1. About this Privacy Policy

This Privacy Policy explains how **myGaru OÜ** ("myGaru"), a company registered in Estonia, Harju maakond, Tallinn, Kesklinna linnaosa, Pärnu mnt 105, 11312, handles personal data. It covers two distinct contexts:

Part A applies when you visit mygaru.com, myGaru's public website.

Part B applies when myGaru processes data in its capacity as a provider of identity, data-collaboration and advertising-technology services on the digital properties of its partners and publishers. This is the context relevant to myGaru's registration on the IAB Europe Global Vendor List under the Transparency and Consent Framework (TCF).

Part C sets out provisions that apply in both contexts.

This Privacy Policy does not replace the Terms of Service that govern business use of the myGaru platform, or the privacy notices of the publishers, telecom operators and data partners who, in the context described in Part B, decide why and how personal data is used and therefore act as the controllers of that data.

myGaru is the controller of the personal data described in Part A. In the context described in Part B, myGaru generally acts as a processor on behalf of its partners, and as a controller only for limited operational purposes such as security, fraud prevention and the integrity of its own service.

Contact details are in Part C.

Part A. When you visit mygaru.com

mygaru.com is a marketing website. It does not require you to create an account, and it does not use cookies for analytics, advertising or tracking. The cookies present on the website are described in the Cookie Policy.

What myGaru collects

Contact form data. If you use a contact form, myGaru receives the information you submit, such as your name, email address, company and message. This is transmitted through a function hosted by Cloudflare and delivered by email through the provider Resend to myGaru's inbox. Your IP address, as seen by the hosting layer, is processed as part of handling the request.

Security and connection data. myGaru's hosting and security providers process technical data such as your IP address and request information in order to deliver and protect the website. On pages that contain a form, Cloudflare Turnstile processes browser and device signals to distinguish genuine visitors from automated traffic.

Embedded video. On pages that contain video, the embedded Vimeo player causes your browser to send your IP address, browser information and the page address to Vimeo. The players are configured with Do Not Track enabled.

Why myGaru processes this data, and on what legal basis

- To operate, deliver and secure the website, including protection against automated abuse. Legal basis: myGaru's legitimate interests in running a functioning and secure website (Article 6(1)(f) GDPR).
- To respond to enquiries you submit through a contact form, and to take any steps you request before entering into a contract. Legal basis: myGaru's legitimate interests, or steps taken at your request prior to a contract (Article 6(1)(f) or 6(1)(b) GDPR).

Who receives this data

myGaru uses the following service providers in connection with the website: Cloudflare (hosting and security), Resend (email delivery) and Vimeo (embedded video). They process the data on myGaru's behalf or, in the case of Vimeo, as the provider of the embedded player.

Retention

Contact-form information is kept only for as long as needed to handle your enquiry and any related follow-up. Security and log data is retained for short operational periods in line with the providers' standard configurations.

International transfers

Some of these providers process data outside the European Economic Area, including in the United States. Where that is the case, the transfer is made subject to appropriate safeguards, such as the European Commission's standard contractual clauses or the EU-US Data Privacy Framework, where applicable.

Part B. When you encounter myGaru as an identity and advertising-technology provider

This Part explains how myGaru processes data when you use a website, app or other digital property operated by one of its partners (a publisher, a telecom operator or a data partner) that works with the myGaru platform. myGaru is a registered vendor on the IAB Europe Global Vendor List and participates in the Transparency and Consent Framework. myGaru's entry on the Global Vendor List sets out the authoritative and current list of purposes it relies on and the legal basis for each.

myGaru's role

In this context, the partner that operates the property decides why and how data is used and is the controller. myGaru generally acts as a processor, providing the technical identity, matching and activation services on that partner's instructions and within the permissions configured for each dataset. myGaru does not decide the purposes of the underlying advertising or business activity. myGaru acts as a controller only for limited operational purposes such as security, fraud prevention and the integrity of its own service.

How myGaru identifies a session without using your phone number

myGaru's identity layer is telecom-driven. Where a phone number is transformed within the telecom operator's own controlled environment before myGaru receives anything. myGaru then operates only on derivative, pseudonymous identifiers:

- a short-lived session identifier (OTP);
- an internal pseudonymous identifier (Ephemeral UID); and
- a partner-scoped identifier (Partner UID), which is different for the same person across different partners.

The real phone number does not enter myGaru's operational systems.

What myGaru does not do

- myGaru does not store your real phone number in its operational systems.
- myGaru does not store your third-party cookies in its operational systems.
- myGaru applies a minimum audience size, by default 100 individuals, to its audience and analytics operations in order to reduce the risk of any individual being singled out.
- myGaru does not knowingly process special categories of data, such as data revealing religion or political opinions.

Opting out of myGaru identification

You can opt out of being identified through the myGaru identifier at https://mygaru.com/options. Where you reach that page through a participating telecom network, myGaru is able to recognise you through its telecom-driven identifier and record your opt-out. myGaru uses that identification on the page only to check and apply your preference, not for advertising or profiling. Once you have opted out, myGaru no longer identifies you through its identifier for new uses.

Cookies and similar storage in this context

When providing its services on a partner's property, myGaru and its infrastructure may set or read pseudonymous cookies or use similar device storage, for example identifiers named vmuid, nuid and niseis, with a duration of up to 60 days. These are

myGaru's vendor technologies, used in the advertising context, and they are not set when you browse mygaru.com. They are declared in myGaru's TCF Device Storage Disclosures, published at https://mygaru.com/.well-known/deviceStorage.json.

Categories of data

Depending on the relevant flow and the permissions set by the partner, the data processed in this context may include:

- pseudonymous and derivative identifiers (OTP, Ephemeral UID, Partner UID);
- technical connection data such as IP address, processed transiently for security and delivery;
- where a partner has enabled signal collection on its own property, usage and interaction signals, such as pages visited or actions taken;
- where a partner has connected its own first-party data, attributes held within that partner's own environment, which may include general or approximate location, demographic information, interests and behavioural signals; and
- consent and permission status received from the partner.

First-party data connected by a partner remains within that partner's own controlled environment. myGaru does not operate a central store of partners' raw first-party data.

What myGaru does with the data

- Connecting a partner's authorised first-party data to the platform.
- Creating and matching audience segments in a privacy-centric way, including data clean room operations, so that partners can collaborate without disclosing their underlying data to each other.
- Determining whether a given session is eligible for an advertising campaign, and supporting the delivery and display of advertising.
- Producing aggregated and non-identifying reporting and measurement.
- Ensuring security, preventing fraud and maintaining the integrity of the service.

Legal basis

For advertising-related processing, myGaru relies on the consent that the publisher or other partner collects from you through its consent management platform under

the Transparency and Consent Framework. Where that consent is not given, or is withdrawn, myGaru does not begin the relevant processing for new uses on that property.

myGaru relies on legitimate interests only for security, fraud prevention and the technical integrity of its service. This paragraph also constitutes myGaru's legitimate interest claim for the purposes of the Transparency and Consent Framework.

Retention

- The short-lived session identifier (OTP) is transient and is used only within the authorised session and no more than 6 hours in some cases.
- Pseudonymous campaign-matching structures are held only for the duration of active advertising use. Where a campaign remains technically active but a segment is no longer being matched, those structures are held for a short standby period that does not exceed 72 hours from the last matching request.
- Aggregated reporting outputs do not contain identifying data.
- First-party data connected by a partner is retained under that partner's own settings and instructions, not by myGaru.
- Security logs and audit records are retained in line with applicable security, compliance and auditability requirements.

Who receives the data

The participants in this context are the telecom operator, which provides the identity layer, the data partner and the publisher, which act as controllers, and integrated advertising-technology providers such as demand-side and supply-side platforms. As noted above, those advertising-technology providers receive only the campaign-eligibility result needed for the authorised flow, not your identity or profile.

International transfers

myGaru operates locally in each market it serves, and for advertising activity it processes personal data and derivative identifiers within the relevant market. A limited group-level support function may have access to operational information and aggregated, non-identifying reporting only, and not to personal data or

derivative identifiers. Where any transfer of personal data outside the European Economic Area occurs, it is made subject to appropriate safeguards.

Your rights and how to exercise them

Because myGaru generally acts as a processor in this context, requests are normally handled through the relevant controller. You can exercise your rights:

- through the publisher's consent management platform, where you can change or withdraw your consent at any time, which stops the relevant processing for new uses;
- through your telecom operator's own channels and, where it is offered, through the myGaru control point integrated into the telecom operator's interface, where you can manage your consent, permissions and advertising preferences;
- directly, through the myGaru preference page at https://mygaru.com/options, where you can opt out of being identified through the myGaru identifier, as described under "Opting out of myGaru identification" above; and
- through the data partner whose data is involved.

You can also contact myGaru at info@mygaru.com, and myGaru will support the relevant controller in giving effect to a valid request within the authorised scope.

Part C. Provisions that apply in both contexts

Security

myGaru applies technical and organisational measures appropriate to the data it processes. These include encryption of stored data and of data in transit, including mutual authentication between systems, separation of management environments, access controls, the rotation of identifiers, and logging and auditability of relevant actions.

Your right to complain

If you have a concern about how your personal data has been handled, you can contact myGaru using the details below. You also have the right to lodge a complaint with a data protection supervisory authority. myGaru's home authority is the Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon).

Changes to this Privacy Policy

myGaru may update this Privacy Policy from time to time. Any changes will be posted on this page with a revised "last updated" date.

Contact

myGaru OÜ
Harju maakond, Tallinn, Kesklinna linnaosa, Pärnu mnt 105, 11312, Estonia
Email: info@mygaru.com