LYAÉ · ROTTERDAM

Privacy Policy

How LYAÉ collects, uses, and protects your personal data

DRAFT — PENDING LEGAL REVIEW

Last updated: [DATE] · Effective from: [DATE]
This document is not yet legally reviewed or published. See the closing note on the final page.

1. Who we are

LYAÉ is a permanent make-up (PMU) salon based in Rotterdam, the Netherlands.

Trading name	LYAÉ
Legal entity	[legal entity name]
Address	[street, postal code, city, Netherlands]
KVK (Chamber of Commerce) number	[KVK number]
VAT (BTW) number	[VAT number]
Email	[privacy contact email, e.g. privacy@lyae.nl]
Phone	[phone number]

LYAÉ is the **data controller** for the personal data described in this policy: we decide why and how your personal data is processed when you visit our website, book a treatment or course, buy a gift card, or otherwise interact with us.

This policy covers both `lyae.nl` (the public site and booking flow) and `backoffice.lyae.nl` (our internal staff system) to the extent the latter processes data about you as a client.

2. What personal data we collect

We only collect what we need to run the salon, process your booking, and meet our legal obligations (bookkeeping, tax, consumer protection). Specifically:

2.1 Booking and client data

- **Identity and contact details**: first and last name, email address, phone number, home address (street, postal code, city, country).
- **Booking details**: which treatment or course you booked, date/time, the staff member assigned, price, deposit amount, payment status, cancellation/reschedule/no-show history.
- **Health information (treatment bookings only)**: allergies, medication use, and other contraindications relevant to your PMU treatment, collected via the digital intake/consent form. This is a **special category of personal data** under Article 9 GDPR and is processed only with your explicit consent, captured together with your signature on that form.
- **Your electronic signature**: a hand-drawn signature captured in-browser at booking time, together with the IP address and timestamp of signing, as evidence that you reviewed and agreed to the consent form. The signed form is rendered to PDF and stored as described in §4.
- **Photos**: "before/after" treatment photos may be taken and stored in your client file. A photo is only shown publicly on our portfolio page if a staff member has explicitly marked it as public — uploading a photo to your

file and publishing it are two separate, deliberate steps, and you can ask us to remove any published photo at any time.

- **Staff notes**: free-text notes a staff member adds to your file, either general or tied to a specific appointment.

2.2 Payment data

- Deposit and balance payment amounts, timestamps, and status.
- We do **not** store your card number, IBAN, or other payment credentials ourselves — card/iDEAL/Bancontact payments are handled directly by our payment provider, Mollie (see §7). We retain only the payment status and Mollie's own reference id for the transaction.
- In-person balance payments are recorded by staff (amount and time only — we do not record whether you paid by cash or card).

2.3 Gift cards

- If you buy a gift card: your name, email, phone number, and (if you send it to someone else) the recipient's name and email.
- If you redeem a gift card someone bought for you: the redemption is linked to the offering it was purchased for, not to the original buyer's identity beyond what's needed to process it.

2.4 Invoices

- Legally-required invoice data: name and address as provided at the time of the transaction, invoice line items, VAT breakdown, and a digital signature over the invoice PDF (see §9 on retention — invoices are kept for a fixed statutory period independent of your other data).

2.5 Reviews

- If you leave a review: your rating, review text, and the email address you submit it with. Your email is used only to verify you're an existing client and to deliver a reward coupon if eligible — it is **never shown publicly** next to your review. Reviews are only published after a staff member has approved them.

2.6 Website usage data

- **Strictly necessary cookies only, by default**: your login session (backoffice staff only), and your language/theme preference. These are exempt from cookie consent because the site cannot function correctly without them.
- **Analytics cookies**: only set if you explicitly opt in via the cookie banner. You can change or withdraw this choice at any time via the "Cookievoorkeuren" link in the site footer. As of this writing, no analytics or tracking script is actually active on the site — the opt-in mechanism exists ahead of any such feature being added.
- We do not use advertising or cross-site tracking cookies.

2.7 Staff data (if you work for LYAÉ)

- Name, email, role, Google account identifier (used for sign-in), and two-factor authentication setup. This policy focuses on client-facing processing; staff are separately informed about their own data as employees/contractors.

3. Why we process your data, and our legal basis

Purpose	Data used	Legal basis
Taking and managing your booking	Name, contact details, address, booking details	Contract (Art. 6(1)(b))
Processing deposit/balance payment	Payment status, amounts	Contract (Art. 6(1)(b))
Consent form & health disclosures	Health info, signature, IP, timestamp	Explicit consent (Art. 9(2)(a)) + contract
Booking confirmations, reminders, cancellations	Name, email, booking details	Contract (Art. 6(1)(b))
Gift cards	Buyer/recipient name, email, phone	Contract (Art. 6(1)(b))
Publishing an approved review	Rating, review text (not email)	Consent (Art. 6(1)(a))
Review-reward coupon	Email, booking history	Legitimate interest (Art. 6(1)(f))
Invoices & financial records	Invoice data, buyer name/address	Legal obligation (Art. 6(1)(c))
Staff accounts & access control	Staff identity/auth data	Legitimate interest (Art. 6(1)(f))
Fraud/abuse prevention (reviews)	Booking history, confirmation status	Legitimate interest (Art. 6(1)(f))
Session, language, theme preference	Cookies	Strictly necessary — exempt
Analytics (opt-in only)	Analytics cookie	Consent (Art. 6(1)(a))

We do not use your data for automated decision-making or profiling that has a legal or similarly significant effect on you. Staff-artist assignment when multiple qualified staff are available is a simple availability match, not profiling.

4. How your data is stored and protected

- **Hosting**: our website, database, and file storage run on servers operated by monsterasp.net, hosted in a data center in **Germany**, within the EU/EEA. Your data does not leave the EU/EEA as part of normal operation.
- **Health disclosures and signed consent documents** are held in encrypted form in our database (not as ordinary files), and are never served through a public, directly-guessable web link — they can only be retrieved by an authenticated, two-factor-verified staff member through a dedicated secure endpoint.
- **Invoices** (including their digital signature) are likewise stored encrypted and are only accessible to authenticated staff.
- **Payments** are processed by Mollie; we never see or store your full card or bank details.

- **Backoffice access** requires Google sign-in plus a mandatory second authentication factor (an authenticator app code) for every staff account — a password alone is never sufficient to reach client data.
- **Portfolio photos** you have not consented to make public are never exposed via a public URL.

No security measure is perfect, but the design above — encryption at rest for sensitive documents, mandatory two-factor authentication for staff, EU-only hosting — reflects a deliberate attempt to keep your data proportionate to its sensitivity.

5. Who we share your data with

We do not sell your personal data. We share it only with the service providers ("processors") who help us run the salon, each bound by a data processing agreement, and only for the purpose described:

Processor	Purpose	Location
monsterasp.net	Website hosting, database, outgoing transactional email	Germany (EU)
Mollie	Payment processing (deposits, balances, gift cards, no-show invoices)	EU
Google (OAuth)	Staff sign-in only — not used for client accounts	EU/US (Google's standard safeguards)
Firebase Cloud Messaging	Push notifications to staff devices only	EU/US (Google's standard safeguards)

A full, current register of our processors — including whether a data processing agreement is signed with each — is maintained internally and available on request (see §11).

We may also disclose personal data where required by law (for example, to Dutch tax authorities as part of our statutory bookkeeping obligations, or to law enforcement with a valid legal basis).

6. How long we keep your data

Data	Retention
Booking, customer, and consent-form records	Kept as part of your ongoing client history, reviewed periodically; earlier erasure available on request (subject to the tax exception below)
Invoices (name, address, amounts, VAT)	Fixed statutory period, **minimum 7 years**, automatically enforced and deleted — kept independently of your general client record
Signed consent forms & health disclosures	Deleted on request; document scrubbed while the fact a valid signature was captured is kept as a compliance record
Gift cards	Card validity period plus the invoicing retention period (also a financial record)
Reviews	Kept while displayed publicly; removed on request
Cookies	Session cookies expire when your session ends; preference is remembered until changed

Where we anonymize your client record on request (§8), we keep the underlying booking/financial skeleton (dates, amounts, status) without your name or contact details attached, because Dutch bookkeeping law does not allow us to delete financial records outright — but this skeleton can no longer be linked back to you.

7. Payments

Deposit payments, balance payments, gift card purchases, and no-show invoices are processed through **Mollie**, a licensed EU payment service provider. When you pay, you are redirected to Mollie (or your bank/card issuer) to complete the transaction; we only receive confirmation of the payment's status back from Mollie, not your card or bank details.

8. Your rights

Under the GDPR, you have the right to:

- **Access** — ask us what personal data we hold about you. We can provide a full export of your client record (bookings, consent forms, notes, reviews, coupons, gift cards, invoices, notification history) on request.
- **Rectification** — ask us to correct inaccurate data.
- **Erasure** ("right to be forgotten") — ask us to delete your personal data. Where we're legally required to keep certain records (e.g. invoices, for Dutch tax law), we anonymize rather than fully delete: your name/contact details are scrubbed from your booking and financial history, health disclosures and your signed consent document's contents are removed, and portfolio photos of you are deleted, while the underlying

booking/financial entries remain (unlinked from your identity) to satisfy our legal retention obligations. Invoice buyer name/address are the one exception kept intact, and only for the invoice's own fixed statutory retention window, per §6.

- **Restriction of processing** — ask us to pause non-essential processing of your data (for example, we will stop issuing you an automatic review-reward coupon) while a dispute or request is resolved.
- **Data portability** — receive the personal data you gave us in a structured, commonly-used, machine-readable format.
- **Object** — object to processing based on our legitimate interest.
- **Withdraw consent** — where processing is based on consent (e.g. the health disclosures on your consent form, or an analytics cookie), withdraw it at any time; this doesn't affect processing already carried out before withdrawal.
- **Lodge a complaint** — with the Dutch data protection authority, the **Autoriteit Persoonsgegevens** (autoriteitpersoonsgegevens.nl), if you believe we have not handled your data lawfully.

To exercise any of these rights, contact us at [privacy contact email]. We will respond within one month, as required by the GDPR.

9. Children

Our services are intended for adults. PMU treatments are not offered to minors without appropriate parental/guardian involvement as required by our professional and legal obligations; we do not knowingly collect personal data from children without such involvement.

10. Cookies

We use only the cookies described in §2.6. Strictly necessary cookies (session and preference) are always active and cannot be turned off, as the site depends on them to function. Any additional, non-essential cookie category (such as analytics) is off by default and only activated if you explicitly opt in through our cookie banner. You can review or change your choice at any time via "Cookievoorkeuren" in the site footer.

11. Contact us

Questions about this policy, or to exercise any of the rights in §8:

LYAÉ
[street, postal code, city, Netherlands]
Email: [privacy contact email]
Phone: [phone number]

12. Changes to this policy

We may update this policy from time to time — for example, if we add a new feature that processes data differently, or if the law changes. The "Last updated" date at the top of this page reflects the most recent revision. Material changes will be highlighted on the site.

This policy describes the LYAÉ booking and backoffice system as built. It should be read and approved by Alyan's legal/privacy advisor before publication, per the standing gap tracked in `docs/production-readiness.md` §5.