# GDPR: Our measures to protect personal data

Last updated: Mar 7, 2022

## The basics

**Sana Labs is committed to protecting and respecting your privacy.**

We will:

- always keep personal data safe and private;
- never sell personal data;
- allow users to manage and review their marketing choices at any time; and
- allow users to update, correct, and delete their personal data at any time.

**What type of personal data do we store?**

We store:

- User account information, such as first name, last name, and email.
- Device information, such as browser type, IP address, operating system, and device type.
- User satisfaction-related data, such as NPS score, timestamps, and comments.
- Any additional information you share through email and chat communication with Sana Labs or in relation to your use of our services or websites.

**What is the process for changing and/or removing personal data?**

If your company or organization is providing our Services to you, you may request to change and/or remove personal data by reaching out to your account administrator. You may also reach out to Sana Labs's legal team at legal@sanalabs.com, and we will forward your request to the relevant administrator.

If you are a consumer user for a free and/or trial account, you may reach out directly to legal@sanalabs.com to exercise your right under GDPR.

You can read more about how we handle your personal data at our Privacy Notice.

## How have we adapted our data protection practice in light of the Schrems II decision?

In light of the Schrems II decision, we are taking the following steps in order to ensure we are aware of and can mitigate potential risks from data transfers to non-EU entities:

1. We have mapped all transfers of personal data to third countries, including a mapping of each data field, classified by risk sensitivity, by purpose, by adequacy, and by sub-processor.

2. We have adopted the appropriate safeguards and transfer tools based on the location of data processing by our sub-processors. For sub-processors based in and operating within the EU, and declared as adequate by the European Commission, we rely on

appropriate safeguards under Article 45 GDPR. For sub-processors based outside of a jurisdiction declared as adequate by the European Commission, we rely on appropriate safeguards under Article 46 GDPR: Standard Contractual Clauses (SCCs) and Model Contractual Clauses (MCCs). We continue to monitor updates from the European Commission to ensure that the appropriate safeguards and transfer tools remain valid.

3. We periodically assess the risk of the law or practice of a third country impinging on the effectiveness of the appropriate safeguards in the context of our specific data transfers through the following steps:
    a. Completing model request forms when necessary to highlight elements that pertain to the potential risk of data access by public authorities in third countries
    b. Monitoring data breaches of our sub-processors' systems and, in the event of, maintaining contingency plans
    c. Geo-fencing personal data within the EU/EEA in order to reduce risk of data transfer between EU and non-EU countries

4. We have identified and adopted supplementary technical and organizational security measures to bring the level of protection of the data transferred up to the EU standard of essential equivalence. The supplementary technical and organizational security measures can be referred to in our Data Processing Agreement. We may adopt additional custom security measures on a case-by-case basis to fit the needs of our partners.

5. We have ensured that our sub-processors maintain effective documentation of their supplementary technical and organizational security measures, and in the case that no supplementary measure is suitable, we immediately avoid, suspend, or terminate the transfer to avoid compromising the level of protection of the personal data.

6. We have taken appropriate formal procedural steps to document supplementary measures taken by our sub-processors and to enter up-to-date Standard Contractual Clauses where relevant, and to ensure that the identified supplementary measures do not contradict, directly or indirectly, the Standard Contractual Clauses and are sufficient to ensure that the level of protection guaranteed by the GDPR is not undermined.

7. We re-evaluate and monitor, on an ongoing basis, and where appropriate in collaboration with data importers, developments in the third country to which we have transferred personal data that could affect our initial assessment of the level of protection and the decisions we may have taken accordingly on our transfers.

We understand and comply with the declarative that accountability is a continuing obligation. We make time to understand your concerns regarding the privacy of your personal data. We view respecting privacy as a fundamental pillar in our approach to handling personal data. Do not hesitate to contact us if you have any questions about our approach to safeguarding your privacy, our processing of your personal data, or if you wish to exercise your rights.