Privacy Policy

Last updated: November 2026

This English version is provided for convenience. In the event of any discrepancy, the German version prevails.

General Information

In this privacy policy, we (on:mint GmbH, “we”) inform you about the processing of personal data when you use our website, our services, and the other offerings described below.

Personal data is any information relating to an identified or identifiable person. This includes, above all, information that allows conclusions to be drawn about your identity, such as your name, phone number, address, or email address. Certain identifiers, such as your IP address or the device ID of the device you use, are also personal data.

1. Contact

Unless section 3.1 provides otherwise, the contact person and controller responsible for the processing of your personal data within the meaning of the EU General Data Protection Regulation (GDPR) is on:mint GmbH,

Am Hamburger Bahnhof 4
10557 Berlin, Germany
privacy@onmint.io
www.onmint.io

For all questions regarding data protection in connection with our products and services or the use of our website, you can also contact our data protection officer at any time. The data protection officer can be reached at the postal address above and at the email address given above (reference: “Attn: Data Protection Officer”). Please note that when you use this email address, its contents are not read exclusively by our data protection officer. If you wish to exchange confidential information, please first use this email address to request direct contact.

2. Data Processing on Our Website

2.1 Visiting Our Website and Connection Data

Each time you use our website, we collect connection data that your browser transmits automatically to enable you to visit the website. This connection data comprises the so-called HTTP header information, including the user agent, and includes in particular:

- IP address of the requesting device;
- method (e.g., GET, POST), date, and time of the request;
- address of the website visited and path of the requested file;
- where applicable, the previously visited or requesting website or file (HTTP referrer);
- information about the browser and operating system used;
- version of the HTTP protocol, HTTP status code, size of the file delivered;
- request information such as language, content type, content encoding, and character sets.

The processing of this connection data is strictly necessary to enable you to visit the website, to ensure the continuous functionality and security of our systems, and for the general administration of our website. In addition, the connection data is temporarily stored in internal log files for the purposes described above,

limited in content to what is necessary, for example in order to identify and act against the cause of repeated or malicious requests that endanger the stability and security of our website.

The legal basis is Article 6(1)(b) GDPR if the page is accessed in the course of initiating or performing a contract, and otherwise Article 6(1)(f) GDPR, based on our legitimate interest in enabling access to the website and in the continuous functionality and security of our systems. In this case, accessing and storing information on your device is strictly necessary and takes place on the basis of the laws implementing the EU ePrivacy Directive in the EU Member States, in Germany under Section 25(2) No. 2 of the German Telecommunications Digital Services Data Protection Act (TDDDG).

For data protection reasons, we do not store or analyze log files permanently.

2.2 Cloudflare

We use the "Cloudflare" service. The provider is Cloudflare Inc., 101 Townsend St., San Francisco, CA 94107, USA ("Cloudflare").

Cloudflare offers a globally distributed content delivery network (CDN) with Domain Name System (DNS). Technically, the transfer of information between your browser and our website is routed through Cloudflare's network. This enables Cloudflare to analyze the data traffic between your browser and our website and to act as a filter between our servers and potentially malicious traffic from the internet. Cloudflare blocks threats and limits abusive bots and crawlers that would slow down access to the website or attack our systems. For these purposes, Cloudflare may also use cookies or other technologies, such as the following:

- "__cf_bm" (30 minutes): security cookie, bot detection, and defense against cyberattacks;
- "_cfuvid" (session): detection and management of incoming connections to enforce Cloudflare's policies for reducing traffic and preventing abuse.

The use of Cloudflare is based on our legitimate interest in providing our website as error-free and securely as possible (Article 6(1)(f) GDPR). In this case, accessing and storing information on your device is strictly necessary and takes place on the basis of the laws implementing the EU ePrivacy Directive in the EU Member States, in Germany under Section 25(2) TDDDG. We have concluded a data processing agreement with Cloudflare. Personal data is transferred to the USA on the basis of the adequacy decision for the USA because Cloudflare is certified under the EU-U.S. Data Privacy Framework.

Details and further information on security and data protection at Cloudflare can be found here: https://www.cloudflare.com/privacypolicy/

2.3 Contacting Us

You have various ways to contact us, in particular the contact form, a phone call, or an email to the contact addresses given above. In this context, we process data exclusively for the purpose of communicating with you.

The legal basis is Article 6(1)(b) GDPR to the extent your information is needed to answer your inquiry or to initiate or perform a contract, and otherwise Article 6(1)(f) GDPR, based on our legitimate interest in enabling you to contact us and in answering your inquiry.

The data we collect when you contact us is deleted automatically once your inquiry has been fully processed, unless we still need your inquiry to fulfill contractual or legal obligations (see section 7).

2.4 Newsletter

With our newsletter, we regularly inform you about current developments in digital provenance, data integrity, and controlled data use, as well as about our services. To subscribe to the newsletter, we collect your email address and, for events, also your name and, where applicable, your company name.

For newsletter subscriptions, we use the so-called double opt-in procedure, meaning that we will only send you newsletters by email after you have confirmed, by clicking a link in our notification email, that you are the owner of the email address provided. If you confirm your email address, we store your email address, the time of subscription, and the IP address used for subscribing for the duration of your subscription. The sole purpose of this storage is to be able to send you the newsletter and to prove your subscription. After you unsubscribe or withdraw your consent, we retain this information only to prove your subscription, for up to three years, and then delete it. You can unsubscribe from the newsletter at any time. An unsubscribe link is included in every newsletter. A message to the contact details given above or in the newsletter (e.g., by email or letter) is, of course, also sufficient.

We use so-called pixels (tiny, invisible image files) in our newsletters to measure the open rate, as well as links for which we can measure clicks before forwarding to the target page. This data processing takes place exclusively in aggregated form for statistical analysis and for the optimization and further development of our content and customer communication. No usage analysis at the level of individual newsletter recipients takes place. We also record whether newsletters could be delivered and which email addresses could not be reached. This data is not combined with other data. You can prevent the measurement of the open rate by disabling the loading of images in your email client.

If you have not confirmed your newsletter subscription, we delete your data promptly.

We use Brevo, a service of Sendinblue GmbH, Köpenicker Straße 126, 10179 Berlin, Germany (“Brevo”), to send our newsletter. We use Brevo for email marketing when you subscribe to the newsletter on our website and for transactional emails, for example when you download a white paper. We have concluded a data processing agreement with Brevo. Brevo stores your data in Germany or the European Union and transmits it in encrypted form. To the extent that Brevo works with sub-processors whose parent company is not based in the European Union, the adequacy decision for the USA applies to U.S. companies certified under the EU-U.S. Data Privacy Framework, and/or Brevo and its sub-processors have concluded standard contractual clauses and taken additional measures to protect the data. In connection with the use of Brevo, anonymized data on newsletter usage (e.g., clicks, opens) is used for aggregated statistical analysis.

The legal basis for sending the newsletter, the aggregated usage analysis, and the determination of deliverability is your consent under Article 6(1)(a) GDPR. The legal basis for retaining the proof of subscription after you unsubscribe is Article 6(1)(f) GDPR; our legitimate interest lies in being able to prove that consent was given.

2.5 Job Applications

You can apply for open positions by email or through our career portal. The purpose of collecting the data is to select applicants for the possible establishment of an employment relationship. To process your application, we collect the data you provide (usually: first and last name; email address; application documents such as certificates, references, and résumé; earliest possible start date; the channel through which you became aware of the job posting; and, where applicable, phone number, salary expectations, Xing or LinkedIn profile). Please note that confidentiality cannot be guaranteed if applications are sent by unencrypted email. As a rule, you can also apply for our positions by mail.

The legal basis for processing your application documents is Article 6(1)(b) GDPR.

We store your personal data upon receipt of your application. If we accept your application and an employment relationship is established, we store your application data for as long as it is required for the employment relationship and to the extent statutory provisions require its retention.

If we reject your application, we store your application data for no longer than three months after the rejection, unless you consent to longer storage. If you have separately given your consent, we will store the data submitted with your application in our applicant pool for another twelve months after the application

process has ended, in order to identify other positions that may be of interest to you and to contact you again if appropriate. After this period, the data is deleted. You can withdraw this consent at any time with effect for the future by sending an email to privacy@onmint.io.

2.6 Use of Cookies and Similar Technologies for Analytics and Marketing Purposes

To improve the presentation of content on our website, we use cookies and similar technologies (e.g., local storage, fingerprints, pixels, web beacons) to statistically record and analyze general usage behavior based on access data. In addition, we use services of external providers that process the access data generated when you use our website in order to enable the delivery of interest-based advertising, for example in connection with search queries.

We use optional cookies and similar technologies for marketing and analytics purposes only if you have given your consent to the data processing under Article 6(1)(a) GDPR. Accessing and storing information on your device takes place on the basis of the laws implementing the EU ePrivacy Directive in the EU Member States, in Germany under Section 25(1) TDDDG. To the extent that our app at app.onmint.io uses these technologies, the following sections apply accordingly.

2.6.1 Consent Management (Cookie Banner)

We use our own cookie banner to obtain and manage your consent. It appears when you first visit our website, informs you about the data processing on our website, and gives you the option to consent to all, some, or none of the data processing by optional tools.

Your selection is stored as the entry “onmint-cookie-consent-v1” in your browser’s local storage in order to document the consents you have given and withdrawn and to take them into account on later visits. The entry remains stored until you delete it. If you delete the website data in your browser, we will ask for your consent again on a later visit.

This data processing is necessary to provide you with the legally required consent management and to comply with our documentation obligations. The legal basis is Article 6(1)(f) GDPR, based on our interest in meeting the legal requirements for consent management. In these cases, accessing and storing information on your device is strictly necessary and takes place on the basis of the laws implementing the EU ePrivacy Directive in the EU Member States, in Germany under Section 25(2) TDDDG.

Withdrawing your consent or changing your selection: You can withdraw your consent or change your selection at any time. To do so, click the “Cookie Settings” link in the footer of our website.

2.6.2 Google Tag Manager

Our website uses Google Tag Manager, a service provided for persons in the European Economic Area and Switzerland by Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, and for all other persons by Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA (“Google”).

We use Tag Manager to manage the tools and external services we use on our website; it allows the use of so-called tags. A tag is a code element stored in the website’s source code, for example to control which page or service elements and tools are activated and loaded, and in which order. The tool triggers other tags, which in turn may collect data and are explained further in this privacy policy. In some cases, the data is processed on a Google server in the USA.

The data processing is based on Article 6(1)(f) GDPR in order to provide our website and integrate the services we use. In these cases, accessing and storing information on your device is strictly necessary and takes place on the basis of the laws implementing the EU ePrivacy Directive in the EU Member States, in Germany under Section 25(2) TDDDG.

We have concluded a data processing agreement with Google Ireland Limited for the use of Google Tag Manager. If personal data is transferred from Google Ireland Limited to Google LLC in the USA, the transfer takes place on the basis of the adequacy decision for the USA because Google LLC is certified under the EU-

U.S. Data Privacy Framework.

More information on Google Tag Manager can be found in Google's information on Tag Manager.

2.6.3 Google Analytics

Our website uses the web analytics service Google Analytics 4, provided for persons in Europe, the Middle East, and Africa (EMEA) by Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, and for all other persons by Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA ("Google"). We integrate Google Analytics 4 via Google Tag Manager. If you have not consented to the use of analytics tools, your data will not be collected by Google Analytics 4.

Google Analytics 4 uses JavaScript and pixels to read information on your device and cookies to store information on your device. This serves to analyze your usage behavior and to improve our website. On our behalf, Google combines the access data into pseudonymous usage profiles and transfers them to a Google server in the USA. We will process the information obtained to evaluate your use of the website and to compile reports on website activity.

As part of the analysis, Google Analytics 4 also uses artificial intelligence, such as machine learning, for automated analysis and enrichment of the data. For example, Google Analytics 4 models conversions where not enough data is available, in order to optimize analysis and reports. The data collected as part of the usage analysis by Google Analytics 4 is enriched with data from Google Search Console and linked with data from Google Ads, in particular to measure the success of our advertising campaigns (so-called conversions).

Data processed:

- IP address;
- user ID and device ID;
- referrer URL (previously visited page);
- pages viewed (date, time, URL, title, time spent);
- downloaded files;
- clicked links to other websites;
- achievement of certain goals (conversions);
- technical information (operating system; browser type, version, and language; device type, brand, model, and resolution);
- approximate location (country, region, and, where applicable, city, based on the anonymized IP address).

Privacy settings:

- anonymization of the IP address;
- advertising features disabled;
- personalized advertising disabled;
- retention period of 2 months (with no reset of the retention period upon new activity);
- cross-device and cross-site tracking (Google Signals) disabled;
- data sharing disabled (in particular Google products and services, benchmarking, technical support, account specialists).

Cookies used:

- "_ga" (2 years) and "_gid" (24 hours): recognizing and distinguishing visitors by a user ID;
- "_ga_XXX" (2 years): retaining information about the current session;
- "FPID" (2 years): implementing server-side tracking and recognizing and distinguishing visitors by a user ID;

- “FPLC” (20 hours): cross-domain tracking with URL parameters as part of server-side tracking, using the hashed identifier of the FPID cookie.

The legal basis for this data processing is your consent under Article 6(1)(a) GDPR. Accessing and storing information on your device then takes place on the basis of the laws implementing the EU ePrivacy Directive in the EU Member States, in Germany under Section 25(1) TDDDG.

We have concluded a data processing agreement with Google Ireland Limited for the use of Google Analytics 4. If personal data is transferred from Google Ireland Limited to Google LLC in the USA, the transfer takes place on the basis of the adequacy decision for the USA because Google LLC is certified under the EU-U.S. Data Privacy Framework.

2.6.4 Google Ads Conversion Tracking

Our website uses “Google Ads Conversion Tracking”, a service provided for persons in Europe, the Middle East, and Africa (EMEA) by Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, and for all other persons by Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA (“Google”). We integrate Google Ads Conversion Tracking via Google Tag Manager. If you have not consented to the use of marketing tools, your data will not be collected by Google Ads Conversion Tracking.

The service records and analyzes customer actions defined by us (such as clicking a button, viewing a page, downloading a file, or submitting a form). We also record events (such as time spent on the page, scrolling, and interaction with the page and forms). This helps us evaluate the success of campaigns and ads and optimize the design of our website. In addition, we use and analyze parameters in the URL (such as the source of the visit, e.g., a domain, the type of campaign, and the visit channel, such as email or search engine) in order to better measure campaigns and attribute them to users.

For this purpose, the service uses cookies, JavaScript, pixels, and other technologies. Google also processes the data to improve the quality and accuracy of conversions. The data generated in this context may be transferred by Google to a server in the USA for analysis and stored there.

The following cookies are set and read by Google:

- “_gcl_au” (90 days): conversion tracking, storage of ad clicks;
- “FPAU” (90 days): usage analysis, recording of interaction with ads, and reporting;
- “IDE” (390 days): recognizing and distinguishing visitors by a user ID, recording of interaction with ads, delivery of personalized ads.

The legal basis for this data processing is your consent under Article 6(1)(a) GDPR. Accessing and storing information on your device then takes place on the basis of the laws implementing the EU ePrivacy Directive in the EU Member States, in Germany under Section 25(1) TDDDG.

If personal data is transferred from Google Ireland Limited to Google LLC in the USA, the transfer takes place on the basis of the adequacy decision for the USA because Google LLC is certified under the EU-U.S. Data Privacy Framework.

More information can be found in Google’s privacy policy: https://policies.google.com/privacy

2.6.5 Server-Side Tracking

Our website uses services of TAGGRS B.V., Coehoorn van Scheltingaweg 1P, 8442 EZ Heerenveen, Netherlands (“Taggrs”), for server-side tracking. With the help of Taggrs’ services, usage, browser, and device data, including the IP address and the user agent, is collected and further processed on the server side. The purpose of the processing is to evaluate usage data in order to compile statistics and to measure and optimize conversions. This serves to adapt and improve our website and our content. Taggrs uses servers of the service provider TransIP B.V., Vondellaan 47, 2332 AA Leiden, Netherlands, within the European Economic Area.

The legal basis for this data processing is your consent under Article 6(1)(a) GDPR. Accessing and storing information on your device then takes place on the basis of the laws implementing the EU ePrivacy Directive in the EU Member States, in Germany under Section 25(1) TDDDG.

2.6.6 LinkedIn Insight Tag

Our website uses LinkedIn's "Insight Tag", provided for persons in the European Economic Area and Switzerland by LinkedIn Ireland Unlimited Company, Wilton Place, Dublin 2, Ireland, and for all other persons by LinkedIn Corporation, 1000 W Maude Avenue, Sunnyvale, CA 94085, USA ("LinkedIn"). We integrate the LinkedIn Insight Tag via Google Tag Manager. If you have not consented to the use of marketing tools, your data will not be collected by the LinkedIn Insight Tag.

The Insight Tag collects data about your visit to our website (including the URL visited, referrer URL, IP address, device and browser characteristics, and timestamps) and events defined by us (e.g., conversions). This allows us to measure the success of our LinkedIn advertising campaigns (conversion tracking), to show visitors to our website interest-based ads on LinkedIn (retargeting), and to obtain aggregated reports on the audiences of our website.

The following cookies are set and read by LinkedIn:

- "li_gc" (6 months): storing the consent status for non-essential cookies;
- "lidc" (24 hours): routing;
- "bcookie" (1 year): browser ID;
- "li_sugr" (90 days): browser ID for matching;
- "UserMatchHistory" (30 days): synchronization of LinkedIn Ads IDs;
- "AnalyticsSyncHistory" (30 days): time of synchronization.

The legal basis for this data processing is your consent under Article 6(1)(a) GDPR. Accessing and storing information on your device then takes place on the basis of the laws implementing the EU ePrivacy Directive in the EU Member States, in Germany under Section 25(1) TDDDG.

If personal data is transferred from LinkedIn Ireland to LinkedIn Corporation in the USA, the transfer takes place on the basis of the adequacy decision for the USA because LinkedIn Corporation is certified under the EU-U.S. Data Privacy Framework.

More information can be found in LinkedIn's privacy policy: https://www.linkedin.com/legal/privacy-policy. You can opt out of interest-based advertising by LinkedIn here: https://www.linkedin.com/psettings/guest-controls/retargeting-opt-out

2.6.7 Microsoft Advertising

We use Microsoft Advertising with Universal Event Tracking (UET). The provider is Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland ("Microsoft"), a subsidiary of Microsoft Corporation, One Microsoft Way, Redmond, WA 98052, USA. With UET, we record how visitors interact with our pages after clicking on one of our ads in order to measure the success of our ads (conversion tracking). For this purpose, Microsoft uses cookies such as "_uetsid", "_uetvid", and "MUID".

The legal basis for this data processing is your consent under Article 6(1)(a) GDPR. Accessing and storing information on your device then takes place on the basis of the laws implementing the EU ePrivacy Directive in the EU Member States, in Germany under Section 25(1) TDDDG.

If personal data is transferred to Microsoft Corporation in the USA, the transfer takes place on the basis of the adequacy decision for the USA because Microsoft Corporation is certified under the EU-U.S. Data Privacy Framework.

More information can be found in Microsoft's privacy statement: https://privacy.microsoft.com/en-us/privacystatement

2.7 Live Chat (Lime Connect)

Our website uses the live chat of Lime Connect (Userlike) GmbH, Im Mediapark 8, 50670 Cologne, Germany. It is used to enable quick and easy communication with you and to answer contact requests.

In particular, the following data may be processed:

- connection and device data (including IP address, user agent, URL visited and previously visited; information about your device, operating system, and browser);
- usage data (including number of page views and page visits, time of access, time of the last page view and of the last interaction with the live chat);
- communication data (including chat transcript, chat topic, chat status, duration and date of the chat);
- data you provide, if any (such as name and email address).

The following information is stored on and read from your device for this purpose:

- cookie "uslk_umm_{organization-id}_s": storage of the ID of the current chat, an authentication token, the blocking status, and, where applicable, the data you provided;
- local and session storage "uslk_umm_{organization-id}": storage of the number of page views and page visits, the last restorable state of the chat, the time of the last interaction with the live chat and of the last page view, and whether the chat was closed;
- local storage "loglevel:userlike": storage of the current log level for the live chat;
- local storage "chakra-ui-color-mode": storage of the selected color scheme;
- session storage "uslk_umm_interacted": storage of whether an interaction with the live chat has taken place (binary).

To protect your privacy, we have made the following privacy settings:

- additional information such as name or email address is optional;
- privacy mode to minimize data collection and display;
- live preview disabled so that texts not yet sent are not displayed;
- automatic deletion of chat transcripts after six months at the latest;
- confirmation of and link to the privacy policy before the chat starts.

The legal basis for storing and reading information on your device is your consent under Section 25(1) TDDDG, and for the subsequent processing of personal data, your consent under Article 6(1)(a) GDPR. You give your consent via the consent view of the chat widget before the chat opens. You can withdraw it at any time with effect for the future.

More information on the tool and the data processing can be found at: https://connect.lime-technologies.com/de/legal/privacy-policy/

2.8 Reporting Illegal Content

If you report illegal content to us, we process your name, your email address, and the content of your report in order to review the report, confirm its receipt to you, and inform you of our decision. The legal basis is Article 6(1)(c) GDPR in conjunction with Article 16 of the Digital Services Act (DSA). We disclose your identity to the affected customer only if strictly necessary. Section 7 applies to the storage period.

3. Use of Our Services

This section applies to our services Content Credentials, IP Management, Asset Management, and mintys, which you use under our General Terms and Conditions via the app, the application programming interface (API), or the MCP server (an interface based on the Model Context Protocol).

3.1 Responsibility

Where our customers process personal data contained in content via our services, the respective customer is the controller for that data. We process this data on the customer's behalf under our Data Processing Agreement (onmint.io/en/dpa). Data subjects should address requests regarding their rights to that customer. We are the controller for the customer account, contract processing, and billing.

3.2 Account and Login

For your account, we process your email address, your name if provided, the name of your company or organization, your VAT identification number if applicable, the plans booked, and login and log data. Login is passwordless; we create an account the first time you log in. The legal basis is Article 6(1)(b) GDPR.

For login, we use the Web3Auth service, which belongs to Consensys Software Inc., USA. Web3Auth processes your email address or your social login identifier and technical connection data in order to carry out the login. In the process, data is transferred to the USA; section 6 applies to this transfer. If you log in with an existing account with another provider (social login), we receive from that provider the information required for login, in particular your name and email address. Details on the processing by Web3Auth can be found in the Consensys privacy notice: https://legal.consensys.io/plain/privacy-policy/

3.3 Content, Provenance Records, and Blockchain

We process your content and the information you provide about it, such as authorship, origin, and AI status, in order to embed Content Credentials, watermarks, and labels, to maintain the work history in IP Management, and, to the extent booked, to store files in Asset Management. The legal basis is Article 6(1)(b) GDPR. If your content depicts or names other persons, we base the processing of their data on Article 6(1)(f) GDPR; the legitimate interest lies in making the origin and integrity of content verifiable. AI detection does not serve to identify persons. We do not train AI models on your content.

We store and process content exclusively in data centers of Scaleway SAS in the European Union; no transfer to third countries takes place.

Public provenance records display the information you release to anyone. On the public Polygon blockchain, we store only hash values and technical identifiers, no content. A file cannot be reconstructed from a hash value; only someone who possesses the file itself can match it. We store the mapping data exclusively in the EU. Blockchain entries remain in place permanently.

Without booked storage, we keep files only for as long as necessary for processing and download. When the contract or a booked storage plan ends, you can retrieve your data for another 30 calendar days; we then delete it unless a statutory retention obligation applies. At your request, register entries and provenance records remain in place.

3.4 Payment

We process payments through Stripe Payments Europe, Limited, Dublin, Ireland ("Stripe"). Stripe processes in particular your name, your email address, billing information, and payment data. The legal basis is Article 6(1)(b) GDPR and, for invoices and their retention, Article 6(1)(c) GDPR. More information can be found in Stripe's privacy policy: https://stripe.com/privacy

3.5 Usage Data

We analyze data on the use of the services that is unrelated to content, such as usage volume and error logs, for billing (Article 6(1)(b) GDPR) and for the security and improvement of the services (Article 6(1)(f) GDPR).

3.6 Contract Emails

We send order confirmations and contract-related notices by email through service providers acting on our behalf. The legal basis is Article 6(1)(b) and (c) GDPR.

4. on:mint Verify

With on:mint Verify, our browser extension (listed in the Chrome Web Store as “on:mint Content Credentials”) and our verification page at onmint.io/verify, you can check media content such as images, videos, and documents without an account for provenance records, Content Credentials based on the standard of the Coalition for Content Provenance and Authenticity (C2PA), machine-readable AI labels, and indications of AI generation. Use is subject to our Terms of Use for on:mint Verify. A check takes place only if you actively request it: in the extension via the context menu or the icon, and on the verification page by uploading a file.

The check takes place in two steps. First, a hash value (digital fingerprint) is generated from the selected content and transmitted to our application programming interface (API) in order to compare it with the inventory available at on:mint. Only if the comparison produces no match is the content itself transmitted for further checking.

In the process, technically necessary connection data, in particular your IP address, the hash value, where applicable the content itself, and the check result are processed. This information may constitute personal data if the content depicts or names an identified or identifiable person or if the information can otherwise be attributed to such a person.

The processing serves to provide the check you requested and to ensure the functionality and security of our API. The legal basis is Article 6(1)(f) GDPR. Our legitimate interests lie in providing you with the requested checking function and in protecting our systems against misuse and attacks. We use checked content exclusively for the check and in particular not for training AI models.

We process transmitted content only temporarily for the duration of the check, do not store it permanently, and delete it once the check is complete. Hash values and technically necessary connection data are generally processed only for the duration of the check and deleted afterward.

The extension accesses content only after you have actively requested the check. To the extent that it accesses information on your device in doing so, this is strictly necessary for the checking function you requested and takes place in Germany on the basis of Section 25(2) No. 2 TDDDG. The extension does not read your browsing history, does not create usage profiles, and does not use the processed data for advertising purposes. Our processing of user data in connection with the extension complies with the “Limited Use” requirements of the Chrome Web Store User Data Policy.

We use Scaleway SAS, 8 rue de la Ville-l’Évêque, 75008 Paris, France, as a processor for hosting our API. Processing takes place exclusively within the European Union; no transfer to third countries takes place.

5. Disclosure of Data

We generally disclose the data we collect only if:

- you have given your express consent under Article 6(1)(a) GDPR;
- the disclosure is necessary under Article 6(1)(f) GDPR to protect our interests or to establish, exercise, or defend legal claims, and there is no reason to assume that you have an overriding legitimate interest in

your data not being disclosed;

- we are legally obligated to disclose the data under Article 6(1)(c) GDPR, or the disclosure is legally permissible and necessary under Article 6(1)(b) GDPR for the performance of contractual relationships with you or for taking pre-contractual steps at your request.

Part of the data processing may be carried out by our service providers. In addition to the service providers mentioned in this privacy policy, these may include in particular data centers that operate our website, our services, and databases (website hosting and email delivery: Lovable Labs AB, Regeringsgatan 25, 111 53 Stockholm, Sweden; database and backend services for the website: Supabase; hosting of our services and of on:mint Verify: Scaleway SAS, Paris, France), as well as IT service providers that maintain our systems and consulting firms. If we disclose data to our service providers, they may use the data exclusively to perform their tasks. We have carefully selected and engaged these service providers. They are contractually bound by our instructions, have appropriate technical and organizational measures in place to protect the rights of data subjects, and are regularly monitored by us.

In addition, data may be disclosed in connection with official inquiries, court orders, and legal proceedings if this is necessary for legal prosecution or enforcement.

6. Data Transfers to Third Countries

We may use services whose providers are partly located in so-called third countries (such as the USA) or transfer personal data there, i.e., countries whose level of data protection does not correspond to that of the European Union. If the European Commission has issued an adequacy decision (Article 45 GDPR) for these countries, we base the transfer on it. This applies, for example, to transfers to Argentina, Israel, Japan, Canada, the Republic of Korea, New Zealand, Switzerland, Uruguay, or the United Kingdom. In the case of the USA, this applies only if the U.S. recipient is certified under the EU-U.S. Data Privacy Framework.

If no adequacy decision has been issued for the country concerned, we have taken appropriate precautions to ensure an adequate level of data protection for any data transfers. These include, among others, the European Union's standard contractual clauses or binding corporate rules (Article 46 GDPR).

Where this is not possible, we base the data transfer on the derogations in Article 49 GDPR, in particular your express consent or the necessity of the transfer for the performance of a contract or for taking pre-contractual steps.

If a transfer to a third country is intended and there is neither an adequacy decision nor appropriate safeguards, it is possible, and there is a risk, that authorities in the respective third country (e.g., intelligence services) may gain access to the transferred data in order to collect and analyze it, and that the enforceability of your data subject rights cannot be guaranteed. If your consent to the data transfer is obtained via the consent banner, you will also be informed of this.

7. Storage Period

As a rule, we store personal data only for as long as necessary to fulfill the purposes for which we collected it. Thereafter, we delete the data without undue delay, unless we still need it until the statutory limitation period expires for evidentiary purposes for civil law claims or because of statutory retention obligations.

For evidentiary purposes, we must retain contract data for three years from the end of the year in which our business relationship with you ends. Any claims become time-barred under the regular statutory limitation period at the earliest at that time. Even after that, we must still store some of your data for accounting reasons. We are required to do so by statutory documentation obligations that may arise, for example, from the German Commercial Code (HGB), the German Fiscal Code (AO), the German Banking Act (KWG), and the German Money Laundering Act (GwG). The retention periods prescribed there range from two to ten years.

8. Your Rights

You have the right at any time to request information about the processing of your personal data by us. When providing this information, we will explain the data processing to you and provide an overview of the data stored about you. If data stored by us is incorrect or no longer up to date, you have the right to have this data rectified. You can also request the erasure of your data. If erasure is exceptionally not possible due to other legal provisions, the data will be restricted so that it is only available for that legal purpose. You can also have the processing of your data restricted, for example if you believe that the data we store is inaccurate. You also have the right to data portability, meaning that we will send you a digital copy of the personal data you have provided upon request. You also have the right not to be subject to a decision based solely on automated processing that produces legal effects concerning you or similarly significantly affects you, including, where applicable, the right to obtain human intervention on the part of the controller, to express your point of view, and to contest the decision.

To exercise the rights described here, you can contact us at any time using the contact details given above. This also applies if you wish to receive copies of safeguards demonstrating an adequate level of data protection. If the relevant legal requirements are met, we will comply with your data protection request.

Your requests to exercise data subject rights and our responses to them are retained for documentation purposes for up to three years and, in individual cases where there is reason to do so, beyond that for the establishment, exercise, or defense of legal claims. The legal basis is Article 6(1)(f) GDPR, based on our interest in defending against any civil claims under Article 82 GDPR, avoiding fines under Article 83 GDPR, and fulfilling our accountability obligation under Article 5(2) GDPR.

Finally, you have the right to lodge a complaint with a data protection supervisory authority. You can exercise this right, for example, with a supervisory authority in the Member State of your residence, your place of work, or the place of the alleged infringement. In Berlin, where on:mint GmbH is based, the competent supervisory authority is: Berlin Commissioner for Data Protection and Freedom of Information (Berliner Beauftragte für Datenschutz und Informationsfreiheit), Alt-Moabit 59–61, 10555 Berlin, Germany.

9. Right to Withdraw Consent and Right to Object

You have the right to withdraw any consent you have given to us at any time. As a result, we will no longer continue the data processing based on that consent in the future. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal.

To the extent that we process your data on the basis of legitimate interests, you have the right to object to the processing of your data at any time on grounds relating to your particular situation. If your objection concerns data processing for direct marketing purposes, you have a general right to object, which we will implement even without you stating any reasons.

If you wish to exercise your right to withdraw consent or to object, an informal message to the contact details given above is sufficient.

10. Obligation to Provide Your Data

To the extent that the provision of your data is required to conclude a contract (e.g., to order services), to fulfill legal obligations, to contact us, or to use other services and functions (e.g., to subscribe to the newsletter), the corresponding input fields are marked as mandatory (usually with an asterisk (*)). In this case, without this data, a contract cannot be concluded, the specific service cannot be provided, or the function cannot be used.

Other information not marked as mandatory is voluntary. Providing such data is then not required to conclude a contract, to provide the service, or to use the function and has no influence on the performance of the contract.

11. Automated Decision-Making

No automated decision-making, including profiling, within the meaning of Article 22 GDPR that produces legal effects or similarly significantly affects you takes place.

12. Changes to This Privacy Policy

We update this privacy policy from time to time, for example when we adapt our website or our services or when legal or regulatory requirements change.