Privacy policy

Effective October 20, 2026

Armand OCTEAU, entrepreneur individuel, registered under SIREN number 999229016, whose business address is located at 30 bis boulevard Littré, 78600 Le Mesnil-le-Roi, France and Sarah LÉVY, entrepreneur individuel, registered under SIREN number 999229008, whose business address is located at 24 avenue du Ponant, 92390 Villeneuve-la-Garenne, France

Only the French version is binding.

CONTENTS

Article 1. Data controller 1
Article 2. The Solyzon websites 1
2.1 Visiting the websites 1
2.2 Contact form 1
2.3 Job application 1
2.4 Student offer request 1
2.5 Vulnerability report 2
2.6 Spam protection of the forms 2
2.7 Newsletter 2
2.8 Sol, the websites' assistant 2
2.9 Audience measurement 2
Article 3. The account's data 2
3.1 Identity and email addresses 2
3.2 Date of birth 3
3.3 Postal address, optional 3
3.4 Phone number, optional 3
3.5 Picture 3
3.6 Sign-in methods 3
3.7 Devices and sessions 3
3.8 Security log 3
3.9 Proof of acceptance of the terms 4
3.10 Organisations 4
3.11 Emails sent by the publisher 4
3.12 Data that the publisher does not request 4
Article 4. Cookies and browser storage 4
4.1 On the websites 4
4.2 On the account 4
Article 5. Typing the postal address 5
Article 6. Legal bases 5
Article 7. Who receives the data 5
7.1 The applications the person signs in to 5
7.2 Organisations 5
7.3 The Solyzon team 5
7.4 Service providers 6
7.5 Transfers outside the European Union 6
Article 8. Retention periods 6
Article 9. Hosting and security 7
Article 10. The person's rights 7
Article 11. Changes to the policy 7

ARTICLE 1. DATA CONTROLLER

The purpose of this policy is to specify which personal data the Solyzon websites and the Solyzon account process, the purposes of such processing, its duration and the recipients of the data. The websites are solyzon.com and the Solyzon websites published under this domain name, listed in the legal notice. As regards the account, it supplements the account terms of use.

The websites and the account are published by Armand OCTEAU, sole proprietor, SIREN 999 229 016, whose business address is 30 bis boulevard Littré, 78600 Le Mesnil-le-Roi, France and Sarah LÉVY, sole proprietor, SIREN 999 229 008, whose business address is 24 avenue du Ponant, 92390 Villeneuve-la-Garenne, France. These sole proprietors operate together under the trade name Solyzon and are responsible for the processing described below.

Where an account is created and managed by an organisation, the organisation determines how its members' accounts are used and is the controller of that processing. The publisher then acts on its behalf as a processor, within the meaning of article 28 of the General Data Protection Regulation, and processes this data solely in order to provide the account, in accordance with its instructions. The publisher remains responsible for the security of the account and of the security log.

For any question concerning their data or in order to exercise their rights, the data subject is invited to write to contact@solyzon.com.

ARTICLE 2. THE SOLYZON WEBSITES

2.1 Visiting the websites

Mere consultation of the websites does not require any data to be provided. The entry server nevertheless records the full IP address, the requested page, the time and the browser in its technical log, for the purpose of diagnosing an outage or an attack. The country of the connection, inferred from the IP address by the network that protects the websites, is used solely to offer the language, currency and offers available in that country, and is not recorded.

2.2 Contact form

The contact form collects the name, email address, message and, at the person's discretion, their telephone number and details relating to their request. This data is used to reply to the person. The message is transmitted by email to the Solyzon team from Solyzon's servers.

2.3 Job application

The application form collects the name, email address, profile, field, an optional link, a message and a CV. This data is used to review the application and to reply to the person. The CV is stored in a Solyzon storage space to which only the team has access, after identification, and the email sent to the team contains only the link to it.

2.4 Student offer request

The student offer request collects the first name, last name, school email address, institution, programme, chosen products, proof of enrolment and, for the future entrepreneur pack, the website address and the company's SIREN number. This data is used to verify that the person is eligible for the offer and to grant it. The SIREN number is verified in the French government's public company directory, and the website address is consulted by Solyzon's servers in order to verify that it is online. During data entry, the name of the institution and of the programme

is transmitted to the public higher education database of the French ministry responsible for higher education, in order to suggest institutions and programmes, without any information identifying the person.

2.5 Vulnerability report

The vulnerability report form collects a description of the vulnerability and, at the person's discretion, their email address, in order to keep them informed and to thank them.

2.6 Spam protection of the forms

Each form is analysed by Herse, Solyzon's spam filter, which runs on Solyzon's servers. Herse receives the content of the form, its attachments, the IP address, the browser and the time spent filling it in, and returns a verdict. Where a message is classified as spam, its text may be retained in order to improve the filter, with the exception of vulnerability reports. In order to limit abuse, the IP address and the email address are also used to count submissions, in the servers' working memory, for one hour at most.

2.7 Newsletter

Subscribing to the newsletter requires the email address. It is used to send news about Solyzon and its products. Each newsletter contains an unsubscribe link that terminates the subscription in one click.

2.8 Sol, the websites' assistant

Sol is an artificial intelligence that answers questions about the products, the services and the company, on the basis of the content of the websites. Its answers may contain mistakes, and only the pages of the websites, Solyzon's quotes and Solyzon's terms bind Solyzon. Sol receives the question entered, the page on which it is asked and the language, on Solyzon's servers. The answer is generated by a language model that runs on Solyzon's servers. The exchanges, questions and answers, are retained on Solyzon's servers in order to improve Sol's answers, without the person's name or IP address, and any email address, telephone number, IBAN or card number appearing in a question is masked before it is stored. In order to limit abuse, the IP address is also used to count the day's questions, in the servers' working memory. The conversation is also retained in the browser until it is closed. The person is not required to provide their name or email address, and is advised not to enter personal information in a question.

2.9 Audience measurement

With the person's consent, given in the cookie panel, the websites measure their audience by means of Google Analytics: pages viewed, visit duration, source, device and country. The IP address is anonymised before being recorded, and the measurement is never used for advertising. In the absence of consent, no measurement tool is loaded.

ARTICLE 3. THE ACCOUNT'S DATA

3.1 Identity and email addresses

The publisher processes the person's first name, last name, email address, language and time zone. An account may have several addresses, including a primary one and a recovery one, each verified by a code. This data is used to create the account, to recognise the person, to send them verification codes and security alerts, and to present screens in their language.

3.2 Date of birth

The date of birth is mandatory at open sign-up, firstly because the publisher refuses persons under 15, the minimum age for the account, and secondly because it is required for certain services. It is optional for an account created by an organisation. An application receives it only where the person authorises it separately.

3.3 Postal address, optional

At sign-up, the person may give their postal address. It is optional, it pre-fills the person's invoices and it is erased together with the account.

3.4 Phone number, optional

The telephone number is not requested at sign-up: the person may add it in their account settings in order to receive reminders. It is never used as a sign-in or recovery method, the publisher not using text messages for that purpose. An application receives it only where the person authorises it separately.

3.5 Picture

The person may choose a picture. Failing that, the account receives a default avatar, a face of Sol, which is identical for every account that has it and therefore identifies no one. An application never receives another application's picture address: each receives an address of its own.

3.6 Sign-in methods

The publisher processes the sign-in methods that the person registers: the public key of their passkeys with the name the person gives them, their password in a hashed form that cannot be read back, the secret of their authenticator app, encrypted, and their backup codes, hashed. When the person chooses a password, and if needed at their next sign-in, the publisher checks whether it appears in a known data breach, by sending to the Have I Been Pwned service only the beginning of its fingerprint, which does not allow either the password or the person to be identified.

3.7 Devices and sessions

In order to recognise a device already used and to warn the person of an unusual sign-in, the publisher records, for each device, the browser used, a prefix of the IP address, which keeps only part of it, an approximate place, deduced from a geolocation database hosted by the publisher itself and not from an external service, and the date of the first and the last sign-in. The publisher also records each open session, with its start, its last activity and its end. A device that has not been used for any sign-in for four hundred days is erased, together with its ended sessions.

In order to limit abuse, in particular a series of passwords tried at random, the full IP address is used to count attempts, in the servers' working memory, for one hour at most, after which it is erased. The entry server, which receives each request before the account, also records the full IP address, the page requested and the time in its technical log, for the purpose of diagnosing an outage or an attack.

3.8 Security log

The security log records the operations carried out on an account, their date and the device used, for example a sign-in, the addition of a sign-in method or a change of address. It retains a prefix of the IP address and the browser used, and the detail of each line contains only

identifiers and field names, never content. It serves to protect the account, to investigate an incident and to reply to a person who disputes an operation. The person may also consult it in their account settings.

3.9 Proof of acceptance of the terms

At sign-up, then at each new version, the publisher retains the version of the terms of use and of the privacy policy that the person accepted, with the date of acceptance. This proof enables the publisher to establish what the person accepted in the event of a dispute.

3.10 Organisations

Where an account belongs to an organisation, the publisher retains the person's role in the organisation and the address with which the person joined it. The organisation's applications receive that address, which prevents an employer from receiving the person's personal address.

3.11 Emails sent by the publisher

The publisher sends the emails necessary for the account: verification codes, invitations, new sign-in alerts, security changes, address changes and account recovery. Security emails cannot be turned off. The person configures informational emails, such as product news, in their preferences, and an unsubscribe link terminates them in one click.

3.12 Data that the publisher does not request

The publisher never asks for the person's gender.

ARTICLE 4. COOKIES AND BROWSER STORAGE

4.1 On the websites

The websites retain the following information in the browser:

- `solyzon_consent`, the choice made in the cookie panel, for one hundred and eighty-two days, after which the panel asks the question again;
- `solyzon-currency`, the currency chosen to display prices, until the person clears it;
- the conversation with Sol and the position in a list, in order to return to it, until the browser is closed.

This information does not leave the browser and does not require consent, since it serves solely for the operation of the websites.

Only with the person's consent does Google Analytics set the `_ga` and `_ga_03CE6BP9C7` cookies, for thirteen months. The person may change their choice at any time through the "Cookies" link at the bottom of each page: a refusal deletes these cookies.

In order to distinguish a person from a robot, the Sol assistant and the newsletter subscription use Cloudflare Turnstile, which analyses the browser without setting a tracking cookie.

The Grammage badge, at the bottom of the pages, is loaded from getgrammage.com, another Solyzon website, without any cookie being set.

4.2 On the account

The account sets the following cookies on accounts.solyzon.com. They serve to operate sign-in, to secure it and to remember the chosen language, and have no advertising or audience-measurement purpose.

- `__Host-sz_op_session`, the account session, which avoids signing in again for each application, fourteen days without activity and ninety days at most.

- `__Host-sz_device`, the device cookie, which designates the device in the records described above and makes it possible to keep several accounts open in the same browser and to recognise a new device, four hundred days.
- `accounts_lang`, which remembers the language chosen in the language selector, one year.
- `__Secure-sz_interaction` and `__Secure-sz_interaction_resume`, which track a sign-in in progress, fifteen minutes at most.

The session and the two cookies of the sign-in in progress each come with a cookie of the same name followed by `.sig`, which carries its signature and prevents any forgery. Each application the person signs in to then sets its own session cookies on its own domain.

ARTICLE 5. TYPING THE POSTAL ADDRESS

During entry of the postal address at sign-up, the text entered is transmitted, in order to suggest addresses, to the IGN (Géoplateforme) for France and its overseas territories, and to komoot (Photon service) for other countries, by Solyzon's servers, without any information identifying the person.

ARTICLE 6. LEGAL BASES

On the websites, answering a contact message, reviewing an application, examining a student offer request and following up a vulnerability report fall under measures taken at the request of the person. Protecting the forms against spam, the technical log and Sol's answers fall under Solyzon's legitimate interest in protecting its websites and informing its visitors. The newsletter and audience measurement fall under consent, which the person may withdraw at any time.

For the account, the processing of identity data, sign-in methods, sessions and the postal address falls under the performance of the requested service, namely the provision of the account. The security log, device checks and abuse limiting fall under the publisher's legitimate interest in protecting the account and the service. The proof of acceptance of the terms falls under the publisher's legitimate interest in being able to establish what was accepted. Sending optional information falls under consent, which the person may withdraw at any time.

ARTICLE 7. WHO RECEIVES THE DATA

7.1 The applications the person signs in to

A Solyzon application receives the account information that it needs. An application external to Solyzon receives only what the person accepts on the consent page, with an identifier of its own, and the person may withdraw that access at any time in their account settings. Each application retains its own data in its own database, linked to the account by an identifier only, and an external application processes what it has received in accordance with its own privacy policy.

7.2 Organisations

An organisation's administrator sees the managed accounts of their organisation and its members, and may suspend them and reset their sign-in methods. A managed account displays the words "managed by" followed by the name of the organisation.

7.3 The Solyzon team

By default, the Solyzon team sees only the information that support requires: the state of the account, its sign-in methods without their secrets, its sessions, its licences and its invoices. It

never sees the content of applications. To consult content or act on the person's behalf, a team member submits a reasoned request, which the person accepts in their account settings for a limited period and for a single product. Each access is recorded in a log, which the person may consult in the "Solyzon access" section of their account. A court order or a security incident may justify access without agreement, which then requires the approval of two team members, and the person is informed afterwards, unless the law prohibits it.

7.4 Service providers

The publisher relies on a limited number of service providers and sends the websites' and the account's emails itself from its own servers. The network of Cloudflare, Inc. protects access to the websites and the account against attacks: the exchanges between the browser and Solyzon's servers pass through it, IP address included, and Cloudflare Turnstile distinguishes people from robots on the Sol assistant and the newsletter subscription. Google Ireland Limited receives the audience measurement data described in article 2.9, with the person's consent. The French government's public company directory receives the SIREN number of a student offer request. The IGN, in France, and komoot GmbH, in Germany, receive the address entry texts described in article 5. Have I Been Pwned receives only the beginning of the fingerprint described above, which does not constitute personal data.

7.5 Transfers outside the European Union

Cloudflare, Inc. is established in the United States, and Google Ireland Limited may have the audience measurement data processed by Google LLC, in the United States. These companies are certified under the EU-U.S. Data Privacy Framework, which the European Commission has recognised as ensuring an adequate level of protection, and are also bound by the Commission's standard contractual clauses. No other data of the websites or the account leaves the European Union.

The publisher sells no data and does not use it for advertising purposes.

ARTICLE 8. RETENTION PERIODS

On the websites:

- a contact message, three years after the last exchange with the person;
- an application, two years after the last exchange, unless the person requests earlier erasure, and the CV stored in the storage space, fourteen days, the team retaining it thereafter with the application;
- a student offer request, for the duration of the offer, then one year, and the proof of enrolment stored in the storage space, fourteen days;
- a vulnerability report, three years after it is closed;
- the newsletter email address, until unsubscription;
- the entry server's technical log, thirty days;
- audience measurement data, fourteen months;
- the exchanges with Sol, six months, and the IP address used to count the day's questions, two days at most.

For the account:

- The security log, one year.
- The proof of acceptance of the terms, five years after the account ends.
- A session, fourteen days without activity, and ninety days at most.
- A device, four hundred days after its last sign-in.

- The full IP address used to limit abuse, one hour at most.
- The entry server's technical log, thirty days.
- Invoices, ten years, in accordance with article L. 123-22 of the French Commercial Code, including after the account is deleted.
- A deleted account, thirty days during which it is suspended and can be restored, then it is deleted. Its data remains thereafter in backups, which retain six months of history at most, and then disappears.
- Other data, for as long as the account exists. The postal address, date of birth, telephone number and picture are erased together with the account, subject to the foregoing.

ARTICLE 9. HOSTING AND SECURITY

The data of the websites and of the account is hosted by Solyzon, on its own servers, in France. Passwords are hashed, the secrets of authenticator apps are encrypted, and the security log cannot be altered after the fact: only new lines may be added to it.

ARTICLE 10. THE PERSON'S RIGHTS

The rights of individuals are detailed on the GDPR page of solyzon.com. The person has a right of access, rectification, erasure, restriction, objection and portability over their data. The person may export their data, delete their account and correct their profile from the "Data and privacy" section and the other sections of their settings, and may also exercise their rights by writing to contact@solyzon.com. The publisher replies within one month. If the person considers that their rights are not respected, they may lodge a complaint with the Commission nationale de l'informatique et des libertés (CNIL).

ARTICLE 11. CHANGES TO THE POLICY

The publisher may change this policy, in particular to follow a change in the websites, the account or the law. The version in force is the one published on solyzon.com with its date, and an older version remains available on simple request.



SOLYZON
Armand OCTEAU, EI, SIREN 999 229 016
Sarah LÉVY, EI, SIREN 999 229 008
Marque déposée à l'INPI, n° 5215907, classe 42
https://solyzon.com