



# Privacy Policy

## Introduction

On the Online platform from Dialog Data is stored. As the developer of Dialog, Dialog B.V. (hereinafter: Dialog) takes the protection of the Data and privacy of customers, clients and other data subjects seriously. We have taken several organisational and technical measures to ensure this.

We comply with the latest legislation on privacy and personal data protection, including the European Commission's Decision 2016/679, the GDPR/GDPR guidelines, and the guidelines of Decision 95/46/EC of the European Commission.

## Definitions

Firstly, we'd like to explain to you what we mean by the following terms.

## Parties

**Dialog:** Dialog B.V. (Chamber of Commerce registration number 84510722) is the name of the company that designed, developed and maintains the Online platform.

**Online platform:** The Online platform Dialog that is available at <https://app.dialog.nl/>.

**Clients:** The organisations that purchase the Online platform licences or additional services from Dialog.

**End User:** The employees working for the Controller who use or will use the Online platform.

**Manager:** The managing officers of End Users.

**Administrator:** The persons at the Controller who are responsible for the administration of the Online platform.

**Data Subjects:** Natural persons whose Data are Processed in the Online platform. In this case, these are the End Users, Managers and Administrators of the Controller who will use the Online platform. In addition, external parties who provide feedback to End Users, such as customers, are also Data Subjects.

## Data

**Personal Data:** Data that can be traced back to a natural person and relate to the person.

**User information:** Information that an End User enters in the Online platform. Examples include business and development objectives, feedback received and given, and written evaluations.

**Organisation-specific Information:** Information about the structure of an organisation, objectives of the team and the organisation, core values and competencies and information on the assessment cycle.

**Data:** The collective name for Personal Data, Organisation-specific Information and User Information.

## GDPR terminology

**Processing:** To record, modify, collect, organise, structure, store, update, retrieve, consult, use, provide by means of transmission, distribute or otherwise make available, align, combine, restrict, erase or destruct Data.

**Controller:** The organisation that instructs Dialog to Process Data.

**Processor:** Dialog Processes Data on the Controller's instructions and is therefore the Processor.

**Sub-processor:** A party that Processes Data on behalf of Dialog for the Controller.

**Supervisory Authority:** The independent public authority responsible for the supervision of compliance with the law in connection with the Processing of Data. In the Netherlands, this is the Dutch Data Protection Authority.

**Data Breach:** A security breach regarding Data resulting in adverse consequences, or a risk of adverse consequences, for the protection of Data.

## Documentation

**Privacy Policy:** This extensive document sets out our working methods on how we handle Data.

**Privacy Notice:** In this document, we point out to all End Users who use or will use the Online platform what their rights are and how we Process their Data.

**Security Policy:** This document explains the technical measures we have taken to safeguard the security of Data in the Online platform.

**Cookie Policy:** This document explains how we use cookies on the Online platform.

**Service Level Agreement (SLA):** This document sets out our working arrangements regarding our services, including our support and release policy.

# Contents

<b>Definitions</b>	<b>2</b>
Parties	2
Data	2
GDPR terminology	3
Documentation	3
<b>Contents</b>	<b>4</b>
<b>1. Basis, origin and rights</b>	<b>6</b>
1.1 The basis for Processing	6
1.2 Origin of Data	6
1.3 Controller's Rights	7
1.4 Rights of Data Subjects	9
1.5 Pointing out rights	10
1.5.1 Controller	10
1.5.2 Data subjects	10
<b>2. Register of Processing activities</b>	<b>13</b>
2.1 Name and contact details of Dialog	13
2.2 Data Protection Officer (DPO)	13
2.3 Lead supervisory authority	13
2.4 Purpose of Data Processing	13
2.5 Categories of Data Subjects regarding whom Data is Processed	14
2.6 Categories of Data	14
2.6.1 Personal data	14
2.6.2 User information	15
2.6.3 Organisation-specific information	16
2.6.4 Non-Personally identifiable Data	16
2.7 Function of Sub-processors	16
2.8 Location of Sub-processors	17
2.9 Categories of Data per Sub-processor	18
2.10 Overview of Processing Agreements with Sub-processors	19
2.11 Agreements regarding deletion of Data	19
2.12 Organisational and security measures	20
<b>3. Testing and analyses</b>	<b>21</b>

<b>4. Privacy by design &amp; privacy by default</b>	<b>22</b>
4.1 Privacy by design	22
4.2 Privacy by default	22
<b>5. Data breaches</b>	<b>24</b>
5.1 Protocol	24
5.2 Register of data breaches	24

# 1. Basis, origin and rights

## 1.1 The basis for Processing

In order to Process Data from Data Subjects under the GDPR, a basis is needed to be able to do so (Articles 15 up to and including 22 GDPR). Dialog makes use of two of the following principles: the contract with the Controller for which the Data Subject works, and the individual consent of the Data Subject.

### Contract with Controller

The Online platform contains data that is important for the Controller who uses the Online platform. This includes, inter alia, organisational, team and individual objectives, development plans, agreements made, meeting updates and other data important for the implementation of the HR and development cycle of the Controller for whom a Data Subject works. Dialog does not ask Data Subjects for permission to use their Data for the purposes described above.

### Consent of Data Subjects

When the Online platform does collect Data from a Data Subject, but it does not fall under the contract with the Controller where the Data Subject works, specific consent of the Data Subject is always requested.

The Data Subject always indicates whether Dialog may use the Data to analyse their behaviour in the Online platform or to improve functionalities on the platform.

Dialog is the Controller of the aggregate anonymised information made available in Google Analytics.

## 1.2 Origin of Data

When the Controller starts using the Online platform, it is customary for Dialog to take care of the initial set-up on the instructions of the Controller. The Controller then provides all the information needed to set up the Online platform. This information consists, inter alia, of:

- Names and email addresses of employees
- Names of teams and their connections to other teams
- Link between employees and the teams they form part of
- Names of managers of employees
- Organisation and team objectives
- Competence models

All information added to the Online platform after the initial setup will be added manually by the Administrators of the Controller, by End Users, or by Dialog on the Controller's instructions.

### 1.3 Controller's Rights

Rights	Interpretation of the law
Right to data portability	The Controller may at any time send a request to <a href="mailto:support@dialog.nl">support@dialog.nl</a> to obtain information from the Online platform in Excel format.
Right to be forgotten	<p>The Controller may send a request to have one or more Data Subjects, teams or all Data erased.</p> <p>Dialog erases the Data after expiry of a period of thirty days after the request to do so.</p> <p>This thirty-day delay is for the purpose of reducing the risk of accidentally erasing Data. Within these thirty days we can still retrieve Data.</p> <p>As soon as Dialog has erased the Data, Dialog will send an email about this to the Administrators of the Controller.</p>
Right of access	<p>Administrators are given the rights they need to see all Data that we store on behalf of the Controller. They can do this directly on the Online platform.</p> <p>Should there be any additional questions regarding access to Data, the Administrators can address their questions to <a href="mailto:support@dialog.nl">support@dialog.nl</a>.</p>
Right to rectification and supplementation	<p>The Controller may at any time send a request to <a href="mailto:support@dialog.nl">support@dialog.nl</a> to rectify or supplement Data in the Online platform.</p> <p>Depending on the technical consequences of the rectification or supplementation, we decide how and when Dialog will implement this. We will record the arrangements made in this respect in an email.</p>
Right to restriction of processing	<p>The Controller may at any time send a request to <a href="mailto:support@dialog.nl">support@dialog.nl</a> to restrict the Processing of Data in the Online platform.</p> <p>Depending on the technical consequences of the rectification or supplementation, we decide how and when Dialog will implement this. We will record the arrangements made in this respect in an email.</p>
Right to automated decision-making and profiling	Dialog does not Process Data for the purpose of automated decision-making or profiling.



Right to object to data processing	<p>The Controller may send an email to <a href="mailto:support@dialog.nl">support@dialog.nl</a> containing an objection to specific data processing.</p> <p>Dialog will then consult with the Controller to find a way of dealing with this objection. We will record the arrangements made in this respect in an email.</p>
------------------------------------	--

In addition, the Controller always has the right to file a complaint with the Dutch Data Protection Authority. This can be done on the website [www.autoriteitpersoonsgegevens.nl](http://www.autoriteitpersoonsgegevens.nl).

## 1.4 Rights of Data Subjects

Data subjects have the following rights under the GDPR. The text is directed at the Data Subjects and comes directly from the Dialog Privacy Statement.

<b>Rights</b>	<b>Interpretation of the law</b>
Right to Data portability	You can always send a request to <a href="mailto:support@dialog.nl">support@dialog.nl</a> to obtain information from the Online platform in Excel format.
Right to be forgotten	It is in your organisation's interest that Data concerning you remain intact in the Online platform. You cannot therefore explicitly ask to be forgotten, unless it is no longer in the Controller's interest that your Data is still being Processed.
Right of access	As a user, you can ask us at any time which Data we Process. Feel free to send us a request by email to <a href="mailto:support@dialog.nl">support@dialog.nl</a> .
Right to rectification and supplementation	As a user, you can ask us at any time whether we can rectify or supplement Data. We will always do so in consultation with your organisation if we suspect that the addition will compromise the intact state of the Data.
Right to restriction of Processing	As a user, you may send us a request to restrict the Processing we carry out. Please send this request to <a href="mailto:support@dialog.nl">support@dialog.nl</a> . We will then consult with the organisation you work for to see if this is possible and when we can do it.
Right regarding automated decision-making and profiling	No Data is Processed for the purpose of automated decision-making or profiling purposes.
Right to object to data processing	You can send an objection email to <a href="mailto:support@dialog.nl">support@dialog.nl</a> requesting us to Process less Data. Dialog will investigate with the Controller whether there is a way to limit the Processing of specific Data.

In addition to the above rights, you always have the right to lodge a complaint with the Dutch Data Protection Authority. You can do this on the website [www.autoriteitpersoonsgegevens.nl](http://www.autoriteitpersoonsgegevens.nl).

## 1.5 Pointing out rights

### 1.5.1 Controller

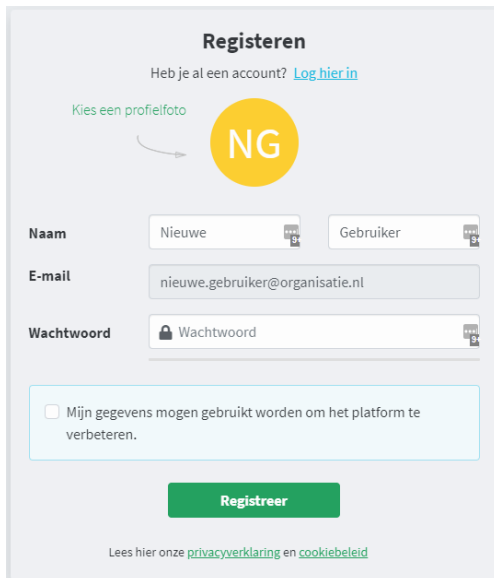
Dialog alerts the Controller who will use the Online platform by means of this Privacy Policy to its privacy rights.

The most recent version of this Privacy Policy can be found at <https://www.dialog.nl/voorwaarden>. The password for this page can be requested from your organisation's primary contact person or via [support@dialog.nl](mailto:support@dialog.nl).

### 1.5.2 Data subjects

Dialog points out to Data Subjects who use or will use the Online platform what their rights are and how Data is used in the Privacy Statement. This Privacy Statement can be found in several places on the platform:

End users see the Privacy Statement during the registration of their account in the Online platform.



The screenshot shows a registration form titled "Registeren". At the top, it asks "Heb je al een account?" with a link "Log hier in". Below this is a section for profile picture selection, labeled "Kies een profielfoto", with a yellow circular placeholder containing the letters "NG". The form contains several input fields: "Naam" with two sub-fields "Nieuwe" and "Gebruiker", "E-mail" with the value "nieuwe.gebruiker@organisatie.nl", and "Wachtwoord" with a lock icon. A checkbox is present with the text "Mijn gegevens mogen gebruikt worden om het platform te verbeteren." Below the form is a green "Registreer" button. At the bottom, there is a link: "Lees hier onze [privacyverklaring](#) en [cookiebeleid](#)".

If a Single Sign-on (SSO) is used, the Privacy Notice is shown after the first successful login.

## Privacy voorkeuren

Voordat je Dialog kunt gaan gebruiken, vragen we je eerst onze privacyverklaring en cookiebeleid te lezen. Daarnaast vragen we je om ons toestemming te geven voor het gebruik van jouw gegevens ter verbetering van het platform. Dit is uiteraard niet verplicht, maar het helpt ons enorm met de doorontwikkeling van het platform.

Mijn gegevens mogen gebruikt worden om het platform te verbeteren.

Lees hier onze [privacyverklaring](#) en [cookiebeleid](#)

**Opstaan**

After completion of the registration, the Privacy Notice is always available at the Account page.

### Privacy


Wij vinden jouw privacy enorm belangrijk. Daarom heb je continu zelf de controle over jouw gegevens. Hier kun je jouw voorkeuren wijzigen.

Mijn gegevens mogen gebruikt worden om het platform te verbeteren.

Lees hier onze [privacyverklaring](#) en [cookiebeleid](#)

**Opstaan**

External feedback visitors will be given a link to the Privacy Statement on the page where they can fill in feedback.

 **Feedbackverzoek van Serge Bekenkamp**


"Hoi Jesse, wil je mij feedback geven op deze doelen en competenties? Alvast bedankt."

Heb je nog aanvullende feedback? \_\_\_\_\_

Schrijf hier jouw feedback...

**Versturen**

Serge bepaalt zelf of de feedback wordt gedeeld met managers of collega's

 **Dialog**

Lees hier onze [privacyverklaring](#) en [cookiebeleid](#)

On the basis of the Right to Information (Articles 13 and 14 GDPR), Dialog only has an obligation to provide information to Data Subjects in order to clearly inform them of how we Process their Data. For this reason, End Users do not need to agree to the Privacy Statement.

The Privacy Notice is available in both Dutch and English.

The platform always displays the most recent Privacy Statement.

## 2. Register of Processing activities

### 2.1 Name and contact details of Dialog

<b>Name of organisation:</b>	Dialog B.V.
<b>Address:</b>	Ondiep-Zuidzijde 6
<b>Postcode:</b>	3551BW Utrecht
<b>Country:</b>	The Netherlands
<b>Chamber of Commerce no.:</b>	84510722
<b>Telephone number:</b>	+ 31 30 7600 290
<b>Email address:</b>	<a href="mailto:support@dialog.nl">support@dialog.nl</a>
<b>Website:</b>	<a href="http://www.dialog.nl">www.dialog.nl</a>

### 2.2 Data Protection Officer (DPO)

Dialog does not have a Data Protection Officer (DPO). Pursuant to Article 37 of the GDPR, there is no reason to appoint a DPO.

The role of Privacy Officer is not a full-time position within Dialog. The tasks and responsibilities are part of the position of the IT Manager.

All privacy-related questions relating to the Online platform can be sent directly to [support@dialog.nl](mailto:support@dialog.nl).

### 2.3 Lead supervisory authority

Dialog has no lead supervisory authority. The Online platform does not Process any cross-border Data in various EU Member States and does not do any Processing that has an impact in several Member States.

### 2.4 Purpose of Data Processing

In the Online platform, Data is processed on behalf of the Controller. Dialog Processes this Data to enable End Users and Managers of the Controller to set clear goals and pursue them in daily practice. The Online platform facilitates targeted and simple questions and feedback. In doing so, we encourage continuous dialogue within organisations and simplify the HR cycle. The legal basis is the contract between Dialog and the Controller.

This is the only purpose for which the Data is processed.

## 2.5 Categories of Data Subjects regarding whom Data is Processed

### End users, Managers and Administrators

When End Users, Managers and Administrators use the Online platform, Data is Processed. In this way, new objectives are laid down, feedback is given to one another or assessments are recorded. These can all be traced back to an individual.

### Feedback providers

There are two categories of feedback providers: external and internal feedback providers.

External feedback providers are feedback providers outside the Controller's organisation. This external feedback provider does not have his or her own account for the Online platform, but enters a closed environment where he or she provides feedback to an End User, Manager or Administrator. He/she only has access to that which the End User, Manager or Administrator has requested feedback on. We only store the following data from external feedback providers:

- Email address (in order to be able to send the request and any follow-up on the feedback by email)
- Name (filled in by the external feedback provider himself/herself)
- Feedback given

Internal feedback providers are feedback providers within the Controller's organisation. These persons have their own account for the Online platform and any feedback given is linked to this account.

## 2.6 Categories of Data

We distinguish four types of Data: Personal Data, User Information, Organisation-specific Information, and Non-Personally Identifiable Data.

### 2.6.1 Personal data

Category	Description
Name	Full name of the Data Subject.
Email address	Work email address of the Data Subject.
Telephone number	Work phone number of the Data Subject. (Optional)

## 2.6.2 User information

Category	Description
Performance targets	Name and description of the substantive performance targets of the Data Subject. This may be linked to the organisational or team objectives to which these objectives contribute.
Development objectives	Name and description of the Data Subject's development objective. This may be linked to an organisation's competence or core value.
Evaluations	Written reflections, evaluations and assessments by or for the End User.
Feedback	Written feedback received by the Data Subject and given in the Online platform.
Private notes	Managers and Administrators can add private notes to the Data Subject in the Online platform.
Position	This is the position linked to the Data Subject in the Online platform.
Engagement	Data subjects can answer questions, which are used to measure the engagement of the Data subject.

When End Users, Managers and Administrators explicitly consent to the use of their Data to improve the Online platform, we may use the User Information above to improve the platform. We will then use this User Information to get a better idea of how users use the Online platform. In practice, it is rare for us to use this User Information and we prefer to use fictitious data, as set out in our Privacy by Design & Default.



### 2.6.3 Organisation-specific information

Category	Description
Organisation and team objectives	Description of the organisation and team objectives.
Core values and competences	Description of the core values, job-specific and team-specific competencies.
Organisational structure	Overview of the organisational structure. Comparable to an organisational chart.
Assessment cycle	Information on the organisation's assessment cycle.

### 2.6.4 Non-Personally identifiable Data

When End Users, Managers Officers and Administrators explicitly consent to the use of their Data to improve the Online platform, we also Process Non-Personally Identifiable Data. This Data helps us to get a better idea of how End Users use the Online platform.

### 2.7 Function of Sub-processors

Dialog works with Sub-processors to facilitate the Online platform. Examples include the party hosting the servers, or the party that sends automated emails to the Data Subjects. We refer to these organisations as Sub-processors.

Sub-processors receive only the data they need to perform their tasks.

Category	Name of Sub-processor	Explanation
Server and database hosting	TransIP BV	TransIP hosts the servers and databases for the Online platform.
Datebase backup storage	Amazon.com Inc.	Automatically generated, encrypted backups of the production database are stored at Amazon Web Services (AWS).
Customer service tickets	Zendesk Inc.	In the Online platform, a 'Help' widget is shown. Via this widget, the Help Centre can be called up with articles containing frequently asked questions about the use of the platform. In addition, the

		widget offers the possibility to send a message to the Dialog Support team.
Email automation service	SMTPeter BV	The Online platform sends fully automated emails to End Users. Via SMTPeter, these emails are distributed from the Online platform to the End User.
SMS	ONLINECITY.IO ApS	The Online platform sends a SMS-message with a registration link when users don't have access to an e-mail address. ONLINECITY.IO sends this message to the End User.
Platform optimisation*	Google LLC (Google Analytics)	Google Analytics collects (after explicit opt-in*) non-personally identifiable data about the use of the platform.
Documents	Amazon.com Inc.	Users can upload documents to the Online platform. The are stored at Amazon Web Services (AWS).

\* Information will only be sent to Google LLC (Google Analytics) with the explicit consent of the Data Subject prior to the Processing of this information.

\*\* Data will only be sent to Zendesk Inc. after sending a question to the Dialog Support team via the support widget in the Online platform, or after sending an email to [support@dialog.nl](mailto:support@dialog.nl). Zendesk's support widget places four non-personally identifiable cookies in a user's browser. More information about these cookies can be found in the Cookie Policy of Dialog.

## 2.8 Location of Sub-processors

Name of Sub-processor	Location of head office	Location of data centre	Data centre within the EU?
TransIP BV	The Netherlands	The Netherlands	Yes
Amazon.com Inc.	United States	Germany	Yes
Zendesk Inc.	United States	Germany	Yes
SMTPeter BV	The Netherlands	The Netherlands	Yes
ONLINECITY.IO	Denmark	Belgium	Yes

Google LLC (Google Analytics)	Ireland	Ireland	Yes
-------------------------------	---------	---------	-----

When Dialog starts working with new Sub-processors for the functioning of the Online platform, Dialog will proactively inform the Administrators of the Controller of this in writing at least 30 days prior to the first new Processing with the new Sub-processor.

## 2.9 Categories of Data per Sub-processor

Sub-processors receive only the Data they need to perform their task. If a Sub-processor does not need the Data, the Sub-processor will not receive the Data.

Category	TransIP BV	Amazon.com Inc.	Zendesk Inc.	SMTPeter	ONLINECITY. IO	Google LLC (Google Analytics)
Personal Data:						
Name	Yes	Yes*	Yes**	Yes	Yes***	No
Email address	Yes	Yes*	Yes**	Yes	No	No
Phonenumber	Yes	Yes*	No	No	Yes	No
User information:						
Substantive objectives	Yes	Yes*	No	Yes	No	No
Development objectives	Yes	Yes*	No	Yes	No	No
Evaluations	Yes	Yes*	No	No	No	No
Feedback	Yes	Yes*	No	Yes	No	No
Private notes	Yes	Yes*	No	No	No	No
Position	Yes	Yes*	No	No	No	No
Engagement	Yes	Yes*	No	No	No	No
Organisation-specific data						
Organisation and team objectives	Yes	Yes*	No	Yes	No	No
Core values and competences	Yes	Yes*	No	Yes	No	No
Organisational structure	Yes	Yes*	No	No	No	No

Assessment cycle	Yes	Yes*	No	Yes	No	No
------------------	-----	------	----	-----	----	----

\* Backups of the production database of the Online platform are stored in encrypted form with AWS services of Amazon.com Inc. For more information, see the Security Policy of Dialog.

\*\* Data will only be sent to Zendesk Inc. after sending a question to the Dialog Support team via the support widget in the Online platform, or after sending an email to [support@dialog.nl](mailto:support@dialog.nl). Zendesk's support widget places four non-personally identifiable cookies in a user's browser. More information about these cookies can be found in the Cookie Policy of Dialog.

\*\*\* Via settings in the Online platform, it is possible to select at the level of the organisation that feedback asked and given, and any responses to it, will not be included in emails. In this case, Yes is changed into to No.

## 2.10 Overview of Processing Agreements with Sub-processors

Name of Sub-processor	Date of signature of the Processing Agreement
TransIP BV	25/11/2021
Amazon.com Inc.	22/10/2021 (As part of the AWS Customer Agreement)
Google LLC (Google Analytics)	25/5/2018
Zendesk Inc.	9/12/2021
SMTPeter BV	7/1/2021
ONLINECITY.IO	9/12/2021

## 2.11 Agreements regarding deletion of Data

Dialog retains the Data of the Controller and the Data Subject for as long as this Data is required by the Controller. There are three scenarios in which Dialog deletes Data:

1. At the Controller's general request;
2. When an Administrator at the Controller deletes the End User's account from the Online platform.
3. When the agreement between the Controller and Dialog expires and is not renewed.

Dialog deletes the Data of the Controller and Data Subjects after expiry of a period of thirty days after one of the above scenarios, unless mutually agreed otherwise. Once Dialog has deleted the Data, Dialog will send an email about this to the Controller's Administrators.

Dialog may not delete accounts of Data Subjects without the Controller's prior consent.

Responsibility for the timely deletion of accounts of End Users who leave employment lies with the Controller. This is laid down in a Data Processor Agreement and is emphasised in the Service Level Agreement.

## **2.12 Organisational and security measures**

Dialog ensures that Data is properly secured. To prevent loss and unlawful Processing, Dialog has taken appropriate technical and organisational measures.

These measures can be found in the Security Policy.

### [ISO27001:2017 +A11:2020](#)

Dialog has a ISO27001:2017 +A11:2020 certification. Upon request, the following documents will be provided:

- Dialog - Verklaring Van Toepasselijkheid - ISO27001\_2017 +A11\_2020
- Dialog - DigiTrust Certificaat ISO 27001 Dialog (16 juni 2021)

### 3. Testing and analyses

To test the security of the Online platform - and all Data stored for this purpose - Dialog regularly performs various types of tests and analyses to identify any vulnerabilities and takes action if needed. We perform the following tests at least once a year:

- 1 Penetration test/Advanced Security Scans
- 2 Data Protection Impact Assessment (DPIAs)
- 3 Risk analysis of organisation and information security

Information about these tests and analyses and the measures we have taken on the basis of the results can be found in the Security Policy.

## 4. Privacy by design & privacy by default

During all phases of the product development of the Online platform, the privacy of Data Subjects is taken into account. We would like to emphasise this in our 'Privacy by design' and 'Privacy by Default' methods.

### 4.1 Privacy by design

Dialog uses the following English-language definition of 'Privacy by design'.

**Privacy by Design** states that any action a company undertakes that involves processing personal data must be done with data protection and privacy in mind at every step. This includes internal projects, product development, software development, IT systems, and much more. In practice, this means that the IT department, or any department that processes personal data, must ensure that privacy is built into a system during the whole life cycle of the system or process.

The following actions have been taken to demonstrate that privacy by design is central to Dialog:

Purpose	Actions
Design and user experience (UX) testing	<ul style="list-style-type: none"><li>• Designers use fictitious characters to create designs and user stories.</li><li>• Designers use fictitious characters when designing new functionalities.</li><li>• UX testers use fictitious data to verify UX hypotheses.</li><li>• During the design process of new functionalities, privacy is a recurring theme.</li></ul>
Development and testing	<ul style="list-style-type: none"><li>• During the tech demo, feature demo, feature test and regression tests, privacy is a recurring subject. Is there any (new) Data that is collected with this functionality? If so, for what purpose? Has the privacy documentation been updated for this additional data? The same applies with regard to the use of any new tools.</li><li>• Developers and testers use a database with fictitious users to build and test functionality.</li></ul>

### 4.2 Privacy by default

Dialog uses the following English-language definition of 'Privacy by design'.

**Privacy by Default** means that once a product or service has been released to the public, the strictest privacy settings should apply by default, without any manual input from the end user. In addition, any personal data provided by the user to enable a product's optimal use should only be kept for the amount of time necessary to provide the product or service.

The following actions have been taken to demonstrate that privacy by default is central to Dialog:

Purpose	Actions
Use	<ul style="list-style-type: none"> <li>● Data Subjects themselves determine whether they consent to the use of their Data to improve the Online platform.</li> <li>● Data subjects themselves manage the frequency of the number of messages they receive from the platform.</li> <li>● If the Controller instructs the deletion of Data, Dialog will always comply with this.</li> </ul>
Maintenance	<ul style="list-style-type: none"> <li>● When resolving any customer problems, developers only use production databases if they cannot imitate the problem using a database of fictitious users. They always try the latter first.</li> <li>● The Data Subjects only see other persons and Data to whom and which they are entitled on the basis of their position.</li> <li>● Only employees of Dialog who, directly or indirectly, support Administrators, Managers and End Users in the use of the platform, have their own administrator account with possibilities for accessing customer Data.</li> <li>● Production databases are encrypted before they are stored in Cloud Storage.</li> <li>● Production databases are never forwarded via email, Slack or other communication, or on USB sticks or external hard drives.</li> <li>● Passwords for various servers and services are only accessible to Dialog employees who must have access to them in order to perform their duties.</li> </ul>
Sale	<ul style="list-style-type: none"> <li>● In sales calls, data of real users is never shown.</li> </ul>
Continued development	<ul style="list-style-type: none"> <li>● Analyses of the use of the platform are only performed with non-personally identifiable data. This includes: <ul style="list-style-type: none"> <li>○ Data from an anonymised data set;</li> <li>○ Google Analytics;</li> </ul> </li> </ul>



## 5. Data breaches

### 5.1 Protocol

In the event that Dialog discovers a Data Breach, Dialog will inform the Controller affected by the Data Breach.

We follow the agreements made in the Processing Agreement.

### 5.2 Register of data breaches

There have been no data breaches to date.

This concerns all Data Breaches and, therefore also Data Breaches that should be reported to the Supervisory Authority.