ombra

Data processing agreement

Last updated: 19 October 2026
ombra · Abeliaerf 37, 4125 WH Hoef en Haag, the Netherlands · KVK 88959945 · VAT NL004674188B20

You are responsible for your clients' data. ombra processes it only for you. This is how.

Who does what

This data processing agreement is part of ombra's terms and conditions. You conclude it when you accept the terms. It follows article 28 of the GDPR and article 9 of the Belgian Act of 30 July 2018 on the protection of personal data.

You, the psychologist, therapist or practice with an account, are the **controller**: you decide why and how your clients' data is processed. ombra, established at Abeliaerf 37, 4125 WH Hoef en Haag, the Netherlands (KVK 88959945), is the **processor**: we process it only for you. Would you like a signed copy? E-mail support@ombracare.com.

We send messages about this agreement, such as notice of a personal data breach, to your account's e-mail address. If we should inform someone else, for example your data protection officer, let us know at privacy@ombracare.com.

1. Subject and duration

ombra processes personal data for you in order to provide ombra, as annex A describes. Health data is expressly included. This agreement runs for as long as you use ombra, and after that until we have returned and deleted your data (article 12).

2. Only on your instructions

We process your data only on your instructions. They are set out in this agreement and the terms, and you give them by using ombra: what you enter, set, connect, export or delete. You agree any other instruction with us in writing, at privacy@ombracare.com.

If the law obliges us to do something else, we let you know in advance, unless that law forbids it. If we believe an instruction infringes data protection law, we tell you at once.

If we seriously breach this agreement, you can ask us to stop the processing at once. Taking your data with you is then still always possible.

3. No use for our own purposes

We do not use your data for ourselves. We do not sell it, do not use it for advertising or research, do not build profiles with it, do not combine it with that of other practices, do not send it to AI services and do not train AI models with it (no AI on your records).

We give your data to no one else, unless you ask us to or the law obliges us to. If we have to hand something over, we let you know in advance, unless the law forbids it.

We use the Belgian national register number (rijksregisternummer) or the Dutch citizen service number (BSN) only to recognise your client in your record, never as our own identifier or for anything else. We use technical data without content, such as times and error codes, to make ombra work and to improve it.

4. Confidentiality

Everyone who can reach your data for ombra has a written duty of confidentiality, also after that work ends. Annex D says who can reach health data, and why. We keep that list up to date and give it to the Belgian Data Protection Authority (Gegevensbeschermingsautoriteit, GBA) if it asks for it.

5. Security

We take appropriate technical and organisational measures to protect your data (article 32 GDPR), suited to the sensitivity of health data. They are set out in annex B. We keep them in line with the state of the art. If we replace a measure, it is with one that protects at least as well.

6. Access by ombra

No one at ombra has standing access to the content of your workspace. An administrator reaches your data only through a temporary administrator role, and only:

- if you ask us to, for example to help you;
- to fix a fault or investigate a security incident;
- if the law obliges us to.

Each time we record who, when and why. In addition, break-glass accounts have lasting rights, only for when everything else fails; we record that use too. On your request we tell you whether and when an administrator reached your data.

7. Sub-processors

You authorise us to engage the sub-processors in annex C. We impose on them at least the same obligations as in this agreement, and we remain responsible to you for their work.

We e-mail you about a new or different sub-processor at least 30 days before it starts work, with what it does, with which data and where. You do not need to sign up for anything for this. If you have a well-founded reason to object, let us know within that period. If we cannot find a solution together, you may cancel free of charge, and we refund what you paid in advance.

8. Data outside the EU

Your data is stored in the European Union, as annex C describes. If it nevertheless goes to a country outside the European Economic Area, for example for support by Microsoft, then only within your instructions and with the safeguards the GDPR requires, such as an adequacy decision or the European Commission's standard contractual clauses.

You receive a copy of those safeguards on request. If we can no longer offer the protection, we stop that transfer. How we deal with requests from authorities, you can read under Security.

9. Help with your clients' rights

Your clients have rights over their data, and you have obligations as a care provider: in Belgium under the Patients' Rights Act (Wet patiëntenrechten) and the Kwaliteitswet, in the Netherlands under the WGBO. ombra helps you meet them:

- You print a record overview or save it as a PDF, for access or a copy.
- You correct or complete data. Notes keep all their versions.
- ombra records who opens or changes a record. That log is in your export, so you can tell a client who opened the record. Searching and the overview on Vandaag (Today) are recorded per workspace, not yet per record (the audit log).
- After the retention period you delete a record permanently.

If an application or registration must be removed, for example because someone asks for it, e-mail support@ombracare.com: we then delete it for you. If we ourselves receive a question from a client about their data, we forward it to you without undue delay. We do not answer it ourselves, and release nothing without your instruction or a legal obligation.

10. Personal data breaches

If we discover a breach of security that affects your data, we notify you without undue delay. We do not wait until our investigation is complete. We e-mail your account's address, with what we know at that moment:

- what happened, and when;
- which data it affects, and roughly how many clients and records;
- the likely consequences;
- what we are doing to resolve it and limit the harm;
- whom you can contact for more information.

If we do not yet know everything, we add to it as soon as we know more. We pass on a personal data breach at a sub-processor to you in the same way. You decide whether you notify the supervisory authority, within the 72 hours the law gives for it, and your clients: in Belgium that is the Gegevensbeschermingsautoriteit (GBA), in the Netherlands the Autoriteit Persoonsgegevens (AP). We help you with this. We keep a register of every incident.

11. Help with a DPIA

Are you carrying out a data protection impact assessment (DPIA), or must you consult the supervisory authority beforehand? Then we give you, free of charge, what you need about ombra: this agreement, the security measures, the sub-processors and answers to your questions.

12. Retention, return and deletion

As long as you use ombra, we delete no record data on our own initiative. You decide what may go. In Belgium the Kwaliteitswet requires a record to be kept for at least 30 and at most 50 years after the last contact. ombra lets you delete a record only once those 30 years have passed, and shows you under Instellingen → Gegevens (Settings → Data) which records have reached that point. When you delete it after that is your decision.

In the Netherlands the WGBO as a rule requires 20 years, and a client can ask you to destroy the record. If a record must go earlier than ombra allows, e-mail privacy@ombracare.com from your account's e-mail address: until ombra can do it itself, we delete it for you.

If you stop using ombra, you choose: we return everything and delete it afterwards, or we delete without returning. By default we first return everything, as article 12 of the terms says:

1. You download your complete export.
2. You have 30 days to download it again or reopen your account.
3. After that we delete everything in your workspace, including the log. It disappears from the database backups within 35 days. We clean up earlier versions of documents once they are older than 35 days; after that they can still be recovered for 35 days. If we restore a backup in that time, we delete it again.

Have you already secured your data and do you not want a new export? Then e-mail privacy@ombracare.com from your account's e-mail address, and we delete without returning. For that route you do not need to download a new export. You can change your choice until the deletion begins. Your own legal duty to retain records continues to apply.

We keep a copy of the log with identifiers only, without names or content, for 365 days for security. Returning your data costs nothing. On request we confirm the deletion in writing. If the law requires us to keep something longer, we tell you what and why, and use it for nothing else.

13. Information and audits

We give you, free of charge, all the information you need to show that these agreements are being kept: this agreement, the security measures and answers to your questionnaires.

Do you want an audit, by yourself or by an independent expert bound by confidentiality? Let us know at least ten working days in advance, and we agree together when and how, on a working day and in a way that keeps other customers' data safe. You bear the costs of your own audit; we do not charge for our own time. If it turns out we do not keep this agreement, we put that right as quickly as possible, at our expense. If a supervisory authority requests an investigation, we cooperate.

14. Liability

For this agreement, the liability in article 13 of the terms applies. It does not detract from your clients' rights under article 82 of the GDPR.

15. Changes and precedence

We change this agreement as article 16 of the terms says: for a good reason, at least 30 days in advance, and only once you accept the new version. If the law changes, we adapt the agreement to it. Where personal data is concerned, this agreement takes precedence over the terms.

These obligations continue to apply for as long as we keep data for you. You can download this agreement as a PDF, save it or print it as part of your agreements with ombra.

This agreement was drawn up in Dutch, and this is an English translation. Where the two differ, the Dutch text prevails.

Annex A. The processing

For what

Providing ombra: keeping records, storing notes and documents, planning appointments, managing applications and a waiting list, keeping track of groups and their registrations, publishing forms and a booking page, connecting calendar and mail, sending mail in your name, and exporting everything.

What ombra does with it

Receiving, storing, organising, displaying, encrypting, sending in your name, exporting and deleting data.

About whom

- your clients, including minors, and their representatives;
- applicants and people who book an appointment;
- group participants and those who register for a group;
- people who appear in a record, such as referrers, general practitioners, contact persons and relatives;
- colleagues with whom you share an intake space or group;
- people in your connected calendar and mailbox.

Which data

- **Identity and contact**: name, date of birth, address, e-mail addresses, telephone, language, pronouns and the rijksregisternummer or BSN.
- **Care administration**: health insurance fund (ziekenfonds) or health insurer (zorgverzekeraar), referrer, general practitioner, emergency contact, form of care, fee and payment status.
- **Health**: reason for seeking help, goals, session notes with all their versions, homework, documents, group notes and attendance.
- **Applications and bookings**: what someone fills in on your application or registration form, with the questions and the privacy text of that moment. For a booking: name, contact details, message and the chosen time.
- **Calendar and mail**: appointments with their participants from your connected calendar; which mails have been read, answered or dealt with; your drafts; of every mail sent, a fingerprint and the status. ombra fetches the content of your mail live and does not store it.

- **Log**: who opened or changed which record, and when.

Special categories of data

Health data (article 9 GDPR) and a national identification number, the rijksregisternummer or BSN (article 87 GDPR). You record other special categories of data only if your care requires them.

How long

For as long as you use ombra, and after that as article 12 says.

Annex B. Security measures

- **Storage in the EU**: Microsoft Azure in Ireland (Microsoft Azure North Europe), with a copy of the database backups in the Netherlands (Microsoft Azure West Europe).
- **Encryption**: all connections (TLS 1.2 or newer) and all storage (AES-256). Documents, mail drafts, notes on group sessions and the keys of connections are encrypted once more by ombra itself (AES-256-GCM), with the key in a separate key vault.
- **Separation**: the database shields each workspace from the others. Colleagues see only what you share with them, such as a shared intake space or a group.
- **Signing in**: with a password, through Google or Microsoft, with a one-time code by e-mail, or with a passkey that asks for a face, fingerprint or PIN on the device. On a device that has not signed in with a code from the mail, Google, Microsoft or a passkey in the last 90 days, ombra also asks for a code from the mail after the password. Passwords are stored only as an unreadable hash. An authenticator as an extra lock; sensitive steps then ask for a new code, and a passkey counts as both locks. Sign-in sessions end after 30 minutes without activity and after at most 12 hours.
- **Log**: who opens, changes or exports a record, without content; searching and Vandaag (Today) per workspace. An export of a complete account sends us an alert.
- **Documents**: a malware scan before anyone can open an upload.
- **Network**: the database and storage cannot be reached from the internet. Outgoing traffic goes only to Microsoft and Google. A web application firewall stands in front of the app.
- **Backups and recovery**: a standby copy of the database in a second datacentre takes over automatically; continuous backups of 35 days, with a copy in a second region; documents spread over several datacentres, with their earlier versions. Target: at most 15 minutes of changes lost after an error, an hour after the loss of a whole region, and working again within 4 hours. A recovery drill every quarter.
- **Administration**: no ordinary, standing access to data, a temporary administrator role with a second step at sign-in and a recorded reason, break-glass accounts only for when everything else fails, a duty of confidentiality, a quarterly review of who has which rights, access revoked on the day someone stops, and encrypted work computers.
- **Development**: separate environments, with only invented data outside the real app; every change reviewed and automatically tested, with a security scan; components automatically checked for known vulnerabilities; the measures reviewed at least once a year.

More explanation under Security.

Annex C. Sub-processors

Sub-processor	For what	Where
Microsoft Ireland Operations Ltd. (Microsoft Azure)	Hosting ombra: the app, the database, documents, keys and logs, the malware scan of uploads and secure access (Azure Front Door with a firewall).	Ireland (Microsoft Azure North Europe), with a copy of the database backups in the Netherlands (Microsoft Azure West Europe). Connections arrive at Microsoft's nearest point of presence.

The full list, with the services ombra uses for its own work and the connections you make yourself, is under Sub-processors.

Annex D. Who has access

Who can reach your clients' health data, in which role, and what binds them to confidentiality (article 9 of the Belgian Act of 30 July 2018).

Who	Role	Bound by
You, and those you give access	Care and practice administration. Colleagues see only what you share with them: members of a shared intake space the applications in that space, group therapists their group.	Your professional secrecy, and what you agree with them.
ombra's administrators	Technical administration: fixing a fault, investigating a security incident or helping you when you ask. Only through a temporary administrator role, or in an emergency through a break-glass account, and we record who, when and why.	A written duty of confidentiality.
Microsoft staff	Running the datacentres and the cloud services. No ordinary access to the content.	Microsoft's data processing agreement and their duty of confidentiality.