360dialog Data Processing Agreement according to Art. 28 GDPR ("DPA")

This DPA is **Appendix 1** to the Agreement between the Parties (“Main Agreement”) where **the Partner/Client** shall be the Controller and **360dialog GmbH** shall be the Processor, and becomes effective the day both, the Main Agreement and this DPA, are properly signed by all parties.
360dialog reserves the right to update this DPA if necessary and the Client acknowledges that always the most up to date version will apply.

Terms used and defined in the GDPR shall have the same meaning in this DPA.

1 Details of the Processing

1.1 Controller may submit Personal Data to the Processor, or the Processor may have access to Personal Data of the Controller while the parties execute the Main Agreement. Details as to the Categories of data being processed, the data subjects, and the kind of processing are described in **Appendix DPA1**.

1.2 Personal Data will be Processed for purposes and duration of the Main Agreement.

2 Controller Responsibility

Within the scope of the Main Agreement, Controller shall be solely responsible for complying with the statutory requirements relating to data protection and privacy, in particular regarding the disclosure and transfer of Personal Data to the Processor and the Processing of Personal Data, Art. 28 III 1 GDPR.

3 Obligations of Processor

3.1 Processor shall process Personal Data only within the scope of Controller’s Instructions, Art. 28 III 2, lit. a) GDPR. If the Processor believes that an Instruction of the Controller infringes the Data Protection Law, it shall immediately inform the Controller without delay, Art 28 III 3 GDPR.

3.2 Processor shall take the appropriate technical and organizational measures to adequately protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data according to Art. 28 III 2, lit. c), Art. 32 GDPR, described in **Appendix DPA2.**

3.3 Processor shall ensure that any personnel whom Processor authorizes to process Personal Data on its behalf is subject to confidentiality obligations with respect to that Personal Data. The undertaking to confidentiality shall continue after the termination of this DPA, Art 28 III 2 lit b) GDPR.

3.4 Processor will notify the Controller without undue delay after it becomes aware of any Personal Data Breach, Art 33 II GDPR. At the Controller’s request, Processor will promptly provide the Controller with all reasonable assistance necessary to enable the Controller to notify relevant Personal Data Breaches to

competent authorities and/or affected Data Subjects, if Controller is required to do so under the Data Protection Law.

3.5 Other than to the extent required to comply with applicable law, following termination or expiration of the DPA, Processor will delete or return all Personal Data (including copies thereof) processed pursuant to this DPA and Art 28 III 2 lit g) GDPR. If Processor is unable to delete Personal Data for technical or other reasons, Processor will apply measures to ensure that Personal Data is blocked from any further Processing.

3.6 Processor will enable Controller to fulfill the rights of the data subject as stipulated in Chapter III of the GDPR (information, rectification and erasure, data portability, right to object, as well as automated decision-making in individual cases) within the statutory deadlines at any time and provides the Controller with all the information necessary, Art 28 III 2 lit e) GDPR.

3.7 Processor supports Controller in complying with the obligations set out in Articles 32 to 36 GDPR (data security measures, reporting data breaches to the supervisory authority, notification of the data subjects affected by a data breach, data protection impact assessment, prior consultation), Art 28 III 2 lit f) GDPR.

4 Audits

4.1 Processor shall, in accordance with Data Protection Laws and in response to a reasonable written request by Controller, make available to Controller such information in Processor's possession or control related to Processor's compliance with the obligations under Data Protection Law in relation to its Processing of Personal Data, Art 28 III 2 lit h) GDPR.

4.2 Pursuant to Art 28 III 2 lit h) GDPR, Controller may, upon written request and at least 30 days' notice to Processor, during regular business hours and without interrupting Processor's business operations, conduct an inspection of Processor's business operations or have the same conducted by a qualified third party auditor subject to Processor's approval, which shall not be unreasonably withheld.

4.3 Processor shall, upon Controller's written request and on at least 30 days' notice to the Processor, provide Controller with all information necessary for such audit, to the extent that such information is within Processor's control and Processor is not precluded from disclosing it by applicable law, a duty of confidentiality, or any other obligation owed to a third party.

5 Place of data processing

All data processing by Processor shall take place within the EU / EEA only, unless explicitly specified otherwise for specific purposes or functions in **Appendix DPA2.** In the latter case, Processor shall ensure that the data is processed in compliance with Art. 45, 46 GDPR.

6 Sub-Processors

6.1 Processor is entitled to use sub-processors with the consent of the Controller according to Art. 28 II, III 2, lit. d), IV GDPR. Any change of such sub-processors must be reported to Controller. The sub-processors are listed in

 Appendix DPA3.

6.2 Where Processor engages sub-processors, Processor will enter into a contract with the sub-processor that imposes on the sub-processor the same obligations that apply to Processor under this DPA. Where the sub-processor fails to fulfill its data protection obligations, Processor will remain liable to the Controller for the performance of such sub-processors obligations.

6.3 Where a sub-processor is engaged, the Controller must be granted the right to monitor and inspect the sub-processor's activities in accordance with this DPA and the Data Protection Law, including to obtain information from the Processor, upon written request, on the substance of the contract and the implementation of the data protection obligations under the sub-processing contract, where necessary by inspecting the relevant contract documents.

7 Contacts, Data Protection Officer

Processor has appointed a Data Protection Officer with the details set forth in **Appendix DPA4.** Processor shall inform Controller of any change in that position.

Appendix DPA1

Categories of data being processed	Data Subject(s)
Password to the 360dialog Hub	Clients / Partners
Content of the opened support ticket (company data, contact person, phone number, website + description of the issue)	Clients / Partners
Contractual data – (company data: legal name, address, logo, email, contact persons, phone number, financial data)	Clients / Partners

Categories of data being processed for messaging	Data Subject(s)
User ID (phone number registered on WhatsApp)	End Users / Clients
Message Content	End Users / Clients
Metadata (size, time, date of the message)	End Users / Clients

Categories of data being processed for CAPI	Data Subject(s)
User ID	End User
Conversion type	End User
Purchase amount	End User
AD_ID	End User
CTWA_CLID	End User

Categories of data being processed for Insights	Data Subject(s)
User ID	End User
Message Content	End User
Metadata (size, time, date of the message, conversion ID, template ID, message status)	End User

Appendix DPA2

0 Data Protection Concept & Technical and Organizational Measures (TOM)

in accordance with Art. 32 EU-GDPR

360dialog GmbH
Version 2.2

1 Overview

This data protection concept / these TOMs govern the data processing of 360dialog GmbH, Torstraße 61, 10119 Berlin, Germany. This company is also the responsible party within the meaning of Art. 4 No. 7 DSGVO.

360dialog GmbH undertakes to treat all personal data, both of customers and of business partners, employees, and other data subjects

- lawfully, in good faith and transparently,
- for a specific purpose,
- correctly,
- only in the necessary content and temporal extent of the data minimization obligated
- and securely
- and to enable the data subjects to exercise their rights.

360dialog views data protection as a continuous improvement process and strives to regularly review and improve compliance with all applicable requirements.

Technical and organizational measures are intended to ensure that all organizations that use, process, or collect Personal Data themselves or on their behalf comply with the statutory provisions of the GDPR.

When assessing the appropriate level of protection, particular account must be taken of the risks associated with processing, in particular those arising from destruction, loss or alteration, whether accidental or unlawful, or unauthorized disclosure of or access to personal data that have been transmitted, stored or otherwise processed.

2 Confidentiality (Article 32(1)(b) GDPR)

2.1 Access control

The purpose of access control is to prevent unauthorized persons from gaining access to data processing systems with which personal data are processed or used. Measures for access control can include automatic access control systems, the use of chip cards and transponders, access control by gatekeepers and alarm systems to

secure buildings and rooms. Servers, telecommunication systems, network technology and similar systems must be protected in lockable server cabinets. In addition, it is also advisable to support the access control by organizational measures (e.g., service instructions which provide for the locking of the offices during absence).

The following measures prevent unauthorized access to offices and data processing systems of 360dialog and server locations.

2.1.1 Access to office premises

The spatial access security is provided by:

- Key / key allocation for offices with sensitive data
- Visitor regulation: External persons are generally only allowed to enter the office rooms by prior appointment. They must be accompanied by an employee throughout the entire time. This does not apply to regularly returning external persons (e.g., cleaning personnel from external cleaning companies).

2.2 Physical access control

The purpose of access control is to prevent unauthorized persons from using data processing systems that are used to process and use personal data. Possibilities are, for example, boot password, user identification with password for operating systems and software products used, screen saver with password, the use of chip cards for login as well as the use of CallBack procedures. In addition, organizational measures may also be necessary, for example to prevent unauthorized access (e.g., guidelines for setting up screens, issuing orientation guides for users to choose a "good" password).

By principle, all access to personal data is access-protected.

In detail, the following accesses to data are possible:

2.2.1 Access to the application systems via web interface (regular use)

Every user (360dialog employees and all users approved by the client) must authenticate themselves to access personal data - usually by means of a username and password. The required access is managed by Auth0 (https://auth0.com/), a cloud-based solution for identity management.

2.2.2 Access to the backend systems (e.g., for administrative tasks, access usually via SSH or VPN)

- IT systems are protected against unauthorized access by firewall systems and IP whitelisting. All servers require authentication, usually by stored, user related encrypted SSH keys. These keys must have a minimum key length of 2048 bit and must be password protected. Access to databases is only possible via a VPN after successful strong authentication at the respective server, so that protection by username and password is considered sufficient.

- There is an IP whitelisting on API level to allow access only to authorized systems.
- A screen saver with password protection is installed on workstations.

2.3 Access inspection

Access control measures shall be designed to ensure that only data for which access is authorized can be accessed and that personal data cannot be read, copied, altered, or removed without authorization during processing, use and after storage. Access control can be ensured, among other things, by means of suitable authorization concepts that enable differentiated control of access to data. In doing so, it is important to differentiate both the content of the data and the possible access functions to the data. Furthermore, suitable control mechanisms and responsibilities must be defined to document the granting and withdrawal of authorizations and to keep them up to date (for example, when hiring, changing jobs, or terminating employment). Special attention must always be paid to the role and capabilities of administrators.

2.3.1 Minimum of authorized persons

With 360dialog, the number of persons with access to the above-mentioned data processing equipment is reduced to a minimum. As described in the regulation of access control, a distinction is made between the following groups of persons:

2.3.2 360dialog system and database administrators

- System administrators can enter the access and access authorizations granted by the management into the system and issue corresponding authorization features in a logged form (e.g. SSH keys), perform system maintenance and updates, view server logs, and generally perform server-related administrative tasks.
- Database administrators can log directly into the respective databases and tables at the database level to perform administrative tasks and create backups.
- Access at database or operating system level is only possible for 360dialog employees.

2.3.3 360dialog developers and integration specialists

- Developers and integration specialists at 360dialog can access log files and databases for maintenance, servicing, troubleshooting and cause analysis or related work tasks.
- They require the approval of the management, which has been delegated by instruction to the departmental management. The group of persons is also agreed with the client.

2.3.4 User

- Within the application level, there are different user roles and groups, each of which is coordinated with the client. Both users of the client and employees of 360dialog can have access here. Normal users can only log into the application systems via the respective web interfaces and perform the tasks corresponding to their respective access rights.
- As soon as an employee no longer needs access due to leaving the company or his specialist task, his personal access is blocked again and the associated data is irretrievably deleted. This is usually done by periodic checks, at the request of the customer or when the contractual relationship ends.

2.3.5 Password rules

Passwords assigned by 360dialog meet the following guidelines:

- a minimum length of 8 characters, empty passwords are not allowed,
- a character mix of at least three categories: lower case, upper case, numbers and special characters (!@#$%^&*)
- no easy to guess term and no trivial password (from a list of the 10,000 most common passwords),
- no use of historical passwords (the history knows 10 passwords),
- no part of the username is part of the password.

User passwords that are intended for users of the client are either assigned directly by the client or configured by authorized employees of 360dialog according to the respective password guidelines.

Once passwords have been created, they must be changed regularly (at least every 6 months).

The first password must be sent to the user in a secure way and/or the user must be requested to change it at least immediately after the first login. If username and password are required for authentication, the corresponding password is never displayed in plain text on the screen. This applies to all access options - whether via web interface, SSH access or database access, and whether by employees of 360dialog or authorized users of the customer.

2.3.6 Password management

Application passwords at 360dialog are managed via 1Password, hosted on a dedicated machine with its own database in the data center. Infrastructure credentials are managed via Hashicorp Vault.

2.3.7 Secured transmission of authentication secrets (credentials) in the network

All registrations that are made over a network are always encrypted. For web-based user interfaces, these TLS / HTTPS are encrypted and encoded via and as JSON Web Token (JWT). For direct access to servers, this is optionally encrypted via SSH or VPN (IPSec, openVPN, or similar).

2.3.8 **Logging of access**

- Access attempts (both successful and rejected) to the servers at SSH level are stored in the server logs and kept for 3 months.
- Access attempts to the web interfaces are recorded and logged in Auth0 (https://auth0.com/) Auth0 In case of brute force attacks or password abuse, Auth0 becomes active and blocks access.

2.3.9 **Encryption and data deletion**

Printed project and contract documentation is shredded with a shredder, level 2.

2.3.10 **Physical deletion of data carriers**

All data on laptops is secured using hard disk encryption (e.g., FileVault) and securely deleted when the devices are reused. When office hardware is sold or server hard disks are returned to the data center, data carriers are physically deleted and randomly written to prevent reconstruction of the original data.

External data carriers are not used for backup, transport and storage.

2.3.11 **Fraud Prevention**

Evaluation of the Client/Partner registration for fraud purposes through sending user / transaction / device data via the Fraud API to SEON Technologies Kft. for enriching the data and delivering a risk score in our own interest.

2.4 **Separation Control**

The purpose of the separation control is to ensure that data collected for different purposes can be processed separately. This can be ensured, for example, by logical and physical separation of the data.

2.4.1 **Separate processing**

The messaging data of the respective clients are processed completely separately from each other and assigned to unique logical, isolated database tables. Buffers and lookup tables that are shared but ensure logical client separation are an exception.

2.4.2 **Separation of test and production systems**

Test and production systems are logically separated from each other.

2.4.3 **Economy in data collection**

It is up to the customer to decide whether and which personal data is collected and processed beyond the functions offered by 360dialog.

2.5 **Pseudonymization (Art. 32 para. 1 lit. a GDPR; Art. 25 para. 1 GDPR)**

The processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the need for

additional information, provided that this additional information is kept separately and is subject to appropriate technical and organizational measures.

2.5.1 Deletion periods instead of pseudonymization

A pseudonymization will only be carried out at the request of the client and by prior agreement, as a pseudonymization can render historical personalization data unusable. Instead, data retention policies are agreed upon and the data is deleted in its entirety.

2.5.2 Pseudonymization for evaluation purposes

KPIs (=key performance indicator) are stored historically for evaluation purposes. These are merely counters that represent a certain period of time and whose resolution does not allow any conclusions to be drawn about users.

2.5.3 Pseudonymization before transfer

An internal directive regulates: if personal data from the production system is passed on in the context of an analysis, it is pseudonymized, unless it is of importance for the presentation of the facts.

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

3.1 Transfer control (passing on control)

The purpose of the control of disclosure is to ensure that personal data cannot be read, copied, modified or removed without authorization during electronic transmission or during their transport or storage on a data carrier. It should be possible to check and establish where personal data are to be transmitted by data transmission equipment. To ensure confidentiality in electronic data transmission, encryption techniques and virtual private networks can be used, for example. Measures for data carrier transport or data transfer are transport containers with locking devices and regulations for the destruction of data carriers in accordance with data protection regulations.

3.1.1 Transfer within the systems

Data is normally transmitted via dedicated data lines, but at least encrypted via a VPN with IP whitelisting.

3.1.2 Transmission to external systems

- All APIs are only accessible via HTTPS.
- No data is transferred to external systems unless expressly agreed. In these cases, data is transmitted exclusively via secure and encrypted channels.
- Should a transmission become necessary, SFTP with username/password (according to the guidelines) is usually used. Data access to APIs or via webhooks, requires username/password (according to guidelines). Logging is done via the SFTP server logs. In the case of regular data transports

to one and the same recipient, so-called key files (GPG) will be exchanged, which then makes the (separate) transmission of a password unnecessary.
- Transmission on electronic data carriers (USB sticks, mobile hard disks, notebooks, smart devices) is not permitted and in special cases requires the express permission of the management and the client.
- No personal data is permanently stored on the workstations of 360dialog itself, but such data can be viewed temporarily on the respective monitors.

3.1.3 Risk minimization through network separation

- All 360dialog servers are located behind the corresponding gateways consisting of router and firewall, the access to the systems can only be done via these gateways. The gateways reject connections that come from a network that is not explicitly enabled. There is a physical separation of internal and external connections via separate network segments for the 360dialog platform (third-party systems such as WhatsApp can be located in other data centers).

3.1.4 Handling emails

Personal data may not be transmitted via email. In exceptional cases, and following express agreement with the client, compressed and encrypted files may be used, provided that this is a one-off matter. Employees must obtain approval for this from their supervisor.

3.1.5 Documentation

Data recipients, duration of the planned transfer and deletion periods are implemented as specified in the respective DPA or these TOMs.

3.2 Input Control

The aim of input control is to ensure, with the aid of suitable measures, that the detailed circumstances of data input can be checked and established subsequently. Input control is achieved by logging, which can take place at various levels (e.g., operating system, network, firewall, database, application). It must also be clarified which data is logged, who has access to logs, by whom and at what occasion/time they are controlled, how long they must be kept and when the logs are deleted.

3.2.1 Logging

- Accesses by system administrators are only logged to the extent that their respective logon procedures and the commands they start on the server shells are recorded. All other commands (e.g., commands started in graphical consoles) are not recorded. A history of 1000 commands is kept for the captured commands and logon operations are kept for 3 months. Access by system administrators is not used for processing or active access to

personal data, but for the care, maintenance and updating of the server systems themselves.

- Accesses by database administrators are only logged to the extent that the commands they enter directly in the console administration programs are recorded, and a history of 1000 commands is kept by them. If graphical management programs are used, the commands executed there are not recorded. Access by database administrators is not intended to process or actively access personal data, but to maintain, service and update the databases themselves.

3.2.2 Traceability / Logging

For all other (regular) users who use the corresponding application programs to process personal data, the last processor is logged. However, the exact modification itself is not recorded here. It can be derived with the appropriate effort in individual cases.

3.2.3 Responsibility for deletions

- Responsibility for deletion is with the owner of the respective data.
- Data deletion in commissioned processing is governed by the respective DPA". The instruction is transferred from the authorized group of persons of the customer to the project or customer managers at 360dialog. Any deletion requires a written instruction.

3.2.4 Deletion of data

- Live communication data are deleted upon delivery to end recipient, in any case latest seven (7) days after having been received.
- Any other data are deleted if they are no longer needed for the purpose(s) they were originally processed for.
- Contractual data may be stored in some cases until statutory limitation periods for civil claims have expired. In such case the data will be stored outside the live system.
- Data will be stored for the duration of statutory retention periods. In such cases the data will be stored outside the live system. Typical retention periods are:

Annual deadlines always end at the end of the last calendar year.	Retention period	Legal basis
Time sheets (general)	2 years	§ 16 Para. 2 ArbZG
Application documents	until the expiry of possible limitation periods for claims	§ Section 15 (4) AGG, Section 61 (1) ArbGG
DEÜV certificate on data transmissions	by the end of the calendar year following the last test	§ 25 DEÜV

Double taxation certificate	6 years	§ Sec. 39b (6) in conjunction with Sec. § Section 41 (1) EStG
Travel reimbursement	6 years	§ Section 41 (1) EStG in conjunction with R 38 of the wage tax guidelines
Infection Protection Act - health certificate and final documentation of instruction.	until the employee leaves the company	§ 43 Para. 5 IfSG
Payroll account (tax)	6 years	§ 41 para. 1 EStG
Wage records (social security)	until the end of the calendar year following the last audit	§ 28f para. 1 p. 1 SGB IV

3.2.5 Deletion of data upon request

- Data have to be deleted upon request in case the requirements of Art. 17 GDPR are met. In such cases deletion has to be carried out without undue delay.
- The data subject requesting deletion will have to be authenticated by appropriate methods if there is uncertainty.
- In case of such request the DPO has to be notified.

4 Availability and resilience (Art. 32 (1) lit (b) GDPR)

The aim of availability control is to ensure that personal data is protected against accidental destruction or loss. Data processing systems are 'resilient' if they are so robust that their functionality is guaranteed even under heavy access or heavy use. This applies not least with regard to the targeted overloading of servers in order to ensure availability despite an external attack, for example through so-called DoS or DDoS attacks ("Distributed Denial of Service"). This also includes issues such as uninterruptible power supply, air conditioning, fire protection, data backups, safe storage of data media, virus protection, RAID systems, disk mirroring, etc.

4.1.1 Redundant provision of critical systems

All central platform functionalities and cloud storages are redundantly maintained as a full-fledged cluster or master-slave configuration. This includes:

- web server
- Queues and buffer storage
- Databases and key value stores
- Business logic

Disk systems are set up with at least basic fault tolerance (RAID5 or RAID6).

4.1.2 Backup concept

To protect the data from accidental loss, backups are made of this data. These backups are encrypted and stored separately from the productive data on a separate server in the same data center (if

desired, also as a further copy with another service provider). Due to the encryption of the data, a lower level of protection for physical access is appropriate here - which nevertheless does not allow general access to the data processing systems and data carriers located there - since the data cannot be used without the appropriate authorization and access key.

No data backups are made on movable, physical data storage devices such as tapes or CD-ROMs and there is no need to store the data storage devices.

Due to the centralized data storage approach, different backup strategies can be applied. In the area of the database, multiple redundant replications in master/slave operation is carried out as well as daily backups to external data carriers. In the event of a failure of the database master, this enables a fast failover to a corresponding slave server without having to accept data loss.

4.1.3 Rapid recoverability (Art. 32 para. 1 lit. c GDPR)

In the event of an application or user error and the associated loss of data, database backups can be used. Restoration is carried out promptly in accordance with the defined service level agreement. Restoration processes are documented so that a quick response is possible. Replacement systems are available as hot or spare parts depending on requirements

4.1.4 Separate partitions

Operating system and data are kept on separate hard disks.

4.1.5 Emergency plan / Disaster Recovery

Emergency situations are practiced regularly. In the event of a disruption, the relevant contact persons on the client's side are informed immediately. The contact persons are documented in the contracts with the client and are updated accordingly in case of changes.

5 Procedures for regular review, assessment, and evaluation (Art. 32 para. 1 lit. d GDPR; Art. 25 para. 1 GDPR)

5.1 Data Protection Management

The company has introduced a data protection management system (from ER Secure) and with

René Rautenberg,
ER Secure GmbH,
In der Knackenau 4,
82031 Grünwald

an external data protection officer.

5.2 Trainings, Reviews

- Documentation of relevant processing of personal data, including regular updates and checks

- Training and commitment of all employees to data secrecy
- Annual sensitization of employees
- Annual review of the effectiveness of technical protection measures
- Requests for information and deletion are received via legal@360dialog.com and interfaces and are implemented at least monthly

5.3 Incident-Response-Management

The platform is protected by a firewall. fail2ban is used as an intrusion prevention system (IPS). Email spam is detected and filtered by GSuite Business' spam filtering.

5.3.1 Information and Escalation

Security incidents are reported internally to the SysOp, the Solution Architect, the Head of Product and to the management. Depending on the classification of the incident, the external data protection officer is also consulted, or the client is informed insofar as he is affected by the incident.

5.3.2 Documentation

In each case, a ticket is created in the ticket system, which is used to collect all information about the incident and its resolution. The remedy is accepted by the responsible team leaders and, if necessary, executed towards the client. Post-mortem culture enabled.

5.4 Data protection-friendly default settings (Art. 25 (2) GDPR) / Privacy by Design, Privacy by Default

- Every development employee is informed about the concepts "Privacy by Design" and "Privacy by Default". No more personal data is collected than is necessary for the respective purpose. Implementation is the responsibility of the employee; control is the responsibility of the Head of Product and the Solution Architect.
- Additionally, personal data will only be processed in joint agreement with the client.
- Retention periods are chosen to be as short as possible (30 or 90 days). Exceptions are agreed with the client.

5.4.1 Exercise of the right of revocation

Affected parties can object to the tracking of their information. Notifications and conversations require the users' consent anyway.

5.5 Order Control

The aim of the order control is to ensure that commissioned data processing within the meaning of Art. 28 GDPR is carried out without corresponding instructions from the client. In addition to data processing on behalf of the client, this item also includes the performance of maintenance and system support work both on site and by remote

maintenance. If the contractor uses service providers in the sense of order processing, the following points must always be agreed with them.

5.5.1 Implementation of the right to issue instructions

Data access by authorized users is further restricted and regulated by the client himself, or via the "Contract for order processing in accordance with Art. 28 GDPR", set up and released by 360dialog.

5.5.2 Regulations/restrictions on order processing

Only work that is included in the service description to be drawn up may be carried out. All work steps going beyond this must be agreed in advance with the responsible body on the side of the client and approved in writing. The contractor agrees the schedule for the execution of the order with the client in advance.

The Contractor shall inform the Customer immediately of cases of serious operational disruptions, suspected violations of data protection, errors detected or other irregularities in the handling of the Customer's data. The Contractor shall remedy these immediately.

5.5.3 Subcontractor

Subcontractors are selected on the basis of defined due diligence criteria and safety measures. Necessary agreements on order processing or EU standard contract clauses are made. The right to issue instructions is defined in writing. In case of suspicion, the subcontractor is informed, and the level of protection and data destruction is checked by 360dialog.

Attachment

Partners and interfaces

The following interfaces can be used in the respective context. Further details are defined and documented on a project-specific basis.

1 Message Gateways

Message Gateways deliver messages via the respective data processors:

- WhatsApp Ireland Limited, 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland

Security concept:
https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf

2 Issue Tracking

Product development, maintenance, incidents, configuration settings, data management tasks and changes to users and rights are documented via an issue tracking system.

- Atlassian Pty Ltd, c/o Atlassian, Inc., 350 Bush Street, San Francisco, CA 94104, USA

3 Hosting

Commissioned computer centers (at the time of printing of this document) are

1. Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland
2. Amazon Web Services EMEA SARL, avenue John F. Kennedy, L-1855, Luxembourg

Appendix DPA3

360dialog GmbH Sub-Processors

Company/ Sub-Processor	Relevant for Product			Service provided/Scope
	WABA	Campaigns	Insights	
Adyen N.V.	x	x		SaaS for financial and payment services.
Amazon Web Services EMEA SARL	x	x	x	Data Center/Hosting at AWS Frankfurt. No personally identifiable data. See Terms & Conditions.
Atlassian Pty Ltd	x		x	Issue Tracking Personally identifiable information only if provided by the Controller in a support ticket and when it's required to troubleshoot.
Auth0® (Okta, Inc)	x			Identity & Access Management to 360dialog Hub.
Google Ireland Limited	x	x	x	GCP-Data Center/Hosting in Frankfurt, Email-/App-Provider used for communication with customers.
HubSpot, Inc.	x		x	Sales software. Personally identifiable information about partners (mostly company, contract and contact data).
Intercom R&D Unlimited Company	x	x		Customer Support, Issue Tracking. Data hosted at AWS.
Mixpanel, Inc.	x			Product analytics. Personally identifiable information about users. Needs to be opted in via accepting analytics cookie (click).
OpenReplay	x			Screen recording of the user during the session, to facilitate trouble shooting for the Customer Support and the client or partner. Only with the user's consent.
PandaDoc, Inc.	x			Contract management system for customers of 360dialog. Personally identifiable information about contract recipients.
Rockset, Inc.			x	Serverless SQL analytics engine, providing real-time analytics on diverse datasets with a seamless, serverless architecture, empowering DPAs to derive actionable insights efficiently (with native SQL query support, automated indexing, and unified data access)
Stripe Payments Europe, Ltd.	x	x		Payment services.

Company/ Sub-Processor	Relevant for Product			Service provided/Scope
	WABA	Campaigns	Insights	
Twilio Ireland Limited (SendGrid)	x			Cloud-based SMTP provider, Manages technical details from scaling of the infrastructure to ISP outreach and reputation monitoring to whitelist services and real time analytics
Userpilot, Inc.	x			Improvement and testing of the current user experience of the product. Data hosted at AWS.
Zoho Corporation B.V.	x	x		CRM, contract and invoice management system for customers of 360dialog. Personally identifiable information about invoice and contract recipients.

Appendix DPA4

Technical and administrative contact for Controller:

support@360dialog.com
+49 30 609 859 530

Data Protection Officer:

René Rautenberg,
ER Secure GmbH
In der Knackenau 4,
82031 Grünwald, Germany
+49.89.55294870,
info@er-secure.de