LEGAL · DATA-PROCESSING SCHEDULE, NETHERLANDS

The Article 28 terms for how the Suite processes your data.

This schedule forms part of the Blauw Belastingen B.V. terms of use and sets out that company's obligations as processor under Article 28 GDPR. It applies from 14 September 2026, when and as those terms do. Annex 2, the sub-processor list, is published separately at /legal/sub-processors/ under its own version identifier. Until then, and for an organisation established anywhere other than the Netherlands, the schedule that applies is the one forming part of the TIF Synergy Ireland Limited terms.

Not yet superseded. This archived copy of version 2026-09-14-NL is currently also the current version. Check the **current page** to confirm whether a newer version now applies.

VERSION

Effective date and version identifier.

STATUS	Published 8 September 2026. This schedule applies from 14 September 2026, and not before that date. It is published in advance so that it can be read, stored and taken advice on. This version is permanent: once published, a version is never edited or removed, and a change mints a new identifier.
VERSION IDENTIFIER	`2026-09-14-NL` — published 8 September 2026, applies from 14 September 2026.
TOOL VARIABLE	`None of its own.` This schedule forms part of the terms of use and is tracked under that document's `TERMS_OF_USE_VERSION`, which is `2026-09-14-NL` for a customer whose contracting entity is Blauw Belastingen B.V. Annex 2 carries its own `SUBPROCESSOR_LIST_VERSION`, which is not this identifier and changes independently of it.
CURRENT VERSION	/legal/nl/data-processing-schedule/ — check here for whether a newer version has since superseded this one.

Downloadable copy. This schedule must be provided in a form you can store and reproduce. A link to this page is not that; the PDF below is.

WHO PROCESSES YOUR DATA

The processor.

Blauw Belastingen B.V.

Trading as	TIF Synergy
Legal form	Private limited company (besloten vennootschap), incorporated in the Netherlands
Chamber of Commerce (KVK) number	58905375 (Handelsregister, Netherlands Chamber of Commerce)
VAT number	NL853231886B01
Registered office and address of establishment	Oudezijds Achterburgwal 173, 1012 DJ Amsterdam, the Netherlands
Email	info@tifsynergy.com

Schedule DP: TIF Suite data-processing schedule

Published 8 September 2026. This schedule applies from 14 September 2026. Version: `2026-09-14-NL`.

When this schedule applies. This schedule applies from 14 September 2026. It is published on 8 September 2026 so that you can read it, store it and take advice on it before then. **Being published is not the same as applying to you. Nothing in this schedule**

applies to any organisation before 14 September 2026, no organisation moves to it before that date and **you will not be asked to accept it before that date.**

Blauw Belastingen B.V., named below, is the processor under this schedule. It develops the tools, hosts them and operates them, and it engages the providers listed in annex 2 to host, index, read, screen and support them. **TIF Synergy Ireland Limited is not in the chain under this schedule and processes nothing on your behalf under it.**

For a customer established anywhere other than the Netherlands, and for every customer until 14 September 2026, the processor is TIF Synergy Ireland Limited under the schedule that forms part of that company's terms, and this company is that company's sub-processor. **This schedule is not the one that applies to that customer.**

Version: `2026-09-14-NL`. Published: 8 September 2026. Applies from: 14 September 2026. Sub-processor list: annex 2, which carries its own version identifier and changes under clause DP6.

Which of our companies you are contracting with. This schedule applies where your contracting entity is **Blauw Belastingen B.V.**, which is the company that contracts with organisations established in the Netherlands.

Until 13 September 2026 your contracting entity is TIF Synergy Ireland Limited wherever your organisation is established, including in the Netherlands, under the terms published at https://www.tifsynergy.com/legal/ie/terms-of-use/ and the data-processing schedule that forms part of them, and those are the documents that apply to you.

Those terms say that if your organisation is established in the Netherlands your contracting entity changes to Blauw Belastingen B.V. only when the terms this schedule forms part of are in force and you have accepted them. **Those terms are in force from 14 September 2026, which is the date stated at the top of this document, and not before.** Until you accept them the Irish terms and the schedule that forms part of them continue to apply to you. **When you accept them, the Irish terms end** for your organisation and these terms and this schedule apply to you from that point onwards. Nothing agreed under the Irish terms before that date is undone, and any clause of those terms or of that schedule that is stated to continue after they end continues.

If your organisation is established anywhere else, your contracting entity is TIF Synergy Ireland Limited and those documents continue to be the ones that apply to you.

How we decide whether your organisation is established in the Netherlands is at clause DP1.5.

This schedule forms part of the TIF Suite terms of use. Words defined in those terms have the same meaning here. Where this schedule and the rest of the terms conflict on the handling of personal data, this schedule governs.

DP1.1 This schedule applies where we process personal data on your behalf in connection with a tool. For that processing **you are the controller and we are the processor**. In this schedule "personal data", "controller", "processor", "sub-processor", "processing", "personal data breach" and "supervisory authority" have the meanings given in the General Data Protection Regulation (Regulation (EU) 2016/679).

DP1.2 Who we are. We are **BLAUW BELASTINGEN B.V.**, trading as TIF Synergy, a private limited company incorporated in the Netherlands, KvK number 58905375, registered office Oudezijds Achterburgwal 173, 1012 DJ Amsterdam, the Netherlands, VAT identification number NL853231886B01.

We develop the tools, we provide them to you under these terms and we operate them. The providers that host, index, read, screen and support them are engaged by us. **They are listed in annex 2 and clause DP6.2 explains what that means for you.**

Supervisory authorities, stated for each thing we do rather than in the abstract. For the personal data we process on your behalf under this schedule, **you are the controller and your own supervisory authority is the competent one**; we do not displace it. For the data we hold as controller, described at clause DP1.3, we are established in the Netherlands and our supervisory authority is the **Autoriteit Persoonsgegevens**. **You may in any case complain to the supervisory authority of the place where you live or work.**

DP1.3 What this schedule does not cover. We are the **controller**, not your processor, for the data we hold about the individual people who use a tool: their account, their sign-in, their preferences and the record of what they did in the tool. That is described in our privacy notice and it is not governed by this schedule. **You are not asked to authorise**

anything in relation to it and you are not responsible for it. Annex 2 tells you which of our providers touch which of the two.

DP1.4 Nothing in this schedule makes either of us a joint controller with the other.

DP1.5 How we decided which of our companies you contract with. Between 28 August 2026 and 13 September 2026 there is nothing for this clause to decide: your contracting entity is TIF Synergy Ireland Limited whatever you tell us. For the change described in the header of this schedule, which begins on 14 September 2026, we work out whether your organisation is established in the Netherlands from two things your organisation gives us: **the VAT identification number**, a number beginning `NL` meaning the Netherlands and any other prefix meaning somewhere else, and **the registered office address**. Where we hold both, we read both. Where we hold only one, that one decides. Where the two point in different directions, the Netherlands answer applies. **Where we hold neither, your contracting entity does not change and the terms published by TIF Synergy Ireland Limited continue to apply to you.** That answer does not change unless we agree it with you in writing, so a later change in where your organisation is established does not by itself move your contract to the other company.

DP1.6 When we say "we do" something, we may do it through a sub-processor. Where this schedule says we do, hold, operate or provide something, we may do it ourselves or through a sub-processor listed in annex 2. **We remain fully liable to you for it under clause DP6.3.**

DP2.1 The subject matter, nature and purpose of the processing, the types of personal data and the categories of data subject are set out **per tool in annex 1**.

DP2.2 Duration. We process for as long as the terms of use are in force between us, plus the period in clause DP10.

DP2.3 Your obligations as controller: lawfulness. You warrant that you have a lawful basis under Article 6 of the General Data Protection Regulation and where relevant a condition under Article 9 or Article 10, for the content you put into a tool and for our processing of it on your behalf and that the instructions you give us are lawful.

DP2.4 Your obligations as controller: telling your own data subjects. You are responsible for giving the individuals whose personal data appears in your content the information they are owed under Articles 13 and 14. That includes the people described in

annex 1 who are not your own staff, **in particular the people you invite to complete a questionnaire in TaxTrack, who are not party to our terms with you and may not know we hold anything about them.**

DP2.5 Your obligations as controller: the categories at annex 1. You undertake not to put into a tool the categories of data annex 1 asks you not to put in and **you accept that we do not detect them and do not claim to.**

DP2.6 Your obligations as controller: keeping your administrator contact current. You keep the administrator contact on your account accurate, because that is the address the notice mechanism at clause DP6.4 uses and it is how your right to object under DP6.5 reaches you.

DP2.7 Your rights under this schedule, in one place. You instruct us and we act only on those instructions (DP3). You authorise our sub-processors, you are told before the list changes and you may object (DP6). You are told about a personal data breach (DP9.1) and we help you with your own assessments (DP9.2). You choose whether we delete or return your content (DP10.1). You may ask us for the information that demonstrates our compliance and you may audit us (DP11).

DP3.1 We process personal data on your behalf **only on your documented instructions**, including in relation to transfers of personal data to a country outside the European Economic Area, unless we are required to process by Union or Netherlands law that applies to us or a sub-processor we engage is required to process by Union law or by the law of the member state that applies to it. Where that happens we will tell you before we process, unless that law forbids us to tell you on important grounds of public interest.

DP3.2 What counts as your instructions. Your instructions are: the terms of use including this schedule, your configuration and use of the tool and any further written instruction you give us. We have no other instructions and we act on no others.

DP3.3 We do not use your content for our own purposes. We do not process the content you put into a tool for any purpose of our own. In particular we do not use it to train, fine-tune, evaluate or improve any artificial-intelligence model, ours or anyone else's, we do not use it to develop or improve our products and we do not use it to produce statistics or insights beyond operating the tool for you. What the providers listed in annex 2 may do with your content is at DP3.3.2, which states the one exception rather than leaving it to be found.

DP3.3.1 We do not make your content available to another customer, except where one of your own users chooses to publish an item into a shared area of a tool. **Annex 3 says which tools have such an area and what separation applies to each tool** and a tool that has one tells the user at the point of publishing.

DP3.3.2 What our providers may do with your content, stated with the one exception rather than without it. The providers listed in annex 2 are engaged under written terms restricting them to processing on our documented instructions and we instruct none of them to use your content for training, fine-tuning or model improvement. **One of those providers also carries out security and abuse screening as part of providing the service, which is not something we instruct and which we cannot switch off.** That is described at clause DP7.7. **We would rather state the exception than state a rule that has one.**

DP3.4 If we think an instruction is unlawful. If in our opinion an instruction you give us infringes the General Data Protection Regulation or another data-protection provision of Union or member state law, we will tell you immediately.

DP4.1 We make sure that every person we authorise to process personal data on your behalf is bound by a **written confidentiality undertaking that survives the end of their engagement with us** or is under an appropriate statutory or professional obligation of confidentiality.

DP4.2 We limit access to your content to the people who need it to provide, secure or support the tool. **We record who has that access and when it was granted.**

DP5.1 We implement and maintain the technical and organisational measures set out in **annex 3**, which are appropriate to the risk under Article 32 of the General Data Protection Regulation.

DP5.2 We may change those measures as technology and threats change. **We will not reduce the overall level of security below what annex 3 describes** and a change that lowers it is a change to these terms under clause 7.3 rather than an operational adjustment.

DP5.3 Annex 3 describes what we actually operate. It does not describe controls we intend to build. **The same applies to every statement of fact in this schedule about how a tool behaves or what we are able to do** and where a capability exists in some tools and not others we say so per tool rather than for the estate.

DP6.1 General authorisation. You give us a **general authorisation** to engage sub-processors to process personal data on your behalf, on the conditions in this clause DP6.

DP6.2 The current list. The sub-processors we engage are listed in **annex 2**, which is published at a permanent address, is kept current and marks for each entry who engaged it. **Your authorisation under DP6.1 covers every entry in annex 2 marked as processing content you put into a tool.** The other entries are listed for transparency: they process data for which we are the controller, so they are not your sub-processors and you are not asked to authorise them.

Annex 2 is one list serving both of our companies, so **it also lists us**. **Under this schedule we are your processor and not a sub-processor, and you are not asked to authorise us.** The "engaged by" column records that we were engaged by TIF Synergy Ireland Limited. **That records the chain under that company's schedule and it is not yours**: under this schedule we are your processor directly and we engage the other entries ourselves.

DP6.3 Back-to-back terms and our liability. We engage every sub-processor under a written contract imposing data-protection obligations that are in substance the same as those in this schedule, in particular the obligation to provide sufficient guarantees of appropriate technical and organisational measures. **Where a sub-processor fails to fulfil its data-protection obligations, we remain fully liable to you for its performance.**

DP6.4 Notice of a change. Before we add or replace a sub-processor that will process your content, we will give you at least **30 days' notice**. Notice is given by updating annex 2 with the date the change takes effect **and** by emailing the administrator contact for your organisation, which you give us when your organisation is set up or when you first accept these terms.

DP6.5 Your right to object. You may object to an addition or replacement, on reasonable data-protection grounds, within those 30 days. If you object we will work with you to find a solution. If we cannot, **you may stop using the affected tool and we will delete or return your content under clause DP10, at no cost to you** and neither of us owes the other anything further in respect of that tool.

DP6.6 Urgent replacement. We may engage a replacement sub-processor immediately, without the 30 days, where it is necessary to keep the tool secure or available. We will tell

you as soon as we reasonably can and your right to object under DP6.5 then runs from that notice.

DP6.7 A change to a sub-processor entry in annex 2 is us performing this clause. It does not change these terms and it does not need your agreement beyond the authorisation you have already given.

DP7.1 Where the tools run. All four tools are hosted in the European Economic Area, in Microsoft Azure regions inside it and are operated by us from the Netherlands. **Annex 2 says which region each service runs in.**

DP7.1.1 Where a tool sends a request to an AI service is a different question from where the tool is hosted, so we answer it separately rather than letting the answer to the first stand for both. TaxMap does not send anything to an AI service today. A mapping-proposal feature that does is being built. It is not available, and this schedule will state what it sends and where those requests are processed before it is made available. TaxTrack sends uploaded documents only to Microsoft's document-reading service in West Europe. TaxTag's AI processing runs on a deployment confined to Microsoft's EU data zone. **TaxLex composes its answers on a deployment inside Microsoft's EU data zone by default and two of the models you can choose in TaxLex, `gpt-5.4-nano` and `gpt-5.4-pro`, are published by Microsoft only as globally routed deployments. Microsoft may process a request sent to either of those two in any region in which the model is deployed, including outside the European Economic Area.** What that means for what you send is at DP7.2.

DP7.2 What leaves the European Economic Area and we would rather tell you than have you find it.

> **Email TaxLex sends.** TaxLex sends email through SendGrid, in the United States. Two kinds go this way: password-reset email, and a Pillar Two alert digest for those who receive it. What reaches SendGrid is the recipient's name, work email address and the body of the message. **The digest body is drawn from published legislative and regulatory sources, and the selection of items in it indicates which jurisdictions the recipient follows. No content you put into a tool is ever sent through this route.**
>
> **The text of a question you send to a globally routed model in TaxLex.** TaxLex lets a user choose which model answers a question. **Two of the models offered, `gpt-5.4-nano` and `gpt-5.4-pro`, exist only as globally routed deployments**, so when a user selects one of them Microsoft may process that request in any region in which the model is deployed, including outside the European Economic Area. **What is sent is the text of the question and the material**

assembled to answer it. Content from documents in your library is not sent to either of those two models: where library content is in the material assembled to answer a question, TaxLex uses a deployment inside Microsoft's EU data zone instead. **Where a TaxLex request is served from is not fixed in advance.**

Microsoft's own access to the services the tools run on. Microsoft personnel and Microsoft companies outside the European Economic Area can reach data held in those Azure services. Microsoft documents four routes and we would rather set them out than describe them as support: **engineers may need remote access when a service is down or needs a repair automated tooling cannot make; data processed for security purposes, which is normally pseudonymised and in limited cases includes your content, may be transferred to any Azure region worldwide; network traffic may occasionally be routed outside the EU Data Boundary to keep the service available; and limited sign-in directory data, including a username and an email address, may be replicated outside that boundary.** This applies to all four tools and it is not something you or we trigger.

DP7.2.1 One step happens on every TaxLex question whichever model is chosen, so we state it separately rather than inside a bullet about one of them. Before any model sees your question, TaxLex turns that question into a search vector using a Microsoft AI service. **Everything said in DP7.3 about the safeguards applies to that step as well and annex 2 says where that step runs.**

DP7.3 The transfer mechanism, described as it actually is rather than in the shorter version a reader might expect.

The transfers described in DP7.2 are made by us, because we hold the accounts with the providers concerned. We are established in the Netherlands and there is no step in the chain between you and us that leaves the European Economic Area, so nothing needs a transfer mechanism before those transfers. We say that expressly rather than leaving you to work it out.

For **SendGrid** we transfer directly. **Twilio's data protection addendum does not put a single mechanism behind it. It ranks two and applies whichever ranks highest and is available at the time, so we describe the ranking rather than naming the half of it a reader might expect.**

Ranked first is the EU-US Data Privacy Framework. The addendum records that Twilio Inc. is self-certified under it, which brings the transfer within the European Commission's adequacy decision for that framework, Implementing Decision (EU) 2023/1795. **Ranked behind it and designated by the addendum to apply automatically if that self-certification is withdrawn, terminated, revoked or otherwise invalidated are the**

standard contractual clauses adopted by the European Commission in Implementing Decision (EU) 2021/914: **module three, processor to sub-processor, for content you put into a tool and module two, controller to processor, for the data we hold as controller about the people who use a tool**, because we transfer the first as your processor and the second in our own right. **Twilio must tell us in writing if the self-certification falls away. Twilio Inc. is the organisation self-certified under the framework and the named data importer under the clauses, whichever Twilio company holds the account, so this is the position either way.**

We are telling you how the addendum is arranged. We are not offering the certification to you as a safeguard of ours and we do not ask you to rely on it. A self-certification can be withdrawn. The adequacy decision standing behind it is under challenge before the Court of Justice. **That is exactly why the second mechanism is worth stating: if the first one goes, this transfer moves to signed clauses by the operation of the addendum itself rather than by a new negotiation with the provider.**

Microsoft is different in structure and the difference matters to you. Our contract is with **Microsoft B.V.**, a company established in the Netherlands, so that transfer does not leave the European Economic Area at all. **The transfers described in the second and third bullets of DP7.2 are made by Microsoft rather than by us** and Microsoft is obliged to put its own safeguards on them. It does: the Microsoft Products and Services Data Protection Addendum annexes the 2021 standard contractual clauses between two Microsoft companies for transfers out of the European Economic Area and commits that all such transfers are subject to those clauses. **We are not a party to those clauses and we do not describe ourselves as the exporter under them.** What we hold instead is Microsoft's contractual commitment: that it will engage no other processor without the safeguards that addendum requires, that it remains fully liable for that processor's performance, that it will challenge and narrow any government demand for your data and never give unfettered access and that transfers may be suspended or the agreement terminated if the law changes to your material disadvantage. **Microsoft's EU Data Boundary commitments sit alongside all of that. They are a commitment about where processing is performed. They are not a transfer mechanism. We do not rely on an adequacy decision for the Microsoft transfers described in DP7.2. The one route where an adequacy decision does operate is SendGrid. We set that out where we describe SendGrid rather than denying it here**, because Twilio's addendum ranks the framework ahead of the clauses and a blanket denial would be untrue of the SendGrid route.

DP7.4 Our assessment of those transfers. We have carried out a transfer impact assessment covering every transfer of personal data outside the European Economic Area in connection with the tools, using the six-step method in the European Data Protection Board's Recommendations 01/2020 read with the Court of Justice's judgment in *Schrems II* (C-311/18). **We make it available to you on request.**

DP7.5 Not used. The number is kept so that the numbering of this schedule does not move between versions.

DP7.6 What may enter an AI-assisted engineering or support session. We build, maintain and support the tools ourselves, using AI-assisted engineering and support software. Where a problem is investigated, data is migrated or a request you have raised with us is worked on, content held in a tool can enter that software. **This is not a feature of any tool and it does not happen during your ordinary use of one.** It happens when the service is worked on. **The providers that may process your content on this route are the ones listed in annex 2, and no other. We restrict what may enter such a session. This clause is where that restriction binds us.** Synthetic or redacted data must be used first. Your content may enter such a session only where the task genuinely requires it and an extract cannot answer the question. **Whole documents, national identification numbers, special category data and bulk exports must not enter such a session at all.** We keep a record of the occasions when your content does enter one. **We tell you on request how we give effect to these restrictions.** Where a tool sends your content to a Microsoft AI service, clause DP7.7 applies to that as it applies to the tools.

DP7.7 What Microsoft does with content sent to its AI services. Where a tool sends your content to Microsoft's Azure OpenAI Service, Microsoft does **not** use it to train or improve its own models or OpenAI's. **Microsoft's licence terms commit it not to use customer data to train any generative AI foundation model except on the customer's own documented instructions, and we give no such instruction.** That is Microsoft's default position and not something we had to buy. **Microsoft also runs abuse monitoring, which is a separate mechanism from training and is on by default.**

What that involves, stated from Microsoft's licence terms rather than from the shorthand. Microsoft's terms say that, as part of providing the service, it temporarily stores what a tool sends to it and what the service sends back, in order to monitor for and prevent abusive or harmful use. Where its automated systems flag something, authorised Microsoft employees may review that content to investigate and verify potential

abuse. **For a customer whose deployment sits inside Microsoft's EU data boundary, Microsoft's terms commit that those authorised employees are located in the European Economic Area. We do not tell you that every deployment we use sits inside that boundary, because which of them do is not established. What we are able to say, tool by tool, is at DP7.1.1, and it records that two of the models selectable in TaxLex are published by Microsoft only as globally routed deployments.** Microsoft's published documentation describes a narrower ordinary practice, under which content that is flagged and then reviewed by automated means is not additionally stored by the abuse-monitoring system and under which review by a person is the exception introduced where automated review does not meet Microsoft's confidence thresholds or is unavailable. **Where Microsoft's licence terms and its documentation differ we tell you what the licence terms say. Where content is stored for abuse monitoring, Microsoft's published position is that the store sits in the geography your resource is in and that this is so whether the deployment is a globally routed one or a data-zone one, because a globally routed deployment changes where processing happens and not where data is kept at rest. Microsoft publishes no retention period for this store and we will not state one.**

Switching it off requires Microsoft's approval for modified abuse monitoring, which we do not hold and for which, on Microsoft's published eligibility criteria, we do not expect to qualify. **This is processing Microsoft carries out in order to provide the service rather than for a purpose of its own** and Microsoft's own agreement limits the purposes it may pursue as an independent controller to billing, compensation, internal reporting and financial reporting, in each case **without accessing or analysing the content you put into a tool.**

DP8.1 Taking into account the nature of the processing, we help you by appropriate technical and organisational measures, so far as it is possible, to answer requests from individuals exercising their rights under Chapter III of the General Data Protection Regulation.

DP8.2 If an individual contacts us directly about content you put into a tool, **we will not answer the substance of the request ourselves.** We will tell them to contact you and we will pass the request on to you without undue delay.

DP8.3 How we help, in practice. We handle these requests by hand rather than through a feature in the tool. Ask us and a person deals with it. We aim to respond to you within five

working days.

DP8.4 Two things we do not delete when we act on an erasure instruction. You should factor both into your own answer to the individual. The first is records we are required by law to keep. The second is the audit trail of who did what in the tool and **what we can do to that trail differs by tool, so we say it per tool rather than for all four:**

> **TaxTag.** The audit record is rewritten to remove the details identifying the individual and the record of the action itself remains. The trail is kept for 24 months.
>
> **TaxLex, TaxMap and TaxTrack.** The audit record remains as written. **We do not today have a way to strip the identifying details out of it**, so the record of the action and of who took it, stays. Annex 1 gives the retention period for each.

Where you need an audit record removed rather than retained, ask us and we will tell you what is possible in that tool before you answer the individual.

DP8.5 We cannot reach content Microsoft holds in the store it keeps for the abuse monitoring described at clause DP7.7. **That store is not exposed to us, Microsoft publishes no retention period for it and switching the monitoring off requires an approval we do not hold.**

DP9.1 Breaches. We notify you of a personal data breach affecting personal data we process on your behalf **without undue delay and in any event within 72 hours** of becoming aware of it. **We become aware of it when we become aware of it or when any sub-processor we engage becomes aware of it, whichever is earlier.** Our notice will describe the nature of the breach, the categories and approximate number of data subjects and records concerned so far as we know them, the likely consequences and the measures we have taken or propose to take.

DP9.2 We help you meet your own obligations under Articles 32 to 36 of the General Data Protection Regulation, taking into account the nature of the processing and the information available to us. That includes helping you with a data protection impact assessment and with any prior consultation with a supervisory authority that **you** are required to carry out.

DP9.3 We tell you if we become aware that a feature of a tool, as you have configured it, is likely to affect your own assessment of the risk of the processing.

DP10.1 When the tool stops being provided to you, **you choose whether we delete your content or return it.** Tell us which. If you tell us nothing, we will give you at least **30 days** from the day the tool stops being provided to get your content out and we will then delete it.

DP10.2 Where the tool has a self-service export you can use it yourself. **Where it does not, ask us and we will get your content out to you within that period, in a structured, commonly used and machine-readable format wherever the tool allows one.** We do this by hand rather than through a feature in the tool. If the format you need is not one the tool can produce, we will tell you what it can produce before the period runs out rather than at the end of it.

DP10.3 After that we delete the content and existing copies of it, unless Union or Netherlands law requires us to keep it or Union law or the law of the member state that applies to a sub-processor requires it to keep it, in which case we will tell you what is being kept and why.

DP10.4 Two exceptions you should know about. Backups are deleted on our ordinary backup rotation rather than immediately and remain protected by this schedule until they are. Audit records are treated as described in clause DP8.4.

DP11.1 We make available to you the information necessary to demonstrate compliance with Article 28 of the General Data Protection Regulation. We may do that through a standard response pack rather than a bespoke answer each time.

DP11.2 We allow for and contribute to audits, including inspections, conducted by you or an auditor you appoint. An audit is at your cost, on at least 30 days' written notice, during business hours, no more than **once in any twelve-month period** and conducted so as not to disrupt the tool or the confidentiality of our other customers' data.

DP11.3 The once-a-year limit does not apply where a supervisory authority requires an audit or where one follows a personal data breach affecting your content.

DP11.4 Your auditor must not be a competitor of ours and must sign a confidentiality undertaking before the audit begins.

DP12.1 This schedule carries the **same version identifier as the terms of use it forms part of**. It is published as a separate document rather than printed at the end of them, at its

own address, in a form you can save and reproduce. Every superseded version stays available at a permanent address. **The version identifier ends in -NL, which records that this is the version of the terms under which Blauw Belastingen B.V. is your contracting entity.**

DP12.2 If we change this schedule we will publish the changed version, say what changed and say the date it applies from and we will tell you before it applies. Clause 7.3 of the terms of use governs how we make that change.

DP12.3 Annex 2 is different and changes under clause DP6. It carries its own version identifier and its own dated record of changes. **Updating annex 2 is us performing clause DP6. It is not a change to this schedule or to the terms.**

DP12.4 When a change to annex 2 is also a change to this schedule. We treat a change to annex 2 as a change to this schedule under DP12.2 as well and give you notice accordingly, where it:

- changes **whose data** an entry processes, in particular where an entry begins to process content you put into a tool when it did not before,
- changes **who engaged** an entry, so that the chain between us and that entry gets longer or shorter,
- changes **where the processing happens**, into or out of the European Economic Area or between countries outside it,
- changes the **mechanism** a transfer outside the European Economic Area is made under or replaces a sub-processor's **data-protection terms with materially different terms**, even if the provider, the country and the mechanism all stay the same.

Anything else that is not simply a change of a provider's name, its role, the service it performs or its region within the European Economic Area and anything we are unsure about, we treat the same way. Each of these is something you rely on for your own record of processing and your own transfer assessment, so where there is doubt we would rather tell you twice than not at all.

Annex 1: what we process, per tool

This annex forms part of schedule DP and carries the same version identifier.

Subject matter and duration. The provision of the TIF Suite tool you use, for as long as the terms of use are in force between us, plus the period in clause DP10.

Nature and purpose. Hosting, storing, indexing, retrieving, transforming and displaying the content you put into the tool, so that the tool does what you use it for, together with securing it, backing it up, keeping an audit record of what was done in it and supporting you when you ask us to.

Types of personal data. Whatever personal data appears in the content you choose to put into a tool. **You decide what that is and it is unbounded from our side.** In practice it includes names, work contact details, job roles, ledger and payroll entries, entity and engagement details and the free text of documents, questions and responses. **See the note below on data you should not put in at all.**

Categories of data subject.

Your own staff, in all four tools.

Named individuals responsible for a task, a deadline or a sign-off, in TaxTrack.

People outside your organisation whom you invite to complete a questionnaire, in TaxTrack. These people are not party to our terms with you and may not know we hold anything about them. **Telling them is your responsibility as controller and clause DP2.4 says so.**

Any individual named in a document, a ledger line or a file you upload, in TaxTag and TaxMap. For a transfer-pricing local file that means employees. For a trial balance or a general-ledger extract it can mean payroll data.

Any individual named in a question you type or a document you upload, in TaxLex.

Per tool. The table below states, for each tool, what is stored about the user, what content is held, whether the tool is AI-assisted and what is sent, where it is hosted and how long each category is kept.

Tool	What it stores about you as a user	What content it holds	AI, and what is sent	Where it is hosted	How long
TaxLex	Email, name, organisation, role, your saved preferences. Sign-in and session records. A log of your actions	The text of your questions, which TaxLex keeps. Your questions and the answers, saved as chat history. A separate short record of each question asked, shortened to the first 1000 characters. Feedback you give us. Prompts you save.	Yes. Your question and the source passages found for it are sent to Microsoft's Azure OpenAI Service to compose the answer. Uploaded image-only PDFs are read by Microsoft's document-reading service. You choose which model answers. **Two of the models offered, `gpt-5.4-nano` and `gpt-5.4-pro`, exist only as globally routed deployments, so Microsoft may process a request sent to either outside the EEA. Content from documents in your library is never sent to those two**: where	Azure West Europe. Answer composition runs on an account in Azure Sweden Central, which is in the EEA, on a deployment inside Microsoft's EU data zone by default. What leaves the EEA: account emails through SendGrid in the United States; the text of a question where Microsoft processes it on a globally routed deployment, which is the case whenever a user picks one of the	Chat history up to 24 months from the last message, and you can delete a chat yourself at any time. The question record 90 days. Feedback 90 days. Session records 7 days. Uploaded files 24 months from last use. Audit records 7 years. Saved prompts and

Tool	What it stores about you as a user	What content it holds	AI, and what is sent	Where it is hosted	How long
		Engagement details you enter. Files you upload to your library and the text extracted from them	library content is in the material assembled to answer a question, TaxLex uses a deployment inside Microsoft's EU data zone instead	two models named alongside; and Microsoft's own access to the services from outside the EEA, by the four routes at clause DP7.2	engagement details are kept until you delete them
TaxTag	No profile is stored. Your email, role and organisation are read from your sign-in for each request and held in your session. Your actions are recorded in an audit log against your sign-in identifier	Word templates, spreadsheets and mapping files you upload. Documents the tool generates. Templates you save to your library, whether private to you or shared with your organisation	Yes, in one place. When you ask for tag suggestions, the text of that document, including its headers and footers, is sent to Microsoft's Azure OpenAI Service. **It is not sent at all unless you first declare the document contains no real client data.** No structured data file is ever sent, and your name, email and the file name are not sent	Azure West Europe. The AI call runs on a deployment confined to Microsoft's EU data zone	Uploads and generated documents are deleted 24 hours after you finish with them. Library templates are kept until you delete them. Audit records 24 months, with your identity removed if you ask us to erase your data
TaxMap	Email, display name, your sign-in identifier, the date your account was created. Nothing else. We do not even store which organisation you belong to	Account listings, general ledger and trial-balance extracts you upload, held as you uploaded them. The working copy of that data. The mappings, transformations and cleaning steps you configure. A record of every material action	Not today. TaxMap's column-matching suggestions compare column names against a fixed dictionary and by ordinary text matching, and **nothing you put into TaxMap is sent to any AI provider**. A mapping-proposal feature that does use AI is being built and will be made available. When it is, the names of your columns and the mapping structure you have configured are sent to Microsoft's Azure OpenAI Service. **The figures, ledger lines and account balances in your file are not sent**	Azure West Europe. **Where the mapping-proposal requests will be processed is not established and clause DP7.1.1 will state it before that feature is made available.** Microsoft's own access to the services from outside the EEA applies, by the four routes at clause DP7.2	Kept until you delete the workflow, which deletes what belongs to it. There is no automatic deletion timer. Audit records are kept long-term
TaxTrack	Email, your role, your sign-in identifier, the date you were added. A record of your sign-ins and sign-outs, which includes your IP address and browser. Your acknowledgement of our disclaimer, with the version and the date	Your workflows, tasks, deadlines, sign-offs and rejections and who is responsible for each one. Assessment notices and other documents you upload and the fields read out of them. Questionnaire responses, including from people outside your organisation you invite	No chat or text generation. Uploaded assessment notices are read by Microsoft's document-reading service, which pulls out fields such as amounts, dates and names using a standard pre-trained model. A person confirms what it read before it enters the record. Dutch social-security numbers are removed at two points: when a document you upload is read and again when a person confirms what was read. **They are not removed from every record the tool keeps**	Azure West Europe, including the email service, which is set to hold data in Europe. Nothing leaves the EEA	Workflows are kept while they exist. Uploaded documents move to cheaper storage at 7 years and are deleted at 10 years, matching the longest record-keeping rule we cover. In-app notifications 90 days. **The audit trail is kept indefinitely and is not deleted on an erasure request**, because it is the evidence trail of a tax record

Data you should not put into a tool

Do not put a Dutch burgerservicenummer, an Irish personal public service number or any equivalent statutory identification number of another country, into any tool. We have no statutory basis to hold one.

Do not rely on any tool to take one out for you. No tool in the Suite is a filter, none of them is designed to detect a statutory identification number and we do not claim that any of them does. Where a tool carries out any removal of its own, it is a convenience inside that tool and it is not something you should build a process on.

Please also think carefully before uploading documents containing special category data within Article 9 or criminal-offence data within Article 10. The tools have no capability to detect either and we do not claim one.

Annex 2: sub-processor list

Annex 2 is published as a separate document at https://www.tifsynergy.com/legal/sub-processors/. It carries its own version identifier, `SUBPROCESSOR_LIST_VERSION`, its own dated record of changes, and every superseded version stays available at that address followed by that version's identifier.

It is published separately on purpose. Under clause DP6 we can change a sub-processor entry without changing these terms, so the list has to be able to change while this schedule does not. **We record the version of annex 2 that was in force when you accepted, together with its address, so that what you were shown can be identified later.**

Annex 3: our security measures

This annex forms part of schedule DP and carries the same version identifier. It describes measures operated today, not measures we intend to build. Clause DP1.6 applies: we operate these measures ourselves and through the providers listed in annex 2, and **we remain fully liable to you for them under clause DP6.3.**

Common to all four tools. Each of these applies to every tool without qualification.

TLS 1.2 or better in transit, with HTTP redirected to HTTPS.

Encryption at rest using Azure platform-managed AES-256 keys.

Sign-in through Microsoft Entra with RS256 token validation against the published key set and no shared secrets in the sign-in path.

Secrets held in Azure Key Vault and reached by managed identity.

Hosting in Microsoft Azure regions in the European Economic Area, as described at clause DP7.1.

All product functionality sits behind sign-in. The only public surfaces are TaxMap's waitlist form and TaxTrack's invitation-only questionnaire link, which carries its own token check and neither gives access to a tool.

Each tool scopes a request for stored content to the identity of the signed-in user, established from the validated sign-in token rather than from anything the request supplies.

A record of material actions is written in every tool.

A restriction on what may enter an AI-assisted engineering or support session, set out at clause DP7.6.

What separates your data from another customer's, stated per tool because the mechanism genuinely differs.

TaxLex. Content held in the library carries an organisation partition and its storage path mirrors that partition, with the organisation taken from the signed-in user's validated token and never from anything in the request. Retrieval of library content is filtered to the caller's own organisation, and a second, independent check applied after retrieval discards any result that does not belong to it. **The second check is deliberate redundancy: an automated test disables the first control and asserts that the second one still refuses.**

TaxTrack. Every database container is partitioned by organisation and the organisation value is re-fetched from the Suite on each authenticated request rather than accepted from the token or from the request body, so a caller cannot assert an organisation it does not belong to.

TaxTag and TaxMap. Separation is per user rather than per organisation. Every request is scoped to the signed-in user through a single check applied consistently across the tool's routes, so one user does not reach another user's uploads, workflows or saved work. **Neither tool holds an organisation boundary in its data layer today and neither is described here as if it did.**

One shared area, in TaxTag. TaxTag has a shared template library. Anything one of your users chooses to publish into it is visible to other users of the tool, **including users outside your organisation**. Nothing reaches it unless one of your users publishes it there. TaxTag asks that user to confirm the item contains no real client content before it can be shared. **No other tool has a shared area of any kind.**

The record of what happened in a tool, stated per tool for the same reason.

TaxMap. Enforced by the database itself. The application's database role holds insert and select on the audit table and holds neither update nor delete; deletion sits with a separate role which cannot log in at all, having no password; and an automated test asserts on every build, against a real database, that an attempted change or deletion is actually refused. **This is the only place in the Suite where the store, rather than the application's own restraint, is what prevents an audit record being altered.** It protects the trail against the application's own credential. The administrative role that owns the tables and runs migrations is not restricted by it.

TaxTrack. The audit record is written before the change it records and the operation fails if the record cannot be written, so a change to your data cannot complete without a record of it. No part of the application updates or deletes an audit record.

TaxLex. Audit records are written and are never amended or deleted by any part of the application.

TaxTag. Audit records are written to a file that the application can rewrite and does rewrite in one defined case, to remove identifying detail where an erasure request requires it. Every event is also forwarded to a separate Microsoft monitoring store, using an identity that can add records there and can neither alter nor delete them.

Measures in individual tools that go beyond that baseline.

TaxTag scans uploaded Word files for zip-bomb and template-injection patterns before accepting them.

TaxTrack disables key-based access to its database and its storage entirely and scans uploaded files for malware before they can be read.

What we do not have, stated so you do not have to ask.

Multi-factor authentication is not enforced.

There are no customer-managed encryption keys.

We hold no SOC 2 and no ISO 27001 certification.

No independent third party has assessed our security and no penetration test has been carried out.

We do not yet run our security testing on a set cadence, so nothing here should be read as saying these measures are regularly tested. We can tell you when each of them was last checked and by whom.

QUESTIONS?

Write to info@tifsynergy.com with any question about this schedule.