FREE TEMPLATE

The Vendor Letter

Ask your software vendor where your data goes.

Free template from Nielsen AI. Built from the questions Curt sent one of his own software vendors in 2026, and from what its answers taught him. Not legal advice: it gets you the facts, and a lawyer tells you what they mean for your purpose.

Before you write

Your software vendor has probably already answered half of this somewhere. Spend twenty minutes looking first, because a letter that asks what the website already says gets a link back and nothing else.

1. Find three documents: the **data processing agreement** (DPA, sometimes called a data processing addendum or Auftragsbearbeitungsvertrag), the **sub-processor list**, and the **terms for the specific service** you use.
2. Read the clause on where data is stored, and the clause on sub-processors. Note the clause numbers.
3. Check whether the **marketing page** and the **trust centre or security page** agree. In one check of my own tools, the marketing page said "stored and processed within Europe" and the trust centre put the logs in Virginia.
4. Ask only what those documents leave open. Quote the clause you're asking about.

The letter

Send it to the data protection address in the DPA or privacy policy. If that inbox stays silent for two weeks, open a support ticket with the same text: some vendors route information requests to support, not to the DPO.

Subject: [Service name]: sub-processors and processing location (DPA [clause numbers])

Dear Data Protection team,

I am a customer of [vendor] (account: [your account email]) and use [service name] on the [plan name] plan. Before I describe this service in my own privacy statement, I need written confirmation on the following.

1. **Sub-processors.** Which sub-processors take part in providing [service name], for what purpose, and in which country does each one process data?
2. **Storage and processing.** Where is [the data you put in, e.g. customer email addresses] stored at rest, and where is it processed while the service runs (sending, backups, support access, logs)? [If a clause promises a location, quote it:] Clause [X] states "[quote]". Does that cover processing as well as storage?
3. **Where this is published.** Where is the sub-processor list for [service name] published, and how are customers told when it changes?
4. **Which contract applies.** Does the DPA apply to my plan automatically, or do I need to accept it somewhere?
5. **[One question specific to your use.]** For example: is the time of consent stored for each newsletter subscriber, and can I export it? Or: what is deleted, and when, if I cancel?

Please treat this as a request for information under clause [X] of the DPA, and let me know if another channel is the right one.

Kind regards,
[Name, company, address]

Reading the answer

A good answer names countries and companies, quotes or corrects the clause you cited, and separates storage from processing without being asked. The best answer I've had conceded a gap in the vendor's own documentation instead of reading its clause more broadly than the wording allowed.

Watch for:

- **"Your data is hosted in [country]"** with nothing about processing. Storage and processing are different questions. Ask again with the word "processed".
- **A link to a general security page** instead of an answer to the clause you quoted.
- **"We use industry-standard safeguards"** in reply to "which country".
- **Two answers that disagree.** It happens, sometimes because the second reply answers an older question. Quote both back, ask which holds, and don't publish either until you know.
- **A conclusion you inferred yourself**, for example a region read off a DNS record. Treat it as a reason to ask, never as the answer. I made exactly this mistake once, and the vendor's DPO corrected the method.

Keep the record

Save the letter, the answer, the date, the person who answered and any attachment in one place, and write down what your privacy statement now says because of it. If the vendor changes its answer later, you'll want to show what you were told and when.

Countries: the Swiss test

For a Swiss business, the question is whether the country is on **Annex 1 of the Data Protection Ordinance** (the Federal Council's list of states with adequate protection). EU and EEA states are on it. Apply the test to every sub-processor's country, not only the vendor's own.

For the **USA**, the country alone doesn't decide it: Annex 1 covers only US companies certified under the **Swiss-US Data Privacy Framework**, so check the specific company, and each US sub-processor, at dataprivacyframework.gov. For a country that isn't on Annex 1, the transfer needs other safeguards, such as standard contractual clauses. That is a question for counsel.

Note: don't write "outside the EEA" about your own data: Switzerland isn't in the EEA, so that phrase puts your own country on the wrong side of the line.

---

*Nielsen AI · Curt Nielsen · Basel · **nielsenai.ch**. If you'd rather have someone run this across every tool you use, that's the **Data Path Check** (Datenweg-Check).*

This template online