Authgear

Free checklist · 20 questions

The Sovereign Login Checklist

20 questions to ask any identity provider about where your users' data lives, who can reach it, and whether you can leave.

Your login system holds every user's email address, phone number, password hash, MFA secrets and sign-in history. When a customer, regulator or procurement team asks "where does our user data live, and who can get at it?", the answer starts here.

A UK or EU data centre answers only part of that question. Sovereignty also depends on who runs the system, whose law applies to them, whether you can move away, and which other companies see the data along the way.

Copy the questions into your vendor questionnaire, or use them to check the setup you already have. General guidance, not legal advice: talk to your data protection officer or a lawyer about your own situation.

1 Where does the data sit?

- [ ] 1 **In which countries are the primary database, the backups and any disaster-recovery copy stored?**
  Good answer: Country names for each, not "Europe" or "our global infrastructure".
- [ ] 2 **Where do login and audit logs, monitoring and analytics data go?**
  Good answer: The same countries as the database, or a named list. Logs are often shipped somewhere else.
- [ ] 3 **Can we fix the region in the contract?**
  Good answer: Yes, in writing, with notice before anything moves.
- [ ] 4 **Is our deployment dedicated or shared with other customers?**
  Good answer: A clear answer, and which parts are shared if any.

2 Who operates it?

- [ ] 5 **Who has administrative access to the servers and database?**
  Good answer: Named teams or roles, and the countries they work from.
- [ ] 6 **Where are support staff, and can they see our user records?**
  Good answer: Countries named; access to user data only when needed and with your agreement.
- [ ] 7 **Are support and admin access logged, and can we see those logs?**
  Good answer: Yes, and you can ask for them. Remote access from another country can count as a transfer in its own right.
- [ ] 8 **Can we audit the deployment, or have someone do it for us?**
  Good answer: Yes, with audit rights written into the contract.

3 Whose law applies?

- [ ] 9 **Which company do we sign with, and where is its parent company?**
  Good answer: Both named, with countries. The parent matters as much as the local subsidiary.
- [ ] 10 **Whose infrastructure does the service run on, and where is that company incorporated?**
  Good answer: Named, so you can ask questions 9–12 about them too.
- [ ] 11 **Which foreign laws, such as the US CLOUD Act, apply to you or your hosting provider?**
  Good answer: A plain answer. "None apply" or "this one applies, and here's how we handle requests".
- [ ] 12 **How do you handle requests from government authorities, and will you tell us?**
  Good answer: A written process, and a commitment to tell you unless the law forbids it.

4 Can you leave?

- [ ] 13 **Can we export all user data, including password hashes and MFA enrolments?**
  Good answer: Yes, in a documented format, so users don't have to reset passwords or re-enrol.
- [ ] 14 **Can we import our existing users with their passwords?**
  Good answer: Yes, for the hash formats you use today. Ask which ones.
- [ ] 15 **Does it use open standards such as OpenID Connect, SAML and LDAP, or proprietary SDKs?**
  Good answer: Open standards, so your apps don't depend on one vendor.
- [ ] 16 **Is the software open source, and could we run it ourselves if we had to?**
  Good answer: Yes, under a licence that allows it, with the same features as the hosted version.

5 Who else touches it?

- [ ] 17 **Which email, SMS and WhatsApp providers send our one-time codes and magic links, and where are they?**
  Good answer: Named providers and countries, or you connect your own. These providers see phone numbers, email addresses and the codes themselves.
- [ ] 18 **Who stores the backups, and where?**
  Good answer: A named provider and country. Backups are full copies of everything.
- [ ] 19 **Do you publish a sub-processor list, and will you tell us before it changes?**
  Good answer: Yes, public, with advance notice of changes.
- [ ] 20 **Which other services see user data, such as bot protection, monitoring or error tracking?**
  Good answer: A complete list. Check each one against questions 1–12.

Questions 2, 17 and 18 are the easiest to miss. The database can sit in London while logs, backups and SMS codes travel elsewhere.

Authgear

How Authgear Answers These Questions

Authgear is open-source login and identity software. If you need to choose where your users' data lives and who runs the system, there are two ways to run it.

Self-host on infrastructure you choose

- **Open source under Apache-2.0.** The self-hosted version has every feature of Authgear Cloud.
- **You decide where it runs:** your own servers, or a UK or EU infrastructure provider you pick (questions 1–4 and 10).
- **Your team operates it.** You control admin access and logs (questions 5–8).
- **You connect your own email, SMS and WhatsApp providers,** so you choose who sees one-time codes and magic links (question 17).
- **Paid support** for self-hosted Authgear is available as part of Enterprise.

Private cloud: we run it for you, in the region you choose

- **A dedicated deployment** that we operate for you, in any region, including the UK and the EU.
- **Audit rights.** Private cloud customers can keep audit rights over their deployment (question 8).
- **Contract with our UK company.** UK and EU customers can sign with it directly (question 9).

For both

- **Open source, so you can always run it yourself** (question 16). Coming from Keycloak? Import your users with their passwords (question 14).
- **LDAP and Active Directory** are supported.
- **Independently audited:** ISO 27001 and SOC 2 Type II.

Book a 30-minute sovereignty review

We'll go through these questions with you: where your login data sits, who can reach it, and how to keep it in the UK or EU, whether that's with Authgear or not. Afterwards you get a short written summary of the options that fit. Free, no obligation, in English.

Scan the code with your phone camera, or click the button.

Book a Sovereignty Review →

General guidance, not legal advice. Authgear makes no claim that any setup meets a particular law or certification scheme.