Privacy Policy for the Platform and Dashboard

This notice explains which data we process when you visit soulsystem.app, request a demo call, purchase a subscription as a partner and use the dashboard at partner.soulsystem.app. If you buy a reading on a partner's page, the “Privacy Policy for Partner Pages” applies to that purchase.

1. The controller

The controller responsible for processing your data is:

Divinebeingmetatron Ltd.
Mesopotamias 8
7041 Oroklini, Larnaka
Cyprus
Telephone: +357 99 729287
Email: kontakt@soulsystem.app
Email for privacy enquiries: privacy@soulsystem.app

“We” in this notice always means this company. You can send any questions about your data to the privacy enquiries address.

2. Key points

- We process your data to display the website, respond to your demo enquiry, manage your subscription, operate your dashboard and pay your remuneration.
- You enter payment details directly with Stripe. We do not store card numbers. We only store bank account details if we pay you manually: in a country without Stripe Connect, or if you expressly ask us to pay you by bank transfer (section 9).
- We only measure our advertising on Meta if you allow “Marketing” in the banner on soulsystem.app. Your browser loads nothing from Meta for this; we report from our server, including from the checkout (sections 3.2 and 4). There are no advertising pixels or audience measurement services from third parties in the dashboard.
- We do not sell your data.
- You can request access, rectification, erasure and an export of your data, and unsubscribe from promotional emails at any time (sections 11 and 20).

3. Visiting soulsystem.app

3.1 Opening the page

When you open soulsystem.app, your browser sends technical information to our hosting provider Vercel: your IP address, the date and time, the page requested, the page you came from, and information about your browser and device. Vercel processes this information on our behalf to deliver the page and defend against attacks.

The legal basis is our legitimate interest in a secure and accessible website (Article 6(1)(f) GDPR).

3.2 Banner and storage in your browser

On soulsystem.app, we show you a banner. There you choose which services you allow. The banner remembers your choice in your browser. You can change it at any time.

The banner comes from Cookiebot, a service of Usercentrics A/S (Havnegade 39, 1058 Copenhagen, Denmark). Your browser loads it from Cookiebot's servers in the EU. In the process, Cookiebot receives your

IP address and derives your country from it so that the right banner appears. The legal basis for loading the banner is our legitimate interest in showing you the banner reliably and in the form that fits your country (Article 6(1)(f) GDPR). Cookiebot stores your choice in the "CookieConsent" cookie in your browser, together with a random key without any details about you. Your choice is valid for up to 12 months; after that, the banner asks you again. You can change it at any time using the "Cookie settings" link in the footer of soulsystem.app.

As proof of your choice, Cookiebot records the following on servers in Ireland, in an emergency in a fallback data centre in the Netherlands: your IP address in shortened form, the date and time, information about your browser, the address of the page on which you made your choice, the random key and your choice. Cookiebot deletes this record after 12 months. Cookiebot processes this data on our behalf. The legal basis is our obligation to obtain consent and to be able to demonstrate it (Article 6(1)(c) GDPR in conjunction with Article 7(1) GDPR and section 25(1) TDDDG).

On soulsystem.app, we also store in your browser the access cookie that opens the restricted pages before launch once you enter the access code.

Without your consent, we only store in your browser what is strictly necessary for the page to work in the way you are currently using it (section 25(2), no. 2 TDDDG). Section 16 lists the individual items.

Services that are not strictly necessary for this only start once you agree in the banner (section 25(1) TDDDG, Article 6(1)(a) GDPR). You can withdraw your consent at any time using the "Cookie settings" link. The withdrawal is effective from the moment you declare it. Processing carried out before then remains lawful.

With your consent, we use these services:

Service	Provider	Purpose	Duration
Google Analytics	Google Ireland Limited, Ireland	measures how visitors use soulsystem.app	cookies up to 2 years, measurement data at Google 2 months (section 19)
Meta, under "Marketing" in the banner	Meta Platforms Ireland Limited, Ireland	shows us which ads on Meta lead to subscription signups and helps Meta show our ads to suitable people	"ss-meta" cookie 90 days (section 16); identifiers from the checkout with us until the first payment has been reported, at the latest until the subscription ends or you switch the reports off (section 19)

Google Analytics only loads once you agree to it in the banner. If you decline, it does not load. After you agree, Google receives your IP address, identifiers from the cookies and information about your browser and device. The Google Analytics cookies apply only to soulsystem.app itself, not to other addresses under soulsystem.app such as partner.soulsystem.app. Google processes this data on our behalf, including in the USA (section 18).

Advertising on Meta: We advertise soulsystem.app on Meta (Facebook, Instagram). So that we can see which ads lead to subscription signups, and so that Meta can show our ads to people who are interested in them, we report individual steps to Meta. This only happens if you allow "Marketing" in the banner. If you decline or do not respond, the page loads nothing from Meta, we set no cookie for this purpose and we send nothing to Meta.

If you allow "Marketing", the following applies:

- Your browser loads nothing from Meta. A small script of our own sets the "ss-meta" cookie on soulsystem.app with a random identifier for your browser and, if you came through an ad on Meta, the identifier of that ad (section 16).
- When you open a page of soulsystem.app, your browser reports this to our own address partner.soulsystem.app. From there, our server sends it to Meta (Conversions API); on the pricing page, as a view of the prices. This includes which step it was, the address of the page without any additions,

the two identifiers from the cookie, an identifier of the report, information about your browser and device, and your IP address.

- When you click a link on soulsystem.app to the checkout at partner.soulsystem.app, we add your consent, the two identifiers and the time of the click to the link only at that moment. The checkout accepts your consent only up to 30 minutes after the click and immediately removes this information from the address bar before Stripe's payment form loads. If you copy a link from soulsystem.app or the address of the checkout, it does not contain your consent. This way the checkout knows about your consent without its own banner and without a cookie. Section 4 explains what the checkout then reports to Meta.
- What you enter in forms, such as your name, address or tax number at checkout, and your payment details are never sent to Meta. Your email address is only sent to Meta as a hash value (SHA-256), and only from the checkout (section 4).
- We and Meta Platforms Ireland Limited are joint controllers for collecting this information and transmitting it to Meta (Article 26 GDPR). Meta's Controller Addendum (https://www.facebook.com/legal/controller_addendum) applies to this. In essence: we inform you here and obtain your consent. Meta is responsible for your rights of access, rectification, erasure, restriction and data portability regarding the information Meta stores after the transmission (Articles 15 to 20 GDPR); you can contact Meta directly for this, and if you write to us, we will forward your request to Meta. You can exercise your rights against us and against Meta. Meta is responsible for what it then does with the information, for example for reporting on our advertising and for delivering ads: Meta's Privacy Policy (https://www.facebook.com/privacy/policy). Meta also processes the information in the USA (section 18).
- The legal basis is your consent (Article 6(1)(a) GDPR; for the cookie and reading information from your browser, section 25(1) TDDDG). You can withdraw it at any time using the “Cookie settings” link in the footer of soulsystem.app. From then on, we delete the “ss-meta” cookie, add nothing more to links to the checkout and report nothing more from soulsystem.app to Meta. If you opened the checkout with your consent, you can switch off the reports for your subscription in the dashboard under “Settings” > “Subscription and billing” with a single click (section 4) or by writing to the privacy enquiries address (section 1). Anything transmitted before then remains lawful.

3.3 Fonts and scripts

We deliver fonts and scripts ourselves: like the pages of soulsystem.app, they come through our hosting provider Vercel (section 3.1). Your browser does not request them from any third-party servers. The exceptions are the banner and Google Analytics from 3.2; Google Analytics only runs with your consent. We also deliver the script for our advertising on Meta (section 3.2) ourselves. It loads nothing from Meta and only sends data to our own address partner.soulsystem.app, and only with your consent.

3.4 Videos

On soulsystem.app, we show an explainer video. We deliver the video and its preview image ourselves, like the pages, through our hosting provider Vercel (section 3.1), without a third-party video service. The video only loads when you play it.

3.5 Demo call

You request a demo call by sending us a message; section 3.6 applies.

3.6 Messages to us

If you send us an email or use the contact page, we process your message, email address and name to respond. The legal basis is taking steps prior to entering into or performing a contract (Article 6(1)(b) GDPR), or otherwise our legitimate interest in answering enquiries (Article 6(1)(f) GDPR).

4. Purchasing a subscription

You purchase your subscription through the checkout at partner.soulsystem.app. We process:

- your country, email address, name and business address with street address, postcode and town,
- the company name if you subscribe as a company, and your VAT identification number if you provide it,
- your confirmation that you are entering into the subscription for your trade, business or self-employed professional activity, with its wording and time,
- the selected plan and term,
- your browser's language and time zone,
- the referral code if you come through a partner's referral,
- your acceptance of the terms, including their version, wording, language and the time of acceptance.

If you subscribed earlier through the old checkout with "Private person", we continue to store that choice, the postcode we passed to Stripe and your declaration requesting immediate commencement, including its time (section 19).

Payment is handled by Stripe. We ask for your country, email address, name, business address and, if you provide them, your company name and VAT identification number at the checkout on our page and pass them on to Stripe for the subscription, invoice and tax. You enter your payment details directly with Stripe. We do not see or store card numbers. Stripe provides us with the identifiers and status of the payment and subscription, and the details needed for your invoice. Your country determines the currency. Stripe calculates tax for us. In countries with Stripe Connect, we pass a VAT identification number you provide to Stripe as a tax ID; Stripe checks its format and, in the European Union and the United Kingdom, also checks it against the authorities' database. In all other countries, Stripe receives it only as a note; Stripe does not check it there, and it does not appear on your invoice.

There is only one free period per card or other payment method, across all partner accounts. For this purpose, after signup we store an identifier of your payment method and compare it with earlier signups of all partner accounts: for a card (including via Apple Pay or Google Pay) and for a bank account, the fingerprint generated by Stripe; for PayPal, the identifier of your PayPal account; and for Link, a code of your email address at Link that cannot be reversed without our secret key. We use the same comparison to check that no one refers themselves (section 12).

If no subscription is created after checkout, for example because the country of your billing address is not the country you selected at checkout, the checkout tells you so. We do not send you an email about it.

The legal basis is our contract with you (Article 6(1)(b) GDPR). We retain invoices and payment data because tax laws require us to do so (Article 6(1)(c) GDPR).

Checkout protection: When you open the checkout, when you change the plan or country and when you click “Start for free”, our hosting provider Vercel's bot protection checks whether a human is placing the order. It reads technical characteristics of your browser, and your IP address and request headers are sent to Vercel. Payment data and form fields are not sent to Vercel in this process. If the protection classifies a request as automated, no checkout opens or your order is not sent. Please contact us in that case. We also count attempts per IP address and per email address. We never store the address itself for this purpose, only a code that cannot be reversed without our secret key. From the old checkout, we also keep the counters of the emails we sent when no subscription was created, per address and per domain, again only as codes.

The legal basis for this protection is our legitimate interest in protecting the checkout and all partners against abuse (Article 6(1)(f) GDPR). Access to your device is strictly necessary for this purpose (section 25(2), no. 2 TDDDG).

Advertising on Meta: If you come from soulsystem.app and allowed “Marketing” in the banner there (section 3.2), the link to the checkout carries your consent and the two identifiers from the “ss-meta” cookie; the

checkout accepts them only up to 30 minutes after your click (section 3.2). Only then does our server report to Meta (Conversions API): when you click “Start for free” in the checkout, when your subscription is concluded and when the first payment for your subscription is received, even if it is due straight away at signup. Each report includes which step it was, the address of the checkout without any additions, an identifier of the transaction, the two identifiers from the link and your email address, only as a hash value (SHA-256), so that Meta can match the step to your Meta account if you have one. When you click “Start for free”, your IP address, information about your browser and device, the selected plan and the term are also sent; at signup, information about your browser and device and the amount of the signup (€0 during the free period) with its currency; with the first payment, the amount and currency.

So that we can report the signup and the first payment, we store the two identifiers and shortened information about your browser and device with us, first with the checkout session and, after signup, with your subscription. We do not pass them to Stripe, not even via the address of the page (section 3.2). If no subscription is concluded, we delete them after two days at the latest. Otherwise we delete them as soon as we have reported the first payment, at the latest when your subscription ends or you switch the reports off. On your subscription, we also record your consent with the time of your click, whether you have switched the reports off and when we reported the signup and the first payment, so that we can demonstrate your consent and nothing is sent to Meta twice. The legal basis for this record is our obligation to be able to demonstrate your consent (Article 6(1)(c) GDPR in conjunction with Article 7(1) GDPR). In the dashboard under “Settings” > “Subscription and billing”, you can see whether the reports are on and switch them off with a single click; after that, the checkout reports nothing more to Meta about your subscription. Without your consent on soulsystem.app shortly before you open the checkout, the checkout reports nothing to Meta. Section 3.2 applies to joint controllership and the legal basis.

5. Account and sign-in

For your account, we store your email address, name, language and plan. You sign in using a one-time code that we email to you, or a password. If we offer Google sign-in and you use it, Google learns that you are signing in to our service, and we receive your email address and name from Google.

We store when you first and last signed in, and we record each sign-in with its time and method (code, password or Google).

We set a cookie to keep you signed in. It expires when you close your browser. If you select “Stay signed in” when signing in, the cookie remains for up to 400 days. This checkbox is never preselected. Selecting it constitutes your consent (section 25(1) TDDDG). You withdraw that consent by signing out.

The legal basis for your account and sign-in is our contract with you (Article 6(1)(b) GDPR).

6. Dashboard

In the dashboard, we process what you enter and upload:

- your page and Buybox settings, the addresses where you embed the integration, with the times they are added, and the address of your thank-you page,
- your logo and photo, the reading's name, and your confirmation concerning rights, including its time,
- your support address, to which your buyers' replies are sent,
- your details under “My page” > “Ads”: your Meta pixel ID, your Meta access token (we store it encrypted and never display it again) and your Google Ads conversion ID and label, as well as, in our log, when you changed them,
- your messages to support and cases you forward to us.

“Offered by” block: The setup wizard asks for your name, address and email address. We display these three details publicly on your page in every plan. This allows visitors to see whose offer they are viewing.

Sales: For each sale through your page, you see the order number, date, product, amount and country, as well as the source of the purchase. For instalments, you see one row for each paid instalment. You do not see your buyers' names or email addresses.

Your own Reading: If you order a Reading for yourself, we process your details as for buyers; the “Privacy Policy for Partner Pages” applies. From your dashboard, you also open a demo portal with two fixed demo Readings for fictitious people, one in German and one in English, in the template and colour theme you have chosen and with your brand name.

File checks: We accept the logo and photo you upload as PNG, JPG or WebP files of up to 5 MB. We check whether the size and the beginning of the file match its file type, and remove a file that does not match.

Test connection: If you click “Test connection” under “My page” > “Ads”, our server uses your access token to ask Meta about your pixel. Meta receives your pixel ID and access token in the process. We only show you whether the test succeeded and do not store the result. We only record the time, so that tests are not run too often in a row.

The legal basis for the dashboard is our contract with you (Article 6(1)(b) GDPR).

7. Help centre and support

The help centre contains articles. At launch, people handle your support enquiries. We store your enquiry, an image if you attach one, and the conversation history to help you and make the handling of your case traceable. The legal basis is our contract with you (Article 6(1)(b) GDPR).

8. Messages in the dashboard

Messages to us in the dashboard, including those to arrange an appointment, run on our own platform, without a third-party chat service and without an appointment tool. The legal basis is our contract with you (Article 6(1)(b) GDPR).

9. Payouts, self-billing invoices and Stripe

In countries with Stripe Connect, we pay your remuneration through a payout account with Stripe; in all other countries, manually by bank transfer (below, "Manual payout").

When you set up your payout account, Stripe Payments Europe Limited (Ireland) verifies your identity as an independent controller to fulfil statutory anti-money-laundering obligations. Stripe's privacy policy (https://stripe.com/privacy) applies. For this purpose, we provide Stripe with your country, your email address, your brand name (or your name if there is no brand name) and your partner number with us. If you subscribed earlier through the old checkout with "Private person", we also provide Stripe with this information. Otherwise, you choose at Stripe yourself whether you set up your account as an individual or as a company. The legal basis is our contract with you (Article 6(1)(b) GDPR).

With Stripe Connect, you enter your identification and bank details directly with Stripe. We then store only your Stripe account identifier and its status, not bank details.

Self-billing invoices: Once a month, we settle your remuneration by issuing a self-billing invoice. We store each self-billing invoice with its status (accepted or disputed), the time and the identifier of the transfer to your Stripe account or, for a manual payout, the date, amount and reference of the transfer. The self-billing invoice shows your country and the billing address from your subscription at Stripe, where it is available there. You can optionally provide your tax status and VAT identification number.

Chargebacks: We record how many chargebacks there have been for purchases through your page. This determines notices to you, suspension of payouts and, in repeat cases, our review of whether to pause your sales, as provided in the Partner Terms.

Manual payout: If your country is not covered by Stripe Connect, we pay you manually by bank transfer. For this purpose, we process the bank details that you provide in the dashboard in the box "Your payout": the account holder's name, the IBAN or account number, the BIC or SWIFT code, the name and country of the bank and any further details your bank requires for a transfer from abroad, such as a bank code. We store when you last changed the details and, after every time you save them, send you an email without bank details to your email address. Our log contains each time you save your details and each time we mark your bank details as verified, in each case with the time and the payout method, without the bank details themselves. Before the first transfer, we verify that the account belongs to you, and we verify new bank details after every change, before the next transfer; for this, we may request proof, such as a bank statement or an identity document. We delete the proof as soon as the verification is complete. We record when we last marked your bank details as verified. With this, we store the verified version of your details (the time at which you saved them) and the last four characters of the verified account, never the full number. For each manual payout, we store the date, amount, method and reference and, in our log, also the verified version, the last four characters of the verified account and the last four characters of the account to which we made the transfer. As usual, you receive a self-billing invoice. If your bank deducts a fee for receiving the transfer and you want it reimbursed, we process the proof you send us for this, such as a bank statement, and the reimbursement; we keep both as accounting records for as long as tax laws require. You may black out other entries on the statement before sending it. Our bank, your bank and intermediary banks process the transfer as independent controllers, including outside the EU (section 18).

Payout without a Stripe account in a country with Stripe Connect: If you do not have a Stripe account there that can receive payouts and, at your request, we pay your balance by PayPal or bank transfer, we process your PayPal address or bank details for this purpose. You receive a self-billing invoice as a PDF. PayPal or the banks involved process the payment as independent controllers.

The legal basis is our contract with you (Article 6(1)(b) GDPR). We retain self-billing invoices and payments, including the reimbursement of an incoming transfer fee with its proof, because tax laws require us to do so (Article 6(1)(c) GDPR). We base the verification of your bank details for manual payouts on our legitimate interest in not paying out to third parties (Article 6(1)(f) GDPR) and, where a law requires it, on that legal obligation (Article 6(1)(c) GDPR).

10. Custom domain

If you connect a custom domain, we store the domain name and the status of its records. You sign in with your domain provider yourself, not through us. Only your provider processes your domain's registrant details. The legal basis is our contract with you (Article 6(1)(b) GDPR).

11. Emails

We send our emails through Resend. Stripe may send receipts for your payments and notices of a failed payment to your email address on our behalf.

Contract-related emails: order acknowledgement, contract confirmation, confirmation of the free period and the start of subscription billing, email before the end of a paid year, invoices, new self-billing invoice or your monthly statement, notices about your payout account, about chargebacks and about a payout on hold, messages about your support enquiries, confirmation of cancellation or withdrawal, reasons for a measure and notice of changes to the terms. For setup, you receive “Your page is live” once. If your page has never been live and you have not cancelled, we send you the reminder “Your page is not live yet” once, no earlier than 72 hours after your subscription signup. In addition, there is the email “New in Learning” when something new is ready for you in the learning area; you can switch it off under Settings. We store when we sent these emails. The legal basis is our contract with you (Article 6(1)(b) GDPR), or a legal obligation for mandatory information (Article 6(1)(c) GDPR).

Offers: We send offers for our own plans to the email address used for your subscription purchase. This is

the offer for a new year in the email before the end of a paid year. The legal basis is our legitimate interest in advertising our own similar services (Article 6(1)(f) GDPR, section 7(3) UWG).

You can object at any time by contacting us. You will incur no costs other than transmission costs at basic rates. After you object, you will receive no further offers. Contract-related emails continue. A cancellation confirmation never contains an offer.

12. Partner referrals

If you refer a new partner or join through a referral yourself, we store who referred whom and check that no one refers themselves. The legal basis is our contract with you (Article 6(1)(b) GDPR).

13. Content notices

If you report content to us through our contact point for users (legal notice, section “Contact points under the Digital Services Act”) or through the reporting form, we process your notice and our decision, as well as your name and email address where provided. If an email address is available, we acknowledge receipt and later inform you of the decision. In the reporting form, name and email address are mandatory fields. For notices concerning offences under Articles 3 to 7 of Directive 2011/93/EU, you do not have to provide either (Article 16(2)(c) DSA); please use the contact point for such notices. We only disclose your name and email address to the partner whose content is involved if strictly necessary to resolve the case. If a notice concerns your content as a partner, we store the notice, our decision and the reasons in your file.

The legal basis is a legal obligation under the EU Digital Services Act (Article 6(1)(c) GDPR).

14. Cancellation and withdrawal

If you cancel or withdraw, we store your declaration, the time of receipt and our confirmation. Separately, if you provide it, we store your voluntary answer to “Why are you leaving?” and any retention offer you accept.

If you use the withdrawal form (electronic withdrawal function, available without signing in), you enter your name, your partner address or the email address of your account, and an email address for the confirmation. If you are signed in, your name and partner address are already filled in.

The legal basis is our contract with you and a legal obligation (Article 6(1)(b) and (c) GDPR), and, for the voluntary answer, our legitimate interest in improving our service (Article 6(1)(f) GDPR).

We protect the form in the same way as the checkout (section 4). Vercel's bot protection checks whether a human is submitting the form. It reads technical characteristics of your browser, and your IP address and request headers are sent to Vercel. We also count attempts per IP address and per email address for the confirmation, stored only as a code that cannot be reversed without our secret key. If the protection classifies a request as automated or a limit is reached, the form does not accept the withdrawal and instead gives you our email address to send it to. The legal basis for this protection is the same as for the checkout protection (section 4).

15. Switching and exporting your data

You can export your data in the dashboard: page and Buybox settings, your texts, images and files, your integration addresses, your sales list as you see it, and your self-billing invoices and invoices. You receive these as JSON and CSV with the original files.

When your contract ends, you can retrieve your exportable data for at least another 30 days, also through support. After that, we delete your photo, “Offered by” details and Buybox settings, together with the corresponding values in the change log. The logo and the name of the Reading remain for buyer portals. This page cleanup takes place regardless of outstanding invoices. Under Payouts > Invoices, you can access

the PDFs of your self-billing invoices, statements and monthly statements after the end of the contract, without a time limit, for as long as your account exists. Separate account deletion at your request waits while credit balances, negative balances, outstanding self-billing invoices, buyer instalments or claims against you still need to be handled. Once your account has been deleted, we no longer send you emails about self-billing invoices, monthly statements and fraud warnings. A confirmation of your cancellation that is still pending goes to the addresses we stored with your cancellation. Records and embed addresses are retained in accordance with section 19.

16. Storage in your browser

These items are strictly necessary for the services to work in the way you are currently using them. They do not require your consent (section 25(2), no. 2 TDDDG). The exceptions are “Stay signed in”, which you select yourself, and Google Analytics and the “ss-meta” cookie for our advertising on Meta, which only run with your consent (section 3.2).

Where	Item	Purpose	Duration
soulsystem.app, before launch only	Access cookie after entering the access code	opens the restricted pages for you	30 days
soulsystem.app	Cookiebot's “CookieConsent” cookie with your choice in the banner and a random key	remembers what you have allowed	up to 12 months
soulsystem.app, only with your consent	Google Analytics cookies that recognise your browser and your visit, for soulsystem.app itself only	visitor measurement (section 3.2)	up to 2 years
soulsystem.app, only with your consent to “Marketing”	“ss-meta” cookie with a random identifier for your browser and, if you came through an ad on Meta, the identifier of that ad, without your name, for soulsystem.app itself only	matching ads and subscription signups for our advertising on Meta (section 3.2)	90 days
Checkout	Bot protection reads technical browser characteristics without a cookie	protecting the order	only during the check
Checkout, after you click “Start for free”	Cookie with a check value for your order, without any details about you	opens the second and third checkout screens only in the browser in which you ordered	48 hours
Withdrawal form	Bot protection reads technical browser characteristics without a cookie	protecting the form	only during the check
Checkout, before launch only	Test access cookie after entering the access value	opens the checkout before launch	12 hours
Checkout and payouts	Stripe cookies when you open checkout or the “Payouts” page	payment, payout account and fraud prevention	under Stripe's cookie policy (https://stripe.com/legal/cookies-policy)
Sign-in	Sign-in cookie; with “Stay signed in”, also a marker for this choice without any details about you; when signing in with Google, also a check value for the return from Google	keeps you signed in	until you close the browser; up to 400 days with “Stay signed in”

Where	Item	Purpose	Duration
Dashboard	Cookie for language and appearance when you switch them	remembers your choice	1 year
Demo portal	the same items as in a buyer's portal, depending on the template (section “Storage in your browser” of the “Privacy Policy for Partner Pages”)	as in a buyer's portal	as in a buyer's portal

If you upload a file larger than 6 MB in the dashboard, the program the dashboard uses for large uploads also creates an entry in your browser's local storage: with the file's size, type and last modified date, its storage location with us including your partner number, the time of the upload and the upload address, without the file name. The program creates it so that an interrupted upload can be resumed later. On our side it serves no purpose for this: every upload gets a new storage location, so a later upload never finds the entry again. After a completed upload, the program deletes it. After an error, or if you close the page before then, it remains until you clear your browser's storage.

17. Recipients

We only share your data with service providers needed for operation, with organisations acting as independent controllers and, with your consent, with Meta, with whom we are joint controllers for the reports on our advertising (section 3.2). A data processing agreement under Article 28 GDPR is required for service providers processing data on our behalf.

Recipient	Purpose	Location
Vercel	Website and dashboard hosting, bot protection for the checkout and the withdrawal form	dashboard servers in Ireland; website delivered through Vercel's worldwide network; provider in the USA
Supabase	Database, authentication, storage of your files	Ireland; provider in Singapore
Stripe	Payments, subscriptions, tax, payout account, receipts by email	Stripe Payments Europe Limited, Ireland, with processing also in the USA
Resend	Sending our emails and receiving emails sent to our contact address	USA
IONOS	Mailbox for the privacy enquiries address	provider in Germany
Usercentrics A/S (Cookiebot)	Banner on soulsystem.app and proof of your choice	provider in Denmark; proof stored on servers in Ireland, in an emergency in the Netherlands
Google (Google Analytics), only with your consent	Visitor measurement on soulsystem.app	Google Ireland Limited, Ireland, with processing also in the USA
Google, only if you use Google sign-in	Sign-in	Ireland and USA
Google (Web Risk)	Checks the public addresses of your partner page and your embed addresses against Google's list of unsafe sites	provider Google
Meta Platforms Ireland Limited, only if you click “Test connection”	Checking your pixel	Ireland, with processing also in the USA

Recipient	Purpose	Location
Meta Platforms Ireland Limited, only with your consent to “Marketing” on soulsystem.app	Reporting page views on soulsystem.app, clicks on “Start for free” in the checkout, subscription signup and first payment to measure our advertising, as joint controllers (sections 3.2 and 4)	Ireland, with processing also in the USA
Our bank, your bank and intermediary banks, for manual payouts; PayPal only at your request (section 9)	Payout of your remuneration	depends on the bank, including outside the EU
Hetzner Online GmbH	Encrypted backups	Germany
GitHub	Backup and test restoration	provider in the USA
Our tax advisers and authorities	To the extent required by law	Cyprus and EU

Backups: Encrypted daily backups of the database and files are stored in Hetzner Object Storage (Hetzner Online GmbH, Germany). GitHub processes the data for the backup run and test restoration. During this process, the data is temporarily unencrypted on the execution machine. Hetzner does not receive the decryption key. Deletion normally takes effect in backups after approximately 30 days. Failed runs can make this take longer; the seven most recent daily snapshots are retained.

Stripe acts as an independent controller when verifying your identity and fulfilling its own statutory obligations (section 9). Visitors to your page see the details in the “Offered by” block (section 6).

18. Countries outside the EU

Some service providers are based in the USA or process data there. The following applies: if the provider is listed under the EU-US Data Privacy Framework, the transfer relies on the European Commission's adequacy decision. Otherwise, the European Commission's standard contractual clauses in our agreement with the provider apply (Articles 44 et seq. GDPR). On request, we will identify the basis for each provider and send you a copy of the clauses.

According to the providers' information, the following currently applies:

Provider	Basis
Vercel	EU-US Data Privacy Framework
Stripe	EU-US Data Privacy Framework
Resend	EU-US Data Privacy Framework
Google	EU-US Data Privacy Framework
Meta	EU-US Data Privacy Framework
GitHub	EU-US Data Privacy Framework and standard contractual clauses under the GitHub Data Protection Agreement
Supabase	Standard contractual clauses. The provider is based in Singapore; your data is stored in Ireland.

If we pay you manually to an account outside the EU or the EEA, your name, bank details, the amount and the reference go to your bank in that country and to intermediary banks. The basis is that the transfer is necessary for the performance of our contract with you (Article 49(1)(b) GDPR).

19. Retention periods

We retain your data only as long as needed for its purpose. We retain it longer where required by law or for as long as claims under the contract may arise.

Data	Duration
Invoices for the subscription, with payments and refunds	10 years from the end of the year in which the transaction occurred
Self-billing invoices with status, time and transfer identifier	for as long as tax laws require
Bank details for manual payouts (section 9)	until you change them, when the new details replace the old ones; otherwise also after the contract ends, until your account is deleted (row “Account deletion on request”), when we delete them as well; in our bank's records of a transfer, for as long as tax laws require
Verified version and last four characters of the account for manual payouts (section 9)	with the record of the last verification, until we mark new bank details as verified, at the latest until your account is deleted; for each payout, in our log, like the self-billing invoices, for as long as tax laws require, also after your account is deleted
Log entries for manual payouts: each time you save your details and each time we mark your bank details as verified, with the time and the payout method, without the bank details themselves (section 9)	for as long as claims under the contract may arise, also after your account is deleted
Proof of the account for manual payouts (section 9)	until the verification is complete; the record of the verification, for as long as claims under the contract may arise
Proof and reimbursement of an incoming transfer fee for manual payouts (section 9)	for as long as tax laws require
Acceptance of the terms, your confirmation that you are subscribing as a business customer, a declaration requesting immediate commencement from an earlier subscription, times contract-related emails were sent	for as long as claims under the contract may arise
Cancellation and withdrawal with receipt time and confirmation	for as long as claims under the contract may arise
Voluntary answer to “Why are you leaving?”	for as long as we need it to improve our service
Accepted retention offer	as part of the invoice, like the invoice; as evidence, for as long as claims under the contract may arise
Confirmations concerning rights to the logo and photo	while the file is used, then for as long as claims relating to it may arise
Integration addresses with the time they are added	until you remove them, otherwise for as long as claims under the contract may arise
Your objection to promotional emails	as long as we store your email address, to ensure you receive no further offers
Content notices with decisions and reasons	for as long as we need to evidence the notice and the decision
Support enquiries	for as long as we need them for your enquiry; for withdrawal or cancellation, as for the declaration
Photo, “Offered by” details and Buybox settings after the contract ends	30 days for retrieval; then page cleanup, regardless of outstanding invoices
Logo and reading name	for existing buyer portals, as long as the platform operates
Account deletion on request	after the contract and retrieval period end; outstanding financial matters and claims are handled first
The two identifiers for Meta and the shortened information about your browser and device from the checkout, stored only with us (section 4)	without a subscription signup, two days at the most; otherwise until we have reported the first payment for your subscription to Meta, at the latest until your subscription ends or you switch the reports off

Data	Duration
Your consent to “Marketing” with its time, switching the reports off, and the record of when we reported the signup and the first payment to Meta (section 4)	for as long as we store the details of your subscription
Details under “My page” > “Ads” (section 6)	until you remove them, in which case we delete them immediately; otherwise until your account is deleted (row “Account deletion on request”)
Identifier of your payment method (section 4)	for as long as we need it so that there is only one free period per payment method and no one refers themselves
Attempt counters for the checkout and the withdrawal form, and counters of emails from the old checkout sent when no subscription was created, stored only as codes (sections 4 and 14)	for as long as we need them to protect against abuse
Proof of your choice in the banner at Cookiebot (section 3.2)	12 months
Google Analytics measurement data linked to cookies or identifiers (section 3.2)	2 months
Server logs in our Vercel account	for as long as we need them for secure operation
Backups	deletions take effect through backup rotation, after approximately 30 days

20. Your rights

You have the right to:

- access your data,
- have inaccurate data rectified,
- have data erased where we are not required to retain it,
- restrict processing,
- receive your data in a commonly used format,
- withdraw consent, effective from the moment you declare withdrawal,
- lodge a complaint with a data protection supervisory authority.

Objection: If we process data on the basis of our legitimate interests, you may object on grounds relating to your particular situation. You may object to email advertising at any time without giving a reason (Article 21 GDPR).

To exercise these rights, contact the privacy enquiries address in section 1. You may lodge a complaint with the supervisory authority in the country where you live or work. Our competent authority is the Commissioner for Personal Data Protection in Cyprus.

Without your email address, country and payment details, we cannot enter into a subscription with you. Without Stripe's identity verification, we cannot pay your remuneration through Stripe, and without your bank details and the account verification, we cannot pay it manually (section 9).

A decision that has legal effects concerning you is never made solely by a machine on our side. People handle support enquiries (section 7).

21. Security

Connections to our pages are encrypted. In the dashboard, each partner sees only their own data. Only a small number of people within our organisation who need access for operation and support can access all data.

22. Changes to this notice

If our services or the legal position change, we will update this notice. The current dated version is always available here.