HUMLY

Humly Service Level and Support Policy

Support, Cloud Services availability, updates and hardware warranty service

Version 9 October 2026, revision 3, updated 11 October 2026. Part of the Humly Customer Terms.

This policy describes the support, service levels and product lifecycle commitments that Humly provides for its Products. It forms part of the Humly Customer Terms, and terms defined there have the same meaning here. It replaces the Humly Cloud Service Level Agreement EU and the Humly Premium Support Service Level Agreement.

1. How to get support

1.1 Customers and prospective customers can submit support requests directly to Humly at any time. Response targets run during the applicable support hours. A Partner may provide first-line installation, configuration and user assistance and escalate to Humly; this does not prevent the Customer contacting Humly directly.

1.2 Requests are made through support.humly.com or support@humly.com and receive a case number. Software and Cloud Services requests associated with an eligible Customer's account or email domain receive Premium Support for the applicable Subscription, included support period or active maintenance plan. Hardware is supported through the warranty service in section 5, rather than a separate Premium Support entitlement.

1.3 Security vulnerabilities are reported to security@humly.com, as described in section 7.

2. Support levels

	Basic Support	Premium Support
Included with	Everyone, including prospective customers and users of free products and trials	Paying Customers' Software and Cloud Services: throughout the Subscription, or the included self-hosted support period and any active maintenance plan. Hardware warranty service is covered in section 5.
Who contacts Humly	Anyone	The Customer or its Partner
Support hours	Business days, 09:00–16:00 Swedish local time (CET/CEST)	Business days, 09:00–16:00 in the Customer's designated support time zone, including local daylight-saving changes
First response	Within two business days	Within one business day
Communication	Support portal and email	Support portal, email and Microsoft Teams, and to a reasonable extent other tools provided by the Customer

2.1 Support covers guidance on the installation, configuration and maintenance of Humly Products, and the diagnosis and correction of faults in them. It does not cover Third-Party Services, the Customer's own infrastructure and networks, or products not supplied by Humly.

2.2 Humly prioritises cases according to their impact. A case where the Cloud Services or a core booking function is unavailable to many Users is handled before other work during support hours. If a case cannot be resolved immediately, Humly agrees a course of action with the Customer or Partner and keeps them informed through the support portal.

2.3 Humly responds to all reasonable requests under Basic Support. For Basic Support, business days are Monday to Friday excluding Swedish public holidays. For Premium Support, they are Monday to Friday excluding public holidays at the Customer location designated in the Order or account. If no location is designated, the Customer's principal business location applies. Multi-site Customers may agree a support location with Humly.

2.4 Service levels and support beyond this policy — for example extended support hours, shorter response times or service credits — can be agreed under an Enterprise agreement, quoted case by case in accordance with clause 1.6 of the Customer Terms.

3. Cloud Services availability

3.1 The Cloud Services availability target is at least 99.5% of Business Hours in each calendar month. Business Hours are 07:00–19:00 Monday to Friday in the Customer's designated location under clause 2.3, excluding public holidays there and observing local daylight-saving changes.

3.2 Unavailability is measured from the time it is detected by Humly's monitoring or reported by the Customer, whichever is earlier, until the Cloud Services are restored. It does not include:

(a) planned maintenance notified in accordance with clause 3.4;

(b) unavailability of Third-Party Services such as Microsoft 365 or Google Workspace, or of the Customer's networks, devices or infrastructure;

(c) suspension in accordance with the Customer Terms, or unavailability caused by the Customer's use in breach of them; and

(d) events beyond Humly's reasonable control as described in the Customer Terms, and beta or preview functions.

3.3 If monthly availability falls below target, Humly extends the affected Subscription by one week free of charge if requested in writing within 30 days after that month ends. This is the service-level remedy for unavailability; it does not restrict termination for material breach, liability preserved by Customer Terms 11.4, DPA obligations or rights that cannot lawfully be excluded.

3.4 Humly gives the technical account contact at least seven days' email notice of planned maintenance. Planned maintenance does not exceed ten hours per calendar month and is scheduled where possible at weekends or 19:00–07:00 weekdays, Swedish local time (CET/CEST). Urgent maintenance to address a security threat or prevent a serious incident may occur on shorter notice and counts as unavailability.

3.5 The core Cloud Services are hosted in Germany and the Netherlands unless another location is agreed in the Order. Supplier processing for support and optional functions is described in DPA Annex 3. Customer Data in the core Cloud Services is backed up daily; backups are encrypted, kept for 30 days and subject to the deletion schedule in Customer Terms C.17 and DPA 3.7. Restores are tested regularly.

4. Updates and product lifecycle

4.1 The Cloud Services are updated continuously. Humly gives advance notice of changes that materially affect how Users or administrators work.

4.2 Updates to software and firmware on Hardware are delivered through the Products' standard update mechanisms. Security updates are provided free of charge.

4.3 Self-hosted feature updates and support are available during the included support period and any active maintenance plan. Humly supports the current and previous release within the same major release family. Security updates required by applicable law during the security-support period remain available without additional charge even if maintenance has lapsed. Humly may require installation of an appropriate supported security update, but does not condition a legally required security fix on buying feature updates or support.

4.4 Humly provides Hardware security updates for at least five years from the date each unit is placed on the market, and longer where required by applicable law having regard to the period it is reasonably

expected to remain in use. The period is not measured from the introduction of the model and is independent of the warranty period. For Products subject to the CRA support-period requirements, Humly determines and discloses the applicable support-end month and year before purchase. Security updates issued during that period remain available for at least ten years after issue or the remaining support period, whichever is longer, where the CRA requires it. Statutory commencement and transitional rules apply.

4.5 Humly announces end of sale or end of support of a Product or Software version at least 12 months in advance, unless end of sale is outside Humly's control. Discontinuing sales, replacing a model or ending ordinary maintenance does not shorten an existing security-support commitment or an applicable statutory duty.

5. Hardware warranty service

5.1 To make a warranty claim, the Partner or the Customer reports the fault through the support portal with the serial number and a description of the fault. Humly first tries to resolve the fault remotely. If the Hardware is found to be defective, Humly issues a return authorisation with shipping instructions.

5.2 Humly repairs, replaces or, if the remedy fails, refunds Hardware as provided in Module B. Humly pays shipping of the repaired or replacement unit. The sender pays for sending defective Hardware to Humly unless otherwise agreed. Partner-purchase refunds follow Customer Terms 2.3.

5.3 Hardware outside its warranty period, or damaged in a way not covered by the warranty, can be repaired against a charge after the Customer has accepted a quotation.

6. Customer responsibilities

6.1 The Customer provides the following cooperation. A failure affects response or resolution only to the extent it causes delay or prevents the work; it does not automatically remove support or warranty rights:

(a) keeps the contact details in its account up to date and reads Humly's notices sent to them;

(b) reports disturbances or irregularities in the Cloud Services promptly;

(c) restricts access to the Products to authorised Users;

(d) configures and maintains its Third-Party Services and integrations; and

(e) uses supported versions of the Software and meets the network and installation requirements in the Documentation.

7. Security

7.1 Anyone who believes they have found a security vulnerability in a Humly Product can report it to security@humly.com under Humly's Coordinated Vulnerability Disclosure Policy at www.humly.com/security.

7.2 Personal data breaches affecting Customer Data are handled in accordance with the Data Processing Agreement.

8. Cloud infrastructure and governmental access

8.1 Core Cloud Services. Humly Solutions AB is established in Sweden. The core Humly Control Panel Cloud Services use infrastructure in Germany and the Netherlands, subject to the laws applicable in those countries, including applicable European Union law. Any different hosting arrangement expressly agreed in an Order must identify the relevant infrastructure location and jurisdiction.

8.2 Infrastructure responsibilities. Bradler & Krantz GmbH & Co. KG provides colocation facilities, power, physical security, connectivity and bare-metal hardware, including hardware maintenance, replacement and disposal. Humly administers the servers, operating systems, databases, storage, firewalls, proxies and load balancers, and operates backups and redundancy between the data centres.

Core Cloud Services databases and backups are encrypted at rest, with encryption keys held by Humly. The infrastructure operator has no logical access to Customer Data. Communications with the core Cloud Services are encrypted using TLS.

8.3 Optional functions and supporting services. The core hosting locations above do not describe every optional function or supporting service. Floorplan uses Smplrspace Pte Ltd, established in Singapore, with primary hosting in Singapore and onward providers for functions such as content delivery and monitoring. Optional SMS/Text services use suppliers in Sweden and the United States. Support case handling uses HubSpot in the United States.

The applicable suppliers, functions and processing locations are identified in Annex 3 to the Data Processing Agreement, available through www.humly.com/legal. Those entries apply only to the relevant function or processing activity and do not mean that the Customer's entire Humly Control Panel database is transferred to those suppliers.

8.4 Non-personal data and governmental requests. Humly will assess governmental requests for non-personal Customer Data against applicable law, challenge requests where reasonable legal grounds exist, and limit any lawful disclosure to the minimum necessary. Humly will not voluntarily provide governmental access to Customer Data.

For non-personal data held in the European Union, Humly will prevent access or transfer that conflicts with European Union or applicable Member State law. Humly will inform the Customer before complying with a third-country authority's request, except where the request serves law-enforcement purposes and notification must be withheld to preserve the effectiveness of that activity.

8.5 Contractual safeguards. Humly will require suppliers entrusted with Customer Data to be contractually bound by confidentiality, access restrictions and governmental-request safeguards appropriate to their services.

8.6 Personal data and self-hosted installations. Processing of personal data remains governed by the Data Processing Agreement. For self-hosted installations, the Customer determines the infrastructure location and operates the installation, except to the extent separately agreed. Activated external functions and information provided to Humly for support remain subject to the arrangements applicable to those functions and services.

9. Data export and switching information

9.1 Available export methods. Humly provides CSV exports of business data and a separate encrypted full-database export. These methods serve different purposes:

Export	Format	Intended use
Resource data	CSV	Transfer and further use of resource records
Statistics	CSV	Transfer and further analysis of statistics
User data	CSV	Transfer and further use of user records
Full Customer database	Encrypted Humly database export	Backup or migration between Humly self-hosted and Humly cloud deployments

The business-data categories listed above are confirmed export capabilities, rather than an exhaustive definition of the Customer's exportable data.

9.2 CSV exports. Business data, including Resources, statistics and users, can be exported in CSV format. CSV files can be processed using commonly available spreadsheet and data-processing tools. Import into another product may require mapping or conversion to that product's data structure. Availability of a CSV export does not guarantee that another provider can import it without adaptation.

Customers can contact support@humly.com or use support.humly.com for guidance on obtaining the exports relevant to their deployment and modules.

9.3 Full-database exports. The full Customer database can be exported from Humly Control Panel using an encryption key selected by the Customer. Generation normally takes a few minutes, although larger databases may take longer. This timing concerns generation of the export and does not include download, transfer, import or validation.

The full-database export is intended for backup or migration between Humly self-hosted and Humly cloud deployments. It is not presented as a directly importable format for another provider's product. The Customer should retain the export and its encryption key securely.

9.4 Switching assistance. Customers planning to switch should contact Humly Support with the intended destination, relevant modules and requested timing. Humly will assist with exportable data, relevant metadata and digital assets not covered by the standard exports, as required by the Customer Terms and applicable law.

9.5 Retrieval and deletion. Notice, transition, post-termination retrieval, deletion and any applicable charges are governed by Customer Terms C.15–C.17 and, for personal data, the Data Processing Agreement. The availability of standard exports does not reduce those rights.

10. Changes

10.1 Changes follow Customer Terms clause 15. Humly will not reduce agreed service levels or support during an existing Subscription, included support or maintenance period, or hardware warranty, except as permitted by that clause. Existing perpetual-licence rights and mandatory security-update obligations remain unaffected.