
Mexico City, October 2, 2026

To whom it may concern

Subject: Data Processing Agreement for the CellBlock platform

Version 1.0, in effect as of October 2, 2026.

This Agreement governs the processing of the personal data that a customer institution, laboratory or organization (in this Agreement, "the Customer") records on the CellBlock platform, and that Arlen Ramírez Corona, an individual conducting business under the trade name CellBlock, domiciled in Mexico City, Mexico (in this Agreement, "CellBlock"), processes on the Customer's behalf to provide the service.

This English version is provided for convenience. In case of any discrepancy with the Spanish version, the Spanish version prevails.

It forms part of the Terms and Conditions of Use and of any contract, purchase order or service order between the Customer and CellBlock. When the Customer signs it, or incorporates it into its own instrument, it applies as signed.

1. Role of each party

The Customer is the controller of the personal data it records on the platform: it decides which data is processed, about whom and for what purpose. CellBlock acts as processor: it processes that data only on the Customer's behalf, with no decision-making power over its scope and content, and limits its actions to what this Agreement and the Customer instruct.

If the Customer is a public-sector obligated entity, this Agreement is the legal instrument referred to in article 53 of the Mexican General Law on the Protection of Personal Data Held by Obligated Subjects published on March 20, 2025 (LGPDPPO). In all other cases, it is governed by the Federal Law on the Protection of Personal Data Held by Private Parties (LFPDPPP).

This Agreement is governed by the privacy notice the Customer has made available to its data subjects. If anything in this Agreement contradicts it, that notice prevails.

2. Data and data subjects

CellBlock processes, on the Customer's behalf, the data of the people the Customer registers or authorizes in its laboratory: staff, students, internal and external users.

identification and contact:

name, email address and, if the Customer or the person records it, telephone number

account:

role, membership, work team and account status in the laboratory

use of the service:

reservations, requests, approvals, usage times of each piece of equipment, notes the person writes and, on the Professional plan, the amounts calculated per use

The platform is not designed for sensitive personal data. The Customer undertakes not to record such data in free-text fields such as notes or descriptions.

3. Instructions and purpose

CellBlock processes the data only to provide the contracted service: granting access to the platform, operating reservations and approvals, generating the Customer's reports, sending the emails the service requires, providing support and maintaining security. Configuring the laboratory on the platform constitutes the Customer's instructions.

CellBlock does not process the data for any other purpose, does not sell it, does not use it for advertising or to profile anyone, and does not assume ownership of the information on which it provides the service. The only statistics CellBlock obtains are aggregate metrics on the operation of the platform (for example, availability or number of reservations per day), which do not identify any person or any laboratory.

If CellBlock decides on its own about the processing, against the Customer's instructions, it assumes the role of controller and the corresponding legal consequences.

4. Confidentiality

CellBlock keeps the personal data it processes confidential, even after the relationship ends. Only the owner of CellBlock and the members of her technical team who need it to provide the service have access to it, all bound by the same confidentiality. If the Customer requests it, each of them signs a confidentiality letter.

5. Security measures

CellBlock maintains administrative, technical and physical measures to protect the data against damage, loss, alteration, destruction, or unauthorized use, access or processing, including:

- the application and the database are hosted in Mexico, in the Querétaro region of Oracle Cloud Infrastructure, which encrypts storage volumes at rest
- all communication with the platform is encrypted in transit (HTTPS/TLS); the database does not accept connections from outside the server
- each laboratory is isolated: on every request the server verifies that the person belongs to the laboratory and has the required role
- passwords are stored with an irreversible hashing algorithm (bcrypt), sessions expire and failed sign-in attempts are limited
- administrative access to the server is by cryptographic key only and is limited to the owner and her technical team
- backups are taken before every change in production, and each backup is kept for a maximum of 12 months

The Customer may request a more detailed description of these measures at any time.

6. Subprocessing

To provide the service, CellBlock relies on the following providers, which process data on the Customer's behalf only to the extent their function requires:

PROVIDER	FUNCTION	DATA IT RECEIVES	WHERE
Oracle Cloud Infrastructure	hosting of the server and the database	all laboratory data, encrypted at rest	Mexico (Querétaro)
Resend	sending service emails	name, email and the content of the notice	United States
Google LLC	sign-in with Google, only if the person chooses to use it	name and email of whoever uses it	United States
Stripe, Inc.	card payments, only if the Customer pays that way	name and email of the payer	United States

By signing or accepting this Agreement, the Customer expressly authorizes these subprocessors, under article 55 of the LGPDPPSO. CellBlock only uses providers whose terms of service include data protection obligations equivalent to those in this Agreement.

Google only receives data from people who choose "Continue with Google": anyone can sign in with email and password. If the Customer pays by bank transfer, Stripe is not involved.

CellBlock will notify the Customer, by email to the contact the Customer designates, at least 30 calendar days in advance, before adding or replacing a provider that receives the Customer's data. If the Customer objects, it may terminate the service without penalty and CellBlock will refund the proportional part of what was paid for the period not provided.

7. Transfers

CellBlock does not transfer the Customer's data to third parties unless the Customer instructs it or a competent authority orders it through a substantiated and motivated request. In the latter case, CellBlock will inform the Customer before delivering the data, unless the law prohibits it.

8. Security breaches

If a security breach affects the Customer's data, CellBlock will inform the contact designated by the Customer, by email and by telephone, within a maximum of 72 hours after confirming it. The notice will state at least:

- | the nature of the incident and when it occurred
- | the personal data compromised and, if known, how many people are affected
- | the corrective actions CellBlock has already taken and those it will take
- | recommendations for the affected people
- | the means to obtain more information

CellBlock will cooperate with the Customer so that it can meet its own obligations to notify data subjects and the authority.

9. Data subjects' rights

If CellBlock receives a request for access, rectification, cancellation, opposition or portability concerning the Customer's data, it will forward it to the Customer within the following 5 business days and will not resolve it on its own. CellBlock will give the Customer the information and tools it needs to handle the request within the legal timeframes.

10. Changes to the service conditions

CellBlock will inform the Customer, by email to its designated contact and at least 30 calendar days in advance, of any change to its Privacy Notice, its Terms or this Agreement that affects the processing of the Customer's data. Publishing the change on the website does not replace that notice. While a signed contract is in force, no change reduces the agreed protections without the Customer's consent.

11. Verification

The Customer may request from CellBlock the information needed to verify compliance with this Agreement, and CellBlock will provide it within a reasonable time. On-site reviews or reviews by third parties are agreed in writing, with prior notice and without compromising the security or confidentiality of other customers.

12. Retention, return and deletion

During the contract, CellBlock keeps the data in accordance with the contracted plan and with section 11 of its Privacy Notice. The Customer can download all of its laboratory's data at any time.

When the relationship ends:

- the Customer has 30 calendar days to request an export of its data, which CellBlock delivers in a structured, commonly used format

- CellBlock deletes the data no later than 90 business days after termination, unless the Customer has contracted an extended retention in writing or a law requires keeping it

- if the Customer requests it, CellBlock delivers a signed deletion record stating the date and scope of the deletion

- deleted data may remain in backups until they expire, within a maximum of 12 months, without being used for any other purpose

13. Term

This Agreement applies for as long as CellBlock processes data on the Customer's behalf. The confidentiality and deletion obligations survive the end of the relationship.

14. Governing law and jurisdiction

This Agreement is governed by the laws of the United Mexican States. Disputes are resolved before the competent courts of Mexico City; if the Customer is a federal public entity or an autonomous body, before the federal courts seated in Mexico City.

15. Contact

personal data: privacy@cell-block.tech

breaches and support: support@cell-block.tech

owner: Arlen Ramírez Corona, trade name CellBlock, Mexico City, Mexico

Sincerely,

CellBlock Team

CellBlock · Arlen Ramírez Corona