS OF THE DATA IMPORTER IN CASE OF ACCESS BY PUBLIC AUTHORITIES

12.1 Notification

a) The Data Importer agrees to notify the Data Exporter and, where possible, the data subject promptly (if necessary, with the help of the Data Exporter) if it:

i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

b) If the Data Importer is prohibited from notifying the Data Exporter and/or the data subject under the laws of the country of destination, the Data Importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The Data Importer agrees to document its best efforts in order to be able to demonstrate them on request of the Data Exporter.

c) Where permissible under the laws of the country of destination, the Data Importer agrees to provide the Data Exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

d) The Data Importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

e) Paragraphs (a) to (c) are without prejudice to the obligation of the Data Importer pursuant to Clause 14(e) and Clause 16 to inform the Data Exporter promptly where it is unable to comply with these Clauses.

12.2 Review of legality and data minimisation

a) The Data Importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The Data Importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the Data Importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the Data Importer under Clause 14(e).

b) The Data Importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the Data Exporter. It shall also make it available to the competent supervisory authority on request.

c) The Data Importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

Section IV FINAL PROVISIONS

CLAUSE 13 CONTRACT VIOLATION AND TERMINATION

a) The Data Importer shall promptly inform the Data Exporter if it is unable to comply with these Clauses, for any reason whatsoever.

b) In the event that the Data Importer violates these Clauses or unable to comply with these Clauses, the Data Exporter shall suspend the transfer of personal data to the Data Importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14 paragraph (f).

c) The Data Exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

i) the Data Exporter has suspended the transfer of personal data to the Data Importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

ii) the Data Importer is in substantial or persistent breach of these Clauses; or

iii) the Data Importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such breaches. If the contract involves more than two Parties, the Data Exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

d) Personal data collected by the Data Exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof. The Data Importer shall certify the erasure of the data to the Data Exporter. Until the data is deleted or returned, the Data Importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the Data Importer that prohibit the return or erasure of the transferred personal data, the Data Importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

e) Either Party may revoke its agreement to be bound by these Clauses where

i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or

ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

CLAUSE 14 GOVERNING LAW

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of Germany.

CLAUSE 15 CHOICE OF FORUM AND JURISDICTION

Any dispute arising from these Clauses shall be resolved by the courts of Germany.

****

APPENDIX

ANNEX I

A. LIST OF PARTIES

Processor or Data Exporter:

1. **Name: DISH Digital Solutions GmbH, Metro-Straße 1, 40235 Düsseldorf, Germany**

   Address: Metro-Straße 1, 40235 Düsseldorf, Germany
   Contact person's name, position and contact details: privacy@dish.co
   Signature and entry date: (Signing takes place digitally)
   Role: Processor

Controller / Data Importer:

1. **Name: (as specified during registration for DISH Pay)**

   Address: (as specified during registration for DISH Pay)
   Contact person's name, position and contact details: (as indicated during registration for DISH Pay)
   Signature and entry date: (Signing takes place digitally)
   Role: Data controller

B. DESCRIPTION OF THE PROCESSING OR DATA TRANSFER

1 CATEGORIES OF DATA SUBJECTS WHOSE PERSONAL DATA ARE PROCESSED

- Employees and other staff of the controller ("**Employees**")
- Users of the controller's website ("**End Users**")
- End customers of the controller or their contact persons ("**End Customers**")
- Suppliers of the controller or their contact persons ("**Suppliers**")

2 CATEGORIES OF PERSONAL DATA PROCESSED

- Full name, gender, academic title
- E-mail address
- Payment date, payment amount, means of payment

3 SENSITIVE DATA PROCESSED (IF APPLICABLE) AND RESTRICTIONS OR SAFEGUARDS APPLIED THAT TAKE FULL ACCOUNT OF THE NATURE OF THE DATA AND THE RISKS INVOLVED, E.G. STRICT PURPOSE LIMITATION, ACCESS RESTRICTIONS (INCLUDING ACCESS ONLY FOR EMPLOYEES WHO HAVE UNDERGONE SPECIFIC TRAINING), RECORDS OF ACCESS TO THE DATA, RESTRICTIONS ON ONWARD TRANSFERS OR ADDITIONAL SECURITY MEASURES

- Sensitive payment data (only if not collected directly by the Payment Service Partner)

4 TYPE OF PROCESSING

- Collection
- Storing
- Use
- Transfer (especially to Payment Service Partners)
- Anonymisation

5 PURPOSE(S) FOR WHICH THE PERSONAL DATA ARE PROCESSED ON BEHALF OF THE CONTROLLER

- Provision of technical services for the processing of payments carried out by a Payment Service Partner.

6 DURATION OF THE PROCESSING

- Term of the User Contract

ANNEX II
TECHNICAL AND ORGANISATIONAL MEASURES

Taking into account the state of the art, the implementation costs and the nature, scope, circumstances and purposes of the processing, as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons, the processor shall implement appropriate technical and organisational measures (**"TOM")** to ensure a level of security appropriate to the risks involved when processing personal data.

The TOMs implemented by the processor serve to achieve the protection objectives set out in Article 32 GDPR and include the following:

a) the pseudonymisation and encryption of personal data;

b) the ability to ensure the continued confidentiality, integrity, availability and resilience of processing systems and services;

c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d) a process for regularly reviewing, assessing and evaluating the effectiveness of the TOMs for ensuring the security of the processing.

The individual TOMs implemented by the processor are described below.

1. DATA PROTECTION MANAGEMENT SYSTEM (DPMS)

The processor has a DPMS in place. This includes all measures that ensure a structured data protection organisation. A DPMS is required for the planning, management, organisation and control of data protection and includes at least the structural organisation (roles and responsibilities), the procedural organisation (processes and procedures) and documented policies and procedures. This includes:

#	Technical measures	Implemented
1	IT systems and applications are regularly patched with security updates	☒

#	Organisational measures	Implemented
1	Appointment of a qualified data protection officer and an IT security officer who are integrated into the organisational structure of the processor	☒
2	Authority of the data protection officer to issue instructions within the framework of the fulfilment of his/her tasks	☒
3	Use of structured risk management processes with a focus on data protection and information security risks	☒
4	Maintenance of a record of processing activities pursuant to Article 30 GDPR	☒
5	Standardised and traceable development process for data processing software	☒
6	Compliance with the principles of "privacy by design" and "privacy by default" in IT applications and procedures	☒
7	Regular training of employees in data protection and information security issues	☒
8	Existence of binding data protection and information security policies	☒
9	Definition, communication and documentation of roles and responsibilities within the organisation of the processor	☒
10	Data protection and data security audits of sub-processors	☒
11	Standardised and traceable change process for IT systems and applications (including critical infrastructure components such as firewalls)	☒
12	Control mechanisms that prevent the transfer and use of personal data to/in test or development systems	☒
13	Availability of testing and approval procedures for changes to IT systems and applications (including critical infrastructure components such as firewalls)	☒
14	Changes to IT systems and applications (including critical infrastructure components such as firewalls) and the data to be processed (in particular input, opening, modification, erasure) are logged in a tamper-proof manner and regularly evaluated	☒
15	Procedure for the detection of data protection and security incidents	☒
16	Requirements for the notification of personal data breaches to data subjects and supervisory authorities, including the establishment of internal notification channels	☒
17	Requirements for dealing with and responding to (external) attacks on IT systems, applications and infrastructure components	☒
18	Regular audit of IT systems, applications and infrastructure components with regard to vulnerabilities and the effectiveness of the protective measures taken	☒
19	Regular adaptation of the data protection goals to the current legal requirements	☒

2. ADMISSION CONTROL

The processor is obliged to take measures to prevent unauthorised access to the processing systems (and facilities) with which personal data are processed. This includes:

#	Technical measures	Implemented
1	Use of access controls (such as chip cards, keys or comparable access systems)	☒
2	Safety measures at emergency exits and other entrances and exits	☒
3	Additional security measures in the data centre, for example: cages or lockable shelves	☒
4	Monitoring of properties and buildings	☒
5	Video or camera surveillance system for security zones (data centre)	☒
6	Use of an alarm system	☒

#	Organisational measures	Implemented
1	Existence of building plans and risk-based definition of safety zones in the building	☒
2	Use of a role- or group-based (physical) access authorisation concept	☒
3	Procedure for the allocation and use of keys and authentication functions	☒
4	Procedure for managing access authorisations for external staff (e.g. visitors or cleaning staff)	☒
5	Specifications for access to the building by external persons	☒
6	Logging of access to rooms and buildings (if necessary, with the possibility of evaluating log files)	☒
7	Logging of access to security zones (if necessary, with the possibility of evaluating log files)	☒

3. DATA ACCESS CONTROL

The processor shall take measures to prevent unauthorised persons from using the data processing facilities and procedures. This includes:

#	Technical measures	Implemented
1	Access control requirements for IT systems, applications and infrastructure components	☒
2	Login with username and password	☒
3	Use of personalised user IDs (with which activities can be attributed to users)	☒
4	Logging of access attempts via • the database level • the operating system • the application level • the infrastructure level	☒
5	Definition of relevant log files (possibility to analyse log files if necessary)	☒
6	Measures to protect the log files	☒
7	Test concept/method for testing authentication conventions	☒
8	Two-factor authentication for access in special cases	☒
9	Use of secure transmission protocols for authorisation information/credentials (e.g. keys, passwords, certificates) between IT systems or applications and infrastructure components.	☒
10	Blocking access after a series of invalid credentials for IT systems or applications and infrastructure components	☒
11	Procedure for secure identification and authentication of remote access	☒
12	Remote access logging (possibility to analyse log files if required)	☒

#	Organisational measures	Implemented
1	Formal user management process (including requesting, approving, assigning and blocking access/accounts) for IT systems or applications and infrastructure components	☒
2	Definition of an authentication policy including a concept for password conventions for all users	☒
3	Procedure for resetting user accounts and passwords	☒
4	Deactivation of the account after inactivity (after a certain time)	☒
5	Regular checking of user accounts for validity	☒
6	Deactivation of user accounts at the end of the activity	☒

4. DATA ACCESS CONTROL

The processor shall take measures to ensure that persons authorised to use the data processing facilities only have access to the data in accordance with their access rights. This includes:

#	Technical measures	Implemented
1	Setting up user groups	☒
2	Automatic logout of IT systems, applications and infrastructure components or screen lock after inactivity	☒
3	When granting extensive rights (especially superuser/administrators), the existence of the possibility to monitor or regularly review the activities carried out with these user accounts	☒
4	Possibility/availability of logging user accesses (programme execution, transaction, write, read, access, delete, violations) (possibility to analyse log files if necessary)	☒
5	Rules for the encryption of data storage	☒
6	Encryption of data storage on servers or at the level of databases, IT systems or applications based on the level of criticality	☒
7	Encryption of data storage of stationary/mobile devices	☒
8	Use and monitoring of antivirus software	☒

#	Organisational measures	Implemented
1	Procedures for managing access rights for IT systems, applications and infrastructure components	☒
2	Separation of authorisation approval and authorisation allocation (separation of functions)	☒
3	Definition of responsibilities for issuing permission (including the four-eyes principle for critical cases)	☒
4	Documented authorisation and role concept for different levels: • the database level • the operating system • the application level • the infrastructure level	☒
5	Traceability of the administration of authorisations and roles and the question of who had which authorisations and when	☒
6	Policies prescribe the principle of minimum rights allocation (need to know, need to have); IT security policy	☒
7	Procedure for regularly checking the validity of authorisations for IT systems or applications and infrastructure components	☒
8	Procedure for revoking authorisations for IT systems, applications and infrastructure components	☒
9	Procedure for the immediate notification of changes in authorisations (conversions)	☒

5. DATA TRANSMISSION CONTROL

The processor is obliged to take measures to ensure that personal data cannot be read, copied, modified and/or deleted without authorisation during electronic transfer, transport and/or storage on storage media and that the recipients of the data transfer can be identified and verified using data transmission equipment. This includes:

#	Technical measures	Implemented
1	Encryption standards used are state of the art (depending on risk and protection needs)	☒
2	Logging of data transmission at the relevant interfaces	☒
3	Documentation of the interfaces regarding the data transmitted to and from the service provider	☒
4	Review of automated interfaces through which large amounts of personal data of customers are exchanged	☒
5	Measures against unauthorised mass reading of data on IT systems, applications and infrastructure components	☒
6	Separation of networks (logical or physical)	☒
7	Use of firewalls	☒
8	Use of strict firewall rules	☒
9	Regular patching and maintenance of firewalls, routers and other infrastructure components	☒
10	Use of intrusion detection systems (IDS)	☒
11	Procedure for the secure destruction of paper files	☒
12	Procedure for pseudonymisation or anonymisation of personal data	☒
13	Access to EU/EEA systems for employees (during business trips)	☒

#	Organisational measures	Implemented
1	Policies for the transfer of data to authorised recipients and procedures to ensure that these policies are followed	☒
2	Contracts for the external destruction of data storage facilities	☒
3	Definition of data protection-compliant erasure concepts; erasure concepts also include data backups and archiving systems	☒
4	Creation of erasure protocols and procedures for archiving erasure protocols	☒
5	Documentation of the legal basis for the transfer of data to non-EU/EEA countries	☒
6	Definition of rules on the level of data protection when processing data in non-EU/EEA countries	☒

6. DATA ENTRY CONTROL

The processor is obliged to take measures to ensure that it is possible to verify and establish whether and by whom data has been entered into or modified or removed from data processing facilities. This includes:

#	Technical measures	Implemented
1	Integrity checks before data entry (automatic or manual checks)	☒
2	Adequate logging of data entry	☒
3	Documentation of the administrative activities relevant to data processing	☒

#	Organisational measures	Implemented
1	Differentiated user authorisations for data entry	☒
2	Ensuring that personal data is collected exclusively for a specific purpose	☒
3	Data minimisation through technical and procedural prevention or restriction of the collection of personal data	☒

7. DATA PROCESSING

The processor is obliged to take measures to ensure that personal data processed on behalf of third parties are processed strictly in accordance with the instructions of the controller. This includes:

#	Organisational measures	Implemented
1	Conclusion of data processing contracts or data protection agreements with sub-processors pursuant to Article 28 GDPR	☒
2	Assessment of the required technical measures at the sub-processors before the start of and periodically during the data processing (preliminary and periodic audits)	☒
3	Carrying out data protection validations (preliminary and/or regular audits)	☒
4	Information on the level of data protection in non-EU/EEA countries	☒
5	Information on sub-processors outside the EU/EEA	☒
6	Requirements for the processor are also reflected in the agreements with its sub-processors	☒
7	Declaration on the obligation of all employees to data secrecy and corresponding obligation of subcontracted processors	☒
8	Information on the sub-processors	☒

8. AVAILABILITY CONTROL

The processor is obliged to take measures to protect the personal data against accidental destruction or loss. This includes:

#	Technical measures	Implemented
1	Monitoring of the data centre as well as the hardware and software operation	☒
2	Availability of security systems (software/hardware) to protect against cyber-attacks (DDoS)	☒
3	Data centre built and operated according to the recognised state of the art	☒
4	Availability of an uninterruptible power supply	☒
5	Use of redundant air conditioning components	☒
6	Use of water, fire and smoke detectors	☒
7	Regular maintenance of the data centre components	☒

#	Organisational measures	Implemented
1	Implementation of a suitable backup and recovery concept	☒
2	Specification of emergency and restart procedures	☒
3	Regular testing of emergency procedures	☒
4	Definition of emergency plans with clear responsibilities	☒
5	Definition of a concept for the continuity of IT services	☒

9. DATA SEPARATION

The processor takes measures to ensure that personal data collected for different purposes can be processed separately. This includes:

#	Technical measures	Implemented
1	Physical or logical separation of personal data of different customers at the premises of the processor (including databases and backups, if necessary)	☒
2	Separation of test and production system	☒