



DATA PROCESSING AGREEMENT (DPA)

Standard DPA

gramflows 2026

General data processing agreement between gramflows (processor) and the customer (controller). Applies automatically to all agreements and subscriptions that involve the processing of personal data.

VERSION

v2026.1.2

VALID FROM

1 August 2026

REPLACES

v2026.1.1

ISSUED BY

gramflows

Contents

Application and acceptance 3

1 / Parties and contact details 3

2 / Recitals 4

3 / Rights and obligations of the controller 5

4 / The processor acts on instructions 5

5 / Confidentiality 5

6 / Security of processing 6

7 / Use of sub-processors 7

8 / Transfer to third countries 7

9 / Assistance to the controller 8

10 / Notification of a personal data breach 9

11 / Erasure and return of data 10

12 / Audit and inspection 10

13 / The parties' agreement on other matters 10

14 / Entry into force and termination 11

Appendix A — Information about the processing 13

Appendix B — Sub-processors 17

Appendix C — Instructions and security measures 20

Appendix D — Other matters 25

Version history 26

Application and acceptance

This data processing agreement (hereinafter the "DPA" or the "Clauses") is gramflows' standard agreement for the processing of personal data on behalf of customers. The DPA is accepted automatically as an integral part of any quote, subscription, order or ongoing agreement between gramflows and the customer that involves the processing of personal data on the customer's behalf.

The version of the DPA in force at any given time is available at gramflows.com/dpa. The DPA does not require a separate signature, but gramflows will, on request, provide a signature-ready version to customers whose internal policies require physical or electronic signing.

In this DPA the parties are designated as follows:

- **"The controller" or "the customer"**: the legal person that receives gramflows' services and determines the purposes and means of the processing of personal data.
- **"The processor"**: gramflows (VAT: CZ7309231259), which processes personal data on behalf of the customer in connection with the delivery of the agreed services.

The DPA is based on the Danish Data Protection Agency's (Datatilsynet) standard contractual clauses (most recently updated in March 2024) and has been adapted to gramflows' services. The DPA applies regardless of the specific service the customer receives — including Webmanager, hosting, development, automation (Make/n8n), SEO/content and consulting/advisory. Appendix A specifies the nature of the processing for each individual service.

Order of precedence in the event of conflict

In the event of any inconsistency between this DPA and the commercial agreements between the parties (quotes, orders, subscription terms, SOWs, etc.), this DPA takes precedence with regard to matters of data protection. Commercial terms (price, delivery times, notice of termination, etc.) are governed by the underlying agreement and by gramflows' terms of trade.

1 / Parties and contact details

1.1 The controller

The controller is the customer that has entered into an agreement with gramflows for the delivery of services involving the processing of personal data. The customer's identification (company name, registration number, address and contact person) is set out in the underlying commercial agreement (quote, order confirmation, invoice or subscription record).

The customer is responsible for ensuring that the contact details registered with gramflows are correct and up to date at all times, including contact details for the customer's DPO or other person responsible for data protection, if the customer has appointed one.

1.2 The processor

Company	gramflows
VAT	CZ7309231259
Address	Belehradská 858/23, 120 00 Prague, Czech Republic
Phone	+45 88 70 70 57
Email (general)	support@gramflows.com
Email (DPA matters)	dg@gramflows.com
Contact person	Dennis Erik Gam Nielsen, Owner
Supervisory authority	Úřad pro ochranu osobních údajů (ÚOOÚ), Czech Republic

Supervisory authority

As gramflows is established in the Czech Republic, the primary supervisory authority is the ÚOOÚ. For customers in Denmark, the Danish Data Protection Agency (datatilsynet.dk) acts as the local supervisory authority for the controller itself.

2 / Recitals

1. These Clauses set out the rights and obligations of the controller and the processor when personal data is processed on behalf of the controller.
2. The Clauses are designed to ensure the parties' compliance with Article 28(3) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (the General Data Protection Regulation, "GDPR").
3. In connection with the delivery of gramflows' services, the processor processes personal data on behalf of the controller in accordance with these Clauses.
4. The Clauses take precedence over any corresponding provisions in other agreements between the parties.
5. Four appendices are attached to these Clauses, and the appendices form an integral part of the Clauses:
 - Appendix A — information about the purpose and nature of the processing, the types of personal data, the categories of data subjects and the duration.
 - Appendix B — approved sub-processors and notice periods for changes.
 - Appendix C — instructions and minimum requirements for technical and organisational security measures, as well as audit procedures.
 - Appendix D — other matters (governing law, venue, liability, etc.).

6. The Clauses and their appendices must be kept in writing, including electronically, by both parties.
7. These Clauses do not release the processor from obligations imposed on the processor under the GDPR or any other legislation.

3 / Rights and obligations of the controller

1. The controller is responsible for ensuring that the processing of personal data takes place in accordance with the GDPR (see Article 24 of the Regulation), the data protection provisions of other EU law or the national law of the Member States (including the Danish Data Protection Act) and these Clauses.
2. The controller has the right and the obligation to make decisions about the purposes and means of the processing of personal data.
3. The controller is responsible, among other things, for ensuring that there is a legal basis for the processing of personal data that the processor is instructed to carry out.
4. The controller is responsible for informing the data subjects about the processing in accordance with Articles 13 and 14 of the GDPR.

4 / The processor acts on instructions

1. The processor may only process personal data on documented instructions from the controller, unless required to do so under EU law or the national law of the Member States to which the processor is subject; in that case, the processor informs the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest, cf. Article 28(3)(a).
2. The controller's documented instructions to the processor are constituted by Appendix C to this DPA and by the underlying commercial agreement (including the quote, order confirmation, subscription description or SOW). Additional instructions may be given in writing to dg@gramflows.com.
3. The processor immediately informs the controller if, in the processor's opinion, an instruction infringes the GDPR or the data protection provisions of other EU law or the national law of the Member States.

5 / Confidentiality

1. The processor may grant access to the personal data being processed on behalf of the controller only to persons who are subject to the processor's instructions, who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, and only to the extent necessary. The list of persons who have been granted access must be reviewed on an ongoing basis. On the basis of this review,

access to the personal data may be withdrawn if it is no longer necessary, and the personal data must then no longer be accessible to those persons.

2. At the request of the controller, the processor must be able to demonstrate that the persons concerned who are subject to the processor's instructions are subject to the above-mentioned obligation of confidentiality.

6 / Security of processing

1. Article 32 of the GDPR provides that, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing in question, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor implement appropriate technical and organisational measures to ensure a level of security appropriate to those risks.
2. The controller must assess the risks to the rights and freedoms of natural persons posed by the processing and implement measures to mitigate those risks. Depending on their relevance, these may include:
 - pseudonymisation and encryption of personal data;
 - the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
 - the ability to restore the availability of and access to personal data in a timely manner in the event of a physical or technical incident;
 - a procedure for regularly testing, assessing and evaluating the effectiveness of the technical and organisational measures for ensuring the security of the processing.
3. Under Article 32 of the Regulation, the processor must also — independently of the controller — assess the risks to the rights of natural persons posed by the processing and implement measures to mitigate those risks. For the purpose of this assessment, the controller must make the necessary information available to the processor so that the processor can identify and assess such risks.
4. In addition, the processor must assist the controller in complying with the controller's obligation under Article 32 of the Regulation by, among other things, making available to the controller the necessary information regarding the technical and organisational security measures already implemented by the processor pursuant to Article 32, as well as any other information necessary for the controller to comply with its obligation under Article 32.
5. The processor's minimum security measures are set out in Appendix C.2. If, in the controller's assessment, mitigating the identified risks requires the implementation of measures beyond those already implemented by the processor, the controller must specify in writing to the processor the additional measures to be implemented.

7 / Use of sub-processors

1. The processor must satisfy the conditions referred to in Article 28(2) and (4) of the GDPR in order to make use of another processor (a sub-processor).
2. The processor may not make use of a sub-processor for the fulfilment of these Clauses without prior general written authorisation from the controller.
3. The processor has the controller's general authorisation to use the sub-processors listed in Appendix B. The processor must notify the controller in writing of any planned changes concerning the addition or replacement of sub-processors with at least 30 days' notice, thereby giving the controller the opportunity to object to such changes before the sub-processor(s) concerned are used.
4. Notification of changes to sub-processors is given by email to the customer's primary contact person registered with gramflows and by updating the list at gramflows.com/dpa. It is the customer's responsibility to ensure that the registered contact person receives such notifications and passes them on internally.
5. Where the processor uses a sub-processor to carry out specific processing activities on behalf of the controller, the processor must — through a contract or other legal act under EU law or the national law of the Member States — impose on the sub-processor the same data protection obligations as those set out in these Clauses, in particular providing the necessary guarantees that the sub-processor will implement the technical and organisational measures in such a way that the processing meets the requirements of these Clauses and the GDPR.
6. The processor is responsible for requiring that the sub-processor at least complies with the obligations to which the processor is subject under these Clauses and the GDPR.
7. The sub-processor agreement(s) and any subsequent amendments are sent — at the controller's request — in copy to the controller. Provisions on commercial terms that do not affect the data protection content of the sub-processor agreement need not be sent to the controller.
8. In its agreement with the sub-processor, the processor must include the controller as a third-party beneficiary in the event of the processor's bankruptcy, so that the controller can step into the processor's rights and enforce them against sub-processors.
9. If the sub-processor fails to fulfil its data protection obligations, the processor remains fully liable to the controller for the performance of the sub-processor's obligations. This does not affect the rights of the data subjects under the GDPR, in particular Articles 79 and 82.

8 / Transfer of personal data to third countries

1. Any transfer of personal data to third countries or international organisations may be carried out by the processor only on the basis of documented instructions from the controller and must always take place in accordance with Chapter V of the GDPR.

2. If a transfer of personal data to third countries or international organisations that the processor has not been instructed to carry out by the controller is required under EU law or the national law of the Member States to which the processor is subject, the processor must inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.
3. Without documented instructions from the controller, the processor may not, within the framework of these Clauses:
 - transfer personal data to a controller or processor in a third country or an international organisation;
 - entrust the processing of personal data to a sub-processor in a third country;
 - process the personal data in a third country.
4. The processor's default policy is that all personal data is processed within the EU/EEA. The controller's instruction regarding the transfer of personal data to a third country — if such an instruction is given — as well as the transfer basis under Chapter V of the GDPR (e.g. the European Commission's Standard Contractual Clauses) on which the transfer is based, must be specified in writing in Appendix C.6 or in a separate addendum.
5. These Clauses must not be confused with standard contractual clauses within the meaning of Article 46(2)(c) and (d) of the GDPR, and these Clauses cannot constitute a basis for the transfer of personal data within the meaning of Chapter V of the GDPR.

9 / Assistance to the controller

1. Taking into account the nature of the processing, the processor assists the controller, as far as possible, by appropriate technical and organisational measures in fulfilling the controller's obligation to respond to requests for the exercise of the data subjects' rights under Chapter III of the GDPR. This means that the processor must, as far as possible, assist the controller in ensuring compliance with:
 - the obligation to provide information when collecting personal data from the data subject;
 - the obligation to provide information where personal data has not been collected from the data subject;
 - the right of access;
 - the right to rectification;
 - the right to erasure ("the right to be forgotten");
 - the right to restriction of processing;
 - the notification obligation regarding rectification or erasure of personal data or restriction of processing;
 - the right to data portability;
 - the right to object;

- the right not to be subject to a decision based solely on automated processing, including profiling.
- 2.** In addition to the processor's obligation to assist the controller under Clause 9.1, the processor further assists the controller, taking into account the nature of the processing and the information available to the processor, with:
- the controller's obligation to notify the personal data breach to the competent supervisory authority without undue delay and, where feasible, no later than 72 hours after having become aware of it, unless the breach is unlikely to result in a risk to the rights or freedoms of natural persons;
 - the controller's obligation to communicate the personal data breach to the data subject without undue delay where the breach is likely to result in a high risk to the rights and freedoms of natural persons;
 - the controller's obligation to carry out, prior to the processing, an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment / DPIA);
 - the controller's obligation to consult the competent supervisory authority prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.
- 3.** The necessary technical and organisational measures, as well as the scope and extent of the processor's assistance, are set out in Appendix C.3.

10 / Notification of a personal data breach

- 1.** The processor notifies the controller without undue delay after becoming aware that a personal data breach has occurred.
- 2.** The processor's notification to the controller must, where feasible, take place no later than 48 hours after the processor has become aware of the breach, so that the controller can comply with its obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 of the GDPR.
- 3.** In accordance with Clause 9.2, the processor must assist the controller in notifying the breach to the competent supervisory authority. This means that the processor must assist in providing the following information, which under Article 33(3) must appear in the controller's notification of the breach to the competent supervisory authority:
 - the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
 - the likely consequences of the personal data breach;
 - the measures taken or proposed to be taken by the controller to address the personal data breach, including, where relevant, measures to mitigate its possible adverse effects.

4. Notification of a breach is given by email to the customer's registered primary contact person, as well as by telephone follow-up if the nature of the breach so requires. In urgent cases, the telephone is used as the first point of contact.

11 / Erasure and return of data

1. On termination of the services relating to the processing of personal data, the processor is obliged to erase all personal data processed on behalf of the controller and to confirm to the controller that the data has been erased, unless EU law or the national law of the Member States requires the personal data to be retained.
2. Erasure of personal data is carried out no later than 30 days after termination of the underlying agreement, unless otherwise agreed in writing between the parties, or unless the controller, before the expiry of the 30-day period, requests the return of the data in a structured, commonly used and machine-readable format.
3. Backup data containing personal data is erased in line with the ordinary backup rotation as described in Appendix C, but no later than 90 days after termination.
4. The processor issues written confirmation of erasure to the controller no later than 30 days after the erasure has been completed.

12 / Audit, including inspection

1. The processor makes available to the controller all information necessary to demonstrate compliance with Article 28 of the GDPR and these Clauses, and allows for and contributes to audits, including inspections, conducted by the controller or another auditor mandated by the controller.
2. The procedures for the controller's audits, including inspections, of the processor and sub-processors are specified in Appendix C.7 and C.8.
3. The processor is obliged to grant supervisory authorities that, under applicable law, have access to the controller's or the processor's facilities — or representatives acting on behalf of a supervisory authority — access to the processor's physical facilities upon presentation of appropriate identification.

13 / The parties' agreement on other matters

1. The parties may agree on other provisions concerning the service relating to the processing of personal data — for example on liability — as long as such other provisions do not, directly or indirectly, conflict with the Clauses or diminish the fundamental rights and freedoms of the data subject arising from the GDPR.
2. Such other matters are governed by Appendix D and by the parties' underlying commercial agreement and gramflows' terms of trade (gramflows.com/handelsbetingelser).

14 / Entry into force and termination

1. The Clauses enter into force at the same time as the entry into force of the underlying commercial agreement between the parties and are accepted automatically as an integral part of it. No separate signature is required.
2. The version of the Clauses in force at any given time is available at gramflows.com/dpa. The processor reserves the right to update the Clauses with at least 30 days' written notice to the controller. Material changes are communicated by email to the customer's registered primary contact person.
3. If the controller objects to a planned update, the controller may terminate the underlying commercial agreement with the notice period specified in that agreement or in gramflows' terms of trade. Until the termination takes effect, the previous version of the Clauses applies.
4. Either party may request that the Clauses be renegotiated if changes in the law or inexpediencies in the Clauses give rise to this.
5. The Clauses apply for as long as the service relating to the processing of personal data lasts. During this period, the Clauses cannot be terminated unless other provisions governing the delivery of the service relating to the processing of personal data are agreed between the parties.
6. If the delivery of the services relating to the processing of personal data ceases, and the personal data has been erased or returned to the controller in accordance with Clause 11 and Appendix C, the Clauses may be terminated by written notice from either party.



Information about the processing

The purpose and nature of the processing, the types of personal data, the categories of data subjects and the duration — per service category.

Appendix A — Information about the processing

A.1 Purpose of the processing

The processor delivers one or more of the services below to the controller. The specific services covered in each individual customer relationship are set out in the underlying commercial agreement (quote, order confirmation, subscription record or SOW).

The processor only processes personal data to the extent necessary to deliver the agreed services, and solely on documented instructions from the controller, cf. Clause 4.

A.2 Service categories (nature of the processing)

The table below describes the nature of the processing for each service category. Only the categories included in the individual customer relationship are relevant.

Service category	Nature of the processing
Webmanager (operation and maintenance of existing WordPress sites)	Access to the customer's WordPress installation (files, database, admin accounts) for the purpose of updates, backup, troubleshooting, security measures and support. The processor generally has read and edit access to all data stored in the customer's installation, but only processes personal data to the extent necessary to perform the task.
Hosting (managed WordPress hosting)	Operation of the server infrastructure on which the customer's WordPress installation and associated database are hosted. Storage, backup, monitoring, security filtering (WAF/DDoS) and delivery of content over the internet.
Development (custom builds, new sites, integrations)	Development and implementation of code, integrations and functionality on the customer's sites. Access to test, staging and production environments may be necessary. Testing with the customer's real data takes place only by explicit agreement; otherwise anonymised or synthetic test data is used.
Automation (Make/n8n flows that process customer data)	Design, setup and operation of automated workflows that transfer, transform or enrich data between the customer's systems and third-party services. Personal data may pass through flows in transit; persistent storage in the automation platform is limited to what is strictly necessary.
SEO / content (analysis, ranking, possibly CMS access)	Analysis of keyword data, ranking data, performance data and content optimisation. May include editorial access to the customer's CMS (typically WordPress) to implement on-page optimisation. Personal data is processed only to the extent it is linked to content (e.g. author names) or analytics data.
Consulting / advisory (ad hoc, short-term access)	Time-limited advice, review or resolution of specific issues. Access to the customer's systems is generally minimal and time-limited; access rights are removed immediately after the task is completed.

A.3 Types of personal data

The processing may include the following types of personal data, depending on the service and the customer's specific systems:

Ordinary personal data (GDPR Art. 6):

- Identification data: name, username, customer ID, membership number
- Contact details: email, telephone number, postal address
- Demographic data: date of birth, gender, language
- Technical data: IP address, user agent, session data, cookie ID
- Account data: encrypted passwords, login history, user roles
- Content data: comments, form submissions, uploads, correspondence
- Transaction data: orders, invoices, payment status (not card data)
- Analytics and performance data: page views, click behaviour, conversions

Sensitive personal data (GDPR Art. 9) and national identification numbers (CPR, section 11 of the Danish Data Protection Act):

As a rule, the processor does not process sensitive personal data or CPR numbers. If the customer's systems contain such data, or if a specific service requires the processing of such data, this must be agreed in writing prior to processing, and special technical and organisational measures may be required (e.g. end-to-end encryption, access segregation, dedicated logging). See Appendix C.2 for enhanced security measures when processing special categories of data.

A.4 Categories of data subjects

The processing may include the following categories of data subjects:

- The customer's own customers and members (end users)
- The customer's employees, freelancers and partners
- Visitors to the customer's website
- Newsletter and marketing recipients
- Form submitters, contact-form enquiries, support cases
- Administrators and users of the customer's back-end systems

A.5 Duration of the processing

The processing is not time-limited and lasts until the underlying commercial agreement is terminated or expires.

Retention periods for the various data types held by the processor:

- Production data (data in the customer's active systems): for as long as the agreement is in force, or until the customer erases the data itself
- Backups: 50 days rolling retention (see Appendix C.2)

- Audit and access logs: up to 24 months
- Error logs and support tickets: up to 12 months after the case is closed
- Security logs (login attempts, WAF events): up to 6 months

On termination of the agreement, all personal data is erased pursuant to Clause 11 and Appendix C.4.

B /

Sub-processors

List of approved sub-processors and notice periods for changes.

Appendix B — Sub-processors

B.1 General

The processor has the controller's general authorisation to use the sub-processors listed in the tables below. The sub-processors are divided into:

- **Active sub-processors** — used by default for all or most services
- **Conditional sub-processors** — used only for specific services where they are relevant, and only after prior agreement with the customer

The processor has ensured that a data processing agreement has been concluded with all of the sub-processors below in accordance with the requirements of Clause 7, including that the sub-processors are subject to equivalent data protection obligations. Documentation can be provided to the controller on request.

B.2 Active sub-processors

Name	Location	Nature of the processing
Hetzner Online GmbH (HRB 3204, Reg. Fürth)	Germany (EU)	Hosting of dedicated cloud server / VPS infrastructure. Storage of WordPress installations, databases and encrypted personal data.
Cloudflare Ireland Ltd. (Reg. 554251)	Ireland (EU)	CDN, Web Application Firewall (WAF), DDoS protection, SSL/TLS termination. Processing of IP addresses and request metadata. An EU contract is used; data is routed via EU nodes.
LIVEN STUDIO SAS (SIRET 901 423 434)	France (EU)	Daily incremental backup of WordPress installations (files and database, AES-256 encrypted). Backup retention: 50 days.
Google Ireland Limited (Google Workspace, Reg. 368047)	Ireland (EU)	Google Workspace for internal email, document management and support correspondence. Weekly full backup storage (encrypted backup archives) via Google Drive (EU region).
Make s.r.o. / Celonis SE (Make.com)	Czech Republic / Germany (EU)	Automation platform for the setup and operation of workflows between the customer's systems. Personal data may pass through flows in transit. EU data residency is used where available.
Siber Systems Inc. (RoboForm) — EU SCCs	USA	Secure storage of passwords and credentials for the customer's systems (for operational and support purposes only). AES-256 encrypted with a zero-knowledge architecture. Transfer basis: the European Commission's Standard Contractual Clauses (SCCs) + supplementary measures.

B.3 Conditional sub-processors

Used only if the specific service requires it. The controller is notified specifically before a conditional sub-processor is activated for the customer's agreement.

Name	Location	Use
Idura ApS (formerly Criipto ApS), CVR 35142207	Denmark (EU)	Provider of MitID integration (certified MitID broker). Activated only for solutions with a MitID flow. Processes name and date of birth in the verification flow. CPR is not processed by Idura.

B.4 Tools that are not sub-processors

The following tools are used by the processor in connection with its own work, but do not process the customer's personal data and therefore do not constitute sub-processors under this DPA:

AI tools (Anthropic Claude, Claude Code, etc.)

The processor uses AI tools (including Anthropic Claude and Claude Code) for general development and productivity work that does not involve the processing of the customer's personal data. AI tools are not fed the customer's personal data, customer database dumps, the customer's end-user data, or any other material that can identify the customer's data subjects. Should the processing of the customer's personal data with AI tools become relevant in the future, this will only take place after prior written agreement with the customer, an update to Appendix B of this DPA, and the establishment of an appropriate transfer basis and security measures.

B.5 Notice period for changes to sub-processors

The processor must notify the controller of planned changes concerning the addition or replacement of sub-processors with at least 30 days' notice, cf. Clause 7.3. Notification is given by email to the customer's registered primary contact person and by updating the list in force at any given time at gramflows.com/dpa.

If the controller objects to the change, the controller may choose to terminate the Clauses (and thereby the underlying commercial agreement) with the notice period specified in the underlying agreement or in gramflows' terms of trade.



Instructions and security

The controller's instructions and minimum requirements for technical and organisational security measures.

Appendix C — Instructions and security measures

C.1 Subject matter of the processing / instructions

The processor's processing of personal data on behalf of the controller takes place through the processor performing the services described in Appendix A.2 and in the underlying commercial agreement. This typically includes one or more of the following activities:

- Operation, hosting and maintenance of the customer's WordPress installations or other web solutions
- Development and implementation of code, plugins, integrations and custom functionality
- Setup and operation of automated workflows (Make/n8n)
- SEO and content analysis and editorial implementation
- Backup and restoration of data
- Support, troubleshooting and advice
- Logging of operational actions for the purpose of an audit trail and security

C.2 Security of processing

The level of security must reflect the nature of the personal data being processed. The processor is entitled and obliged to make decisions about which technical and organisational security measures are to be implemented to establish the necessary and agreed level of security.

As a minimum, the processor implements the following measures:

Technical measures

- All data transmission takes place over HTTPS with TLS 1.2 or newer. HTTP Strict Transport Security (HSTS) is enabled where relevant.
- Sensitive data fields (where relevant, e.g. CPR by special agreement) are stored solely AES-256 encrypted. Encryption keys are stored separately from the encrypted data.
- Backup files are AES-256 encrypted both in transit and at rest.
- Web Application Firewall (WAF) and DDoS protection via Cloudflare.
- Dedicated server with a fixed IP. Administrative access is possible only via SSH with key-based authentication.
- Two-factor authentication (2FA) is mandatory for all administrator accounts at the processor and for all administrator access to the WordPress back-end.
- Passwords are stored in an encrypted password manager (RoboForm) with a zero-knowledge architecture and 2FA.
- Automatic and manual security updates of the WordPress core, plugins and server OS on a weekly update cycle.
- Daily incremental backups and a weekly full backup. Backup retention: 50 days. Backups are stored in at least two geographically separated locations within the EU.

- An activity log (audit trail) records administrator actions, login attempts and critical system events.
- Monitoring of uptime, security events and file integrity.

Organisational measures

- Access to personal data is limited to persons with a work-related need (the need-to-know principle).
- All persons with access are subject to a written obligation of confidentiality.
- The list of persons with access is reviewed at least every six months and updated on an ongoing basis when there are staff changes.
- Documented procedures for handling personal data breaches (incident response).
- Documented procedures for backup, restoration and testing thereof.
- The processor keeps up to date on relevant threats and security measures.
- AI tools (Claude, ChatGPT, Copilot, etc.) are not used to process the customer's personal data without prior written agreement, cf. Appendix B.4.

Enhanced security for special categories of data

For agreed processing of sensitive data (GDPR Art. 9), national identification numbers (section 11 of the Danish Data Protection Act) or other data with an elevated risk profile, the processor implements — by prior agreement — supplementary measures such as:

- Field-level encryption with separate key storage
- Enhanced access logging and periodic review thereof
- Strict access rules (separation of duties)
- Narrowed retention

C.3 Assistance to the controller

The processor must, as far as possible — within the scope and extent below — assist the controller in accordance with Clauses 9.1 and 9.2 by implementing the following technical and organisational measures:

- Responding to requests from data subjects (access, rectification, erasure, restriction, data portability, objection) within a reasonable time, but no later than 10 working days from when the request is forwarded by the controller
- Providing a technical export of a data subject's data in a structured format on request
- Assisting with erasure on request, including confirming that erasure has been completed
- Assisting the controller in notifying a personal data breach, cf. Clause 10
- Assisting in the preparation of a data protection impact assessment (DPIA) if the controller deems this relevant

Assistance beyond ordinary operations may be time-consuming. The processor reserves the right to invoice assistance in accordance with the hourly rate in force at any given time if the

assistance significantly exceeds what can reasonably be expected within ordinary operations.

C.4 Retention period / erasure routine

Personal data is stored by the processor for the following periods:

- Production data: for as long as the underlying agreement is in force
- Backup data: 50 days rolling retention
- Log data (audit trail, administrator actions): up to 24 months
- Security log (failed login attempts, WAF events): up to 6 months
- Support tickets and error logs: up to 12 months after the case is closed

On termination of the service, the processor must erase all personal data within 30 days, cf. Clause 11. Backup data is erased in line with the ordinary backup rotation, but no later than 90 days after termination. Erasure is confirmed in writing to the controller.

C.5 Location of processing

Processing of the personal data covered by the Clauses may not, without the controller's prior written approval, take place at locations other than the following:

- Primary production server: Hetzner, Germany (EU)
- CDN/WAF/edge: Cloudflare EU nodes
- Daily backup storage: LIVEN STUDIO SAS, France (EU)
- Weekly backup storage and Workspace: Google Ireland Limited, Ireland (EU)
- Automation platform: Make s.r.o. / Celonis SE, Czech Republic / Germany (EU)
- Password management: RoboForm (Siber Systems Inc., USA) — encrypted zero-knowledge storage
- The processor's own administrative environment: Czech Republic (EU)

All locations — except RoboForm — are situated within the EU/EEA. For RoboForm, storage is zero-knowledge encrypted, which means that the provider technically has no access to the content of stored credentials. The transfer basis for RoboForm is the European Commission's Standard Contractual Clauses (SCCs).

C.6 Instructions regarding transfer to third countries

With the exception of RoboForm (cf. C.5), the controller does not instruct the processor to transfer personal data to third countries or international organisations. Any future transfer requires a new, documented and written instruction from the controller, as well as the establishment of a valid transfer basis under Chapter V of the GDPR (e.g. the European Commission's Standard Contractual Clauses) and the carrying out of a transfer impact assessment.

C.7 Procedures for auditing the processor

The controller is entitled to conduct an audit (including inspection) of the processor's compliance with these Clauses once a year, or more often if special circumstances give rise to it (for example, a personal data breach).

The audit may be conducted by the controller itself or by an independent third party appointed by the controller. During an audit, the processor makes available all relevant information, documentation and systems to the extent necessary to demonstrate compliance.

The audit must be announced in writing at least 14 days in advance and must not unduly disrupt the processor's operations. The controller bears its own costs in connection with the audit; the processor bears its own costs for the necessary participation. In the event of material deficiencies being identified, however, the controller may require the processor to bear reasonable costs of remediation.

In addition, the controller has ongoing access to request documentation of the security measures implemented, including the most recent audit report, erasure reports and backup tests.

C.8 Procedures for auditing sub-processors

The processor is obliged to obtain and review, on an annual basis, documentation of the sub-processors' compliance with Article 28 of the GDPR, including:

- The most recently published audit reports (e.g. ISO 27001, SOC 2, ISAE 3402/3000) where available
- The sub-processor's current privacy policy and security policy
- Documentation of the most recent penetration test and/or vulnerability scan where available

The controller has — if deemed necessary — the right to receive a copy of the above documentation. The controller further has the right — in special circumstances — to conduct its own audit (or have a third party conduct an audit) of a sub-processor, subject, however, to any contractual restrictions applicable to the sub-processor in question.

D /

Other matters

Liability, governing law, venue and order of precedence
in the event of conflict between agreement documents.

Appendix D — The parties' regulation of other matters

D.1 Liability and compensation

The parties' mutual liability and any compensation arising from a breach of this DPA or the GDPR are governed by the commercial agreement between the parties in force at any given time and by gramflows' terms of trade. To the extent nothing else is agreed, the ordinary rules of Danish law on compensation apply.

D.2 Governing law and venue

This DPA is governed by Danish law with regard to data protection matters, as the processing predominantly concerns data subjects in Denmark.

Any disputes arising from this agreement that cannot be resolved amicably are settled at the controller's home venue. For Danish customers, this will typically be the Copenhagen City Court (Københavns Byret) as the court of first instance. The processor may, however, choose to bring proceedings at the processor's own home venue in Prague, Czech Republic.

D.3 Supervisory authority and Lead Supervisory Authority

In accordance with Article 56 and Recital 36 of the GDPR, the following applies with regard to the competent supervisory authority:

- For supervisory cases concerning the controller's processing of personal data (including processing through the processor), the controller's primary supervisory authority is competent as Lead Supervisory Authority. For Danish customers, this is typically Datatilsynet (datatilsynet.dk). The ÚOOÚ (Czech Republic) participates as a concerned supervisory authority.
- For supervisory cases concerning solely the processor's own activities (independently of the customer relationship), the ÚOOÚ (Úřad pro ochranu osobních údajů, uoou.cz) is competent as the primary supervisory authority.
- The processor has the linguistic and administrative resources to handle communication with both Datatilsynet (Danish) and the ÚOOÚ (Czech/English) and assists the controller with relevant communication, cf. Appendix C.3.

D.4 Amendments to the agreement

Amendments or additions to this DPA are issued as a new version of the central standard document at gramflows.com/dpa with at least 30 days' written notice to the customer's registered primary contact person. If the controller objects to a planned change, the controller may terminate the underlying commercial agreement with the notice period specified in this agreement or in gramflows' terms of trade.

D.5 Order of precedence

In the event of any inconsistency between this DPA and the commercial agreements between the parties, this DPA takes precedence with regard to matters of data protection. Commercial terms are governed by the underlying agreement and by gramflows' terms of trade.

D.6 Severability

If one or more provisions of this DPA are declared invalid by a competent court or supervisory authority, this does not affect the validity of the remaining provisions. In that case, the parties must jointly replace the invalid provision with a valid provision that reflects the original intention as closely as possible.

Version history

Version	Date	Changes
v2026.1.2	1 August 2026	Updated entry-into-force date (valid from 1 August 2026). Condensed footer so that the version reference and page number sit on one line on all pages. Editorial standardisation of the company name "gramflows" (consistently written in lower case). No material changes to the data protection provisions.
v2026.1.1	14 May 2026	Clarified venue (asymmetric: the customer's home venue / the processor's home venue in Prague). Added a separate section D.3 on the Lead Supervisory Authority pursuant to GDPR Art. 56. Added a declaration of language capacity for communication with both Datatilsynet and the ÚOOÚ.
v2026.1	14 May 2026	First public version of gramflows' general standard DPA. Replaces all previous customer-specific DPAs.

Note

This document has been prepared on the basis of the Danish Data Protection Agency's standard contractual clauses (March 2024) and adapted to gramflows' services and cross-border configuration (Czech processor, primarily Danish customers). The DPA is based on Datatilsynet's standard template, which is EDPB-approved and applicable across the EU. The document is ready for use, but should be reviewed regularly to ensure consistency with any changes to Datatilsynet's standard template, EDPB guidelines or Czech data protection legislation.



PROCESSOR

gramflows

VAT: CZ7309231259

Belehradská 858/23, 120 00 Prague, Czech Republic

Contact: support@gramflows.com

DPA matters: dg@gramflows.com

Phone: +45 88 70 70 57

Web: gramflows.com · DPA: gramflows.com/dpa

Opening hours: Monday–Thursday 9–17 · Friday 9–15