

# Humly Data Processing Agreement

Processing of personal data on behalf of Humly customers

Version of 9 October 2026, revision 4, updated 11 October 2026. Replaces the version of 8 September 2022. Part of the Humly Customer Terms.

This Data Processing Agreement (DPA) sets out Humly's obligations when processing personal data on behalf of its customers under Article 28 of the General Data Protection Regulation (EU) 2016/679 (GDPR). It forms part of the Humly Customer Terms, and terms defined there have the same meaning here.

Annex 1 describes the processing for each part of the platform, Annex 2 the security measures, and Annex 3 the sub-processors.

## 1. Scope and roles

- 1.1 This DPA applies when Humly Solutions AB (**Humly**) processes personal data on behalf of a customer (the **Customer**) in providing Products under the Humly Customer Terms or any other agreement under which the Customer uses Humly Products, including Products acquired through a Partner (the **Agreement**).
- 1.2 The Customer is the controller of that personal data, or a processor acting for its group companies, in which case Humly acts as its sub-processor. Humly is the processor.
- 1.3 Humly processes certain personal data for its own purposes as a controller — such as the names and contact details of the Customer's contact persons, used to administer the customer relationship, licences and invoicing. That processing is described in Humly's Privacy Notice and is not covered by this DPA.
- 1.4 For self-hosted Software, Humly does not host the installation's database. This DPA applies to personal data Humly receives through authorised support or managed services and activated functions that use Humly or its suppliers, including the optional SMS/Text function. The relevant processing is described in Annexes 1 and 3. Separate licence/account administration by Humly as controller is covered by the Privacy Notice.
- 1.5 The subject matter, nature, purpose and duration of the processing, and the categories of data subjects and personal data, are described in Annex 1. Which of them apply depends on the deployment model and modules the Customer uses.

## 2. Instructions

- 2.1 Humly processes personal data only on the Customer's documented instructions, including with regard to transfers to a third country or an international organisation, unless required to do so by Union or Member State law to which Humly is subject. In that case Humly informs the Customer of the legal requirement before processing, unless the law prohibits this on important grounds of public interest.
- 2.2 The Customer's instructions are this DPA, the Agreement, the Customer's configuration and use of the Products — including the modules and Third-Party Services it enables — and any further written instructions agreed between the parties.
- 2.3 Humly informs the Customer immediately if, in its opinion, an instruction infringes data protection law and may suspend the processing concerned until the instruction is amended or its lawfulness is established. Mere confirmation of an unlawful instruction does not permit Humly to carry it out.

### 3. Humly's obligations

- 3.1 **Confidentiality.** Humly ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- 3.2 **Security.** Humly implements the technical and organisational measures described in Annex 2 to ensure a level of security appropriate to the risk, as required by Article 32 GDPR. Humly may update the measures as technology and risks develop, provided the overall level of security is not reduced.
- 3.3 Humly forwards data-subject requests concerning Customer processing without undue delay and responds only on the Customer's instructions unless required by law. The Customer may use the available Product functions and the CSV exports described in Customer Terms C.15, and request further assistance. Humly assists by appropriate technical and organisational measures, taking account of the nature of processing. Reasonable costs may be charged for assistance beyond normal Product functions, but a fee dispute will not prevent timely performance of Humly's statutory obligations.
- 3.4 **Other assistance.** Taking into account the nature of the processing and the information available to it, Humly assists the Customer in meeting its obligations under Articles 32 to 36 GDPR, including data protection impact assessments and prior consultation with a supervisory authority.
- 3.5 Humly notifies the Customer without undue delay and, except for the limited Floorplan timing provision in clause 5.2, within 48 hours after becoming aware of a personal data breach affecting Customer personal data. The notice gives the nature of the breach, affected categories and approximate numbers of people and records, likely consequences, measures taken or proposed, and a contact point, so far as then known. Humly provides further information as available and cooperates in addressing the breach. It does not wait for a complete investigation before initial notification.
- 3.6 Humly makes available information necessary to demonstrate compliance with Article 28 GDPR and this DPA, and allows and contributes to audits, including inspections, by the Customer or its mandated independent auditor. Relevant certificates and independent reports may be used where sufficient. Routine audits require 30 days' notice, take place during business hours under appropriate confidentiality, are normally limited to once annually and are at the Customer's reasonable cost. Notice and frequency limits do not apply where shorter notice or additional audit is reasonably required following a breach, credible evidence of non-compliance or a supervisory authority's request. Conditions and charges must not frustrate the audit right.
- 3.7 At the Customer's choice, Humly returns or deletes personal data when the relevant processing services end, unless Union or Member State law requires retention. Customer Terms C.15–C.17 provide export, at least 30 calendar days' retrieval after transition or termination, and the agreed deletion schedule. Active data is deleted at the end of retrieval or a later agreed date once switching or return is complete. Isolated backup copies expire no later than 30 days after active deletion; any restored copy is subject to the deletion again. An earlier lawful deletion instruction is honoured, with backup expiry within 30 days after active deletion. Legally retained data is identified and restricted to that purpose. These obligations apply to relevant sub-processors as well as Humly.

### 4. Requests from public authorities

- 4.1 If Humly receives a legally binding request from a public authority, including a judicial authority, for disclosure of personal data processed for the Customer, Humly will, to the extent legally permitted:
  - (a) notify the Customer without undue delay and, where possible, before responding, stating the data requested, the requesting authority and the legal basis invoked;
  - (b) follow the Customer's reasonable instructions to object, limit the request or seek interim measures, to the extent lawful;

- (c) disclose only the minimum personal data necessary to comply, on a reasonable interpretation of the request;
  - (d) assess the request's legality and challenge it, including by appeal, where reasonable legal grounds exist under applicable law; and
  - (e) if it is prohibited from notifying the Customer, use its best efforts to obtain a waiver of the prohibition and document those efforts.
- 4.2 Humly does not voluntarily disclose Customer personal data to public authorities or voluntarily enable their direct access. Legally compelled disclosure or access is handled under this clause and applicable data protection law. Humly notifies the Customer of such access without undue delay where lawful. A foreign authority's order does not itself dispense with Article 48 or Chapter V GDPR.
- 4.3 On request, and to the extent permitted, Humly informs the Customer of the number and type of requests received in the preceding twelve months concerning personal data processed for the Customer.

## 5. Sub-processors

- 5.1 The Customer gives general authorisation for the sub-processors listed in Annex 3. Humly binds each relevant sub-processor by contract to the data protection obligations required by Article 28(4) GDPR, providing protection consistent with this DPA, including the limited Floorplan provisions in clause 5.2. Humly remains responsible to the Customer for the performance of those obligations.
- 5.2 A sub-processor processes Customer personal data only for the deployment model or function identified in Annex 3. Enabling a function authorises the listed processors for that function; it does not waive the notice and objection rights for later changes. The following terms apply only to processing by Smplrspace and its onward processors for Floorplan. Smplrspace's applicable data processing terms, identified by version in Humly's supplier register and available at [www.smplrspace.com/dpa](http://www.smplrspace.com/dpa), supplement this DPA as follows.

For a breach confined to that Floorplan processing, Humly notifies the Customer without undue delay after Humly becomes aware, whether through Smplrspace or otherwise; the contractual 48-hour outer limit does not apply to that supplier-originating breach. Humly will not defer notification pending Smplrspace's confirmation. For changes in that supplier chain, Humly emails notice as soon as it receives it and provides as much advance notice as available, with an effective opportunity to object before the new processing. The contractual 30-day period does not apply to those changes. The Customer may object on reasonable data protection grounds and discontinue the affected Floorplan service under clause 5.4 if the objection cannot be resolved.

Smplrspace's deletion and audit procedures apply to its processing only to the extent consistent with Article 28 GDPR, applicable Data Act rights and the return, deletion and audit rights in this DPA. They do not make deletion conditional on payment or final invoicing, prevent necessary audits, or remove Humly's responsibility. No Floorplan term reduces mandatory protection. Transfers must have valid safeguards for Humly's processor role, including completed Module Three SCCs where that is the relied-on mechanism.

- 5.3 Except for the limited Floorplan supplier-chain provision in clause 5.2, Humly gives at least 30 days' notice before adding or replacing a relevant sub-processor, by updating the published list and emailing the registered account contacts. No notice is required for removal without replacement. The notice identifies the processing affected.
- 5.4 The Customer may object on reasonable data protection grounds within the notified period, normally 30 days. The parties seek a resolution before the disputed new processing begins. If none is available, the Customer may terminate the affected Product or Floorplan function without penalty and receive prepaid fees for the unused term. Refunds follow Customer Terms 2.3: for Partner purchases Humly

credits the Partner that paid Humly, and the Customer obtains the refund from its seller under their purchase agreement; for direct purchases Humly refunds the Customer.

- 5.5 Humly maintains an up-to-date record of the processors in the relevant processing chain and ensures the required protections apply throughout it. Relevant onward processors are identified in Annex 3 and its published register. Addition and replacement in that chain are subject to clauses 5.2–5.4; the obligation is not limited to processors that happen to be known to Humly.
- 5.6 Bradler & Krantz GmbH & Co. KG is a sub-processor for storage and media handling. It provides rack space, power, physical security, connectivity and bare-metal hardware, and maintains, replaces and disposes of that hardware. Humly administers firewalls, load balancing, proxies, operating systems, databases, storage, encryption, certificates and keys, and operates redundancy between the data centres. The operator has no logical access to Customer personal data; storage is encrypted at rest with keys held only by Humly. Its relevant processing is subject to Article 28 contractual protections.
- 5.7 A provider independently appointed by the Customer under its own agreement is not Humly's sub-processor merely because the Customer instructs an exchange of data with it. This may include the Customer's calendar and identity providers, Disruptive Technologies where independently appointed on activation, and a Partner or integrator appointed by the Customer. Resale, invoicing or acceptance of a provider's terms does not alone determine the role. Humly remains responsible for its own integration and subsequent processing, and for any provider Humly engages to process Customer data on Humly's behalf.

## 6. International transfers

- 6.1 Humly stores and processes the Customer's personal data within the European Economic Area (EEA). Personal data is processed outside the EEA only if the Customer has approved this, or to the limited extent stated against a sub-processor in Annex 3 for the modules, purposes and data stated there.
- 6.2 Transfers require a valid Chapter V GDPR basis: an applicable adequacy decision, including the EU–U.S. Data Privacy Framework for a certified recipient and covered processing, or applicable standard contractual clauses with any necessary supplementary measures. Humly verifies the actual recipient, processing and onward chain. For SCC transfers it documents the required transfer assessment. Annex 3 identifies the applicable safeguard.
- 6.3 The Customer is responsible for the lawfulness of its instructions to connect an independently engaged Third-Party Service. Humly remains responsible for its own obligations under Chapter V GDPR when acting on those instructions.

## 7. The Customer's obligations

- 7.1 The Customer is responsible for having a lawful basis for the processing, for informing data subjects — including about the modules and Third-Party Services it uses — and for ensuring that its instructions comply with data protection law.
- 7.2 The Products are not designed to process special categories of personal data, and the Customer will not instruct Humly to do so. Free-text fields, such as meeting subjects and visitor notes, may nevertheless contain such data if Users enter it; the Customer should instruct its Users accordingly.
- 7.3 The Customer responds to data subjects and supervisory authorities about the processing. Where Humly forwards a request or enquiry to the Customer, it does so only to bring it to the Customer's attention; this gives Humly no authority over how the Customer responds.

## 8. Liability

- 8.1 The contractual liability limits in Customer Terms clause 11 apply, including its higher limit for DPA claims and its overall aggregation rule. They do not restrict non-waivable rights of data subjects, mandatory contribution rights under Article 82 GDPR, or rights under applicable SCCs that cannot be limited. Between the parties, compensation under Article 82 is allocated in proportion to responsibility for the damage. Each party bears administrative fines imposed on it.

## 9. General

- 9.1 This DPA sets out minimum obligations. It is Humly's aim that its practice should exceed them; where it does, that practice does not amend this DPA or create an obligation to maintain a higher standard. Nothing in this DPA limits obligations that GDPR imposes directly on either party.
- 9.2 This DPA applies for as long as Humly processes personal data on the Customer's behalf. For that processing, it prevails over other standard contract documents. A signed agreement between Humly and the Customer may expressly amend this DPA, subject to applicable law and the precedence of applicable SCCs.
- 9.3 Changes follow Customer Terms clause 15. Humly will not reduce the protection of personal data while processing under this DPA, including for self-hosted support and managed services, except where a change is required by law. A change to a supplier's online terms does not by itself reduce the Customer's existing contractual rights.
- 9.4 This DPA is governed by the law, and disputes are resolved in the forum, that applies to the Agreement.
- 9.5 Questions about this DPA and data protection: [security@humly.com](mailto:security@humly.com).

## Annex 1 — Description of the processing

### 1. Subject matter, nature and purpose

Humly processes personal data to provide the Products to the Customer: hosting and operating the Cloud Services; synchronising bookings with the Customer's calendar and identity systems; showing availability and bookings on displays and devices; sending notifications and messages; and providing support, managed services and other Professional Services.

### 2. Duration

For the term of the Agreement and until deletion in accordance with clause 3.7.

### 3. Data subjects and personal data by deployment model and module

| Deployment model or module | Data subjects                                                                                                                                                       | Personal data                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Self-hosted</b>         | Individuals whose data is provided for support or managed services; recipients of activated SMS/Text and individuals affected by other activated external functions | Personal data made available for support or managed services and data processed by activated external functions described below. Humly does not host the installation's database.                                                                                                                                                                                                              |
| <b>Cloud</b>               | Users and administrators                                                                                                                                            | Name, email address, user identifier, role and permissions, authentication and single sign-on identifiers, language and other settings, access and audit logs including IP address.                                                                                                                                                                                                            |
| <b>Reservations</b>        | Users; organisers and participants of meetings and bookings                                                                                                         | Subject, organiser, participants and their email addresses, start and end times, event body, and the room, desk, parking space or other resource booked; check-in and no-show status. Badge or card identifier, or PIN, entered on a device to verify that a person may change a booking, which is relayed to the relevant cloud or self-hosted Humly Control Panel installation for checking. |
| <b>Visitor</b>             | Visitors; hosts                                                                                                                                                     | Visitor name, company, email address and telephone number; host; date and time of the visit, arrival and departure; vehicle registration number where visitor parking is used; content of emails sent to visitors through the Products.                                                                                                                                                        |
| <b>SMS/Text (optional)</b> | Recipients of text messages, such as visitors and Users                                                                                                             | Name, mobile telephone number and message content. The function is optional: it requires the purchase of text message credits and activation by the Customer, and no module requires it.                                                                                                                                                                                                       |
| <b>Floorplan</b>           | Users viewing a floor plan in a web browser; administrators editing a map                                                                                           | IP address and browser user agent transmitted to the floorplan service, with technical request and error context as described in Annex 3. User account identifiers, booking and calendar records are not transmitted merely to display a floorplan. Identifiable information in map content is personal data as described in section 4.                                                        |
| <b>Sensors (optional)</b>  | Individuals present in spaces monitored by occupancy sensors                                                                                                        | Occupancy and motion data for rooms and desks; personal data where it relates to a space used by one identifiable person.                                                                                                                                                                                                                                                                      |
| <b>Support</b>             | Users and others whose data is included in a support request                                                                                                        | Any personal data the Customer includes in a support request or makes accessible to Humly during a support session. The Customer limits this to what is necessary.                                                                                                                                                                                                                             |

#### **4. Buildings, resources and devices**

Data describing buildings, floors, rooms, desks, parking spaces, equipment and devices, including their names, identifiers and positions on a floor plan, is not in itself personal data. It becomes personal data when linked to an identifiable individual — for example through a booking, a desk or parking space assigned to a named person, a label containing a person's name, or occupancy data for a space used by one identifiable person — and is then treated as personal data under this DPA.

#### **5. Special categories of data**

The Products are not designed to process special categories of personal data. See clause 7.2.

#### **6. Location of processing**

Data centres in Germany and the Netherlands, and the sub-processors and locations listed in Annex 3.

#### **7. Retention**

The Customer controls how far back and ahead bookings are synchronised. Meetings deleted in the Customer's booking system are removed from active synchronised data; residual copies in backups expire under the 30-day backup cycle and clause 3.7. End-of-service return and deletion follow clause 3.7.

## Annex 2 — Technical and organisational security measures

Humly's information security management system is certified to ISO/IEC 27001:2022. The certified scope is "Development and sales of workplace solutions." Certificate CI-23524/2026, issued on 21 April 2026, references Statement of Applicability version 2.0. The security measures below apply to Humly's processing under this DPA.

| Area                         | Measures                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Governance</b>            | Information security policies approved by management and reviewed at least annually; a named owner of information security; risk assessment of changes, new suppliers and new functionality.                                                                                                                                                                                                                                                                                                                    |
| <b>People</b>                | Confidentiality undertakings for all staff and consultants; security awareness training; access removed promptly when people leave or change role.                                                                                                                                                                                                                                                                                                                                                              |
| <b>Access control</b>        | Unique personal accounts; role-based access on the principle of least privilege; multi-factor authentication for administrative access to production systems; periodic review of access rights; logging of privileged access.                                                                                                                                                                                                                                                                                   |
| <b>Data centres</b>          | Colocation facilities in Germany and the Netherlands with physical access control, surveillance, fire protection and redundant power and connectivity provided by the operator. The operator maintains, replaces and disposes of hardware; all storage is encrypted at rest with keys held only by Humly, so the operator cannot read data on it. Servers, backups and infrastructure such as firewalls, proxies and load balancers, and redundancy between the data centres, are administered solely by Humly. |
| <b>Separation</b>            | Each customer's data is logically separated from other customers' data.                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Encryption</b>            | Data in transit is encrypted with TLS. Devices connect to the Cloud Services over a TLS-encrypted connection and verify the server certificate before communicating. Databases and backups are encrypted at rest, with keys managed by Humly.                                                                                                                                                                                                                                                                   |
| <b>Devices</b>               | Devices store no personal data persistently. Firmware and software updates are cryptographically signed and verified before installation.<br>Devices do not listen on network ports in their default configuration, Bluetooth is disabled by default after provisioning, and remote screen-sharing for support is disabled by default.                                                                                                                                                                          |
| <b>Operations</b>            | Logging and monitoring of systems and security events; vulnerability management and timely patching; change management; penetration testing, normally annually.                                                                                                                                                                                                                                                                                                                                                 |
| <b>Backup and continuity</b> | Regular encrypted backups daily, kept 30 days; documented and tested restore procedures.                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Incidents</b>             | Documented incident response procedures; notification of personal data breaches in accordance with clause 3.5; reporting under the EU Cyber Resilience Act; coordinated vulnerability disclosure through security@humly.com.                                                                                                                                                                                                                                                                                    |
| <b>Suppliers</b>             | Sub-processors assessed before engagement and bound by data processing agreements.                                                                                                                                                                                                                                                                                                                                                                                                                              |

## Annex 3 — Sub-processors

Last updated: 9 October 2026, revision 3. “Applies to” identifies the relevant deployment or function. For self-hosted installations, Support entries apply, together with the entries for any activated function that processes data outside the installation, as described in Annex 1. SMS/Text is separate and optional, requires credits and activation, and is not required by any module. Floorplan processing is subject to clause 5.2. Auth0 and Postmark serve Humly’s own Smplrspace account only and do not process Customer personal data in this Floorplan deployment; they are therefore outside the processing covered by this Annex.

| Entity                         | Applies to     | Service                                                                      | Personal data                                                                                             | Location             | Safeguard outside the EEA                                                                                                                         |
|--------------------------------|----------------|------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| Bradler & Krantz GmbH & Co. KG | Cloud          | Colocation, bare-metal hardware, storage and media handling under clause 5.6 | All Cloud data, on systems administered solely by Humly                                                   | Germany; Netherlands | Not applicable (EEA)                                                                                                                              |
| Tuned Solutions of Sweden AB   | Cloud; Support | Compliance audit                                                             | All Cloud data, Data accessible in the course of support                                                  | Sweden               | Not applicable (EEA)                                                                                                                              |
| Desarrollo                     | Cloud; Support | Cloud operations                                                             | All Cloud data, Data accessible in the course of support                                                  | Spain                | Not applicable (EEA)                                                                                                                              |
| Softhouse AB                   | Cloud; Support | Second-line support                                                          | Data accessible in the course of support                                                                  | Sweden               | Not applicable (EEA)                                                                                                                              |
| Hubspot, Inc                   | Support        | Support case handling                                                        | Name, email address, content of support requests                                                          | USA                  | EU-U.S. Data Privacy Framework                                                                                                                    |
| Twilio, Inc                    | SMS/Text       | Delivery of text messages sent by the Products                               | Name, mobile number, message content                                                                      | USA                  | EU-U.S. Data Privacy Framework                                                                                                                    |
| OMMH Scandinavia AB            | SMS/Text       | Delivery text messages sent by the Products                                  | Name, mobile number, message content                                                                      | Sweden               | Not applicable (EEA)                                                                                                                              |
| Smplrspace Pte. Ltd.           | Floorplan      | Hosting, rendering and editing of floor plans                                | IP address, user agent and relevant technical request/error context; identifiable map content if supplied | Singapore            | EU SCCs Module Three for Humly’s processor-to-processor transfer, with completed annexes, transfer assessment and required supplementary measures |

| Entity                             | Applies to | Service                                                    | Personal data                                   | Location       | Safeguard outside the EEA                                                                                                                                                    |
|------------------------------------|------------|------------------------------------------------------------|-------------------------------------------------|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Google Asia Pacific Pte. Ltd.      | Floorplan  | Hosting of the floor plan service (onward, for Smplrspace) | As for Smplrspace                               | Singapore      | Onward-transfer protection required under the applicable SCCs and Article 28; relevant contracting entity and completed safeguards must be recorded in the supplier register |
| Cloudflare, Inc., USA              | Floorplan  | Content delivery and edge hosting (onward, for Smplrspace) | IP address, user agent                          | Global network | DPF only for transfers to a certified US recipient within its scope; applicable SCC/onward-transfer safeguards for other destinations                                        |
| Functional Software, Inc. (Sentry) | Floorplan  | Error monitoring (onward, for Smplrspace)                  | IP address, user agent, technical error context | USA            | EU-U.S. Data Privacy Framework                                                                                                                                               |
| Datadog, Inc.                      | Floorplan  | Logging and monitoring (onward, for Smplrspace)            | IP address, request metadata                    | USA            | EU-U.S. Data Privacy Framework                                                                                                                                               |