

Data Processing Agreement

Online Platform

15 June 2026 – Version 1.24

Data Processing Agreement for Personal Data in the Dialog Online platform

This Data Processing Agreement applies to Personal Data and business-sensitive information stored in the Dialog Online platform. The Online platform is a product of Dialog B.V. (hereinafter: Dialog). Dialog, registered with the Chamber of Commerce under number 84510722, is represented by Ruben Mink. In this Data Processing Agreement, Dialog is the Processor. The organisation with which Dialog has concluded an Agreement for the use of the Online platform is the Controller. In this Data Processing Agreement, the Controller is the following organisation:

Organisation name: _____

Established in: _____

Represented by: _____

1. What means what

We think it is important that we understand the same thing by the terms in this Data Processing Agreement. These have the meaning as included in the General Data Protection Regulation (GDPR).

A. Personal Data: All information about an identified or identifiable natural person ("the data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Where this Data Processing Agreement refers to Personal Data, all categories are meant as included in Dialog's Privacy policy (2.6) and Appendix 1 of this Data Processing Agreement, that fall under the definition of Personal Data of article 4(1) of the GDPR.

B. Processing: We speak of Processing when we record, modify, collect, organise, structure, store, update, retrieve, consult, use, provide by means of transmission, dissemination or otherwise making available, align or combine, restrict, erase or destroy Personal Data.

C. Controller: This is the organisation identified above and also the client.

D. Processor: This is Dialog as builder and manager of the Online platform. Dialog Processes Personal Data on behalf of the Controller.

E. Subprocessor: Another Processor, including but not limited to group companies, sister companies, subsidiaries and auxiliary suppliers, that the Processor engages to support the performance of the Agreement.

F. Data Subjects: These are living, natural persons whose Personal Data is processed in the Online platform. In this case these are the employees of the Controller who will use the Online platform. In addition, external parties who give feedback to employees of the Controller, such as

customers, are also Data Subjects.

G. Agreement: By this we mean all arrangements made as agreed in the signed quotation for the use of the Online platform.

H. Data Protection Impact Assessment: This is the assessment carried out prior to a Processing, with the aim of mapping the effect of the intended processing activities on the protection of Personal Data, as referred to in article 35 of the GDPR.

I. Supervisory authority: This is the independent government body responsible for supervising compliance with the law in connection with the Processing of Personal Data. In the Netherlands this is the Dutch Data Protection Authority (Autoriteit Persoonsgegevens).

J. Online platform: By this we refer to Dialog's Online platform, found at <https://app.dialog.nl/>.

K. Data breach: This is a breach of the security of Personal Data that accidentally or unlawfully leads to the destruction, loss, alteration or unauthorised disclosure of, or unauthorised access to, transmitted, stored or otherwise processed data, as referred to in article 4(12) of the GDPR.

L. Parties: These are the Processor and Controller.

M. Data Processing Agreement: This agreement, including all appendices.

2. Term of the Data Processing Agreement

A. This Data Processing Agreement applies from the moment the Parties have signed it.

B. This Data Processing Agreement is part of the Agreement and applies for as long as the Agreement lasts.

C. When the Agreement ends, this Data Processing Agreement ends by operation of law.

D. This Data Processing Agreement cannot be terminated separately.

E. After termination of this Data Processing Agreement, the obligations for Dialog continue.

Such as reporting Data breaches to the Controller, where the Personal Data of Data Subjects is involved, providing cooperation to the Controller in checks carried out by the Supervisory authority and the duty of confidentiality.

3. Processing of Personal Data

A. Dialog Processes Personal Data exclusively on the instruction of the Controller and on the basis of its written instructions and for purposes as determined by the Controller. Dialog has no control over the Personal Data.

B. Dialog is the Processor of the Personal Data and undertakes, under the conditions of this Data Processing Agreement, to process Personal Data within the framework of the Agreement. The Controller will inform Dialog of the processing purposes insofar as these are not mentioned in the Agreement or in this Data Processing Agreement.

C. Dialog immediately informs the Controller if Dialog has reason to assume that Dialog can no longer comply with the Data Processing Agreement.

D. Dialog follows the instructions of the Controller and Dialog does not Process the Personal Data in any other way, unless the Controller gives Dialog prior written consent or instruction to do so.

E. Appendix 1 sets out which categories, type and with which processing purposes Personal Data is Processed by Dialog.

F. Dialog complies with laws and regulations, including the GDPR, and Processes the data in a proper, careful and transparent manner.

G. Dialog will, at the request of the Controller, provide all necessary cooperation to the

Controller to give effect to requests from data subjects for access, restriction of processing, data portability, correction or deletion, and/or the exercise of any other right of a data subject under Chapter III of the GDPR. If such requests are directed to Dialog, Dialog forwards these within 5 working days to the Controller (addressed to the primary contact person within the Controller). Dialog will not respond to such requests, or carry them out, without prior explicit written consent of the Controller.

H. When the Controller wishes to carry out a Data Protection Impact Assessment, Dialog provides free of charge all information that the Controller needs.

I. The Personal Data to be processed on the instruction of the Controller remains the property of the Controller and/or the relevant Data Subject(s).

J. The obligations of Dialog arising from this Data Processing Agreement also apply to those who process Personal Data under the authority of Dialog, including but not limited to employees, in the broadest sense of the word.

K. If Dialog believes that the instructions of the Controller are in conflict with applicable laws and regulations, Dialog informs the Controller of this immediately in writing or by email.

L. If a legal obligation requires Dialog to process Personal Data that is not in this Data Processing Agreement, Dialog informs the Controller about this as soon as possible, unless this is prohibited by or under the law.

M. Dialog keeps a record of the processing activities carried out for the Controller, which meets the requirements that the GDPR sets for this, unless the exception of article 30(5) GDPR applies.

N. Dialog ensures that the Controller always has access to the Personal Data and is not entitled to deny the Controller this access, not even if a dispute between Parties were to arise or in a situation of suspension of payments or bankruptcy.

O. Dialog may process Personal Data about users and the use of the service by the Controller when this is necessary to obtain feedback and improve the service. The Controller grants the Processor the right to use and analyse aggregated data about system activities in connection with your use of the Services for the purpose of optimising, improving or expanding the way in which we provide our Services and to enable us to create new features and functionality in connection with the Services. Dialog is considered the controller for such processing and the processing is therefore not subject to this Agreement.

P. When using the service, the Controller will add data to the Software ("Customer Data"). The Controller acknowledges and has no objection to Dialog using the Customer Data in an aggregated and anonymised format for improving the services delivered to customers, research, training, educational and/or statistical purposes.

4. Subprocessors of the Online platform

Dialog works together with other organisations to make the Online platform possible. Think of the organisation that hosts our servers, or the party that sends automated emails to users of the Online platform on our behalf. We call these organisations Subprocessors.

A. Dialog only works together with Subprocessors with which Dialog has concluded a Data Processing Agreement. Appendix 2 contains an overview of these Subprocessors.

B. When Dialog engages other organisations as Subprocessor, Dialog enters into a written agreement with these Subprocessors, in which the Subprocessor, in particular with regard to security and the reporting of data breaches, meets at least the requirements included in this Data Processing Agreement.

- C. When Dialog starts working together with new Subprocessors for the functioning of the Online platform, Dialog will inform the Controller of this proactively, at least 30 days prior to new Processing with the new Subprocessor, in writing.
- D. If the Controller has reasonable grounds to object to the use of new or more Subprocessors, the Controller will inform Dialog of this immediately in writing, but within 14 days of first becoming aware.
- E. If Dialog and the Controller do not reach agreement on working together with the new Subprocessor, the Controller is entitled to terminate the Agreement and this Data Processing Agreement, observing a notice period of one (1) month.
- F. Personal Data is processed exclusively within the European Economic Area (EEA), unless the Controller has agreed in advance in writing to transfer to countries outside the EEA and one of the measures that ensure an adequate level of protection for this Personal Data has been provided.
- G. Dialog remains at all times fully responsible and liable for the fulfilment of its obligations under this Data Processing Agreement.

5. Securing Personal Data and audits

- A. Dialog ensures that Personal Data is well secured and has, to this end, taken appropriate technical and organisational measures to guarantee a level of security appropriate to the risk in accordance with article 32 GDPR. These measures are described in Appendix 3.
- B. In assessing the appropriate level of security, Dialog takes into account the state of the art, the costs of implementation, as well as the nature, scope, context and processing purposes and the risks of varying likelihood and severity for the rights and freedoms of persons, in particular as a result of the destruction, loss, alteration or unauthorised disclosure of, or unauthorised access to, transmitted, stored or otherwise processed data, whether accidentally or unlawfully.
- C. When the Controller believes that Dialog should make a change to the security measures, Parties consult together whether, how and within what term we are going to realise this.
- D. The Controller can check at most once a year whether the Processor complies with this Agreement. If the legislation applicable to the Controller so requires, the Controller can request more frequent audits. To request an audit, the Controller must submit to Dialog a detailed audit plan at least four weeks before the proposed audit date, describing the proposed scope, duration and start date of the audit. If a third party must carry out the audit, this must be agreed in writing mutually between the parties. However, if the processing environment is a “multitenant” environment or a similar environment, the controller gives the Processor the authority to decide, for security reasons, that the audits are carried out by a neutral third-party auditor of the Processor's choice.
- E. If the requested scope of the audit is covered in an ISAE, ISO or comparable assurance report carried out by a qualified third-party auditor within the preceding twelve months, and Dialog confirms that there are no known material changes in the audited measures, the Controller agrees to accept those findings instead of requesting a new audit of the measures to which the report relates.
- F. In any case, the audits must be carried out during ordinary office hours at the relevant location, observing the processor's policy, and they may not unreasonably hinder the processor's business activities.
- G. The Controller is responsible for all costs arising from the checks requested by the Controller. Costs may be charged for requests for assistance from Dialog.

H. If the Supervisory authority or another authority starts an investigation at Dialog or a Subprocessor, Dialog informs the Controller about this immediately in writing or by email. Parties will, in joint consultation, provide their cooperation in the investigation.

6. Confidentiality

A. Dialog keeps the provided Personal Data of the Controller strictly secret, unless this is not possible on the basis of a legal obligation. The same applies to all other information that Dialog is or becomes aware of by virtue of this Data Processing Agreement.

B. Dialog ensures that its personnel and external parties with whom it works also adhere to this confidentiality, by including a confidentiality obligation in the (employment) contracts. Dialog ensures that these persons only gain access if and insofar as that is necessary for the performance of the Agreement.

7. Data breaches

A. In the event of the discovery of a possible Data breach, Dialog informs the Controller about this without unreasonable delay and at the latest within 48 hours, and provides the Controller with all relevant information about it, as appears from the most recent data breach form of the Dutch Data Protection Authority, which in any case includes:

1. The nature of the Data breach, where possible stating the categories of data subjects and personal data records concerned and, approximately, the number of data subjects and personal data records concerned;
2. The name and contact details of the contact point at Dialog where more information can be obtained;
3. The likely consequences of the Data breach;
4. The measures that Dialog has proposed or taken to address the Data breach, including, where appropriate, the measures to mitigate its possible adverse consequences.

B. Dialog guarantees that the information provided, insofar as known to Dialog at that moment, is complete, correct and accurate.

C. After the report of a Data breach, Dialog keeps the Controller informed of new developments around the Data breach and the measures that Dialog has taken to limit and end the scope of the Data breach and to be able to prevent a similar incident in the future.

D. Dialog is not permitted to make a report of a Data breach to the Supervisory authority. In addition, Dialog may not inform the Data Subjects about the Data breach. This is the responsibility of the Controller. If the Controller must make such a report, Dialog provides all reasonable assistance to enable the Controller to make this report(s) within the legal deadlines set for it.

E. Any costs incurred to resolve the Data breach and to be able to prevent it in the future are for the account of the party to whom the data breach is attributable.

F. The Controller only assigns roles and rights in Dialog to Data Subjects who need this for the performance of their function. Access thereby remains limited and the chance of a Data breach is thereby reduced.

G. Dialog keeps a log of Data breaches and information security incidents. Per Data breach or incident, it is recorded which measures have been taken. This log can be found in the Privacy policy.

H. Dialog has set up adequate policy and procedures to:

1. Detect Data breaches at the earliest possible stage;
2. Inform the Controller about a Data breach in accordance with article 7.A;
3. Respond adequately and immediately to a Data breach;
4. Prevent or limit (further) unauthorised access, alteration, and disclosure or otherwise unlawful Processing and to prevent recurrence of this.

I. At the request of the Controller, Dialog provides information about and access to this policy set up by the Processor and these procedures set up by the Processor.

8. Destruction of Personal Data & retention period

A. Thirty days after the termination of the Agreement, Dialog destroys all information linked to the Controller. The information that is deleted in any case includes Personal Data of Data Subjects and business-sensitive information, such as organisation and team objectives, of the Controller.

B. The Controller receives, prior to the destruction referred to in 8.A, if desired a complete copy of all Personal Data by means of a secure file transfer in the format communicated by the Controller to Dialog. At the request of the Controller, Dialog temporarily continues its activities at the end of the Data Processing Agreement under the same conditions, in order to facilitate a possible transfer of the data processing to the Controller.

C. When a request for destruction by a Data Subject comes in to Dialog's support team, Dialog will forward it to the contact person of the Controller.

D. When an employee of the Controller leaves employment, it is the responsibility of the Controller to revoke this employee's rights to the Online platform. In addition, the Controller will make the request to Dialog to delete or transfer the Personal Data of the relevant employee. The same applies to all Data Subjects who leave the employment of the Controller.

E. After the destruction of the Personal Data, Dialog declares in writing to the Controller that Dialog no longer has the Personal Data.

F. The Controller is entitled to engage an independent third party who will verify whether the Personal Data has been completely destroyed. The costs of this will be entirely for the account of the Controller. The results of this investigation will be shared in writing with the Parties by this third party.

G. Dialog ensures that Subprocessors comply with what is stipulated in article 8 of this Data Processing Agreement.

9. Liability

A. To avoid misunderstandings, Parties hereby agree and acknowledge that each Party will be liable and responsible for the payment of administrative fines and compensation to Data Subjects if this payment obligation has been imposed on this Party by the relevant data protection authority or a competent court in accordance with applicable law. Liability issues between the Parties will be governed by the relevant provisions concerning liability as agreed in the Agreement.

10. Final provisions

A. This Data Processing Agreement is part of the Agreement. All rights and obligations from the Agreement therefore also apply to this Data Processing Agreement.

- B. The Controller has the right to periodically evaluate this Data Processing Agreement with the Processor. The Controller takes the initiative for this itself.
- C. This Agreement takes precedence over conflicting provisions regarding the Processing of Personal Data in the Services Agreement or in other earlier agreements or written communication between the Parties.
- D. Deviations from this Data Processing Agreement are only valid when Parties agree this together in writing.
- E. Dutch law applies to this Data Processing Agreement.
- F. Any disputes between Parties are determined by the court in the district of Midden-Nederland, location Utrecht.
- G. The Processor may not transfer the rights and obligations from this Data Processing Agreement to a third party, without written consent of the Controller.

-- sign on the next page --

Thus agreed and signed by us:

Controller:

Signed for and on behalf of: _____

Name: _____

Position: _____

Date and place: _____

Signature: _____

Processor:

Signed for and on behalf of: Dialog B.V.

Name: Ruben Mink

Position: Managing Director

Date and place: _____, Utrecht

Signature: _____

Appendix 1

This appendix sets out which categories and with which processing purposes Data is Processed by Dialog.

We make the distinction into three types of Data: Personal data, Organisation-Specific Information and User information.

Personal data

Category	Description
Name	The full name of the End user.
E-mail address	(Work) email address of the End user.
Phone number	(Work) phone number of the End user (optional).
IP address	The IP address of the End user's device.
Gender	The gender of the End user (optional).
Date of birth	The date of birth of the End user (optional).

User and organisation-specific information

User and organisation-specific information is only processed within the modules that are used by the Controller.

General

The following information is processed in all modules.

Category	Type	Description
Job title	User	This is the job title linked to the End user in the Online platform.
Organisation structure	Organisation	Overview of the organisation structure. Comparable to an org chart.
Job profiles	Organisation	The job titles and associated profiles.
Usage data	User	Non-substantive data about the use of the Dialog Online platform. Think for example of how often someone logs in, requests feedback or reflects. With this we can, among other things, send more relevant messages to End users.
Start date of employment	User	The date on which the End user joined the company.

Performance

The following information is only processed if the Performance module is used.

Category	Type	Description
Performance objectives	User	Name and description of the End user's performance goals. This can be linked to the organisation or team goals to which these objectives contribute.
Development objectives	User	Name and description of the End user's development goals. This can be linked to a competency or core value.
Evaluations	User	Written reflections and evaluations by and about the End user.
Feedback	User	Written feedback that the End user has received and given in the Online platform.
Private notes	User	Employees, Managers and Administrators can keep private notes on End users in the Online platform.
Organisation and team objectives	Organisation	Description of the organisation and team objectives.
Core values and competencies	Organisation	Description of the core values, job-specific and team-specific competencies.
Evaluation cycle	Organisation	Information about the

		organisation's evaluation cycle.
Discussion points 1:1	User	Discussion points that Managers and Employees can record in the platform.

Engagement

The following information is only processed if the Engagement module is used.

Category	Type	Description
Answers	User	End users can answer questions from which the engagement of the end user on various themes is measured.
Themes & Questions	Organisation	The organisation can add themes and questions about which employees receive questions.

Talent

The following information is only processed if the Talent module is used.

Category	Type	Description
Competencies	User	At what level various competencies are mastered by the End user.
Skills	User	At what level various skills are mastered by the End user.
Ambitions	User	The End user can mark job titles as an ambition.
Extended job profiles	Organisation	The Organisation can extend job profiles with information about skills and growth opportunities.

Data Subjects

Category	Description
Users	Employees of the Controller who will use the Online platform.
External feedback providers	External parties, such as customers, who give feedback to users.

Processing purposes

In the Online platform, Personal Data is Processed. Dialog Processes this Personal Data to enable employees and managers of the Controller to set and pursue clear goals in daily practice. In addition, it is possible to easily and specifically request and give feedback to others in the Online platform. With this we stimulate the continuous dialogue within organisations and we simplify the HR cycle. In addition, it is optionally possible to carry out engagement measurements. This purpose is in the explicit interest of the client that deploys the Online platform. This is the only purpose for which the Data is processed.

Duration of the Processing

Dialog Processes the Personal Data only for as long as the Agreement between Parties is valid or the retention period as described in Article 8 of this Data Processing Agreement has not yet expired.

Contact details Dialog

Dialog B.V.
Weg der Verenigde Naties 1
3527 KT, Utrecht
support@dialog.nl
030-7600290

Appendix 2

This appendix sets out with which Subprocessors Dialog works together, which function the cooperation with these Subprocessors has, which categories of Personal Data the Subprocessors receive and where these Subprocessors store their data.

Function of Subprocessors

Dialog works together with Subprocessors to make the Online platform possible. Think of the organisation that hosts the servers or the party that sends automated emails to Data Subjects. We call these organisations Subprocessors.

Subprocessors only receive the data they need to perform their function.

Category	Subprocessor name	Explanation
Server and database hosting	Microsoft Azure	Microsoft Azure hosts the servers and databases of the Online platform.
Database backup storage	Amazon.com Inc.	Automatically created, encrypted backups of the production database are stored at Amazon Web Services (AWS).
Customer service tickets*	Zendesk Inc.	The Online platform displays a 'Help' widget. Via this widget you can access the Help Centre. This Help Centre contains articles with frequently asked questions about using the platform. In addition, the widget offers the option to send a message to Dialog's Support team.
Messages	Copernica BV	The online platform sends fully automated emails to End users. Via Copernica BV these emails are distributed from the Online platform to the End user.
SMS	ONLINECITY.IO ApS	The Online platform sends a registration SMS message if users have no email but do have a mobile phone number. ONLINECITY.IO sends this message to the End user.

Documents	Amazon.com Inc.	Users can upload documents in the Online platform. These are stored at Amazon Web Services (AWS).
Messages	Customer.io (Peaberry Software Inc.)	The online platform sends fully automated messages to End users. Via Customer.io, workflows are set up to send messages at the right moments. In addition, transactional messages such as "Register now" or "Forgot password" are sent.
LLM / AI	Lleverage B.V.	Users can use AI functionalities to receive suggestions about content for the platform and to chat with an AI assistant.
AI	Microsoft Azure	Users can use AI functionalities to summarise content in Dialog and receive suggestions. For this we use tooling from Microsoft: Microsoft Agent Framework.

* Personal data is only sent to Zendesk Inc. after sending a question to Dialog's support team via the support widget in the Online platform, or after sending an email to support@dialog.nl. Zendesk's support widget places four cookies that cannot be traced back to the person in a user's browser. More information about these cookies in Dialog's Security policy.

Categories of Personal Data per Subprocessor

Subprocessors only receive Data they need to perform their function. If a Subprocessor does not need the Data, then the Subprocessor does not receive the Data.

Category	Microsoft Azure	Amazon.com Inc.	Zendesk Inc.	Copernica BV	ONLINECITY.IO	Customer.io	Lleverage B.V.
Personal data							
Name	Yes	Yes*	Yes**	Yes	Yes***	Yes	Yes
E-mail address	Yes	Yes*	Yes**	Yes	No	Yes	No
Phone number	Yes***	Yes*	No	No	Yes***	Yes***	No
IP address	Yes	Yes*	No	Yes	No	Yes	Yes
Gender	Yes****	Yes*	No	No	No	No	No
Date of birth	Yes****	Yes*	No	No	No	No	No
General							
Job title	Yes	Yes*	No	No	No	Yes	Yes
Organisation	Yes	Yes*	No	No	No	No	Yes

n structure							
Job profiles	Yes	Yes*	No	No	No	No	Yes
Usage data	Yes	Yes*	No	No	No	Yes	No
Start date of employment	Yes****	Yes****	No	No	No	No	Yes****
Performance							
Performance objectives	Yes	Yes*	No	Yes	No	Yes	Yes
Development objectives	Yes	Yes*	No	Yes	No	Yes	Yes
Evaluations	Yes	Yes*	No	No	No	No	Yes
Feedback	Yes	Yes*	No	Yes	No	Yes	Yes
Private notes	Yes	Yes*	No	No	No	No	Yes
Organisation and team objectives	Yes	Yes*	No	Yes	No	Yes	Yes
Core values and competencies	Yes	Yes*	No	Yes	No	Yes	Yes
Evaluation cycle	Yes	Yes*	No	Yes	No	Yes	Yes
Engagement							
Answers	Yes	Yes*	No	No	No	No	Yes
Themes & Questions	Yes	Yes*	No	No	No	Yes	Yes
Talent							
Competencies	Yes	Yes*	No	No	No	No	Yes
Skills	Yes	Yes*	No	No	No	No	Yes
Ambitions	Yes	Yes*	No	No	No	No	Yes
Extended job profiles	Yes	Yes*	No	No	No	No	Yes

When an end user sends a message or question via the support widget in the Online platform, the message or question is also sent to Zendesk.

* Backups of the production database of the Online platform are stored encrypted at AWS services of Amazon.com Inc. More information about this can be found in Dialog's Security policy.

** Data is only sent to Zendesk Inc. after sending a question to Dialog's support team via the

support widget in the Online platform, or after sending an email to support@dialog.nl. Zendesk's support widget places four cookies that cannot be traced back to the person in a user's browser. More information about these cookies can be found in Dialog's Security policy.

*** Phone number is an optional data field that is only used for sending a registration SMS message. This only happens if the employee has no email address.

**** Only processed if this option is activated by the Processor.

Locations of Subprocessors

Subprocessor name	Head office location	Data centre location	Data centre within the EU?
Microsoft Azure	United States	Netherlands	Yes
Amazon.com Inc.	United States	Germany	Yes
Zendesk Inc.	United States	Germany	Yes
Copernica BV	Netherlands	Netherlands	Yes
ONLINECITY.IO	Denmark	Belgium	Yes
Customer.io	United States	Belgium	Yes
Lleverage B.V.	Netherlands	Europe	Yes

Appendix 3: Measures

Dialog has taken appropriate technical and organisational measures in the context of the security of the Processing.

Security policy

The measures that Dialog has taken are described in the following document:

- Dialog - Security policy

NEN-EN-ISO/IEC 27001:2023 en

Dialog is certified in accordance with the NEN-EN-ISO/IEC 27001:2023 en standard. For this, reference is made to the following documents:

- DigiTrust UK Certificate ISO 27001 Dialog B.V.pdf
- Statement of Applicability - Dialog 2.0 (April 23rd, 2024) ISO27001_2023