ANNEX 2 – DATA PROCESSING AGREEMENT ("DPA")

This Data Processing Agreement (the "**DPA**") is annexed to the Brevo General Terms and Conditions (available at https://www.brevo.com/legal/enterprise-agreement/) and its purpose is to define the respective roles and obligations of each Party with respect to the processing of personal data by Brevo, either (i) as data processor, on behalf of Customer, the data controller; or (ii) as sub-processor on behalf of Customer, the data processor. In the second case (ii), it is agreed that the instructions contained in this DPA are indirectly transmitted to Brevo through the Customer.

1. DEFINITIONS

1.1. Capitalized terms not defined in this DPA shall have the meaning given to them in the General Terms and Conditions.

1.2. Where terms defined respectively in the GDPR appear in this DPA, they shall be understood as in the GDPR.

1.3. This DPA shall be read and interpreted in light of the provisions of the GDPR. It shall not be interpreted in a manner contrary to the rights and obligations under the GDPR or in a manner that infringes the fundamental rights or freedoms of the data subjects.

1.4. In the event of any inconsistency between this DPA and the provisions of the General Terms and Conditions, this DPA shall prevail.

2. DESCRIPTION OF THE PROCESSING OPERATIONS AND ROLE OF THE PARTIES

2.1. The details of the processing operations, including the categories of personal data and the purposes of the processing for which personal data is processed on behalf of Customer, are specified in Section 13.

2.2. All the Services require at least the processing of Content, as well as the following data relating to the User: identification and contact data (name, address, title, contact details, username); information relating to the organization (geographical location, website), sending information (e-mail address, IP address, date and time) and log of use of the Service. The Services include all the features detailed in the Documentation and the Order Form, as well as the continuous developments that Brevo applies to its standard Software and that are necessary to provide the Service to Customer.

2.3. By default, the duration of the processing is the duration of this Agreement. Customer is solely responsible for managing the retention periods for Content in connection with the provision of Services. It is Customer's responsibility to delete Content as and when the retention period expires. Brevo's sole responsibility is to delete or anonymize such data at the end of its contractual relationship with Customer.

3. GENERAL OBLIGATIONS OF THE PARTIES

3.1. Brevo's Obligations

As a data processor, Brevo undertakes to:

i. comply with the Data Protection Regulation;
ii. process Customer's personal data only for the purposes of providing the data processing services under this DPA;
iii. process Customer's personal data in accordance with Customer's lawful and documented instructions. Instructions consist of the provisions of this Agreement, including this DPA, and of the usage of the Software. If Brevo considers that an instruction constitutes a breach of the Data Protection Regulation, it shall immediately inform Customer. In addition, if Brevo is required to transfer data to a third country or to an international organization it will be processed in accordance with Section 28. a) of the GDPR.

iv. ensure the confidentiality of Customer's personal data; and
v. ensure that the persons authorized to process Customer's personal data are committed to respecting confidentiality and receive the necessary training on the protection of personal data.

3.2. Customer's Obligations

Customer is solely responsible for complying with the obligations incumbent on the data controller under data protection laws. Whether acting as data controller or data processor, Customer is responsible for the performance of its obligations under this DPA and shall:

i. comply with the Data Protection Regulation and any laws applicable to Customer in connection with the use of the Services;
ii. provide Brevo with Customer's personal data necessary for the processing;
iii. document in writing any instructions regarding the processing of data by Brevo;
iv. ensure, beforehand and throughout the processing, that Customer complies with the data controller's obligations under the GDPR;
v. not include in Content any "sensitive" personal data (special category of personal data) within the meaning of Articles 9 and 10 of the GDPR.

4. INFORMATION AND RIGHTS OF DATA SUBJECTS

4.1. It is Customer's responsibility to provide information to the data subjects about the processing operations at the time of collection of their personal data and to obtain all consents (where required) necessary under the Data Protection Regulation for Brevo to process Content and provide the Services in accordance with the Agreement.

4.2. Brevo undertakes to assist Customer, by means of appropriate technical and organizational measures, in fulfilling its obligation to respond to requests made by data subjects to exercise their rights under the Data Protection Regulation.

4.3. In the event that such a request relating to Customer is made directly to Brevo, Brevo shall inform the data subject that they need to contact the data controller. Any operation carried out by Brevo in the context of a request to exercise a right may, where applicable, give rise to additional invoicing, taking into account in particular the technical investigations carried out at Customer's request.

4.4. Notwithstanding the foregoing, Brevo may process directly a data subject's request if (i) the request is an automatic unsubscribe from electronic communications or (ii) the request relates to unsolicited communication, a prohibited use of the Services or a potential breach of this Agreement by Customer or any of Brevo's customers. In both cases, Brevo will carry out the request of the data subject without the prior approval of Customer. In case (ii), Brevo may suspend the possibility of sending any electronic communication to the domain of the data subject.

5. SECURITY

5.1. Brevo specifically undertakes to implement appropriate technical and organizational security measures to ensure a level of security appropriate to the risk in accordance with the applicable Data Protection Regulation.

5.2. The security measures implemented by Brevo under this DPA are detailed in Brevo's Technical and Organizational Measures detailed in Section 14 of this DPA. These security measures apply to Content, including personal and non-personal data. Customer acknowledges that Brevo may update its technical and organizational security measures, in particular in order to comply with any new requirements arising from Data Protection Regulation, throughout the term of the Agreement, provided that they are not degraded.

5.3. Brevo shall notify Customer of any personal data breach within the meaning of the GDPR within a maximum of seventy-two (72) hours of becoming aware of it. This notification shall be accompanied by any useful information to enable Customer, if necessary, to notify the breach to the competent supervisory authority. In the event of a personal data breach, Brevo undertakes to carry out all useful investigations into the breaches of the protection rules in order to remedy them as soon as possible and to reduce the impact of such breaches on the data

subjects, at no additional cost to Customer. Brevo undertakes to inform Customer of its investigations on a regular basis. Brevo undertakes to actively collaborate with Customer to ensure that it is able to meet its regulatory and contractual obligations, at no additional cost to Customer. It is the sole responsibility of Customer, as the data controller, to notify the competent supervisory authority and, if applicable, the data subjects of the personal data breach.

5.4. This Section is without prejudice to Customer's own obligations in terms of securing personal data

6. SUB-PROCESSING

6.1. Customer grants a general sub-processing authorization to Brevo, to conduct specific processing activities under the Agreement. On the Effective Date, authorized sub-processors are detailed in the list accessible in Section 12 of this DPA.

6.2. Provided that Customer has subscribed to receive notifications via the online form, Brevo will notify Customer of any changes regarding the addition or replacement of other sub-processors at least ten (10) Business Days prior to the change to provide Customer with an opportunity to object for legitimate reasons relating to the protection of personal data. If Customer has a legitimate objection to the addition of a sub-processor and Brevo cannot reasonably find an alternative, it will notify Customer. Customer is entitled to terminate the affected Services, otherwise the Parties will cooperate to find a satisfactory solution. If Customer does not object within the said period, the relevant sub-processor may be instructed to process Customer's personal data.

6.3. Any sub-processor is required to comply with the obligations of the Agreement on behalf of and in accordance with the instructions of Customer. It is Brevo's responsibility to ensure that the sub-processor provides the same sufficient guarantees regarding the implementation of appropriate technical and organizational measures so that the processing meets the requirements of the Data Protection Regulation. If the sub-processor does not fulfil its obligations with respect to the protection of personal data, Brevo shall remain fully liable to Customer for the sub-processor's performance of its obligations, subject to the conditions and limitations of liability set out in the General Terms and Conditions.

7. TRANSFERS

7.1. Customer is hereby informed that Content may be processed and is processed outside the European Economic Area by Brevo, its Affiliates or sub-processors for the purposes of the strict performance of the Services by Brevo in its capacity as data processor.

7.2. Brevo undertakes to provide an adequate level of protection for the Content processed, in accordance with the requirements of the Data Protection Regulation including the Standard Contractual Clauses ("**SCCs**") and additional measures.

7.3. Where a transfer is made from the European Economic Area to a country that does not benefit from a European Commission Adequacy Decision, Brevo and the sub-processor(s) will implement any appropriate safeguard mechanisms in compliance with Article 44 of the GDPR.

8. DELETION OF PERSONAL DATA

8.1. Brevo undertakes to destroy or anonymize Customer's personal data within an incompressible period of forty (40) days after the end date of the Agreement. It is the responsibility of Customer to make every effort to save and/or transfer its data to another medium of its choice within this period, in accordance with the terms and conditions specified in the Agreement.

8.2. In the event that EU law or the law of a Member State requires the retention of Customer's personal data, Brevo will inform Customer of this obligation. Brevo undertakes to provide Customer, upon first request, with a certificate of deletion of Customer's personal data.

8.3. At the end of the contractual relationship, Brevo may retain anonymized Content.

9. ASSISTANCE

Brevo undertakes to assist Customer in ensuring compliance with the obligations set forth in Articles 32 to 36 of the GDPR. It is specified that in the context of this assistance, certain measures requested by Customer may be subject to additional invoicing proportional to the time spent by Brevo's teams in handling Customer's request.

10. AUDIT

10.1. Brevo undertakes to provide Customer with all the information necessary to demonstrate compliance with the obligations set forth in the Data Protection Regulation.

10.2. Brevo undertakes to regularly test and evaluate the security measures in place in accordance with the ISO27001:2022 certification process. The results of such testing and evaluation will be evidenced in the ISO certificate that is published annually. Upon written request from Customer, Brevo shall provide Customer or the auditor appointed by Customer with a copy of the latest certificate. Brevo will also provide Customer with any additional information it may require regarding the security measures in place to assist Customer in understanding the scope of such measures.

10.3. Customer may order audits to be carried out on a documentary basis in order to ensure that the processing carried out by Brevo as a data processor is compliant, by sending Brevo a registered letter with acknowledgement of receipt, up to a limit of one (1) audit per year, with the exception of the period between 1st May and 31st August each year (the "**Non-Auditability Period**"). Brevo will have three (3) months to send Customer the requested documents. Confidential items entrusted to Brevo by other clients are not concerned by the audit of documents.

10.4. Customer may conduct an audit, at most once (1) a year, to ensure compliance with the Data Protection Regulation of the processing operations carried out by Brevo as a data processor for the purposes of performing the Services under the conditions defined below:

a) The audit must be preceded by a documentary audit under the conditions of Section 10.3 having revealed substantial points of non-conformity of Brevo;
b) Customer shall notify Brevo of its intention to have an audit performed with a minimum of thirty (30) calendar days by submitting a detailed audit plan outlining the proposed scope, duration and start date of the audit. Brevo will review the audit plan and inform Customer of any concerns or questions (for example, any request for information that may violate Brevo's security and privacy policies). Brevo may object in exceptional and duly justified circumstances (e.g. other audits are being carried out at the same time) and the audit may not be postponed for more than one (1) month;
c) The audit must be carried out outside the Non-Auditability Period;
d) The audit will be conducted by an external auditor selected jointly by the Parties for its expertise, independence and impartiality and who is, in any event, not a competitor of Brevo;
e) The auditor will be required to sign a confidentiality agreement;
f) The auditor agrees to conduct the audit during business hours and without disrupting the operations of Brevo;
g) Verifications may not relate to information or information systems over which Brevo does not have physical and/or logical control.
h) An identical copy of the audit report will be provided to the Parties for their comments;
i) The costs of the audit will be borne exclusively by Customer;
j) Upon receipt of the report, Brevo will implement within a reasonable period of time the appropriate corrective measures to ensure compliance with the Data Protection Regulation.

10.5. The report and information of Brevo collected during the audit or inspection operations shall be considered as Confidential Information and may only be used for the purpose of the audit and necessary corrective actions to the exclusion of any other use by Customer.

11. DATA PROTECTION OFFICER

Brevo has appointed a data protection officer who can be contacted by e-mail at dpo@brevo.com (with a copy of the CSM dedicated to Customer's account) and/or by post at the following address: Brevo, DPO, 9-17 rue Salneuve, 75017 Paris (France).

12. LIST OF SUB-PROCESSORS

Sub-Processor	Sub-Processed Activity	Registered Office	Server Location	Safeguards for the Transfer of Personal Data
Brevo's infrastructure Sub-Processors				
OVH SAS, 2 rue Kellermann, Roubaix, 59100, France	Hosting	France	France	N/A
Google Cloud France SARL Google Cloud Platform (GCP), 8 Rue de Londres, 75009 Paris, France	Hosting	France	Belgium	Adequacy Decision based on the EU-US Data Privacy Framework Standard Contractual Clauses and additional measures
Cloudflare, Inc. 101 Townsend St. San Francisco California 94107, USA	Content Delivery Network & WAF	USA	EU	Adequacy Decision based on the EU-US Data Privacy Framework Standard Contractual Clauses and additional measures
Zendesk, Inc. 989 Market St San Francisco, CA 94103, USA	Ticketing/support tool	USA	EU	BCR, Standard Contractual Clauses and additional measures
Omni Analytics, Inc.	Dashboards	USA	EU	Adequacy Decision based on the EU-US

375 Alabama St, Unit 350. San Francisco, CA 94110, USA				Data Privacy Framework Standard Contractual Clauses and additional measures
Specific services **Optional if Customer uses this specific service**				
Integry Inc. 2261 Market Street #5072 San Francisco CA 94114 United States	Integration with third-party software (list available on demand)	USA	EU/USA	Standard Contractual Clauses and additional measures
Convrrt, Inc. 1525 South Higley Road, Suite 104, PMB 1083, Gilbert, AZ 85296, United States	Creation of customized landing pages	USA	USA	Standard Contractual Clauses and additional measures
Google Gemini (Google Cloud SARL)	AI features	France	EU/USA	Adequacy Decision based on the EU-US Data Privacy Framework Standard Contractual Clauses and additional measures
OpenAI Ireland Limited 1st Floor, The Liffey Trust Centre 117-126 Sheriff Street Upper Dublin 1, D01 YC43, IRLAND	AI Features	Ireland	EU/USA	Standard Contractual Clauses and additional measures
Anthropic Ireland Limited, 6th Floor South Bank House, Barrow Street,	AI Features	Ireland	USA	Standard Contractual Clauses and

Dublin 4, Dublin, Ireland				additional measures
Langfuse GmbH, Oranienburgerstraße 91, 10178 Berlin, Germany	AI Features	Germany	EU	Standard Contractual Clauses and additional measures
Eldar IT d.o.o Trebinjska 32, Belgrade, Serbie	Maintenance of the Salesforce Plugin	Serbia	Serbia	Standard Contractual Clauses and additional measures
SMS providers (to be disregarded if Customer does not purchase SMS and does not intend to purchase SMS)				
Vonage	SMS routing	USA	EU	Standard contractual clauses and additional measures: isolation of data centers in the EU and self-suppression of the SMS meta data
iBasis	SMS routing	Liechtenstein	Austria/Germany	EU law
Twilio SMS	SMS routing	USA	EU/USA	EU-US Data Privacy Framework Standard contract clauses and additional measures BCR
Brevo Group **(Sales Platform Add-on only)**				
Meetfox GmbH Group company owned by Brevo	Brevo Meetings Customer experience & Maintenance	Austria	EU	N/A
Yodel GmbH Group company owned by Brevo	Brevo Phone Customer experience & Maintenance	Austria	EU	N/A

Brevo Group (all Services)				
Brevo GmbH Group company owned by Sendinblue, Köpenicker Straße 126, 10179 Berlin	Customer Experience & Maintenance	Germany	France and Belgium	N/A
Brevo CRM Solutions Group company owned by Sendinblue, A 8a Tower A 8th Floor Knowledge Boulevard Sector 62 Noida Uttar Pradesh – 201301, India	Customer experience & Maintenance Shopify Plugin	India	France, Belgium Shopify Plugin: India	Standard Contractual Clauses and additional measures
Brevo Inc. Group Company owned by Sendinblue, 1000 2nd Ave Suite 3700 Seattle WA 98104, USA	Customer experience & Maintenance	USA	France and Belgium	Standard Contractual Clauses and additional measures

13. DESCRIPTION OF THE PROCESSING

The following tables describe the data processing operated by Brevo while providing the Services.

Marketing & Messaging API Platform

PURPOSE	All processing necessary for the provision of the CRM and digital marketing Services by Brevo.
NATURE OF PROCESSING	On Customer's instructions, Brevo: - Organizes and segments Content; - Automates digital marketing; - Sends electronic communications via various Channels; - Makes Usage Data available to Customer to provide analytics and reporting features. - Collects, hosts, analyzes, displays, and aggregates Content; - Modifies, updates or deletes Content from or Usage Data from the Software. Brevo also provides Customer with the means to implement online tracking devices necessary for the provision of certain functionalities such as Marketing Automation. Customer is responsible for setting the parameters of these tracking devices, informing the data subjects and obtaining their consent.

Emails & SMS Channels	Brevo provides Customer with the means to implement tracking technology (pixel and URL tracking) within electronic communications sent on behalf of Customer. These tracking technologies are necessary to provide the Services and allow the collection of metadata, including personal data related to the recipient's e-mail address: IP address, timestamp, click log, and open log. Brevo uses the data collected from this tracking to (i) provide features that allow Customer to analyze its mailings and know when to send electronic communications at the best time, (ii) monitor the security and availability of the Services and (iii) create statistics and evaluate the use of the Services. Brevo acts as a processor, does not inform the data subjects and does not collect their consent on behalf of Customer. The Services allow Customer to anonymize the data processed by these tracking technologies and to collect aggregated results. This provision constitutes Customer's written agreement to the deployment of these tracking technologies.
Wallet Channel	Associating a Card to a Subscriber.
Push Channel	The processing operations are detailed here. Brevo provides the Customer with an SDK file necessary for the provision of the Services and enabling the collection of metadata related to the Subscriber under the conditions detailed here. Brevo acts as a processor, does not inform the data subjects and does not obtain their consent on behalf of the Customer.
Sales Platform Add-on	Brevo Conversation To run an online chatbot, Brevo may provide Customer with online tracking devices necessary for the provision of certain marketing and e-commerce functionalities. Customer is responsible for setting the parameters of these tracking devices, informing the data subjects and obtaining their consent. Brevo Meetings Brevo Meetings allows Customer to schedule meetings with third parties and customize booking pages. Brevo Phone Brevo provides a cloud-based phone system allowing Customer to access international phone numbers, to find the area code that best fits Customer, and to make outgoing calls.
DURATION OF PROCESSING	By default, the duration of the processing is the duration of this Agreement. Customer is solely responsible for managing the retention periods for Content and Usage Data in the User Interface. It is Customer's responsibility to delete the data as and when the retention period expires. Brevo's sole responsibility is to delete or anonymize such data at the end of its contractual relationship with Customer.
PROCESSED DATA	User data, Content, Contact data, Subscriber data, and Usage Data
Emails, SMS, Channels	In case Customer is exclusively using the Marketing Platform, the following data of the Contact is processed: identification and Contact data as downloaded and entered by the User (name, e-mail address, telephone number, notes, imported documents, Contact attributes, or any Contact information added by Customer), as well as Usage Data. Usage Data that consists of technical information and logs :

	• IP addresses; • ratio of openings and clicks collected by pixel tracking and URL tracking; • date/time of the email sent; • recipient; • subject; • content of the email (can be disabled in the transactional settings). In case Customer is exclusively using the Messaging API Features, Brevo shall only store Usage Data. In such a specific case, Usage Data will include API logs that have a mandatory retention period of seven days.
Wallet Channel	Data linked to the Subscriber (name and surname, identification number or any Contact data chosen by Customer) and to the Card (e.g., card number, status, accumulated benefits, etc.).
Push Channel	Data processed by the SDK relating to the Subcriber: (i) Connection data. The Services use the terminal identifier and cookies to create a Subscriber's account and/or to authenticate the Subscriber's use of the Application. (ii) Terminal Data. Brevo uses limited information from the Contact's terminal in order to provide the Services within the Application, such as device identifier, terminal type, language. (iii) Application(s) specific information. Brevo processes Application-specific information, i.e. information relating to each Contact and the Application he/she uses. This includes the Contact's identifier, sessions, and session duration.
Sales Platform Add-on	<u>Brevo Conversation</u> Visitor's ID of the website visitor (Contact). Brevo may provide additional information on Customer's demand. <u>Brevo Meetings</u> Phone number or email address of the Contact. <u>Brevo Phone</u> Phone number of the Contact.
DATA SUBJECTS	• Users • Contacts, including any person: (i) whose e-mail address and/or telephone number is included in the Content, (ii) whose information is otherwise stored or collected through the Services,. • Subscribers, which means any Subscriber to the Push and/or Wallet Channel(s).

<u>Loyalty Platform</u>

PURPOSE	Provision of the Loyalty Platform.

NATURE OF PROCESSING	All processing activities necessary for the provision of the Loyalty Platform by Brevo, specifically the recording, storage, modification, consultation, deletion, and transmission of Content.
CATEGORIES OF PERSONAL DATA	Transaction data and loyalty data (earns, burns, enrollments, etc.) of Loyalty Subscribers.
DATA SUBJECTS	Loyalty Subscribers.

14. TECHNICAL AND ORGANIZATIONAL MEASURES

The following measures are specified in detail to implement the requirements of Article 32 of the GDPR:

No.	Confidentiality	Implementation of the measure
1.	**Access control** Unauthorized persons must be denied access to data processing facilities used to process personal data .	- *Access to office premises only by or accompanied by authorized persons,* - *Access control system for office premises using a key management system (door locks, entry only with a key, documented key allocation),* - *Storage of confidential documents and staff laptops exclusively under lock and key in lockable, solid cabinets.*
2.	**Access control** Measures must be taken to prevent data processing systems from being used by unauthorized persons.	- *Use of state-of-the-art encryption methods,* - *password procedures and password protection through the mandatory use of a web-based password manager,password policy (complexity, length, history, reuse) including password changes every 180 days* - *Two-factor authentication (multi-factor authentication) for all systems that process personal data* - *Personal and individual user log-in when logging into the system or corporate network,* - *Requirement to lock work devices; MDM software for remote locking in use,* - *Creation of a user master record for each user,* - *Access to servers via a bastion host,* - *Authorization policy for digital access options*
3.	**Access control** Ensuring that authorized persons using a data processing system can only access the personal data covered by their access authorization, and that this data cannot be read, copied, altered or removed without authorization during processing.	- *Design of the authorization concept based on actual needs (least privilege principle)* - *Regular (at least annual) review and recertification of access rights* - *Implementation of a user lifecycle process (Joiner/Mover/Leaver)* - *Exclusively named (non-shared) user accounts, including for administrators* - *Logging (security/user),* - *regular analysis of log files,* - *automated 24/7 monitoring of logs*
No.	**Integrity & Encryption**	**Implementation of the measure**
4.	**Control of disclosure** It must be ensured that personal data cannot be read, copied, altered or removed without authorization during electronic transmission, transport or storage on data carriers, and that it is possible to verify and determine to which destinations the transmission of personal data by data transmission facilities is intended.	- *Transmission and transfer using TLS 1.2 and TLS 1.3 encryption,* - *Password protection for individual documents with separate password transmission,* - *VPN tunnels,* - *firewall, as well as monitoring and restricting incoming and outgoing network traffic to legitimate connections* - *antivirus protection,* - *Creation of a record of processing activities in accordance with Article 30(2) of the GDPR,* - *Proof of dispatch, labelling and inventorying of data carriers.*
5.	**Input control** It must be ensured that it is possible to subsequently verify and determine whether, and by whom, personal data has been modified.	- *Traceability and documentation of data management are ensured by logging systems* - Logging *systems and formalized monitoring processes for the detection of security incidents*
No.	**Availability and resilience**	**Implementation of the measure**

6.	**Availability control** It must be ensured that personal data is protected against accidental destruction or loss.	- *Daily backup procedure,* - *Mirroring of hard drives at the sub-processor (RAID procedure),* - *Uninterruptible power supply at the sub-processor (UPS),* - *Fire alarm system* - *Documented Business Continuity Plan (BCP) as per ISO 27001:2022 requirements* - *Documented Disaster Recovery Plan (DRP) ISO 27001:2022 requirements* - *Regular (at least annual) restoration tests ISO 27001:2022 requirement*
No.	**Confidentiality**	**Implementation of the measure**
7.	**Separation control** It must be ensured that personal data collected for different purposes can be processed separately.	- *Software multi-tenancy and ensuring the logical segmentation of customer data ,* - *Functional & physical separation between staging and production environments* - *Development and test systems are operated exclusively with test data.*
8.	**Order control** It must be ensured that personal data processed on behalf of the controller can only be processed in accordance with the controller's instructions.	- *Demarcation of the respective roles of the controller and the processor through clear contractual arrangements setting out the respective responsibilities of the controller and the processor,* - *clear definition of instructions through a requirement for written form,* - *Regulation of the use of sub-processing,* - *imposing a duty of confidentiality on employees,* - *Appointment of a data protection officer, Training of staff regarding compliance with data protection and data security,* - *Monitoring of sub-processors as per ISO 27001:2022 requirements* - *Implementation of a documented security and risk management process for service providers and sub-processors* - *Ensuring contingency and recovery plans are in place, including for critical service providers*
9.	**Security of processing (across the board)**	- *Conducting and documenting regular risk analyses for the processing of personal data (based on the EBIOS RM framework as well as ISO 27005)* - *Alignment with ISO 27001:2022 standard*
10.	**Operational security and vulnerability management**	- *Implementation of a patch and vulnerability management process* - *Prompt installation of security updates in accordance with risk assessment (critical vulnerabilities within 24 hours)* - *Implementation of measures in the absence of patches in accordance with manufacturer or CERT recommendations* - *Deployment and maintenance of anti-malware and anti-virus solutions*
11.	**Security incidents (incident response)**	- *Establishment of a documented incident response process* - *Classification, reporting, tracking and resolution of security incidents* - *Defined escalation processes and responsibilities* - *Appointment of an incident response team with clear roles and responsibilities* - *Establishment of a crisis management process* - *Use of monitoring mechanisms for the early detection of security incidents*
12.	**Application security**	- *Conducting code reviews and automated security scans (e.g. in accordance with OWASP): SAST & DAST* - *Internal Quality Assurance Team* - *Regular (at least annual) penetration testing* - *Provision of up-to-date test reports on request*

13.	**Data erasure and data portability**	- *Secure deletion of data in accordance with recognized standards (e.g. NIST 800-88 or equivalent)* - *Provision of data exports in a structured, commonly used and machine-readable format*