

Data Processing Addendum

This data processing addendum (in Dutch: verwerkersovereenkomst) sets out how DataFlowr processes personal data on behalf of its customers, as article 28(3) GDPR requires. It belongs to every agreement under which DataFlowr processes personal data, including the use of Claire. This document also exists in Dutch; where the two versions differ in interpretation, the Dutch text prevails.

VERSION 1.0 · AUGUST 2026

Parties

1. DataFlowr B.V., with its registered office at Van Marsbergenstraat 71, 2134 LV Hoofddorp, the Netherlands, registered with the Dutch Chamber of Commerce under number 99021145, hereinafter “DataFlowr”, “we” or “us”;
2. the customer that has entered into an Agreement with DataFlowr, hereinafter “the Customer” or “you”.

Recitals

- A. We provide Claire, the AI layer on top of Exact Online, and consultancy services within the Exact Online ecosystem. In doing so we process personal data on the Customer’s behalf, including the data Claire fetches from the connected Exact Online administration for each question.
- B. For that processing the Customer determines the purposes and means. The Customer is the controller within the meaning of article 4(7) GDPR and we are the processor within the meaning of article 4(8) GDPR.
- C. In this Addendum we record the arrangements article 28(3) GDPR requires. Three annexes belong to this Addendum: Annex 1 describes the processing, Annex 2 the security measures and Annex 3 the subprocessors.

The parties agree as follows.

Article 1 · Definitions

- 1.1 Terms from the GDPR, such as processing, personal data, controller, processor, data subject and personal data breach, carry the meaning the GDPR gives them in this Addendum.
- 1.2 GDPR: Regulation (EU) 2016/679 (General Data Protection Regulation) and the Dutch GDPR Implementation Act (Uitvoeringswet AVG).
- 1.3 Agreement: any agreement between DataFlowr and the Customer under which we provide the Service, including the terms of service and a quotation or order confirmation.
- 1.4 Service: Claire, the subscription to the AI layer on top of the Customer’s own Exact Online administration, and the consultancy services in which we have access to personal data.
- 1.5 Personal Data: the personal data we process on the Customer’s behalf in providing the Service, as described in Annex 1.

- 1.6 Data Subject: the person a piece of Personal Data relates to.
- 1.7 Data Breach: a personal data breach within the meaning of article 4(12) GDPR.
- 1.8 Subprocessor: another processor we engage to carry out specific processing activities on the Customer's behalf.
- 1.9 Addendum: this data processing addendum, including its three annexes.

Article 2 · Roles and scope

- 2.1 This Addendum applies to every processing of Personal Data we carry out in providing the Service. It forms part of the Agreement and needs no separate signature. If you want a signed copy, use the signature page after article 14.
- 2.2 The Customer is the controller and determines the purposes and means of the processing. We are the processor and process solely on the Customer's behalf.
- 2.3 Where the Customer is itself a processor for a third party, for instance an accounting or bookkeeping firm keeping a client's administration, we act as a subprocessor. This Addendum then applies in full. In that case the Customer warrants that its arrangements with the controller permit engaging DataFlowr and that the instructions it gives us fit within those arrangements.
- 2.4 The Customer warrants that the processing of the Personal Data is lawful: that a legal basis exists, that Data Subjects have been informed where required, and that the content of the data and the way it was obtained are not unlawful.
- 2.5 We inform the Customer at once when, in our view, an instruction conflicts with the GDPR or other privacy legislation.

Article 3 · Instructions and processing

- 3.1 We process the Personal Data solely on the Customer's documented instructions, including with regard to transfers to a country outside the EEA, unless a provision of Union or Dutch law requires us to process. In that case we notify the Customer beforehand, unless that law forbids it. The Agreement, this Addendum and the use and configuration of the Service, such as which administrations are connected, which modules are enabled and which questions are asked, together constitute those instructions.
- 3.2 We do not process the Personal Data for our own purposes. We do not sell it, do not use it for advertising and do not train AI models on it. Our model providers process prompts only to answer them; training on customer data is contractually excluded.
- 3.3 We process no longer and no more extensively than the Service requires. Claire fetches data from the connected administration per question; no copy of the administration arises outside Exact Online. We only carry out a change to the administration after the user has explicitly approved it.
- 3.4 Only staff who need it for their work have access to Personal Data, and no further than that work requires.
- 3.5 If a competent authority asks us to hand over Personal Data, we first assess whether the request is binding. We inform the Customer before disclosing, unless the law forbids it, and in such time that the Customer can pursue legal remedies.

Article 4 · Confidentiality

- 4.1 We keep the Personal Data confidential. Everyone processing Personal Data under our authority has committed to confidentiality in writing or is bound by a statutory duty of confidentiality.
- 4.2 Confidentiality does not apply to the extent the Customer has consented to disclosure, disclosure is needed for the Service, or a legal duty to disclose exists.
- 4.3 This article survives the end of this Addendum.

Article 5 · Security

- 5.1 We take appropriate technical and organisational measures as meant in article 32 GDPR, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing and the risks to Data Subjects. The measures are set out in Annex 2.
- 5.2 Financial data is personal data of a sensitive nature. The Service's level of security is set accordingly.
- 5.3 We evaluate the measures periodically and tighten them when the risks or the state of the art call for it. We may amend Annex 2, as long as the measures as a whole do not offer a lower level of protection.
- 5.4 On request we give the Customer the information needed to assess whether the measures are appropriate.

Article 6 · Subprocessors

- 6.1 The Customer grants us general authorisation to engage Subprocessors in providing the Service. The current list is in Annex 3.
- 6.2 We impose data protection obligations on every Subprocessor in writing that are at least equivalent to our obligations under this Addendum, including confidentiality, security and the rules on transfers.
- 6.3 We announce a new or replacement Subprocessor at least 30 days in advance, by email to the account's contact person. We also publish the current list in this document on our website.
- 6.4 The Customer may object in writing within 14 days of the announcement, on reasonable, substantiated grounds relating to data protection. We then look for a reasonable solution together. If none is found, the Customer may terminate the affected part of the Service with effect from the date the change takes effect.
- 6.5 We remain fully responsible towards the Customer for the performance of our Subprocessors' obligations, as article 28(4) GDPR provides.
- 6.6 Exact Online is not our Subprocessor: the Customer connects its own administration under its own agreement with Exact and its own Exact Online account. The same goes for an AI client the Customer chooses itself, such as Claude, ChatGPT or Microsoft Copilot, and for the Customer's own AI provider or API key: those fall under the Customer's arrangements with that provider.

Article 7 · Transfers outside the EEA

- 7.1 Some of our Subprocessors also process Personal Data outside the European Economic Area, in particular in the United States. Annex 3 states this per Subprocessor.
- 7.2 Transfers to a country outside the EEA only take place in accordance with Chapter V of the GDPR (articles 44 to 49): on the basis of an adequacy decision of the European Commission, including the EU-US Data Privacy Framework for recipients certified under it, or with appropriate safeguards such as the European Commission's standard contractual clauses (Implementing Decision (EU) 2021/914), with supplementary measures where needed.

- 7.3 We do not transfer Personal Data on our own initiative to countries or recipients other than those listed in Annex 3.

Article 8 · Assistance with data subject rights

- 8.1 If we receive a request or complaint from a Data Subject about Personal Data, for instance for access or erasure, we forward it to the Customer within three working days, without responding to its substance ourselves.
- 8.2 Taking the nature of the processing into account, we help the Customer with appropriate technical and organisational measures to fulfil Data Subjects' requests under Chapter III GDPR, including access, rectification, erasure, restriction, objection and portability. Much of this the Customer can do itself: conversations can be viewed and deleted in the application and the connection can be revoked directly. What the Customer cannot do itself, we do on request via privacy@dataflowr.nl.
- 8.3 This assistance is free of charge. Only where requests are structural or excessive may we charge reasonable costs; we say so beforehand.

Article 9 · Data breaches

- 9.1 If we discover a Data Breach affecting the Personal Data, we notify the Customer without undue delay, and at the latest within 48 hours of establishing it. We notify the account's contact person, at the email address on record with us.
- 9.2 The notification contains, to the extent then known: the nature of the Data Breach, the categories of Data Subjects and records affected and the approximate numbers, the likely consequences, the measures we have taken or propose, and our contact point privacy@dataflowr.nl. Information that becomes available later, we supply in stages.
- 9.3 The assessment and the notification to the Dutch Data Protection Authority (Autoriteit Persoonsgegevens) and to Data Subjects rest with the Customer as controller. We assist the Customer in meeting that notification duty (articles 33 and 34 GDPR) and do not notify ourselves, unless the law requires us to.
- 9.4 We document every Data Breach affecting the Personal Data: the facts, the consequences and the measures taken.

Article 10 · Assistance with DPIAs and prior consultation

- 10.1 Taking into account the nature of the processing and the information available to us, we reasonably assist the Customer with a data protection impact assessment (article 35 GDPR) and with a prior consultation of the Dutch Data Protection Authority (article 36 GDPR).

Article 11 · Information and audit

- 11.1 On request we make available to the Customer all information necessary to demonstrate that we comply with article 28 GDPR and with this Addendum: documentation of our measures, the annexes to this document and, where available, reports by independent third parties.
- 11.2 The Customer may additionally have an audit carried out, by itself or by an independent expert bound to confidentiality. An audit takes place at most once every twelve months, after written notice of at least 30 days, during office hours and without unnecessarily disrupting operations. The audit gives no access to other customers' data. The once-per-twelve-months limit does not apply when there is a concrete reason, such as a

Data Breach affecting the Personal Data or a substantiated suspicion that we are not complying with this Addendum.

- 11.3 The Customer bears the costs of an audit. If the audit shows that we materially fall short, we bear our own reasonable costs of cooperation.
- 11.4 Both parties treat the findings confidentially. We implement justified improvements within a reasonable period.
- 11.5 Both parties cooperate with the Dutch Data Protection Authority on request in the performance of its tasks.

Article 12 · Liability

- 12.1 The liability arrangement in the Agreement also applies to this Addendum.
- 12.2 Without prejudice to article 12.1, each of us bears the damage and the supervisory authority's fines that result from its own failure to comply with the GDPR or with this Addendum.

Article 13 · Term, end and deletion

- 13.1 This Addendum applies for as long as the Agreement runs, and thereafter for as long as we still process Personal Data in the context of the Service.
- 13.2 After the Agreement ends we delete all Personal Data, including copies, within 90 days. If the Customer asks for return before that moment, we first supply the Personal Data in a common file format. Deletion carries through to backups following the hosting platform's rotation schedule.
- 13.3 The duty to delete does not apply to the extent a provision of Union or Dutch law requires us to retain. We keep that data no longer than that duty requires.
- 13.4 If the Customer revokes the connection to Exact Online, the access tokens lapse at once and we delete them. The data in the Exact Online administration itself remains untouched at Exact; the Customer's own agreement with Exact governs that.
- 13.5 Provisions that by their nature continue, such as confidentiality and liability, survive the end.

Article 14 · Final provisions

- 14.1 Where this Addendum and the Agreement conflict, this Addendum prevails insofar as the processing of Personal Data is concerned.
- 14.2 If the Service, the list of Subprocessors or the law changes, we update this document. We publish the new version on dataflowr.nl with a new version number and date. A change that materially affects the Customer's rights we announce at least 30 days in advance; if the Customer cannot accept it, it may terminate the Agreement with effect from the date the change takes effect.
- 14.3 If a provision of this Addendum is invalid, the remaining provisions continue to apply. The parties replace the invalid provision with a valid one that comes as close as possible to its intent.
- 14.4 Dutch law applies to this Addendum. Disputes go to the competent court in Noord-Holland, the Netherlands, unless the law designates another court.
- 14.5 This Addendum exists in a Dutch and an English version. Where the two differ in interpretation, the Dutch text prevails.

14.6 Notices under this Addendum go to privacy@dataflowr.nl. We use the contact details of the Customer's account.

Signature

This Addendum applies as part of the Agreement, signature or not. If you want a signed copy, fill in both columns below and send the document to privacy@dataflowr.nl. We return a countersigned copy.

DataFlowr B.V.

NAME

TITLE

DATE

SIGNATURE

The Customer

COMPANY NAME

NAME

TITLE

DATE

SIGNATURE

Specification of the processing

Subject matter and nature of the processing

We provide Claire, the AI layer on top of the Customer's own Exact Online administration. Users ask questions in plain language; per question Claire fetches the data needed from the connected administration, drafts an answer with a language model and only carries out a change after the user's explicit approval. In addition, at the Customer's request, automated checks and schedules run, such as the month-end close checks and the cash flow forecast, and we send email notifications about the outcomes. In consultancy engagements we additionally process the personal data the Customer gives us access to for the engagement.

Purpose of the processing

Solely providing the Service as described in the Agreement: answering questions, carrying out approved changes, running checks and schedules, supporting the Customer and guarding the security of the platform.

Duration

For as long as the Agreement runs, and thereafter until the deletion under article 13 is complete.

Categories of data subjects

- Users and employees of the Customer who work with the Service.
- Contacts, customers and suppliers of the Customer, including debtors and creditors, and their employees, insofar as their data sits in the connected administration.
- Other persons whose data appears in the connected administration, in questions asked or in uploaded files.

Categories of personal data

CATEGORY	DATA
Account details	Name, email address, profile picture and the identity of the sign-in method.
Connection data	OAuth access tokens for Exact Online and which administrations are connected.
Conversation data	Questions, answers, the data fetched per question and files users upload.
Administration data	Names, addresses and contact details and financial data from the connected administration, such as invoices, outstanding items, transactions and bank details, insofar as a question or check fetches them.
Logs	Which action ran when and under which account, IP address, timestamp and the client used.

The Service is not intended for special categories of personal data (article 9 GDPR) or criminal offence data. Where they nonetheless sit in the administration, in questions or in files, the measures of Annex 2 apply in full. Financial data is personal data of a sensitive nature; security is set accordingly.

The Customer's own billing details, such as company name, VAT number and invoice history, we process for our own invoicing and accounting. For that we are the controller; that processing falls under our privacy policy, not under this Addendum.

Retention periods

DATA	PERIOD
Account and conversations	For as long as the subscription runs. The transcript of a conversation (questions, answers and fetched data) is additionally deleted automatically 30 days after it was last used, by default; uploaded files go when the conversation is deleted. After the Agreement ends we delete the account, conversations and files within 90 days.
Connection data	Until the Customer revokes the connection or the Agreement ends; the tokens then lapse and we delete them.
Logs	Twelve months, so an incident can be investigated after the fact. After the Agreement ends, the period of article 13 additionally applies.

Rights and obligations of the Customer

The Customer remains the controller: it ensures a legal basis, informs Data Subjects where required, gives instructions that comply with the GDPR and itself manages the users and access rights in its Exact Online administration. The connection runs through each user's own Exact Online account: Claire can do exactly what that user may do in Exact Online, nothing more.

Technical and organisational measures

These measures describe what the Service does today. We evaluate them periodically and may amend them as long as the level of protection does not decrease (article 5).

Encryption and key management

- All traffic with the application and with Exact Online runs over TLS (1.2 or higher).
- The connection to Exact Online runs through OAuth; we never receive or store Exact Online passwords.
- ERP access tokens, client secrets and API keys are stored encrypted with AES-256-GCM, with support for key rotation.
- Long-lived access tokens and invitation tokens are stored as SHA-256 hashes; the token itself is shown once.

Access and authorisation

- Sign-in runs through our identity provider on a European environment, with support for multi-factor authentication and passkeys. Sessions expire after 24 hours.
- Access is separated per organisation. A connection is only reachable by members of the organisation, and each member authorises with their own Exact Online account: per user, Claire can do exactly what that user may do in Exact Online.
- Administrative actions, such as deleting a connection, are restricted to administrators. Modules and tools can be switched on or off per connection; those settings are enforced on every execution.
- Writes to Exact Online always require the user's explicit approval and are recorded such that an action can never run twice.
- Access to production systems is limited to the staff who need it. The internal admin dashboard shows aggregate figures only, no administration data.

Logging and control

- Every tool execution is logged with user, timestamp and client used. The audit log is available to the Customer in the application.
- For list and write tools the audit log holds summaries rather than full results.
- Secrets are redacted from log lines; server logs contain no access tokens.

Data minimisation towards AI models

- Claire fetches data per question; no copy of the administration arises outside Exact Online.
- Towards the AI gateway the user is passed on pseudonymously: an internal code, not a name or email address.
- Redaction is configured at the AI gateway level: email addresses, phone numbers and credit card numbers are redacted before a prompt reaches the model provider. In the month-end close checks the application additionally masks IBANs and email addresses.
- We train no AI models on customer data. For our model providers, training on customer data is contractually excluded.

Application and platform security

- Security headers (including a strict Content Security Policy and HSTS), CSRF protection and rate limiting on the API.
- Automated security checks in the development pipeline: dependency auditing, static analysis and baseline scans.
- A coordinated vulnerability disclosure procedure, published through security.txt.
- The application runs on a managed cloud platform; backups of the database and object storage run through that platform's facilities.

Organisation

- Staff are bound to confidentiality and only receive the access their work requires.
- We periodically assess whether the measures still fit the risks and the state of the art.

Subprocessors

We engage the following Subprocessors. We announce changes as set out in article 6. With every Subprocessor we have a data processing agreement or equivalent contractual arrangements.

SUBPROCESSOR	SERVICE	LOCATION	TRANSFER MECHANISM
Auth0 (Okta, Inc.)	Sign-in and account management	EU environment; US parent company	EU-US Data Privacy Framework
Replit, Inc.	Hosting of application and database	US; infrastructure on Google Cloud	Standard contractual clauses
Google LLC (Google Cloud)	Cloud infrastructure and storage of workspace files	EU and US	EU-US Data Privacy Framework
OpenRouter, Inc.	AI gateway routing questions to the chosen language model	US	Standard contractual clauses
The selected model provider (such as Google, OpenAI or Anthropic)	Drafting answers, through OpenRouter	Depending on the chosen model, EEA or US	Standard contractual clauses or the provider's own DPF certification, agreed between OpenRouter and the provider
Resend, Inc.	Email notifications	US	EU-US Data Privacy Framework

Not Subprocessors

- Exact Online: the Customer connects its own administration under its own agreement with Exact and its own Exact Online account. Exact does not process on our behalf.
- AI clients the Customer chooses itself, such as Claude, ChatGPT or Microsoft Copilot: questions and answers then also pass through that client. That falls under the Customer's agreement with that provider.
- The Customer's own AI provider or API key: that provider is then the Customer's own processor. Our platform key is never sent along.
- Stripe processes the subscription payments for our own invoicing. For that we are the controller; that processing falls under our privacy policy.