

Privacy Policy

Last updated: 5 September 2026

This policy replaces the version dated 17 February 2026.

1. Who we are and how to reach us

The Change Republic GmbH, company number CHE-131.869.164, Rötibodenstrasse 34, 8820 Wädenswil, Switzerland. In this policy we call ourselves "we" and "us". We are the controller for all of the data use described here, which means we decide why and how your data is used.

We offer executive coaching, leadership development, personal branding advisory, workshops and keynote speaking. We also run two AI tools on our website: a chatbot called CoachTünde.ai and a voice assistant we call the AI twin.

For anything about your data, including to exercise the rights in section 12, write to hello@thechangerepublic.com. We answer within 30 days.

We have not appointed a Data Protection Officer. Swiss law does not require us to have one, and we are below the thresholds in Article 37 of the GDPR.

2. Which laws apply

Two sets of rules apply to us, and which one you can rely on depends on where you are.

We are a Swiss company, so the Swiss Federal Act on Data Protection (FADP) applies to everything we do. The FADP was revised with effect from 1 September 2023, and this policy follows the revised version.

We also offer our services to people in the European Union, and we measure how visitors from the EU use our website. That brings us within the scope of the EU General Data Protection Regulation (GDPR) through its Article 3(2). If you are in the EU or the EEA, the GDPR applies to you alongside the FADP, and you have the additional rights set out in section 12.

If you are in the United Kingdom, the UK GDPR applies to you on the same terms.

The two laws are built differently, and it is worth being straight about how. The GDPR requires us to point to a specific legal basis before we may use your data at all. Swiss law does not work that way. Under the FADP we may process personal data provided we do so lawfully, in good faith and proportionately, that we are open about it, and that we use it only for the purpose we collected it for. We need a specific justification, meaning your consent, an overriding interest, or a law, only where our processing would otherwise breach your personality rights, where it involves sensitive data, or where we would be acting against your express wishes.

Because the GDPR is the stricter of the two on this point, we have set out a GDPR legal basis for everything we do, in section 7, and we apply that standard to everybody rather than running two different regimes.

Cookies are governed separately in Switzerland, by Article 45c of the Telecommunications Act, which requires us to tell you about cookies and let you refuse them, rather than to obtain consent first. EU law requires consent before non-essential cookies are set. We follow the EU rule for everyone, which also matches what the Swiss Federal Data Protection and Information Commissioner expects for tracking that a visitor would not anticipate. Session recording is exactly that kind of tracking.

3. What we collect from visitors to our website

This section covers people who simply visit the website. Sections 4 and 5 cover the AI tools, and section 6 covers clients.

Our website runs on Wix. Wix hosts the site and provides the analytics built into it.

Website statistics (Wix). Wix records each visit to our site: your IP address, the city, postal code and region that address maps to, your browser, your device type, which pages you viewed, how long you stayed, and how you arrived, for example from a search engine, a link, or a chat assistant such as ChatGPT.

Most of this is recorded by the Wix platform as part of hosting the site, whether or not you accept cookies, in the way any web server keeps a log of what it served. Our basis for that is our legitimate interest in running the site, keeping it secure and seeing how it performs. The more detailed behaviour tracking inside Wix runs only if you accept analytics cookies.

We use these statistics to see which organisations are interested in our work. We do that by looking up the IP address in the public internet address registries, which show the organisation a block of addresses is registered to. It tells us that someone at a given company read a given page. It does not tell us who, and we do not try to find out. Home and mobile connections identify nobody and we discard them. Our basis is legitimate interest, and you can object at any time under section 12.

Session recording (Microsoft Clarity). If you accept analytics cookies, Microsoft Clarity records your visit. It captures mouse movement, scrolling, clicks and the content of the pages as they appeared to you, and replays them to us as a recording and as heat maps. We use it to see where the site confuses people.

Clarity runs only on your consent. If you decline, or ignore the banner, nothing is recorded. Microsoft masks text typed into form fields by default.

Live chat (Wix Smart Chat). Our site has a chat window. If you write in it, we receive your message, and we are notified while you are still on the site so that we can answer. We collect what you write, and your name and email address if you give them. Our basis is legitimate interest in answering people who contact us, and your consent for anything extra you choose to tell us.

Cookies and consent. We use a consent banner. You can accept all cookies, decline them, or choose which categories you allow, and you can change your answer at any time using the link in the website footer. Your choice is stored in your browser and in a consent record so that we can show, if we are ever asked, that you were given a real choice.

Cookies that are strictly necessary, which means security, load balancing and remembering your consent choice, are set without asking, because the site cannot work without them. Everything else, including Microsoft Clarity, waits for your consent.

Contact forms and booking a call. If you fill in a form or book a call, we collect what you type. Calls are booked through Calendly, which collects your name, email address and the time you chose.

The booking page tells you that booking a call also adds you to our newsletter list, and the booking goes ahead on that basis. You can unsubscribe from the first email you receive, or at any time after that, and we will not add you back. If you would rather not be added at all, say so when you book and we will keep you off the list.

Our online assessments. We offer self assessments on our site, including a career readiness assessment and a team AI readiness assessment. If you complete one, we collect your name, your email address and your answers, so that we can generate your result and send it to you. Completing an assessment also adds you to our newsletter list, on the same terms as above.

Newsletter. We collect your name and email address, and we record which of our emails you opened and which links you clicked, so that we can tell whether the newsletter is worth writing. Our newsletter runs on MailerLite. Every email has an unsubscribe link, and unsubscribing stops the tracking as well as

the emails.

4. The chatbot, CoachTünde.ai

CoachTünde.ai is our coaching chatbot. It runs on Chatbase.

We collect what you type into it, together with the timestamp and a session identifier. If you volunteer your name or email address in the conversation, we collect that too.

We use it to generate the answers, to see where the chatbot performs badly, and to improve it.

Conversation logs are also copied into a Google spreadsheet that we use to review them. That copy contains the same conversation text.

Chatbase uses further companies to run its service, and your conversation passes through them. The ones that matter are OpenAI and Anthropic, which supply the language models that produce the answers. Chatbase also uses hosting, database and security providers to store and protect the conversations. Chatbase keeps the current list of these companies, and we will pass it to you on request. Several of them are in the United States.

This is worth stating plainly because our earlier policy was misleading on the point. When you talk to our chatbot, your words are sent to a large language model run by OpenAI or Anthropic in order to produce a reply. That is how the chatbot works.

The legal basis is your consent, which you give by starting a conversation. You can simply not use the chatbot, and everything else on the site works without it.

Please do not type anything into the chatbot that you would not want stored. Treat it as a coaching tool rather than a confidential channel. Do not use it for health information, and do not use it in an emergency. If you are in crisis, contact your local emergency number or, in Switzerland, Die Dargebotene Hand on 143.

5. The AI twin, our voice assistant

On our AI twin page you can speak to a voice assistant. It runs on ElevenLabs.

We collect the audio recording of what you say, a written transcript of the conversation, the timestamp, a session identifier, how long the call lasted, your IP address, and your browser and device type.

The assistant is also set up to ask for your name, your email address and the company you work for, and to record them if you give them. You do not have to. The conversation works without them, and we would rather you left them out than gave them without meaning to.

We use this to generate the spoken replies, to keep track of the conversation while it is running, to improve the assistant, and to follow up with you if you asked us to.

The legal basis is your consent, which you give by starting a voice conversation. The assistant tells you at the start that it is an AI and that the call is recorded.

ElevenLabs stores this data in the United States. See section 10.

6. What we collect from clients

If you become a client, or your employer engages us, we also collect:

Your name, work email address, telephone number and postal address, and your role.

Coaching content, meaning your goals, our session notes, and the results of any assessment you complete with us, such as the Leadership Circle Profile.

Where a session is recorded, and only where you have agreed to it, the recording and any transcript.

Transcripts of calls. We use an AI notetaker called Tactiq to transcribe consultation calls and coaching sessions, so that we can write up notes and follow up properly.

You are told before the call rather than at the start of it. The booking confirmation says the meeting may be transcribed and asks you to say in advance if you would prefer it switched off. If you say so, we switch it off. We do not transcribe a call where anyone taking part objects.

Billing data, meaning the invoice amount, the payment status and a reference from the payment provider. We never see or store your full card number.

Coaching content is treated as confidential. We do not share it with your employer, even where your employer is paying. Where an employer engages us for a group, they receive themes across the group and never anything attributable to one person.

7. Why we use your data, and on what legal basis

We use your data only for the purposes below. For each one we give the legal basis under the GDPR. As section 2 explains, Swiss law does not require us to name a basis in the same way, so what follows is the GDPR standard, applied to everyone.

To deliver the coaching, training and speaking you or your employer engaged us for. Basis: performance of a contract, Article 6(1)(b) GDPR.

To issue invoices and take payment. Basis: performance of a contract, and our legal obligation to keep accounting records, Article 6(1)(b) and 6(1)(c) GDPR. Swiss company law requires us to keep books for ten years.

To send the newsletter. Basis: your consent, Article 6(1)(a) GDPR. You may withdraw it at any time.

To run the chatbot and the voice assistant. Basis: your consent, given by starting a conversation.

To measure how the website is used, including session recording. Basis: your consent, given through the cookie banner.

To work out which organisations visit our website. Basis: our legitimate interest in understanding who is interested in our services, Article 6(1)(f) GDPR. We have weighed this against your interests. It uses only public registry records, it tells us about organisations rather than about individual people, and you can object at any time. Under Swiss law we rely on our overriding private interest.

To improve our services. We review anonymised prompts and transcripts, and we use AI tools including ChatGPT, Claude and Perplexity for research and drafting. We remove identifying details before anything goes into those tools. Basis: legitimate interest.

To keep our systems secure and to prevent misuse. Basis: legitimate interest.

To meet our legal obligations and to defend legal claims. Basis: legal obligation and legitimate interest.

Your data is not used to train anyone else's AI models. This is worth stating on its own, because it is the question people ask most.

Your data is not used to train or improve anyone else's models. That covers the chatbot, the voice assistant, the call transcripts and the tools we use ourselves for research and drafting. Where a tool offers a setting that controls this, we have turned model training off. Where a tool has no such setting, we use it under terms that exclude customer content from training.

We do use conversations with our own chatbot to improve our own chatbot, meaning its instructions and its answers. That work stays with us and does not feed anyone else's model.

We do not sell your data. We do not share it with advertising networks. We do not use it to build advertising profiles.

8. Automated decisions

We do not make any decision about you by automated means alone that has a legal effect on you or similarly significantly affects you. The chatbot and the voice assistant generate answers automatically, but they do not decide anything about you. Every coaching decision, assessment interpretation and commercial decision is made by a person.

9. How long we keep data

What	How long
Client files and coaching notes	2 years after the engagement ends
Session recordings, where agreed	Deleted once notes are written, and in any case within 12 months
Invoices and accounting records	10 years, as Swiss law requires
Newsletter subscription and engagement history	Until you unsubscribe, then 12 months so that we can show you had subscribed
Chatbot conversations in Chatbase	12 months
Copies of chatbot conversations in our review spreadsheet	12 months
Voice assistant recordings and transcripts	12 months
Website analytics exports containing IP addresses	12 months
Session recordings in Microsoft Clarity	Deleted automatically by Microsoft. We do not download or keep copies
Consent records	5 years, so that we can show what you were asked and what you chose
Assessment answers and results	24 months
Call transcripts from the AI notetaker	Deleted once notes are written, and in any case within 12 months
Chat window conversations	12 months
Enquiries that do not become engagements	24 months

Where we are required to keep something longer to comply with the law or to defend a legal claim, we keep it for as long as that requires and no longer.

10. Who else handles your data

We use the companies below to run our business. Each of them acts on our instructions under a contract, and none of them may use your data for their own purposes.

Website and analytics. Wix, which hosts the website, provides its statistics and runs the chat window. Microsoft, which provides Clarity session recording. Usercentrics, which provides the cookie consent banner. Replit, which hosts our online assessments.

AI tools. Chatbase, which hosts the chatbot, together with its own suppliers, of which the significant ones are OpenAI and Anthropic. ElevenLabs, which provides the voice assistant. Tactiq, which transcribes calls.

None of these companies may use your data to train their own AI models. That applies to OpenAI, which is behind ChatGPT, to Anthropic, which is behind Claude, and to Perplexity, Chatbase, ElevenLabs, Tactiq and Replit.

Email and scheduling. MailerLite for the newsletter. Google, whose Workspace we use for email, calendar, document storage and the spreadsheet holding chatbot logs. Calendly for booking calls.

Meetings and messaging. Zoom for video calls. WhatsApp for messaging where a client chooses that channel.

Payments and accounting. Stripe and PayPal for payments. Bexio for bookkeeping and invoicing. Our bank, and our external accountant.

Research and drafting. OpenAI, Anthropic and Perplexity. We remove identifying details before using these tools.

We also give data to public authorities where the law requires it, and to our lawyers and insurers where we need to establish or defend a legal claim.

11. Sending data outside Switzerland

Several of the companies above are in the United States. They are Microsoft, Chatbase, OpenAI, Anthropic, ElevenLabs, Google, Zoom, Calendly, Tactiq, Replit, Stripe and PayPal, together with the hosting and database providers Chatbase uses. MailerLite is in Lithuania, inside the EU. Wix is in Israel, which the Swiss Federal Council and the European Commission both recognise as providing adequate protection.

For the United States we rely on one of two things, depending on the provider. Where a provider is certified under the Data Privacy Framework, we rely on that certification. The Swiss arm of that framework has been recognised by the Swiss Federal Council since 15 September 2024, and the EU arm since 2023. Where a provider is not certified, we rely instead on the Standard Contractual Clauses approved by the European Commission and recognised by the Swiss Federal Council, together with the extra technical and organisational measures those clauses oblige us to consider.

You should know what this means in practice. United States authorities have powers to demand data from companies based there, and those powers are broader than Swiss or EU law allows at home. The safeguards above reduce that risk without removing it. If that matters to you, do not use the chatbot or the voice assistant, and decline analytics cookies. The rest of the website works without any of them.

You may ask us for a copy of the safeguards we rely on for any specific provider. Write to hello@thechangerepublic.com.

12. Your rights

You have the following rights. They cost nothing to use, and using them will never count against you as a client.

Under both Swiss and EU law you may:

Ask what data we hold about you and get a copy of it.

Ask us to correct anything that is wrong.

Ask us to delete your data.

Ask us to stop or limit a particular use.

Object to any use we base on legitimate interest, including the IP address lookups described in section 3.

Withdraw consent at any time, for the newsletter, the chatbot, the voice assistant or analytics cookies. Withdrawing consent does not make what we did beforehand unlawful.

If you are in the EU, the EEA or the UK, you also have the right to receive the data you gave us in a machine readable format and to have it sent to another provider where that is technically possible.

To use any of these rights, write to hello@thechangerepublic.com. We will answer within 30 days. If a request is unusually complex we may need longer, and we will tell you why before the 30 days are up. We may need to check who you are before we send personal data.

If you are unhappy with how we handled your data, please tell us first, because most things are quicker to fix directly. You also have the right to complain to a regulator.

In Switzerland, that is the Federal Data Protection and Information Commissioner, Feldeggweg 1, 3003 Bern, www.edoeb.admin.ch.

In the EU or the EEA, you may complain to the supervisory authority in the country where you live or work.

In the UK, that is the Information Commissioner's Office, www.ico.org.uk.

13. Security

We protect your data with encryption in transit and at rest, access limited to the people who need it, two factor authentication on every account that supports it, and a password manager rather than reused passwords. We review these arrangements regularly.

If data is lost, stolen or exposed in a way that puts you at high risk, we will report it to the Federal Data Protection and Information Commissioner as soon as possible, as Swiss law requires. Where the GDPR applies we will also report it to the relevant EU authority within 72 hours. We will tell you directly where the law requires it, or where telling you would let you protect yourself.

No system is completely secure. This section describes our practice and is not a guarantee.

14. Children

Our services are for adults. We do not knowingly collect data from anyone under 16. If you believe a child has given us data, write to hello@thechangerepublic.com and we will delete it.

15. Changes to this policy

We update this policy when what we do changes. The current version is always in the legal section of our website, and the date at the top tells you when it last changed.

Where a change matters to you, we will say so through our usual channels, which are the website, the newsletter and our LinkedIn page. We keep the previous version available on request so that you can see what changed.