Rappn GmbH — Privacy Policy

English master version — governing version for users outside German-speaking Switzerland. In the event of any conflict between language versions, the German version prevails for users resident in German-speaking Switzerland and the English version prevails for all other users, unless mandatory local law provides otherwise.

Last updated: 17 April 2026 · Version 2.0

1. Who we are

Rappn GmbH ("Rappn", "we", "us") operates a platform that aggregates and displays supermarket offers in Switzerland and — where you choose to use them — provides features such as favourites, saved offers, shopping carts, shared household carts and personalised notifications.

Our legal details are:

- Rappn GmbH, a Swiss limited liability company (GmbH)
- Company identification number (UID): CHE-165.158.983
- Registered office: Baarerstrasse 43, 6300 Zug, Switzerland
- Commercial Register: Canton of Zug (registered 7 April 2026)
- Contact for any matter, including data protection questions and requests: info@rappn.ch

Under the revised Swiss Federal Act on Data Protection of 25 September 2020 ("FADP") and, where it applies to you, Regulation (EU) 2016/679 ("GDPR"), Rappn is the controller of the personal data described in this policy.

2. What this policy covers

This policy explains how we collect, use, share and protect personal data when you use:

- our websites and landing pages at rappn.ch and related domains;
- our mobile application (iOS, Android);
- any other service that links to this policy (together, the "Services").

It does not cover the websites, apps or in-store practices of third-party retailers. Those third parties are independent controllers of any personal data they collect from you directly.

3. When the GDPR applies to you

Rappn is established in Switzerland and applies the FADP to all users. Where you use the Services from within the European Economic Area or the United Kingdom, and where Rappn offers the Services to you or monitors your behaviour in that territory within the meaning of Article 3(2) GDPR, the GDPR applies in addition. Where the two regimes differ, we apply the higher standard.

4. Personal data we process

We only process personal data that we need to operate the Services, to comply with our legal obligations, or — where we rely on consent — for which you have given us that consent. What we actually hold about you depends on which features you use.

4.1 Data you provide directly

- **Account data:** email address, password (stored only as a salted hash), display name or nickname, preferred language (DE/FR/IT/EN), and, if you tell us, your canton of residence.
- **Profile preferences (optional):** favourite supermarket chains, favourite products, dietary filters (for example vegetarian, vegan, organic, high-protein). You are not required to provide these to use the Services.
- **Cart and list data:** items you add to your shopping cart or list, offers you save, notes you add, and the modification history of these items while the feature is in use.
- **Shared-cart data:** if you create or join a shared household cart, your contributions become visible to the other members of that cart (see Section 6).
- **Loyalty card data:** if you choose to link a supermarket loyalty card, the identifier of that card so we can display offers tied to it. We do not use this data to transact with the retailer on your behalf.
- **Correspondence:** messages you send us by email, in-app chat, or form, together with the metadata of that communication.
- **User-generated content:** for example, scanned barcodes and, when available, scanned receipts for features you choose to use.

4.2 Data collected automatically when you use the Services

- **Technical data:** IP address, device identifiers, device type, operating system, browser type and version, language settings, referring URL, pages or screens viewed, actions taken, timestamps, and crash or error reports.
- **Geolocation:** approximate location derived from IP and — only if you grant permission at the operating-system level — precise location, used to show nearby offers and to determine the correct cantonal offer set. You can revoke this permission at any time in your device settings.
- **Push notification tokens:** if you enable notifications, the identifier provided by Apple or Google that allows us to deliver them, together with delivery logs.
- **Cookies, SDKs and similar technologies:** see the Cookie Policy annex and our in-app or in-site consent interface for your choices.

4.3 Data we receive from third parties

We receive product and offer information (product names, prices, discount percentages, category and dietary attributes, images and descriptions) from the supermarket chains and retailers whose offers we display, or from data sources acting on their behalf. That information is not personal data about you.

If you sign in to Rappn using a third-party identity provider, we will receive the limited profile data that provider shares with us (typically email address and name).

4.4 Sensitive data

Some of the information we process — in particular dietary filters such as "vegan", "vegetarian" or "organic" — may indirectly reveal information about your lifestyle. Article 5(c) FADP and Article 9 GDPR treat certain categories of data with heightened protection. We therefore:

- limit the use of this information to displaying and filtering offers;

- do not use it for marketing profiling without your separate consent; and
- do not infer religious or philosophical beliefs from this information.

5. Why we process your data and on what legal basis

We process your personal data for the purposes and on the legal bases below. Where the GDPR applies, the corresponding Article 6 GDPR basis is indicated in brackets.

- **Providing the Services and performing our contract with you —** creating and maintaining your account, showing offers, enabling carts and favourites, delivering notifications you have enabled (Art. 31(2)(a) FADP; Art. 6(1)(b) GDPR).
- **Complying with legal obligations —** bookkeeping, tax, responses to lawful requests from authorities (Art. 31(1) FADP; Art. 6(1)(c) GDPR).
- **Security and protection of our rights —** operating the Services securely, preventing abuse, investigating suspected misuse, exercising or defending legal claims (Art. 31(1) FADP; Art. 6(1)(f) GDPR).
- **Service improvement and product analytics —** with your consent where required, understanding how features are used so that we can improve them (consent; or Art. 6(1)(f) GDPR depending on the technology).
- **Marketing communications (newsletters, product updates, targeted campaigns, push marketing) —** only with your prior consent, which you can withdraw at any time (Art. 3(1)(o) Swiss Unfair Competition Act; Art. 6(1)(a) GDPR).
- **Personalised recommendations —** with your consent, suggesting offers based on your favourites, past actions and preferences.
- **Sponsored placements —** displaying clearly labelled commercial content from retailers or brands. Audience building or measurement beyond the offer itself requires consent.

You can withdraw consent at any time; withdrawal does not affect the lawfulness of processing before withdrawal.

6. Shared carts (household feature)

If you create a shared cart, you can invite other users to join it. Once a user accepts the invitation:

- the accepting user gives their own consent to participate and to the visibility rules of the shared cart before their account is added;
- each participant sees the products added and the modifications made by other participants within that shared cart;
- only data explicitly added to the shared cart is shared — your private favourites, saved offers and cart history outside the shared cart remain private;
- any participant can leave the shared cart at any time, and can choose whether to remove their contributions or leave them in place;
- the creator of the cart can close it, which ends data sharing for all participants.

We keep a record of who joined and left, and when, so that we can evidence the lawfulness of the processing. A participant cannot consent to the processing of another person’s data: each participant consents for themselves.

7. Automated processing, profiling and AI

We use automated processing, including recommendation models, to:

- rank and personalise offers on your home screen;
- suggest substitutions and basket optimisations when you use those features;
- decide which notifications are most relevant to send you, where you have enabled notifications;
- detect suspected abuse, automation and fraud.

These operations do not, in themselves, produce legal or similarly significant effects on you within the meaning of Article 22 GDPR or Article 21 FADP. If we ever implement fully automated decisions that do produce such effects, we will inform you in advance and offer the rights provided by those articles, including the right to request human review.

8. Who we share your data with

We do not sell your personal data. We share it only in the following circumstances and only to the extent necessary for the purposes described in Section 5:

- **With third-party service providers acting on our instructions** under written agreements that limit them to processing your data for the purposes described in this policy and require them to protect it.
- **With other users,** only to the extent you choose — for example, when you create or join a shared cart (see Section 6).
- **With authorities and third parties,** where we are required to do so by law, by valid legal process, or where disclosure is strictly necessary to investigate, prevent or address fraud, security or safety issues, or to enforce our Terms of Service or defend our legal rights.
- **In the context of a corporate transaction,** such as a merger, acquisition, financing, reorganisation, or sale of all or part of our business or assets. If this happens, we will take reasonable steps to ensure that your data continues to be protected in accordance with this policy, and we will inform you as required by law.

9. International data transfers

Your personal data is primarily processed in Switzerland and the European Economic Area. Some processing may take place outside those regions, including in the United States.

Where we transfer personal data to a country that, in the view of the Swiss Federal Council or (where relevant) the European Commission, does not provide an adequate level of data protection, we put appropriate safeguards in place, including:

- the Standard Contractual Clauses approved by the European Commission, supplemented by the adjustments recognised by the Swiss Federal Data Protection and Information Commissioner (FDPIC);
- additional technical and organisational measures (for example, encryption in transit and at rest, access controls and audit logging), where our risk assessment indicates they are needed; and

- where applicable, reliance on a provider's certification under a framework recognised as providing an adequate level of protection (for example, the EU–US Data Privacy Framework and its Swiss counterpart, to the extent that they apply).

You can request a summary of the safeguards in place for a specific transfer by writing to info@rappn.ch.

10. How long we keep your data

We keep personal data only as long as we need it for the purposes set out in this policy, or as required by law. Where we anonymise data, the anonymised data is no longer personal data and is not subject to these periods.

Data category	Retention period	Rationale
Account and contact data	Duration of the account + up to 12 months after closure	Contract; evidence of account lifecycle
Server, application and edge logs	30 days	Security, fraud prevention
Newsletter email and consent evidence	Until unsubscribe + up to 24 months	Evidence of lawful consent
Cart, favourites, saved offers	Duration of the account	Contract; proportionality
Shared cart data	Duration of the shared cart; inactive carts archived after 6 months and deleted after 12 months	Proportionality
Cart modification history	90 days rolling	Product functionality
Loyalty card identifiers	Until removed by the user or account closure	Contract
Device identifiers and push tokens	Duration of the account + 90 days	Service delivery
Geolocation data	Session only, unless you enable features that require history	Data minimisation
Crash and diagnostics data	Up to 180 days	Stability
Analytics identifiers (with consent)	Up to 14 months	Industry default
Marketing identifiers (with consent)	Up to 180 days or until consent withdrawn	Consent
Consent records	Up to 24 months after consent ends	Evidence of compliance
Support correspondence	Up to 36 months after resolution	Possible legal claims
Records required by law (accounting, tax)	10 years (Art. 958f Swiss Code of Obligations)	Legal obligation

If you close your account, we delete or irreversibly anonymise your personal data within a reasonable period, subject to the retention periods above and to legal obligations that require us to keep specific data longer.

11. Security

We implement technical and organisational measures designed to protect your personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access. These include encryption in transit using TLS, encryption at rest for databases that contain personal data, role-based access controls, least-privilege access, audit logging, backups, and employee confidentiality obligations.

No system is completely secure. If we become aware of a personal data breach that is likely to result in a high risk to your rights and freedoms, we will notify you and the competent authority (the FDPIC and, where applicable, the competent EEA supervisory authority) as required by Article 24 FADP and Articles 33 and 34 GDPR.

12. Your rights

Subject to the conditions and limitations set out in the FADP and, where it applies, the GDPR, you have the following rights in respect of your personal data:

- the right to be informed about the processing of your data and to obtain a copy of your data;
- the right to request correction of inaccurate data or completion of incomplete data;
- the right to request deletion of your data where one of the legal grounds applies;
- the right to request restriction of processing;
- the right to object to processing based on legitimate interests or carried out for direct marketing;
- the right to data portability for data processed by automated means on the basis of consent or contract;
- the right to withdraw any consent you have given, at any time, without affecting the lawfulness of processing before withdrawal;
- the right not to be subject to a decision based solely on automated processing that produces legal or similarly significant effects on you.

You can exercise these rights by writing to info@rappn.ch. We may ask you for information to verify your identity. We aim to respond within 30 days. Where a request is complex or where we receive a large number of requests, we may extend this period by up to two further months and will tell you why.

If you are unhappy with how we have handled your personal data, we encourage you to contact us first at info@rappn.ch. You also have the right to lodge a complaint with a supervisory authority, in particular:

- the Swiss Federal Data Protection and Information Commissioner (FDPIC), Feldeggweg 1, 3003 Bern, www.edoeb.admin.ch; or
- the data protection supervisory authority in your country of residence in the EEA, if the GDPR applies to your use of the Services.

13. Cookies and similar technologies

We use cookies, software development kits (SDKs), pixels and similar technologies to operate the Services and, with your consent, to measure their use and deliver or measure advertising. See the Cookie Policy annex at the end of this document. When you first visit our website or open the app, and from time to time thereafter, you can accept or reject non-essential categories and change your choices at any time via the cookie settings available in the footer of the website or the privacy settings of the app.

14. Children

The Services are intended for a general audience and are not directed at children. We do not knowingly create accounts for, or direct marketing at, children who are below the age at which they can validly give consent to online services in their country of residence (by way of guidance: we treat 16 years as that threshold unless local law provides otherwise).

A person below that age should only use the Services with the involvement of a parent or legal guardian. If we learn that we have collected personal data from a person below the applicable age without appropriate consent, we will delete that data promptly.

15. Changes to this policy

We may update this policy from time to time, for example to reflect changes in our Services or in the law. We will post the updated version with a new "Last updated" date. If the changes are material, we will give you reasonable advance notice by a suitable means (for example, in-app or by email).

16. Contact

If you have any questions about this policy or about how we handle your personal data, please write to us at info@rappn.ch or by post to Rappn GmbH, Baarerstrasse 43, 6300 Zug, Switzerland.

Annex — Cookie Policy

This annex supplements the main Privacy Policy.

A. How we ask for your consent

When you first visit our website or open the app, we display a consent interface with three options: Accept all, Reject all, and Customise. Non-essential cookies and SDKs only load after you have given your consent. You can change your choices at any time through the cookie settings link in the website footer or the privacy settings of the app.

B. Categories

- **Strictly necessary (always on):** required to load the Services, to ensure security, to balance load, and to remember your consent choices.
- **Preferences:** remember your language, canton and interface choices.

- **Analytics:** measure how the Services are used so that we can improve them.
- **A/B testing and performance:** help us compare product variants and measure performance.
- **Marketing and advertising:** enable us or our partners to measure campaigns or build audiences, only with your consent.
- **Crash and diagnostics:** help us keep the app stable and fix errors.

C. Default retention

- Consent cookies: up to 12 months.
- Analytics identifiers: up to 14 months.
- Marketing identifiers: up to 180 days or until consent is withdrawn.
- A/B testing cookies: up to 90 days.

If you block a category, some features may not work or may be limited. Strictly necessary cookies cannot be disabled because the Services cannot be delivered without them.