Data Processing Agreement

This Data Processing Agreement (the "**Data Processing Agreement**") forms part of the agreement signed between you ("the Client") and **THN** to govern the processing of personal data for which the Client is the data controller. THN acts as the processor (collectively, the "Agreement").

I. EFFECTIVE DATE

This Agreement shall enter into force upon completion and signature by both parties (the "**Effective Date**").

II. EFFECTIVENESS

This Data Processing Agreement applies to the personal data processed by **THN** on behalf of and for the Client's account during the provision of services related to the Platform ("**Client Personal Data**").

- The person signing this Data Processing Agreement on behalf of the Client declares to **THN** that he/she has the legal authority to bind the Client and is legally entitled to enter into contracts.
- The person signing this Data Processing Agreement on behalf of **THN** declares to the Client that he/she has the legal authority to bind **THN** and is legally entitled to enter into contracts.
- The term of this Data Processing Agreement aligns with the term of the Agreement. This means that this Data Processing Agreement will automatically terminate upon termination of the Agreement or upon prior termination in accordance with the terms outlined in this Data Processing Agreement, without prejudice to any obligations that **THN**, as processor, may assume thereafter.

III. TERMS OF THE DATA PROCESSING AGREEMENT

1. Definitions:

The following terms shall have the following meanings:

"THN", refers to The Hotels Network, S.L. with NIF B-65542714, located at Calle Muntaner, 262, 3º-1ª, 08021 Barcelona, Spain. Owner, creator and developer of the Platform.

"Client" refers to the entity contracting the services and use of **THN's** Platform.

"End Users" refers to the users of the Client's website.

"Platform" refers to **THN's** software, which is developed and run on a platform and intended to be used by companies for the provision of services. The Platform comprises the following products:

- Personalization:
  Product that is installed on the website that allows THN's clients to display relevant content to End Users depending on their behaviour and to collect data from End Users.
  Commercial Products included:
  - Predictive Personalization
  - Predictive Audience

- BenchDirect:
  Product that is installed on the website that allows THN’s clients to anonymously compare the e-commerce metrics of their website with the metrics of other THN clients’ websites.

- SafeDirect:
  Product that allows THN clients to increase direct bookings by offering travel assistance insurance.

“Data Controller", "Data Processor", **"Data Subject"**, "**Personal Data**", "**Processing**", "**appropriate technical and organizational measures"** and "**Standard Contractual Clauses**", as used in this Data Processing Agreement, shall have the same meanings as described in the European Data Protection Regulation.

“Data Protection Regulations" means: (i) 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 ("**GDPR**"); (ii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; (iii) the Organic Law on Data Protection and Guarantee of Digital Rights ("**LOPDGDDD"**).

2. Scope of data protection law.

The parties acknowledge that European Data Protection Law will only apply to **Client Personal Data** that is covered by the definitions contained in such laws.

3. Identification of the parties

For the purposes of this data processing agreement

- **THN** shall be considered a Data Processor.
- The **Client** shall be considered a Data Controller.

4. Description of treatment and safety standards

A detailed description of the processing to be carried out can be found attached to this Data Processing Agreement as **Appendix 1.** A list of the applicable minimum security standards can be found in **Appendix 2.**

5. Obligations of the Client.

The Client, in its capacity as Data Controller of the Client's personal data, is responsible for ensuring and supervising **THN's** compliance with the Data Protection Regulations throughout the processing**.**

In this regard, prior to contracting the Platform or requesting the activation of additional functionalities, the **Client** undertakes, with respect to the Client's Personal Data provided to **THN** for the provision of the services that are the object of the Agreement, to comply with those obligations that correspond to it as Data Controller in accordance with the provisions of the Data Protection Regulations.

To the extent required under the Data Protection Regulations, **THN** will provide the **Client** with all reasonable assistance to facilitate compliance with its obligations as Data Controller and to demonstrate compliance with these obligations.

IV.GENERAL PROVISIONS ON THE PROCESSING OF PERSONAL DATA

THN undertakes to comply with the Data Protection Regulations with regards to the processing of Client Personal Data.

The purpose of the data processing shall be to provide the Platform service with the terms dictated by the **Client** as specified in **Appendix 1**. This Data Processing Agreement sets out the nature and purpose of the processing, the types of Client Personal Data that THN will process and the data subjects whose Personal Data will be processed.

The obligations of **THN** as Data Processor shall be carried out in accordance with article 28 of the GDPR and article 33 of the LOPDGDD, and specifically are as follows:

a. Process the Client Personal Data only in accordance with the instructions documented and provided by the **Client** (as set out in this Data Processing Agreement or the Agreement, or as directed by the **Client** through the Platform or by any other documented means) for the purpose of providing the service. Under no circumstances may it be used for **THN's** own purposes.

b. Take the necessary measures in accordance with Article 32 of the GDPR, in the terms set out in Clause VII of this Data Processing Agreement and as set out in **Appendix 2**.

c. Promptly notify the **Client** in writing if, in **THN's** opinion as Data Processor, an instruction regarding the processing of Client Personal Data is in breach of the Data Protection Regulations;

d. Not communicate Client Personal Data to third parties, except with the express written authorisation of the **Client**.

e. Ensure that persons authorized by **THN** to process Client Personal Data are adequately trained in personal data protection.

f. If, for the provision of the Services, **THN** has to transfer Client Personal Data to a third country or an international organization under applicable Union or Member State law, **THN** will inform the **Client** of this legal requirement in advance, unless such law prohibits it for important reasons of public interest.

g. Where appropriate, in accordance with the Data Protection Regulations, appoint a data protection officer and communicate his/her identity and contact details to the **Client**.

h. Where applicable under the Data Protection Regulations, keep a written record of all categories of processing activities carried out on behalf of the **Client**, in accordance with Article 30 of the GDPR.

i. Make available to the **Client** all information reasonably requested by the **Client** in order to demonstrate compliance with its obligations regarding the appointment of sub-processors, without prejudice to the provisions specified in Clause VI;

j. Assist the **Client** in fulfilling its obligations under Articles 35 and 36 of the GDPR.

k. Assist the **Client** in fulfilling its obligations under Articles 15 to 18 of the GDPR by providing documentation or assisting the **Client** in retrieving, correcting, deleting or blocking the Client Personal Data;

l. **THN** guarantees that personnel who are to have access to Client Personal Data are bound by a confidentiality obligation with respect to such Client Personal Data, and will comply with the relevant security measures, which must be appropriately communicated to them;

m. Securely delete or return to the **Client** or another Processor designated by the **Client**, the Client Personal Data in **THN's** possession in accordance with the written instructions issued by the **Client** upon termination or early termination of the Agreement, unless the Client Personal Data is required to be retained by Union or Member State law;

- In addition, and subject to reasonable confidentiality protocols:

  a. To allow the **Client** and its authorized representatives to access and review the documents that ensure compliance with the terms of this Data Processing Agreement.

  b. During the term of the Agreement and where required by the Data Protection Regulations, allow the **Client** and its authorized representatives to conduct audits to ensure compliance with the terms of this Data Processing Agreement. Notwithstanding the above, any audit shall be conducted during **THN's** normal business hours, with reasonable advance notice to **THN** and subject to reasonable confidentiality protocols.

  The scope of any audit shall not oblige **THN** to disclose to or allow the **Client** or its authorized representatives access to data or information beyond what is necessary for the purpose of conducting audits by the data controller in accordance with Article 28 of the GDPR.

  In addition, audits shall be limited to once a year, unless **THN** has suffered a security breach in the previous twelve (12) months that has affected Client Personal Data; or an audit reveals a material breach; or there is any other good reason to conduct the audit at a more frequent interval.

V. RIGHTS OF INTERESTED PARTIES

If **THN,** as data processor, receives notice of any claim, complaint, request, enquiry, investigation, proceeding or other action from any data subject, court, regulatory or supervisory authority, or any body, organization or association, which relates in any way to personal data processed by **THN** on behalf of the **Client**, **THN** undertakes to:

- notify the **Client** of such circumstances so that the **Client** may comply with the request to the extent that such notification is legally permissible;

- provide the **Client** with reasonable cooperation and assistance; and

- not respond on its own, unless otherwise instructed in writing by the **Client** or is legally obliged to do so.

VI. SUB-PROCESSORS

The **Client** authorizes **THN** to use sub-processors for the provision of necessary ancillary services to ensure the normal operation of **THN's** services. Specifically, the sub-processors currently providing ancillary services to THN are as follows:

- Amazon Web Services
  Amazon Web Services EMEA SARL
  Avenue John F. Kennedy 38
  1855 Luxembourg
  Luxembourg

Purpose of the processing	Cloud service provider
Data shared with the sub-processor	Depending on the products Client uses: Device identification data and traffic data (IP addresses, MAC addresses, cookie identifiers), customer data etc. For a more detailed description of the processing related to THN's products, please refer to Annex I.
Location of the processing	Ireland (European Union)
International transfer mechanism	Amazon is a signatory to the EU-US Data Privacy Framework.
Additional security measures	AWS Security Centre and Risk and Compliance White Paper

- DATADOG
  Datadog, Inc. New York
  New York Times Bldg
  620 8th Ave, New York, NY 10018
  USA

Purpose of the processing	Monitoring services provider for cloud applications
Data shared with the sub-processor	Depending on the products Client uses: The Hotels Network user data, software execution logs, device identification data and traffic data (IP addresses, MAC addresses, cookie identifiers). For a more detailed description of the processing related to THN's products, please refer to Annex I.
Location of the processing	USA
International transfer mechanism	Datadog is a signatory to the EU-USA Data Privacy Framework
Additional security measures	Technical and organisational measures

- TINYBIRD
  Tinybird Inc.
  45 Pleasant Street

Newburyport
01950, MA USA

Purpose of the processing	Real-time data platform service provider
Data shared with the sub-processor	Depending on the products Client uses: Device identification data and traffic data (IP addresses, MAC addresses, cookie identifiers), customer data, etc.). For a more detailed description of the processing related to THN's products, please refer to Annex I.
Location of the processing	USA
International transfer mechanism	Standard contractual clauses
Additional security measures	Security policies

- Sendgrid (Twilio)

  Twilio Inc.

  101 Spear Street, Fifth Floor

  San Francisco,

  CA 94105, United States

Purpose of the processing	Email delivery platform
Data shared with the sub-processor	Client's email. For a more detailed description of the processing related to THN's products, please refer to Annex I.
Location of the processing	Ireland (European Union)
International transfer mechanism	Twilio is a signatory to the EU-US Data Privacy Framework.
Additional security measures	Twilio Security Overview

For the service of KITT AI, the Customer authorizes the use of the following sub-processors:

- TWILIO

  Twilio Inc.

  101 Spear Street, Fifth Floor

  San Francisco,

  CA 94105, United States

Purpose of the processing	Messaging platform
Data shared with the sub-processor	Final Customer Phone number. For a more detailed description of the processing related to THN's products, please refer to Annex I.
Location of the processing	Ireland (European Union)
International transfer mechanism	Twilio is a signatory to the EU-US Data Privacy Framework.
Additional security measures	Twilio Security Overview

- Sendgrid (Twilio)

  Twilio Inc.
  101 Spear Street, Fifth Floor
  San Francisco,
  CA 94105, United States

Purpose of the processing	Email delivery platform
Data shared with the sub-processor	Client's email. For a more detailed description of the processing related to THN's products, please refer to Annex I.
Location of the processing	Ireland (European Union)
International transfer mechanism	Twilio is a signatory to the EU-US Data Privacy Framework.
Additional security measures	Twilio Security Overview

- Retell AI

  Retell AI Inc
  12985 Saratoga avenue, Saratoga,
  California,
  95070, USA

Purpose of the processing	AI Voice Agent Platform
Data shared with the sub-processor	Final customer voice and conversation. For a more detailed description of the processing related to THN's products, please refer to Annex I.
Location of the processing	Ireland (European Union)
International transfer mechanism	Standard contractual clauses
Additional security measures	Security & Privacy

Furthermore, the **Client** authorizes **THN** to engage additional external sub-processors to process the Client's Personal Data, provided that:

- **THN** notifies the **Client** of the updated list of new sub-processors at least twenty (20) days in advance before allowing said new sub-processors to process Client Personal Data, thus giving the **Client** the opportunity to object to such changes.

In the event that the **Client** objects to the substitution or hiring of a new sub-processor, the parties shall negotiate in good faith alternative solutions that are commercially reasonable.

- **THN** shall require any new sub-processor to protect the Client Personal Data with the same level of strictness required by this Data Processing Agreement and the European Data Protection Act by entering into an appropriate contract to that effect.

- **THN** shall be directly liable to the **Client** and shall hold the **Client** harmless from any damages and/or losses arising from any non-compliance by a sub-processor, of its obligations under this Agreement or under the European Data Protection Act.

The **Client** understands that, by virtue of any confidentiality restrictions that may apply to sub-processors, **THN** may be limited in its ability to disclose sub-processor agreements to the **Client**. In this regard, **THN** agrees to use all reasonable efforts to require any sub-processor it appoints to allow it to disclose the sub-processor agreement to the **Client**. Where, despite its best efforts, **THN** is unable to disclose a sub-processor agreement to the **Client**, the parties agree that, upon the **Client's** request, **THN** shall provide, on a confidential basis, such information as it reasonably can in relation to such sub-processor agreement to the Client. Notwithstanding the above, **THN** shall not rely on such confidentiality restrictions where disclosure of such agreements is necessary for the performance of the **Client's** legal obligations or to establish compliance with such obligations to any administrative or judicial body.

VII. SECURITY OF PROCESSING

THN shall implement and maintain appropriate technical and organizational measures to protect Client Personal Data against unauthorized or unlawful processing and against accidental loss, destruction, damage, theft, alteration or disclosure in accordance with the Data Protection Regulations which, as a minimum, shall comprise the measures set out in **Appendix 2** of this Agreement. In any case, such measures shall be appropriate for the potential harm resulting from any unauthorized or unlawful processing, accidental loss, destruction, damage or theft of the Client Personal Data and appropriate for the nature of the Client Personal Data to be protected. In this regard, **THN** may update the technical and organizational measures, provided that such modifications do not decrease the overall level of security.

If **THN** becomes aware of any security breach that results in the accidental, unauthorized or unlawful destruction, loss, alteration, disclosure or access of Client Personal Data ("**Security Breach**") that **THN** processes while providing the Platform, it will notify the **Client** without undue delay and within a maximum of 48 hours. The notification will be sent to the email address of the main user of the contracted product or to the security breach notification email address provided when signing the Agreement, providing the information as required by Article 33 of the GDPR.

VIII. DATA TRANSFERS

It is part of **THN's** policy to give preference in contracting suppliers to those companies located in the European Economic Area that comply to a higher degree with privacy and data protection standards.

Notwithstanding the above, in the event that **THN** processes Client Personal Data in a country that does not have an adequacy decision (within the meaning of Article 45 of the GDPR), either directly or indirectly through sub-processors, **THN** must obtain prior consent from the **Client** and, where applicable, adopt an appropriate transfer mechanism in accordance with the GDPR.

In the event that the **Client** objects to the international transfer of the data, the parties shall negotiate in good faith alternative solutions that are commercially reasonable.

If **THN** carries out an international transfer for which the transfer mechanism used is no longer valid under the GDPR (e.g. as a result of an invalidating court ruling, etc.), the **Client** shall grant **THN** a reasonable period of time, to the extent permitted by the GDPR, to rectify the non-compliance ("**Remediation Period**"), in order to identify additional safeguards or measures that can be implemented to ensure compliance with the Data Protection Regulations.

IX. VARIOUS

- To the extent that such processing is legitimate under the Data Protection Regulations, **THN** shall have the right to use the data, provided that it is not Client Personal Data, relating to or obtained in connection with the operation, support or use of the Platform for its legitimate internal business purposes, such as supporting billing processes, Platform administration, improvements, benchmarking, product and service development,, compliance with applicable laws (including law enforcement requests), ensuring the security of the Platform and fraud prevention or risk mitigation. In any case, **THN** guarantees the **Client** that, in the event of carrying out any such processing, it will comply with all applicable obligations under the Data Protection Regulations and exempts the Client, undertaking to hold them completely harmless from any kind of damages and liabilities that may arise for the Client (including administrative penalties expressly) if such processing is deemed illegitimate under the Data Protection Regulations or violates any other obligations under the Data Protection Regulations.

In relation to Client Personal Data, **THN** guarantees that it will not be used for its own purposes unless it has irretrievably aggregated and anonymised the data so that it does not identify the Client or any other person or entity, in particular End Users.

- This Data Processing Agreement is subject to the applicable law and the terms of jurisdiction of the Agreement.

- **THN** shall be only held liable if it directly and materially infringes the **Client**´s specific instructions, leading to a direct and proven breach of its obligations under this Agreement or the Data Protection Regulation. Except in cases of such direct infringement, **THN** shall not be liable for any damages, losses, penalties (including those imposed by the Data Protection Authority), third-party claims, or expenses (including reasonable attorneys´ fees, solicitors´ fees, or other professional fees) arising in connection with this Agreement. This indemnification obligation is exclusive and shall not be extended or implied under any circumstances. Furthermore, this indemnification obligation shall prevail over any limitations of liability set out in this Agreement.

- In the event that any provision of this DPA is declared invalid, illegal or unenforceable, the validity, legality and enforceability of the remaining provisions shall not be affected or impaired thereby and such provision shall only be ineffective to the extent of such invalidity, illegality or unenforceability.

- In relation to the Forms Builder service offered by **THN**, the **Client,** acting in its capacity as Data Controller, guarantees the following:

  i. That it will process any personal data obtained from End Users through the forms created through Forms Builder in accordance with the GDPR.
  ii. That it will inform data subjects, who enter their personal data in the forms created through Forms Builders, about the information regarding the processing of their personal data in accordance with article 13 of the GDPR.
  iii. That it will not use the forms created through Forms Builders to collect special categories of personal data regulated in article 9 of the GDPR.

Appendix 1
Description of the data processing related to the product “Personalisation”

Data subjects

Personal data refers to users of the Platform (employees or authorized users of the Client) and End Users of the Client's website.

Data categories

The personal data processed may include the following categories of data:

Related to the users of the Platform:

- Device identification data and traffic data (IP addresses, MAC addresses, backend hash).
- Direct identification information (e-mail address, name and surname).

Related to the End Users of the Client's website:

- Device identification data and traffic data (IP addresses, MAC addresses, backend hash).
- Directly identifiable information (e-mail address, first and last name and any personal data that the Client chooses to collect from users of its website)

Purpose of processing

THN, for the provision of the Personalisation service, uses the information of the End Users of the Client's website (device identification data and traffic data (IP addresses, MAC addresses, backend hash)) in order to enable the Client to create personalisation campaigns.

Types of treatment

- Collection or recording of personal data
- Organisation
- Storage or retention of personal data
- Access to personal data
- Communication of personal data
- Use of personal data

Appendix 1
Description of the data processing related to the product BenchDirect

Data subjects

Personal data refers to users of the Platform (employees or authorized users of the Client) and End Users of the Client's website.

Data categories

The personal data processed may include the following categories of data:

Related to the users of the Platform:

- Device identification data and traffic data (IP addresses, MAC addresses, backend hash).
- Direct identification information (e-mail address, name and surname).

Related to the end users of the Client's website:

- Device identification data and traffic data (IP addresses, MAC addresses, backend hash).

Purpose of processing

THN, for the provision of the BenchDirect service, uses the information of the End Users of the Client's website (Device Identification Data and traffic data (IP addresses, MAC addresses, backend hash), in order for the Client to anonymously compare the e-commerce metrics of its website with the metrics of other THN clients' websites.

Types of treatment

- Collection or recording of personal data
- Organisation
- Storage or retention of personal data
- Access to personal data
- Communication of personal data
- Use of personal data

Appendix 1
Description of the data processing related to the product SafeDirect

Data subjects

Personal data refers to users of the Platform (employees or authorized users of the Client) and End Users of the Client's website.

Data categories

The personal data processed may include the following categories of data:

Related to the users of the Platform:

- Device identification data and traffic data (IP addresses, MAC addresses, backend hash).
- Direct identification information (e-mail address, name and surname).

Related to the End Users of the Client's website:

- Device identification data and traffic data (IP addresses, MAC addresses, backend hash).
- Directly identifiable information (e-mail address, first and last name and any personal data that the Client chooses to collect from users of its website)

Purpose of processing

THN, for the provision of the SafeDirect service, uses the information of the End Users of the Client's website (device identification data and traffic data (IP addresses, MAC addresses, backend hash), in order to enable the Client to offer insurance to its website visitors.

THN, for the provision of SafeDirect services, uses the identification data (name, surnames, ID/Foreigner ID, email, and telephone of the client responsible for processing) to communicate them to the insurance entity so that it can formalize the insurance policy.

Types of treatment

- Collection or recording of personal data
- Organisation
- Storage or retention of personal data
- Access to personal data
- Communication of personal data
- Use of personal data

Appendix 1
Description of the data processing related to the product KITT AI

Data subjects
Personal data refers to users of the Platform (employees or authorized users of the Client) and End Users of the Client's website.
Data categories
The personal data processed may include the following categories of data: ● Directly identifiable information (e-mail address, phone number, voice, and any personal data the user chooses to voluntarily share in the conversation) Related to the End Users of the Client's website: ● Directly identifiable information (e-mail address, phone number), voice and any personal data the final user decides to share voluntarily during the conversation.
Purpose of processing
THN, for the provision of KITT AI services, uses the information of end users of the Client's website and/or the telephone line intended for the service (email address, phone number, call recording, and any personal data that the user decides to voluntarily share during the conversation), so that the Client can make inquiries and manage reservations.
Types of treatment
● Collection or recording of personal data ● Organisation ● Storage or retention of personal data ● Access to personal data ● Communication of personal data ● Use of personal data

Appendix 2
(Applicable safety standards)

Controlling access to systems

The following measures are intended to prevent unauthorized persons from accessing THN's data processing systems. THN has, amongst others, the following measures in place:

- Password protocols (including special characters, minimum length, forced password change).
- There is no access for guest users or anonymous accounts
- Centralized management of access to the system
- Personal and individual user login when logging into the system or company network
- Automatic locking of devices after a certain period of time without user activity (also screensaver with password or automatic pause)
- Firewall

Data access control

The following measures are intended to prevent authorized users from accessing data beyond their authorized access rights and to prevent unauthorized entry, reading, copying, deletion, modification or disclosure of data. THN has, amongst others, the following measures in place:

- Differentiated access rights
- Access rights defined according to functions/roles
- Automated logging of user access through computer systems
- Measures to prevent the use of automated data-processing systems by unauthorized persons using data communication equipment
- Separation of functions

Disclosure control

The following measures are intended to prevent unauthorized access, alteration or deletion of data during transfer, and to ensure that all transfers are secure and recorded. THN has, amongst others, the following measures in place:

- Mandatory use of encrypted private networks for all data transfers
- Encrypted AWS servers
- Secure data transport
- Secure Wi-Fi
- Regulations for the handling of mobile storage media (e.g. laptop, USB stick, mobile phone)

Input control

The following measures are intended to ensure that all data management and maintenance is recorded, and an audit trail should be maintained indicating whether data has been entered, modified or deleted (erased) and by whom. THN has, amongst others, the following measures in place:

- Logging of user activities in IT systems
- That it is possible to verify and establish to which bodies personal data have been or may be transmitted or made available through data communication equipment
- That it is possible to verify and establish which personal data have been entered into automated data processing systems, and when and by whom it was entered

Order Control

The following measures ensure that data is processed strictly in accordance with the instructions of the controller. THN has, amongst others, the following measures in place:

- Monitoring the execution of the contract

Availability control

The following measures are intended to ensure the protection of data against accidental destruction or loss. THN has, amongst others, the following measures in place:

- Installed systems can be restored in case of interruption
- Ensure data storage is on a secure network
- Stored personal data cannot be corrupted by a system malfunction
- Business continuity protocols
- Remote storage
- Anti-virus/firewall systems

Control of segregation

The following measures allow separate processing of data collected for different purposes.
THN has, amongst others, the following measures in place:

- Restriction of access to stored data for different purposes according to staff functions
- Segregation of the company's IT system.
- Segregation of IT test and production environments

Periodic review, assessment and evaluation procedure (Art. 32(1)(d) GDPR; Art. 25(1) GDPR)

The following measures are intended to ensure an organization meets the basic requirements of data protection. THN has, amongst others, the following measures in place:

- Commitment of employees to data confidentiality
- Sufficient data protection training for employees
- Maintaining an overview of processing activities (Art. 30 GDPR)
- Carrying out data protection impact assessments where necessary (Art. 35 GDPR)

- Process for notifying data protection breaches to supervisory authorities in accordance with Art. 4 para. 12 GDPR (Art. 33 GDPR)
- Process for notifying data protection breaches to data subjects in accordance with Art. 4 para. 12 GDPR (Art. 34 GDPR)
- Agreement on contractual penalties for non-compliance with instructions