

Data Processing Addendum (DPA)

Appendix to the VTOBeauty Merchant Terms

1. Parties, roles and conclusion

The Merchant identified by the commercial account is controller of entrusted data and Qoder Sp. z o.o. is processor. This DPA is a binding appendix to the Terms and is concluded when the Terms and DPA are accepted or by a separately signed agreement.

This DPA covers only processing performed by Qoder on the Merchant's documented instructions. It does not govern account, billing, Qoder infrastructure-security or Qoder accounting data for which Qoder acts as controller under the Merchant Privacy Policy or Widget Privacy Policy, depending on the individual and flow.

The DPA applies from conclusion of the agreement for the service term and afterwards for as long as Qoder retains entrusted data.

2. Annex I - subject, nature and purposes

Processing provides the public VTO widget, maintains sessions, applies Merchant configuration, measures use, secures the service, diagnoses faults and supports the Merchant.

- operations: collection through widget APIs, transmission, recording, organisation, retrieval, aggregation, restriction, deletion and backup;
- data subjects: customers and visitors who launch the widget in the Merchant storefront;
- data: pseudonymous widget and try-on session identifiers, shop, product, variant, product type, mode, entry source, time, locale, events, limited action metadata and legal-revision acknowledgement;
- technical connection metadata, including an IP address, may be processed transiently by the CDN, WAF and hosting. It is entrusted data to the extent it is used to deliver and protect the widget on the Merchant's instructions. Qoder acts as a separate controller for the limited processing required for its own infrastructure security, abuse prevention, legal duties and claims, as described in the Widget Privacy Policy;
- the base widget processes photos, camera frames and facial landmarks locally on the user device. They are not entrusted to Qoder unless the Merchant enables a separate transmission feature after the DPA, user notices and any required DPIA have been updated.

3. Merchant obligations and rights

The Merchant ensures lawful instructions, an appropriate legal basis, transparency, minimisation, accurate configuration and lawful data collection. The Merchant must not instruct Qoder to process

special-category, biometric or children's data unless the parties first agree this in writing and implement additional safeguards.

Service configuration, API use and documented requests by authorised Merchant personnel are instructions. The Merchant may issue further agreement-compliant instructions, obtain compliance information, handle data-subject rights and exercise the audit rights below.

4. Instructions, confidentiality and assistance

Qoder processes data only on documented Merchant instructions, including for transfers, unless Union or Member State law requires processing. Qoder informs the Merchant before such processing unless the law prohibits notice.

Only authorised personnel bound by confidentiality and appropriately trained for their duties may access entrusted data. Qoder promptly informs the Merchant if an instruction may infringe applicable law and may suspend it.

Taking account of the nature of processing, Qoder assists with data-subject rights, security duties, consultations and DPIAs. A request received directly by Qoder is forwarded to the Merchant without Qoder deciding it, unless the law requires otherwise.

5. Annex II - technical and organisational measures

- logical tenant separation, role-based access, least privilege and periodic access reviews;
- TLS in transit, secret management outside source code, secure password hashing, and data and backup encryption where provided by the infrastructure layer;
- identifier pseudonymisation, HMAC for legal acknowledgements, metadata minimisation and no raw-photo storage in the standard widget flow;
- administrative and security logging, monitoring, alerts, vulnerability management, updates and incident response procedures;
- backups, controlled restoration, environment separation, restricted test data and secure deletion under the retention schedule;
- supplier assessment, processor agreements, business continuity and periodic review of measures according to risk and service changes.

6. Personal-data breaches

Qoder notifies the Merchant of a confirmed breach affecting entrusted data without undue delay, targeting 24 hours from confirmation. The initial notice may be incomplete and will be supplemented as facts become available.

To the extent available, the notice describes the nature and timing, data and data-subject categories, likely consequences, measures taken or proposed and a contact point. Qoder documents the breach and cooperates with the Merchant's notification duties.

7. Subprocessors and change procedure

The Merchant gives general written authorisation for active subprocessors listed below. Qoder imposes no less protective data obligations on each active subprocessor and remains responsible for their performance as required by Article 28 GDPR.

Qoder gives at least 30 days' notice before adding or replacing a subprocessor. The Merchant may raise a documented data-protection objection within 14 days. The parties seek a solution in good faith; if none is possible, the Merchant may terminate the affected service without a penalty for an unused future period. An urgent security- or law-driven replacement may occur sooner with notice without undue delay.

8. Annex III - subprocessor register as at 13 August 2026

Stripe, Shopify, Microsoft Entra ID and Brevo are not automatically subprocessors of widget data. Their role depends on the relevant account, billing, sign-in or communication flow and is described in the Merchant Privacy Policy.

- Cloudflare, Inc. - active; CDN, WAF, routing, abuse protection and R2 when used in the relevant flow; processing in the EEA and global network; transfers use the applicable Chapter V mechanism, including an adequacy decision or SCCs;
- OVHcloud, including the relevant OVH group company or designated VPS operator - active; application infrastructure, database and backups; primary location in the EEA according to environment configuration;
- Functional Software, Inc. doing business as Sentry - planned and inactive; error diagnostics excluding photos, facial data, payment data, tokens, form contents and Session Replay. Sentry is not authorised to receive entrusted data until Qoder activates it after advance notice and a registry status update.

9. Transfers outside the EEA

Data is processed in the EEA in the first instance. If an active subprocessor or support access causes a transfer outside the EEA, Qoder uses an adequacy decision, the EU-US Data Privacy Framework where applicable, the 2021/914 Standard Contractual Clauses or another valid mechanism, together with a transfer assessment and supplementary measures where required.

On a reasoned request, Qoder provides information necessary to assess the transfer mechanism while protecting other customers' confidentiality and security.

10. Information, audits and inspections

Qoder provides information necessary to demonstrate Article 28 GDPR compliance. It may first provide current policies, reports, independent-assessment results or questionnaire responses.

The Merchant or its independent auditor may conduct a proportionate audit on reasonable notice without compromising security or other customers' confidentiality. Notice and ordinary audit arrangements do not restrict an audit required by an authority or reasonably justified by an incident or material compliance concern.

11. Retention, return and deletion

During the service, raw pseudonymous widget events and acknowledgements are retained for no more than 13 months unless configuration or law requires a shorter period. Truly anonymised aggregates may be kept for up to 120 months.

At termination, at the Merchant's choice, Qoder returns available data or deletes entrusted data from active systems within 30 days. Residual secured backups are overwritten or expire within a cycle no longer than 90 days. Legally required retention is excepted; such data remains isolated and is not used for another purpose.

12. Precedence, changes and contact

For data protection matters, this DPA prevails over conflicting Terms. A separately signed DPA prevails over this standard version for an expressly agreed difference. An Enterprise offer or manual billing does not itself replace a DPA.

A material DPA change is notified and accepted under the Terms. A subprocessor-register update follows the separate procedure above and does not by itself require renewed acceptance of the entire DPA.

Contact for DPA matters, incidents and data-subject rights: kontakt@qoder.pl.