AZERBAIJANI STUDENT ASSOCIATION (AzSA)

Privacy Policy & Data Protection Notice

A comprehensive public notice for members, applicants, subscribers, website visitors, event participants, board members and other people whose personal data AzSA processes.

Controller	Azerbaijani Student Association (AzSA)
Location	Rotterdam, Netherlands
Privacy contact	azsaeur@gmail.com
Version	1.0
Effective date	2 September 2026
Review date	2 September 2027, or earlier after any material change
Status	Publication-ready privacy notice - Board to confirm implementation before publication

Compliance statement. This notice is designed to align with the transparency and accountability requirements of the EU General Data Protection Regulation (GDPR), the Dutch GDPR Implementation Act (UAVG) and relevant Dutch rules on cookies and electronic communications. A privacy notice cannot, by itself, guarantee compliance: AzSA must ensure that its real practices, retention routines, provider contracts, access controls and consent mechanisms match this document at all times.

PUBLIC DOCUMENT

Contents

Plain-language summary

AzSA collects only the information it needs to run membership, communicate with people, operate its website and events, protect its systems and meet legal obligations. We do not sell personal data, do not use targeted-advertising trackers, and do not make membership decisions solely by automated means. Membership applications are reviewed by a human board member. We use third-party services such as Google, a website-hosting provider, email providers, banking/payment services and - if you choose to use them - WhatsApp and Instagram. You may ask to access, correct, delete, restrict or obtain certain data, object to certain processing, withdraw consent, and complain to the Dutch Data Protection Authority. Contact: azsaeur@gmail.com.

1. About this notice and scope

This Privacy Policy & Data Protection Notice explains how the Azerbaijani Student Association (AzSA) processes personal data. It applies whenever AzSA decides why and how personal data are processed in connection with its website, membership, communications, events, community activities, partnerships and administration.

It covers, in particular, applicants for membership; passive and active members; mailing-list subscribers; website visitors; people who contact AzSA; event attendees; people appearing in event photographs or video; board and committee members; volunteers; partners and sponsor contacts; and other individuals who interact with the Association.

Where another organisation independently decides how it processes your data - for example WhatsApp/Meta, Instagram/Meta, your bank, your email provider or a third-party website you choose to visit - that organisation has its own privacy responsibilities and privacy notice. AzSA does not control those independent processing activities.

If AzSA introduces a materially new processing activity, such as a new event-registration platform, analytics service or member portal, the Board will assess the privacy impact and update this notice before or at the time the new processing starts.

2. Who is responsible for your data

Data controller: Azerbaijani Student Association (AzSA), Rotterdam, Netherlands.

Privacy contact: azsaeur@gmail.com. Privacy enquiries are handled by the Board unless AzSA appoints a dedicated Data Protection Officer in the future.

AzSA is the controller when it determines the purpose and means of processing. Service providers may act as processors on AzSA's instructions or, for some parts of their services, as independent controllers. AzSA will document the applicable role and maintain Article 28 GDPR processor terms where legally required.

This notice does not make Erasmus University Rotterdam the controller for AzSA data merely because AzSA serves a student community connected with the university. If a specific activity is jointly run with the university or another organisation, AzSA will identify the relevant roles for that activity.

3. Our data-protection principles

AzSA applies the principles in Article 5 GDPR. In practice, this means that we commit to:

- Lawfulness, fairness and transparency - we identify a valid legal basis and explain processing in understandable language.
- Purpose limitation - we use data for specified, legitimate purposes and do not quietly reuse it for an incompatible purpose.
- Data minimisation - we collect only what is reasonably necessary. We periodically review forms and remove fields that are no longer justified.
- Accuracy - we take reasonable steps to keep relevant records correct and allow people to request correction.
- Storage limitation - we use defined retention periods and delete or anonymise data when it is no longer needed.
- Integrity and confidentiality - access is limited to people who need it, and technical and organisational safeguards are applied according to risk.
- Accountability - the Board keeps appropriate records of processing, contracts, decisions, consent where relied upon, rights requests, retention and data breaches.

4. Personal data we process

The exact data depends on how you interact with AzSA. The current website and association workflow may process the following categories:

Category	Examples
Identity and contact	Name; email address; contact details you choose to provide.
Membership application	Submission timestamp; study status; EUR student number when genuinely needed; university; programme; year of study; the text you submit about why you want to join; email-verification status; application status; queue/free-place status where used.
Membership administration	Membership tier (for example passive or active); start/end status; fees due or paid; member eligibility or participation records that are necessary to administer membership.
Payment and accounting	Payer name; amount; payment date; transaction reference; bank-account information visible to AzSA through its bank or payment provider; accounting records required by law.
Communications	Emails and messages you send to AzSA; replies; mailing-list preference; unsubscribe/opt-out requests; notices sent to you.

Category	Examples
Website and security	Technical request data that may be processed by hosting or security providers, such as IP address, browser/device information, timestamps, requested pages and security logs; short-lived verification/session information; anti-spam signals such as the hidden honeypot field.
Board and volunteers	Board/committee role; association email or contact details; access-authorisation records; governance and handover information.
Events and media	Photographs, video or recordings taken at events; event-related correspondence and, if used in future, registration information clearly disclosed at collection.
Community and social platforms	Social-media handle or message when you contact/tag AzSA; phone number, profile name/photo and group activity that may be visible when you voluntarily join a WhatsApp group, according to your settings and the platform rules.

AzSA does not treat membership in an Azerbaijani community association as proof of a person's nationality or ethnicity and will not infer or record ethnicity from membership alone.

5. Purposes and legal bases

We rely on one or more legal bases under Article 6 GDPR. The appropriate basis depends on the activity. Consent is never used merely because it appears convenient; where consent is relied upon, it must be freely given, specific, informed and unambiguous, and you can withdraw it.

Processing	Purpose	Legal basis
Membership application and decision	Receive and review an application; verify the submitted email; communicate the outcome; prevent duplicate/abusive submissions.	Art. 6(1)(b) - steps at your request before entering the membership relationship; Art. 6(1)(f) - legitimate interests in secure and orderly administration.
Membership administration	Maintain membership status/tier, provide member benefits, administer participation and essential association communications.	Art. 6(1)(b) - performance of the membership relationship; Art. 6(1)(f) - legitimate interests in governance and community administration.
Fees, payments and accounting	Collect membership fees, reconcile payments, maintain financial records and comply with applicable fiscal/accounting obligations.	Art. 6(1)(b); Art. 6(1)(c) where a legal retention/reporting obligation applies; Art. 6(1)(f) for fraud/error prevention.
Public-meeting / announcement mailing list	Send the announcements for which a person voluntarily signed up.	Art. 6(1)(a) - consent. You can unsubscribe at any time.
Member announcements	Send operational or membership-related notices, event information and information reasonably connected with member benefits.	Art. 6(1)(b) and/or Art. 6(1)(f). Separate optional marketing will use consent where required.
Contact and enquiries	Answer questions, handle complaints, correct records and maintain necessary correspondence.	Art. 6(1)(f); Art. 6(1)(b) when the enquiry concerns steps toward or performance of membership/event arrangements.
Website operation and security	Deliver the site, protect forms/board access, detect misuse, troubleshoot incidents and maintain availability.	Art. 6(1)(f) - legitimate interests in secure and reliable systems; consent for non-essential cookies/tracking where legally required.
Event photography and media	Document association activities and communicate about the community.	Normally consent for posed/close-up promotional images; Art. 6(1)(f) may be used for proportionate general event/atmosphere images after a balancing assessment and with practical opt-out measures.
Partners, sponsors and discounts	Manage organisational contacts, negotiate benefits and administer collaborations.	Art. 6(1)(f). Member data are not shared with a partner merely because a partnership exists; a separate basis and notice are required if individual-level sharing becomes necessary.

Processing	Purpose	Legal basis
Legal claims, safety and compliance	Establish, exercise or defend legal claims; respond to lawful authority requests; comply with applicable law.	Art. 6(1)(c) and/or Art. 6(1)(f), depending on the situation.

5.1 Legitimate interests

Where AzSA relies on Article 6(1)(f), the interests include secure operation of the association and website; prevention of misuse; orderly membership administration; member/community communications that people can reasonably expect; maintaining organisational records; protecting legal rights; and proportionate documentation of association activities. AzSA will consider necessity, reasonable expectations and the impact on the individual, and will not rely on legitimate interests where the individual's interests or fundamental rights override the Association's interest.

6. Membership applications, membership and payments

6.1 Application form

The membership form currently asks for identity/contact information and information relevant to the applicant's study situation and motivation. AzSA will keep the form under regular data-minimisation review. A student number should only be required where it is genuinely necessary to verify a student status or benefit; if that purpose no longer exists, the field must be removed.

The free-text application field must not be used to request sensitive personal data. Applicants are asked not to include information about health, religion, political opinions, sexual orientation, criminal allegations or other unnecessary sensitive matters. If such information is volunteered and is not needed, AzSA will delete it as soon as reasonably practicable.

6.2 Human review

Membership applications are reviewed by an authorised human board member. AzSA does not use solely automated decision-making to approve or reject membership applications. Technical checks such as email verification, duplicate prevention and anti-spam controls may operate automatically, but they do not make the substantive membership decision.

6.3 Membership records

After approval, AzSA should retain only the data needed to administer membership. Detailed application information such as a student number and application narrative is not automatically needed for the full lifetime of a membership and is subject to the shorter retention periods in Appendix A.

6.4 Payments

When a membership fee is due, AzSA may receive transaction information from its bank or payment provider. We use that information only to match the payment, administer membership, maintain accounts and comply with applicable legal obligations. We do not publish a member's payment details.

7. Email verification, announcements and mailing lists

7.1 Verification and security messages

The join workflow may send a one-time email-verification code and create short-lived technical tokens. These are used only to confirm control of the submitted email address and secure the form. The current system is designed so verification codes expire after approximately 10 minutes, verification tokens after approximately 2 hours, password-reset codes after approximately 15 minutes and board sessions after no more than approximately 6 hours.

7.2 Public-meeting / announcement subscription

A person who uses “Keep me posted” or an equivalent subscription control is asking AzSA to send the stated updates. This subscription is separate from membership. It is based on consent and is not a condition

of joining AzSA. You can withdraw consent at any time by using the unsubscribe method provided in the message or by emailing azsaeur@gmail.com. Withdrawal does not affect processing that was lawful before withdrawal.

7.3 Member communications

AzSA may send current members necessary or reasonably expected operational communications about membership, events, elections, fees, safety, changes to benefits or association governance. Where an email is genuinely optional direct marketing rather than a membership communication, AzSA will obtain consent if the law requires it.

7.4 Group email privacy

AzSA will use individual delivery, BCC or an appropriate mailing system so that recipients' email addresses are not unnecessarily disclosed to other recipients.

8. Website visits, cookies and embedded services

8.1 Website hosting and technical data

AzSA's website is static and is currently configured for deployment through a hosting/CDN provider such as Netlify. Even when AzSA does not run analytics, the hosting provider may process limited technical information needed to deliver, secure and operate the service, such as IP address, browser/device data, request time and requested resource. AzSA uses such data only as necessary for operation, security and troubleshooting.

8.2 Cookies and similar technologies

AzSA does not currently intend to use advertising cookies, behavioural tracking pixels or third-party advertising analytics. The website may use strictly necessary browser storage for essential security/board functionality. Under Dutch law, non-essential tracking cookies or equivalent technologies require clear information and prior consent. If AzSA later enables such technology, it will provide a compliant consent mechanism before the technology is activated.

8.3 Google Calendar

The site is designed to support a public Google Calendar embed. When an embed is enabled, loading it can cause the visitor's browser to connect directly to Google and may result in Google processing technical data and, depending on configuration, cookies or similar identifiers. AzSA will not load a non-essential third-party embed before consent where consent is legally required. A direct calendar link or iCal subscription may be offered as an alternative.

8.4 External links

Links to third-party websites do not mean AzSA controls those websites. When you follow an external link, the destination provider processes data under its own privacy notice.

9. Events, photographs, video and social media

9.1 Event photography and video

AzSA may photograph or record association events. We will provide a clear event notice, for example in the event description, registration message or at the venue. Posed portraits, close-ups and promotional photographs should normally be used with consent. General atmosphere/crowd images may in suitable cases be based on legitimate interests after considering the context, reasonable expectations, intrusiveness and available opt-out measures.

If you do not want to be photographed, tell a board member or photographer. If a photograph of you has been published and you want it removed, email azsaeur@gmail.com with enough information to identify the image. We will assess and respond promptly. Where publication is based on consent, you may withdraw that consent; where it is based on legitimate interests, you may object.

9.2 Sensitive contexts

Where an image, caption or context could reveal special-category information (for example religious belief, health information or ethnic origin) and that information is being intentionally processed, AzSA will use an appropriate Article 9 GDPR condition, normally explicit consent, or will not publish the material.

9.3 Instagram and social media

AzSA may maintain an Instagram account and may receive direct messages, mentions or tags. If you contact or tag AzSA, we may process the handle and content needed to respond or manage the interaction. Meta/Instagram independently processes data under its own terms and privacy policy. AzSA will not use social-media platform data to build hidden profiles of members.

9.4 WhatsApp community/group chat

Joining a WhatsApp group is voluntary. If you join, your phone number, profile name/photo and messages may be visible to other group participants depending on WhatsApp functionality and your privacy settings. WhatsApp/Meta independently processes data under its own terms. AzSA will not sell or export the group membership list for unrelated marketing. Group invitations should be sent only to people who are eligible for the relevant group and should not be posted publicly.

10. Sponsors, partners and member discounts

AzSA may work with sponsors, cultural organisations, restaurants, businesses and other partners. By default, partners receive only information necessary to manage the relationship, such as the name/contact details of the partner representative and aggregated or anonymous information about attendance or membership.

AzSA does not provide a sponsor or restaurant with a member list simply because that organisation offers a discount. The preferred model is a membership card, code or other verification method that does not disclose the entire membership database.

If a future benefit genuinely requires disclosure of a member's personal data to a partner, AzSA will identify the recipient, data, purpose and legal basis in advance and provide any required separate notice or consent. A person will not lose ordinary membership merely because they decline an optional data-sharing benefit.

For jointly organised events, AzSA will clarify whether the co-organiser is a processor, separate controller or joint controller and will give attendees the relevant privacy information.

11. Special-category data and information about minors

11.1 Special-category data

Article 9 GDPR gives stronger protection to data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic or certain biometric data, health information, and information about sex life or sexual orientation. AzSA does not intentionally request these categories through the general membership form.

If AzSA needs special-category data for a specific activity, it will first identify a valid Article 9 condition, minimise the data, restrict access and provide specific information. Where explicit consent is the appropriate condition, it will be requested separately and can be withdrawn.

11.2 Criminal-offence data

AzSA does not routinely collect criminal-conviction or offence data. Any future processing of such data would require a specific lawful basis and compliance with Article 10 GDPR and applicable Dutch law.

11.3 Minors

AzSA primarily serves university students and adults. The website and membership process are not designed to collect data from children under 16 without additional safeguards. If a person under 16 wishes to use a consent-based service, AzSA will assess whether parental/guardian authorisation is required under the GDPR and Dutch law. If you believe a child's data have been submitted inappropriately, contact us so we can investigate and remove it where required.

12. Who receives data and international transfers

12.1 Internal access

Only authorised board or committee members who genuinely need the information for their role should have access to identifiable membership, application or administrative data. Access must be removed promptly when a role ends or no longer requires it.

12.2 External recipients and service providers

Depending on the activity, personal data may be processed by or disclosed to:

- Google services used for forms/backend functions, spreadsheets, email or calendar functions;
- the website hosting/CDN provider (currently configured for Netlify or a successor provider);
- the recipient's own email provider and internet/network providers involved in message delivery;
- AzSA's bank or payment provider, and the payer's bank, for payment processing;
- Meta/WhatsApp or Meta/Instagram when you voluntarily use those platforms;
- professional advisers, insurers, accountants or legal advisers where reasonably necessary;
- event venues, co-organisers or service providers where necessary for a disclosed event purpose;
- public authorities, courts or regulators where disclosure is required by law or necessary to protect legal rights.

AzSA will not sell, rent or trade personal data. Sponsors and commercial partners do not receive member-level data unless a separate lawful basis and appropriate notice exist.

12.3 Processor contracts

Where a provider processes personal data on AzSA's behalf as a processor, AzSA will maintain the contractual safeguards required by Article 28 GDPR, including appropriate confidentiality, security, subprocessor and deletion/return commitments. The exact legal role can differ by product: some large technology providers act as processor for customer content and as independent controller for separate account/service data.

12.4 International transfers

Some providers or subprocessors may process data outside the European Economic Area. When Chapter V GDPR applies, AzSA will use an applicable transfer mechanism, such as an adequacy decision, the European Commission's Standard Contractual Clauses and supplementary safeguards where required, or another lawful mechanism. Information about the relevant safeguard can be requested from azsaeur@gmail.com.

13. Retention and deletion

AzSA does not keep personal data indefinitely merely because storage is available. The Board will implement and document the retention schedule in Appendix A and periodically review the stored data. When a retention period expires, data will be securely deleted or irreversibly anonymised unless a longer period is required for a specific legal obligation, unresolved dispute, legal claim, safety issue or other documented lawful reason.

Where Dutch tax/accounting law requires certain financial administration records to be retained for seven years, AzSA will retain only the financial records to which that obligation applies. That requirement is not a reason to keep an application essay, student number or other unrelated membership data for seven years.

Provider backups or recovery copies may persist for a limited additional technical period after AzSA deletes the active record. AzSA will rely on appropriate provider deletion terms and will not restore deleted data except for legitimate recovery/security reasons.

14. Your GDPR rights and how to use them

Subject to the conditions and exceptions in the GDPR, you may have the following rights:

- Access - obtain confirmation and a copy of personal data AzSA processes about you, together with required information about the processing.
- Rectification - correct inaccurate data and complete incomplete data.
- Erasure - request deletion where the legal conditions are met, for example where data are no longer necessary or consent is withdrawn and no other basis applies.
- Restriction - ask AzSA to limit processing in certain circumstances.
- Data portability - receive certain data you provided in a structured, commonly used, machine-readable format and, where technically feasible and legally applicable, have it transmitted to another controller.
- Objection - object to processing based on legitimate interests. AzSA will stop unless it demonstrates compelling legitimate grounds that override your interests, rights and freedoms, or the processing is needed for legal claims.
- Direct marketing - object to direct marketing at any time. Where you unsubscribe from a consent-based mailing list, AzSA will stop sending that mailing.
- Withdraw consent - withdraw consent at any time for future processing where consent is the legal basis. Withdrawal does not make past lawful processing unlawful.
- Automated decisions - rights relating to decisions based solely on automated processing that produce legal or similarly significant effects. AzSA does not currently make membership decisions in this way.

14.1 How to make a request

Email azsaeur@gmail.com and state the right you want to exercise. You do not need to use legal language. AzSA may ask for reasonable information to verify identity, but will not request more identification than necessary. If a request is made from the same verified email address used for membership, that may be sufficient in many cases.

AzSA will normally respond without undue delay and within one month. The period may be extended by up to two further months for a complex or numerous request, but AzSA will explain the extension within the first month. Requests are normally free of charge; the GDPR permits a reasonable fee or refusal only for manifestly unfounded or excessive requests.

Some rights are not absolute. For example, AzSA may need to keep a limited financial record to comply with law even if other membership data are deleted. If AzSA cannot fully comply with a request, it will explain why and inform you of complaint options.

15. Security and personal-data breaches

15.1 Security

AzSA will implement technical and organisational measures appropriate to the risk, taking into account the nature and volume of the data and the resources of a small association. Measures include role-based access, strong account authentication, multi-factor authentication where available, restricted sharing permissions, secure provider accounts, protection of administrative credentials, timely revocation of former board access, secure devices, minimised downloads, and regular review of who can access membership data.

AzSA will use organisation-controlled accounts for association systems where reasonably possible and will avoid storing sensitive association data in personal accounts or unmanaged devices. Passwords, secret links, access tokens and private group-invite links must not be published in public source code or documents.

15.2 Data breaches

AzSA maintains a process for identifying, containing, assessing and documenting personal-data breaches. Every personal-data breach must be recorded internally. Where a breach is likely to result in a risk to people's rights and freedoms, AzSA will notify the Autoriteit Persoonsgegevens without undue delay and, where feasible, within 72 hours after becoming aware of it. Where a breach is likely to result in a high risk, affected individuals will also be informed without undue delay unless a lawful exception applies.

People who become aware of a possible AzSA data breach should report it immediately to azsaeur@gmail.com.

16. Automated decisions, profiling and sale of data

AzSA does not sell personal data, does not rent its membership list, and does not exchange member details for sponsorship value.

AzSA does not currently carry out behavioural advertising, cross-site profiling or targeted-advertising analytics on its website.

Membership applications are substantively decided by human board members. Automated technical controls may verify an email address, detect a duplicate, limit repeated login attempts or block obvious spam, but these controls are not used to make a solely automated membership decision with legal or similarly significant effect.

17. Changes, governance and accountability

17.1 Updates to this notice

AzSA may update this notice when its services, providers, legal obligations or processing activities change. The current version and effective date will be displayed clearly. Material changes that significantly affect existing members or subscribers will be communicated by an appropriate channel, such as email or an announcement, where reasonably practicable.

17.2 Governance

The Board is responsible for ensuring that this notice matches actual practice. At least annually, and before introducing materially new processing, the Board should review: data categories; legal bases; form fields; permissions; retention; processor contracts; international transfers; cookie/embedded-service behaviour; rights-request handling; and security measures.

AzSA will maintain a proportionate record of processing activities and a data-breach register. Where a proposed processing activity is likely to result in a high risk to individuals, AzSA will assess whether a Data Protection Impact Assessment is required before the processing begins.

17.3 End of association or transfer of activities

If AzSA dissolves or transfers an activity to a lawful successor, personal data will not simply be handed over wholesale. The Board will determine what must be retained, deleted or lawfully transferred, provide notice where required, and ensure that any successor has an appropriate legal basis and safeguards.

18. Contact and complaints

For privacy questions, requests, withdrawals of consent, objections, correction or deletion requests, contact: azsaeur@gmail.com.

If you believe AzSA has not handled your personal data correctly, please contact us first so the Board can investigate. You also have the right to lodge a complaint with the Dutch supervisory authority:

Autoriteit Persoonsgegevens (AP)
Postbus 93374
2509 AJ Den Haag
The Netherlands
Website: autoriteitpersoonsgegevens.nl

You may submit a privacy complaint to the AP in Dutch or English. Exercising your rights with AzSA does not remove any other legal or judicial remedies available to you.

Appendix A. Detailed retention schedule

This schedule is AzSA's retention standard. The Board must configure systems and manual processes so the periods are actually followed. A longer period is allowed only where a documented legal, dispute, claim, safety or regulatory reason applies.

Data / record	Purpose	Standard period	Notes
Email verification code	Confirm email control	About 10 minutes	Automatically expires.
Email verification token	Permit verified membership submission	About 2 hours	Automatically expires.
Board password-reset code	Secure account recovery	About 15 minutes	Automatically expires.
Board session token	Temporary authenticated board access	Up to about 6 hours	Automatically expires; access removed sooner if role ends.
Incomplete/abandoned application data held in active records	Complete or troubleshoot a started application	No more than 30 days unless the person asks us to continue	Delete if not submitted/needed.
Rejected membership application	Handle the decision, correction and any immediate challenge	3 months after final decision or resolution of a challenge	Then delete or anonymise, unless a legal dispute requires longer.
Approved application - student number and application narrative	Initial eligibility/review record	Delete or anonymise within 90 days after approval unless a documented reason requires a shorter/longer period	Core membership record is kept separately.
Approved member - core record	Administer membership, benefits and governance	For active membership plus 2 years after membership ends	Core means name, email, membership type/status, relevant dates and limited administrative history.
Payment/transaction and accounting record	Reconcile fees and comply with fiscal/accounting duties	7 years where Dutch fiscal law requires it; otherwise only as long as necessary	Keep only required financial information, not unrelated application content.
Public-meeting / announcement subscriber	Send opted-in updates	Until withdrawal/unsubscribe	Remove from active list without undue delay, normally within 30 days.
Minimal opt-out/suppression record, if used	Prevent accidental re-mailing and evidence an opt-out	Up to 24 months	Only email/identifier and opt-out date; do not use for marketing.
Contact correspondence	Answer enquiry and retain necessary history	12 months after the matter is closed	Longer only for ongoing dispute, contract, accounting or legal need.
Event photographs/video	Document and communicate association activities	Review at least every 3 years; remove when no longer needed	Consent-based material is removed on valid withdrawal unless another lawful basis/exception applies.
Website/security logs under AzSA control	Security, troubleshooting and abuse prevention	Target no more than 30 days where configuration allows; otherwise the shortest provider-supported period consistent with security	Incident-related logs may be retained longer for a documented investigation.
Board access/authentication data	Control access to member/admin systems	For role duration; revoke access immediately when role ends; residual authentication record no more than 30 days unless needed for investigation	Official board role/term may be retained separately as a governance record.
Privacy-rights request file	Demonstrate handling of request and correspondence	3 years after closure	Minimise identity documents; do not keep copies unless necessary.
Data-breach register	Legal accountability and prevention	At least 5 years after closure of incident, subject to legal advice and applicable requirements	Includes facts, effects and remedial action; access restricted.

Appendix B. Service-provider and recipient categories

Category	Function	Typical role	AzSA safeguard
Google services	Forms/backend (Apps Script), spreadsheets, email and potentially calendar functions.	Processor for customer content under applicable business terms in some products; independent controller for certain service/account data. Exact role depends on account/product.	Maintain appropriate Google data-processing terms where applicable; restrict sharing; organisation-controlled account; review international-transfer terms.
Website hosting/CDN (currently configured for Netlify)	Serve static website, security, caching, technical request handling.	Processor/service provider for hosted customer data in applicable contexts; independent controller for its own service/account data.	Maintain applicable DPA/terms; minimise logs and tracking; no advertising pixels without separate assessment/consent.
Email providers	Deliver verification, membership and announcement email.	Usually independent controllers for recipients' mailboxes; AzSA's provider may be processor/controller depending service.	Use BCC/individual sending; minimise content; do not expose recipient lists.
Bank / payment provider	Receive membership fees and provide transaction records.	Typically independent controller and/or processor depending product.	Use only payment data needed for reconciliation/accounting; restrict bank access.
WhatsApp / Meta	Optional group chat.	Independent controller for platform processing.	Voluntary use; disclose visibility of phone/profile; do not export list for unrelated marketing.
Instagram / Meta	Public social-media presence and direct messages.	Independent controller for platform processing.	No hidden profiling; seek appropriate permission before reusing user content where required.
Sponsors / restaurant or business partners	Partnership administration and member benefits.	Usually separate controller for their own contact data; no member database access by default.	Prefer anonymous/aggregate data and privacy-preserving benefit verification. Separate notice/basis before member-level sharing.
Authorities / advisers	Legal compliance, claims, audit or professional advice.	Recipient under applicable legal/professional role.	Disclose only what is necessary and lawful.

Appendix C. Legal and official reference sources

This document was drafted against the following primary and official guidance sources available on 2 September 2026. Provider terms can change; AzSA should review them when services or accounts change.

1. **Regulation (EU) 2016/679 (General Data Protection Regulation), especially Articles 5, 6, 9, 12-14, 15-22, 28, 30, 32-34 and 44-49.** https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32016R0679
2. **Uitvoeringswet Algemene verordening gegevensbescherming (UAVG), Dutch GDPR Implementation Act.** https://wetten.overheid.nl/uavg
3. **Telecommunicatiewet, Article 11.7a - rules on storage/access on user devices, including cookies and similar technology.** https://wetten.overheid.nl/BWBR0009950/
4. **Autoriteit Persoonsgegevens - Accountability / privacy policy guidance (Verantwoordingsplicht).** https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/verantwoordingsplicht
5. **Autoriteit Persoonsgegevens - Retention of personal data.** https://autoriteitpersoonsgegevens.nl/en/themes/basic-gdpr/privacy-and-personal-data/retention-of-personal-data
6. **Autoriteit Persoonsgegevens - Privacy rights in practice for organisations; generally respond within one month.** https://autoriteitpersoonsgegevens.nl/themas/basis-avg/privacyrechten-avg/voor-organisaties-privacyrechten-in-de-praktijk
7. **Autoriteit Persoonsgegevens - Cookie guidance: tracking cookies require prior information and consent.** https://autoriteitpersoonsgegevens.nl/en/search?keys=cookies

8. **Autoriteit Persoonsgegevens - Data-breach response and 72-hour notification where required.** https://autoriteitpersoonsgegevens.nl/themas/beveiliging/datalekken/datalek-dit-moet-u-doen
9. **Belastingdienst - Standard seven-year retention for required fiscal administration records (subject to scope and exceptions).** https://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/belastingdienst/zakelijk/btw/administratie_bijhouden/administratie_bewaren/administratie_bewaren
10. **Google Cloud / Google Workspace - Cloud Data Processing Addendum (current customer terms).** https://cloud.google.com/terms/data-processing-addendum/
11. **Netlify - Privacy Statement and GDPR/DPA information.** https://www.netlify.com/privacy/ | https://www.netlify.com/gdpr-ccpa/

End of document