

Data Processing Agreement

Template · Last updated: 2026-10-25 · Fields in [brackets] are completed for each customer before signature.

This agreement under Article 28 GDPR sets out how SYSTHEMA ANALYTICS S.R.L. processes personal data in the Luna360 platform on behalf of the Customer.

1. Parties and subject

Controller (the “Customer”): [legal name], registered office [address], registration number [number], represented by [name, role].

Processor (“Systema”): SYSTHEMA ANALYTICS S.R.L., registered office str. Dragoș Vodă nr. 2, bl. D5, et. 1, ap. 3, Deva, jud. Hunedoara, România, tax ID (CUI) 45945560, Trade Register J20/524/2022, email hello@systema.ro.

1.1. The Customer uses Luna360, a loan management platform provided by Systema as a hosted service, under the service agreement dated [date] (the “Main Agreement”). In doing so, Systema processes personal data on behalf of the Customer.

1.2. This Data Processing Agreement (“DPA”) governs that processing as required by Article 28 of Regulation (EU) 2016/679 (“GDPR”). The nature, purpose, data and data subjects are described in **Annex 1**.

1.3. The Customer is the controller: it decides which data it enters in Luna360, for which purposes and on which legal basis (for example credit assessment, anti-money-laundering checks and reporting to funders). Systema processes the data only to provide Luna360 to the Customer.

1.4. Terms such as “personal data”, “processing”, “data subject”, “personal data breach” and “sub-processor” have the meaning given in the GDPR. If this DPA and the Main Agreement conflict on data protection, this DPA prevails.

2. Obligations of the processor

2.1. **Instructions.** Systema processes personal data only on the Customer’s documented instructions. The Main Agreement, this DPA and the Customer’s use and configuration of Luna360 (for example the data it enters, the reminders it switches on, the exports it runs) are the Customer’s instructions. Systema informs the Customer without delay if it believes an instruction breaks the GDPR or other data protection law.

2.2. **Legal obligations.** If EU or Member State law requires Systema to process the data otherwise, Systema informs the Customer first, unless that law forbids it.

2.3. **Confidentiality.** Only persons who need access to provide, support or secure Luna360 may access the Customer’s data. They are bound by a contractual or statutory duty of confidentiality. Systema does not access the content of the Customer’s data except to provide support the Customer

asked for, to keep the service secure, or when the law requires it.

2.4. **No other use.** Systema does not use the Customer's data for its own purposes, does not sell it and does not combine it with data of other customers. Each customer's data is kept in its own database.

2.5. **Records.** Systema keeps a record of the processing it carries out on behalf of its customers (Article 30(2) GDPR).

3. Security of processing

3.1. Systema implements and maintains the technical and organisational measures in **Annex 2**, appropriate to the risk of the processing (Article 32 GDPR), taking into account that loan and KYC data are financial and identity data.

3.2. Systema may improve the measures over time, provided the overall level of protection does not decrease.

3.3. The Customer is responsible for the security of its own side: it manages its users, roles and permissions in Luna360, keeps its staff's credentials and two-factor devices safe, and removes access for people who leave.

4. Sub-processors

4.1. The Customer gives Systema a general authorisation to engage sub-processors. The sub-processors authorised on the date of signature are listed in **Annex 3**; in particular, Luna360 is hosted by **netcup GmbH** (Germany) in an EU data centre, and its web traffic passes through **Cloudflare, Inc.**

4.2. Systema informs the Customer by email at least **30 days** before it adds or replaces a sub-processor. The Customer may object on reasonable data protection grounds within that period. If the parties cannot agree on a solution, the Customer may terminate the affected part of the Main Agreement without penalty before the change takes effect.

4.3. Systema imposes on each sub-processor, by contract, data protection obligations that are at least as protective as this DPA, and remains liable to the Customer for the sub-processor's performance.

4.4. **Services the Customer connects itself** — for example its own email server or SMS provider (such as 46elks or Twilio), or later a BankID, credit bureau or e-signature provider — are engaged and contracted by the Customer. They are the Customer's own processors, not Systema's sub-processors; Luna360 only sends them the data the Customer's configuration requires.

5. Assistance to the Customer

5.1. **Data subject requests.** Luna360 lets the Customer handle most requests itself: view and correct a client's data, export all of a client's data (access and portability), and anonymise a client when the law allows deletion, with anti-money-laundering retention respected. Systema helps with requests the

tools do not cover. If a data subject contacts Systema directly, Systema forwards the request to the Customer without undue delay and does not answer it itself unless instructed.

5.2. **Other assistance.** Taking into account the information available to it, Systema assists the Customer with data protection impact assessments, prior consultations with the supervisory authority and its security obligations (Articles 32–36 GDPR). Assistance beyond the normal service may be charged at the rates in the Main Agreement, except where it results from Systema’s own breach.

6. Personal data breaches

6.1. Systema notifies the Customer **without undue delay and in any case within 48 hours** after becoming aware of a personal data breach affecting the Customer’s data, so that the Customer can meet its own 72-hour deadline (Article 33 GDPR).

6.2. The notice describes, as far as then known: what happened and when; the categories and approximate number of data subjects and records concerned; the likely consequences; the measures taken or proposed; and a contact person. Information not yet known is provided as soon as it is.

6.3. Systema takes the measures needed to contain the breach and limit its effects, documents the breach, and cooperates with the Customer’s investigation and any notice to data subjects. The Customer decides whether to notify the authority and the data subjects.

7. Transfers outside the EEA

7.1. The Customer’s data is stored in the European Union. Systema does not transfer it to a country outside the European Economic Area unless the transfer meets Chapter V of the GDPR.

7.2. Cloudflare, Inc. may process web traffic (including IP addresses and the content of requests passing through its network) outside the EEA. Such transfers are covered by the EU-US Data Privacy Framework and the European Commission’s Standard Contractual Clauses incorporated in Cloudflare’s data processing addendum.

8. Audits

8.1. Systema makes available to the Customer the information needed to demonstrate compliance with this DPA, including on request a written description of its current security measures and sub-processors.

8.2. The Customer, or an independent auditor bound by confidentiality that it appoints, may audit Systema’s compliance once a year, or after a personal data breach, with at least **30 days’** written notice, during business hours and without disproportionate disruption. Audits of a sub-processor rely on that sub-processor’s own certifications and reports. Each party bears its own audit costs.

8.3. Requests from a supervisory authority are handled in the same cooperative way.

9. Return and deletion

9.1. During the Main Agreement the Customer can export its data from Luna360 at any time (client data export, loan and report exports in Excel/CSV).

9.2. When the Main Agreement ends, Systhema provides, on request made within **30 days**, a complete export of the Customer's database in a common machine-readable format. It then deletes the Customer's database, files and database user within **30 days** after the end of the Main Agreement, and confirms the deletion in writing.

9.3. Encrypted backup copies are overwritten within a further **30 days** at the latest. Systhema keeps data longer only where EU or Member State law requires it, and protects it for as long as it does.

10. Term and liability

10.1. This DPA applies for as long as Systhema processes personal data on behalf of the Customer, and ends with the Main Agreement, except for the obligations in section 9 and any obligation that by its nature continues.

10.2. Each party is liable for its own breach of this DPA and of the GDPR under Article 82 GDPR. Limits of liability agreed in the Main Agreement apply to this DPA, except where mandatory law does not allow them.

11. Governing law and signatures

11.1. This DPA is governed by [Romanian] law. Disputes are settled by the courts competent under the Main Agreement. [For a customer in another Member State, the parties may agree on that Member State's law.]

11.2. Changes to this DPA are made in writing. If a provision becomes invalid, the rest remains in force and the parties replace it with a valid provision that comes as close as possible to its purpose.

	Customer (controller)	Systhema (processor)
Name	[name]	[name]
Role	[role]	[role]
Date	[date]	[date]
Signature		

Annex 1 — Description of the processing

Subject matter	Hosting and operation of Luna360, a loan management platform, for the Customer's lending activity
----------------	---

Nature of processing	Storage, organisation, retrieval, calculation (schedules, interest, reports), transmission (reminders, exports at the Customer's request), anonymisation, backup and deletion
Purpose	Providing Luna360 to the Customer under the Main Agreement; support, security and backups of the service
Duration	The term of the Main Agreement, plus the return and deletion periods in section 9

Categories of data subjects

- Applicants, borrowers and leads (people and representatives of businesses)
- Guarantors, beneficial owners, directors and other persons related to a client
- Contact persons of partner organisations
- The Customer's staff who use Luna360 (users)
- Visitors who send a loan enquiry through the Customer's online form

Categories of personal data (as entered by the Customer)

- Identification: name, personal identity number (e.g. personnummer, CNP), date of birth, organisation number, legal form
- Contact: address, email, phone, language
- KYC and AML: identity verification, PEP and sanctions checks, source of funds, purpose of the relationship, AML risk level, related documents
- Financial: requested and granted amounts, repayment schedules, payments, arrears, late interest, loan changes, revenue, costs and debts from the credit assessment, guarantees and collateral
- Impact and background fields the Customer chooses to collect (for example gender, country of birth, years in the country, situation before the loan, jobs created)
- Mentoring and support sessions, notes, tasks and uploaded documents
- Messages sent to borrowers (email and SMS content, delivery status)
- Users' account data and the audit log (actions, time, IP address, browser)

Special categories. Luna360 is not designed for special categories of data (Article 9 GDPR) or data on criminal convictions (Article 10). The Customer does not enter such data unless it has a legal basis, and then marks the custom fields concerned as sensitive.

Annex 2 — Technical and organisational measures

Area	Measures in place
Separation of customers	Each customer has its own database and its own database user, which can reach only that database. Uploaded files are stored per customer, outside the public web folder.

Area	Measures in place
Access control	Personal accounts only; passwords of at least 12 characters with upper and lower case and a digit; mandatory two-factor authentication for every user; temporary passwords must be changed at first login; sessions end after 120 minutes of inactivity; login attempts are rate-limited.
Permissions	Role-based permissions (six default roles, editable by the Customer). Nobody can grant rights they do not hold themselves. Case officers cannot vote on or decide their own applications.
Sensitive data	Personal identity numbers are masked by default; revealing them requires a separate permission and is logged. Custom fields can be marked sensitive and are then left out of exports.
Audit trail	An append-only audit log records changes, logins, failed logins, exports, document downloads and views of sensitive data, with user, time and IP address. It cannot be edited from the application.
Encryption	All traffic over HTTPS (TLS). Secrets such as mail and SMS passwords and two-factor keys are stored encrypted. Backups are encrypted with AES-256.
Availability and backups	Encrypted backup of every database and file store every night; an automatic restore test every week; backups kept 30 days. A second, off-site copy is stored every night with DIGI Romania S.A. (Digi Storage), encrypted a second time before it leaves the server.
Application security	Protection against cross-site request forgery; input validation; spam protection on public forms (hidden field, minimum fill time, rate limit); exports protected against spreadsheet formula injection; an automated test suite (over 170 tests, including access control and data separation) run on changes to the platform.
Data minimisation and deletion	Built-in data export per client; anonymisation of clients with anti-money-laundering retention respected; reports for funders contain no names or identity numbers and hide groups smaller than 3; leads without activity can be anonymised after a period the Customer sets.
Organisation	Access to production limited to named Systema staff bound by confidentiality; changes to the platform are versioned; incidents are handled under section 6 of this DPA.
Network	The service is reachable only through Cloudflare (protection against attacks and abuse) and a firewall on the server.

Annex 3 — Authorised sub-processors

Sub-processor	Service	Data concerned	Location	Transfer safeguard
netcup GmbH, Daimlerstraße 25, 76185 Karlsruhe, Germany (HRB 705547, Mannheim local court)	Server hosting for the Luna360 application, databases, files and backups	All Customer data	Data centre in Nuremberg, Germany	Not needed (EU)

Sub-processor	Service	Data concerned	Location	Transfer safeguard
Cloudflare, Inc., 101 Townsend St, San Francisco, CA 94107, USA	Network security, protection against attacks, TLS and delivery of web traffic	Data in transit: IP addresses, request data, pages viewed	Global network, including the EU and the USA	EU-US Data Privacy Framework and Standard Contractual Clauses
DIGI Romania S.A., Bucharest, Romania (Digi Storage service)	Off-site storage of backup copies	Backups of all Customer data, encrypted (AES-256, then a second encryption) before transfer — the provider cannot read them	EU [data centre location to be confirmed]	Not needed (EU)