

Vasion Privacy Policy

INTRODUCTION

Vasion takes data privacy seriously and is committed to managing your personal data professionally and in compliance with all applicable data protection laws. We have a global policy that we follow worldwide, which is based on EU and United Kingdom data protection principles.

This Privacy Policy **applies** to:

- People who use our website
- People who inquire about our company, goods or services
- People who purchase, use or who might be interested in our goods or services
- Vasion Job Applicants

and in each case which may have been provided to Vasion, Inc. (formerly PrinterLogic, Inc.) or any of its subsidiary companies (collectively, "Vasion", "we", "us", or "our").

NOTE: Any questions that you may have relating to your personal data and your rights as it pertains to that personal data that Vasion processes as a data processor by and/or on behalf of our customers and/or, personal information submitted by individuals for processing through the platforms hosted by Vasion for the purposes of providing a service to our customers should be directed to the applicable customer and not to Vasion.

Any personal data Vasion may process in connection with any of our services for and/or on behalf of our customers is addressed in our Master Software Agreement and its accompanying data processing addendum between Vasion and its customer.

1. Our Commitment

Part of our commitment is to ensure that there is transparency about how we process personal data. This policy includes an explanation of:

- What data we are processing
- Why we are processing it, what we do with it, and how long we will keep it
- Whether we will share it with anyone else
- The additional safeguards we have put in place to ensure your data is always protected regardless of different data protection laws in different countries
- How we keep your data safe
- Your rights as data subjects under applicable data protection laws

We hope you find this privacy policy helpful. If you have any questions, please contact us

2. Who are we and how can you contact us?

Headquarters:

432 S. Tech Ridge Drive
St. George, Utah, 84770
USA
Phone: 435.652.1288

Our European subsidiaries contact information:

Vasion Tech Limited
16 Great Queen Street
Covent Garden
London WC2B 5AH
United Kingdom
Phone: + 44 (0) 20 3899 3222

Vasion GmbH
Daimlerring 4
65205 Wiesbaden
Germany
Phone: +49 (6122) 7783900

Amtsgericht Königstein HRB 9411
USt-Ident-Nr./VAT Nr.: DE307290479
Geschäftsführer | Managing Director: Ryan Wedig

In each case, please address your correspondence to the Data Protection Coordinator, you may also contact us using the email privacysupport@vasion.com.

3. What personal data do we collect about you?

3.1. We may collect the following personal data from you:

- Contact information, such as, your name, email address, mailing address or phone number
- Unique Identifiers, such as username or password
- Call recordings (including voicemail on individual machines) as well as video conferences used for purposes such as product demonstrations, feedback surveys or product support.
- CV or other information provided to us when you express an interest in working within our organization
- Information about your business such as your company name and website
- Data on how you navigate around our website

3.2. We may receive information about you from other sources, including publicly available databases or third parties from whom we have purchased data, and combine this data with information we already have about you for example: name, email, phone number, and employer. This helps us to update, expand and analyze our records, identify new customers, to create more tailored advertising and products and provide products and services that may be of interest to you. If you provide us personal data about others, or if others give us your personal data, we will only use that information for the specific reason for which it was provided to us.

3.3. If you use our products, we may collect the following personal data

3.3.1 Vasion Print Product

- If you use the print management SaaS version of our product, the software will ask the customer's IT administrator to create an Active Directory of users which will include such user identifying information as the IT administrator chooses to include. Typically, this is username, email address, pin number, and ID number.
- If you use the print management SaaS or on-premise version of our product, the software will also collect the following metadata information relating to each user's usage in order to provide customer with a report, which if you are using the SaaS version will also be shared with Vasion for the purposes of providing you with the product: job title, user, page count, and destination printer. For authorization, we collect and store usernames, names, and email addresses. In the event a customer is not using an identity provider, we store authentication user information including passwords. We do not store any document content, however, the title of each document printed which may or may not, at the user's discretion, contain personal data and/or sensitive or Special Category data is collected.

3.3.2 Vasion's Document Capture, Automated Workflow, Electronic Signature, and Content Management Products

- You may be a user of our product either because your employer has purchased our product and made it available to you or because a third party who is using our product has asked you to upload or otherwise submit content to them and is using our platform to receive that content from you, e.g., an online web form which you are asked to complete and submit. In both cases, your content may or may not, at your discretion (and depending on the instructions of whoever has asked you to submit the content), contain personal data which our product will process on behalf of the employer or the third party that is our customer ("**Content Personal Data**"). The personal data may be your own in which case you will be the "data subject," or it may be that you may submit personal data about other individuals. In both cases, we collect the Content Personal Data and will store it for workflow, retrieval, and archive purposes depending on the instructions of our customer or the user.
- The types of Content Personal Data processed by us is at the discretion of the user and may or may not also contain special category data.

3.3.3 Offer to conclude a Data Processing Addendum: If you are a business customer using our product, on your instructions and within the framework of the service provision, personal data is collected, processed and/or used by us. The customer is responsible for complying with the data protection rules to ensure that we process your personal data collected by our product in accordance with your instructions and data protection laws. The customer can fulfil this obligation by concluding a Data Processing Addendum with us, which meets the legal requirements of the data protection laws. We have incorporated a Data Processing Addendum into our service provision agreements and will ask you to agree to this at the time of purchase.

3.4. How do we use your personal data and what is our lawful basis for doing so?

Vasion may collect and use personal data to allow us to pursue our **legitimate interests**, including to:

- assess the needs of your business to determine suitable products
- provide you with any requested company, product or service information
- provide you with other marketing information about our company, products or services (or those of our selected partners) to keep you informed of any events or promotions that we think may interest you
- send product updates and warranty information
- personalize your user experience or improve our site (refer to section 5 about cookies)
- run a promotion, contest, survey or other site feature, and notify you if you win
- inform you of corporate restructure or reorganisation or sale of our business or assets
- enforce our legal rights or defend legal proceedings and for general administration purposes
- pursue any employment enquiry you may make with us
- process personal data about you which is uploaded into our product by or on behalf of our customer (Content Personal Data) to comply with our contractual obligations to our customer.

3.5. Where we are required to do so to perform **our contract** with our customer, we will:

- administer your customer account and any orders you place with us
- provide our customer with our product and any associated services including technical support
- respond to customer service requests or other questions or concerns

3.6. We may process your information to comply with our **legal obligations** including assisting the Police, tax authorities or other authorised agencies.

4. How long do we keep your personal data?

4.1. In accordance with our Data Retention Policy, which is available upon request, we may retain your personal information for as long as your account is active or as needed to provide you or your company services, comply with our legal obligations, resolve disputes and enforce our agreements.

4.2. If you have expressed an interest in buying products or services from us or from our selected partners, we will retain your contact details and related information concerning your inquiry for three (3) years from the date that we last had contact with you.

4.3. If you have expressed an interest in working with us then, unless you are subsequently engaged by us, we will retain your personal data for a reasonable period of time depending on the role you have applied for. You can ask us to delete your personal data at any time, refer to section 11.

4.4. If you have purchased goods or services from us or from our selected partners:

4.4.1. We will keep the data relating to that purchase (e.g., order forms and invoices and related correspondence) for seven (7) years from the date of the contract.

4.4.2. We will keep the data you have provided to us for as long as your account is active.

4.4.3. If there is a dispute, we will keep the data you have provided to us for as long as is necessary until such dispute is resolved and finally settled.

4.5. Voicemail recordings and recordings of video or voice calls are kept for one (1) year.

4.6. If you are using our product:

- The data collected by the SaaS version of our product will be retained for the duration of the software license and sixty (60) days thereafter or any earlier date when the customer chooses to delete it. A copy of the data is retained in our data center for back-up purposes only for a further period of six (6) months.

- All Content Personal Data will be deleted either at the discretion of the user (where the customer provides such access to the user) or will be automatically deleted by us no later than sixty (60) days after the customer's service contract with us terminates.

4.7. If you have requested that we do not send you marketing information, we will always retain sufficient information to ensure that we remember to comply with your request.

4.8. The periods stated in this section 4 may be extended if we are required by law to keep your data for a longer period or in the event that we need to protect our legal rights.

4.9. You may request the deletion of your personal data at any time by emailing privacysupport@vasion.com and we will respond to your request within thirty (30) days, providing confirmation of deletion or reasons for retention if applicable.

5. Cookies, Links to Other URLs & Social Plug-ins on our Website

- 5.1.** We will use cookies and similar tracking technologies to analyze trends and track users' site movements only after obtaining your explicit consent, and we will provide clear options for you to opt-out at any time.
- 5.2.** Our use of cookies and other tracking technologies in our marketing operations is based on the choices you make in our preference centers which you may access from the footer of our websites or by clicking on a cookie icon that appears on our websites. We process your personal information through the tools provided to us by Amplitude, Adobe Analytics, Adobe Search Cloud (integrated into Google Ads) and 6sense to provide and enhance our advertising services and deliver content or ads of interest. Our use of personal information collected for marketing operations is limited to the following purposes:
 - targeting specific audiences based on users' location and interests related to the search query
 - personalizing the ads that users see based on their search queries
 - optimizing our campaigns based on front-end metrics provided by Google Ads (e.g., clicks and webpage impressions)
 - tracking the performance of our campaigns and measuring key metrics such as clicks, conversions, and return on investment to understand how our campaigns are performing and make data-driven decisions
 - adopting brand safety protection: ensuring we are not displaying our ads on unsafe or inappropriate websites, to protect our brand reputation.
 - adopting of fraud prevention in our campaigns to protect our campaigns from online fraud (e.g. click fraud).
- 5.3.** For more information about cookies generally and how to disable them you can visit: www.allaboutcookies.org.
- 5.4.** As is true of most websites, we gather certain information automatically. This information may include Internet protocol (IP) addresses, browser type, Internet service provider (ISP), referring/exit pages, the files viewed on our site (e.g., HTML pages, graphics, etc.), operating system, date/time stamp, and/or clickstream data to analyze trends in the aggregate and administer the site.
- 5.5.** Our site may contain links to and from other websites (e.g., social media sites such as Twitter, Flickr, YouTube and Facebook). Unless we own such websites, we accept no responsibility for the way in which they process your personal data. You are recommended to check the privacy policy of each website before you submit any personal data to it.
- 5.6.** We use so-called social plugins (buttons) of social networks such as Facebook, Google+, and Twitter.
- 5.7.** When you visit our site, these buttons are deactivated by default, i.e., without your intervention they will not send any data to the respective social networks. Before you can use these buttons, you must activate them by clicking on them. They then remain active until you deactivate them again or delete your cookies.
- 5.8.** After their activation, a direct link to the server of the respective social network is established. The contents of the button are then transmitted from the social network directly to your browser and incorporated in the site.
- 5.9.** After activation of a button, the social network can retrieve data, independently of whether you interact with the button or not. If you are logged on to a social network, the network can assign your visit to the site to your user account.
- 5.10.** If you are a member of a social network and do not wish it to combine data retrieved from your visit to our site with your membership data, you must log out from the social network concerned before activating the buttons.
- 5.11.** We have no influence on the scope of data that is collected by the social networks through their buttons. The data use policies of the social networks provide information on the purpose and extent of the data that they collect, how this data is processed and used, the rights available to you, and the settings that you can use to protect your privacy.

6. Tracking Analytics within the product

- 6.1** We will use third party analytics within the administrative console of our product only with your explicit consent for the purpose of analyzing trends, tracking admin users' movements around the console, gathering demographic information about our admin user base as a whole as well as providing support services directly to admin users such as access to product documentation and information.
- 6.2** The data automatically collected may include information from your web browser (such as browser type and browser language) and details of your visits to the admin console, including traffic data, logs about your login history, identity confirmation, page views, length of visit, and website navigation paths as well as information about your computer and internet connection, including your IP address and connecting software. We collect this data in order to help us provide, support, and improve our product and the admin user experience within our product.
- 6.3** Additionally, we may use similar technologies to collect information about the admin user's interaction with our product in a manner that allows us to reproduce and fix issues and to identify areas of improvement in our product. Admin console users can opt out of the use of this type of tracking technology by following the steps found here.

7. Will we share your personal data with any third parties?

- 7.1.** We may share your personal data with our subsidiaries as identified above but only to process the data for those purposes identified within this Privacy Policy.
- 7.2.** We partner with a third party to display advertising on our website or to manage our advertising on other sites. Our third-party partner may use cookies or similar technologies in order to provide you advertising based upon your browsing activities and interests. If you wish to opt out of interest-based advertising, click [here](#), or if located in the European Union click [here](#). Please note you will continue to receive generic ads.
- 7.3.** We may share your information with third party service providers who process personal information on our behalf for the purposes of providing services to us or to you directly on our behalf to help, e.g., advertising agencies, digital marketing service providers or administrative service providers. When we use third-party service providers, we only share personal data that is necessary for them to provide their services and we have a contract in place that requires them to keep your data secure and not to use it other than in accordance with our specific instructions. These services may include:
 - payment processing
 - providing customer service
 - sending marketing communications
 - conducting research and analysis

These processors include our payment processing providers (e.g., Stripe), website analytics providers (e.g., Adobe), tools we use to prevent spam and other security risks related to the abusive automated software (e.g., Cloudflare), online activities, product feedback or help desk software providers (e.g., Salesforce), CRM service providers (e.g., Salesforce), solutions we use to facilitate transactions (e.g., Tackle.io), tools to track marketing campaigns (e.g. LinkedIn Revenue Attribution), and e-mail service providers (e.g., Twilio).

You can obtain further details relating to our third-party service providers by contacting us using the details set out in section 2.

- 7.4.** If you use our products and services:
 - 7.4.1** We will share your personal data in order to provide cloud computing infrastructure. For the SaaS version of our product, a client is installed locally that communicates with our product which is hosted in Amazon Web Services which customers may elect to be stored on servers in the United States, or in the EEA. For more information about Amazon Web Services please refer to Compliance Resources – Amazon Web Services (AWS).
 - 7.4.2** We may share certain personal data, typically metadata, collected by our product with our staff in order to provide you with services or support as may be requested by you. Your data will be shared with only those staff who have a need to know in order to provide you with such services or support. All staff are bound by confidentiality agreements which are subject to labor laws.
 - 7.4.3** Content Personal Data is stored on AWS servers, and we have contractual provisions in place with AWS to ensure that the Content Personal Data is adequately protected to the standards required by EU and UK data protection laws.
 - 7.4.4** If you are an admin console user based in the US, we will also share certain personal data as listed in the table below.

Company	Type of data shared with Company	Purpose	Data Location
Intercom, Inc. https://www.intercom.com	username, user ID, email and Vasion instance URL for the Vasion SaaS admin console users only	In-application messaging and automation tool for improved customer experience	Data hosted in the US
SalesForce, USA https://www.salesforce.com	name, title, email address for Vasion SaaS admin console users only	Storage of admin user contact information used to engage with admin users for support and feedback	Data hosted in the US

Sprig, Inc. https://www.sprig.com	username, user ID, email and Vasion instance URL for Vasion SaaS admin console users only	To facilitate feedback surveys with admin users	Data hosted in the US
--------------------------------------	---	---	-----------------------

7.5. In certain situations, Vasion may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements or as otherwise required by law such as to comply with a subpoena or other legal processes. We will disclose personal data to public authorities only when and to the extent legally required to do so and will take all feasible measures to notify you of such request unless prohibited by law. If Vasion is involved in a (potential) merger, acquisition, or sale of all or a portion of its assets, with a third party, we may transfer your personal data to that party to ensure that it can continue to provide information that you have requested or for any of the other purposes that we have noted above. We may also disclose your personal data to any other third party with your prior consent.

8. Transferring your data outside of the European Economic Area (“EEA”)

8.1. The site is hosted on Amazon Web Services web servers in the United States. If you use our website and are located in a non-US jurisdiction, such as the European Economic Area (“EEA”), the European Union (“EU”) or the United Kingdom (“UK”), we will transfer data outside these jurisdictions to the United States and ensure that similar protections are afforded to the data as within the EEA, EU, or UK by implementing standard contractual clauses approved by the European Commission or other similar safeguards.

8.2. As it pertains to the use of our product, to lawfully transfer your personal data to our parent company and AWS in the U.S. we use legally approved standard data protection clauses for transfers from a controller to processor recognised or issued further to Article 46(2) of the EU GDPR and the UK GDPR.

8.3. Please contact us if you would like a copy of the standard data protection clauses that we have in place.

9. How do we keep your data safe?

The security of your personal information is important to us. We have robust information security management systems in place both internally and within our products to protect your personal information and we undergo security assessments by internal personnel and third parties, which include infrastructure vulnerability assessments and application security assessments. We implement industry-standard technical and organizational security measures, including encryption, access controls, and regular security audits, designed to protect your personal information. Details of these measures are available upon request.

10. Links

Our website contains links to other sites. Please be aware that Vasion is not responsible for the privacy practices of such other sites. We encourage our users to be aware when they leave our site and to read the privacy statements of each site that collects personally identifiable information.

11. What are your rights in relation to your data?

11.1. Data subjects have certain rights in relation to their personal data. The rights outlined in this section are available to you in relation to any personal data we process about you within the scope of this Privacy Policy. As for your personal data which is processed by our software product on behalf of our customer who has purchased the software (Content Personal Data), we only process Content Personal Data on behalf of our customers and therefore if you wish to invoke one of your rights please contact our customer directly, i.e., your employer or the third party that requested you to provide your personal data to it. If you wish to learn more about how our customer manages the Content Personal Data, you can do so by viewing a copy of the customer’s own privacy policy.

11.2. Your right to access data. We always aim to be as open as we can and allow people access to the personal data we hold about them. Where we hold your personal data, you can make a ‘subject access request’ to us and we will provide you with:

- a description of it
- an explanation of why we are holding it
- information about who it could be disclosed to

- a copy of the information in an intelligible form – unless an exception to the disclosure requirements is applicable.

If you would like to make a “subject access request” please make it in writing to our contact details in section 2 and mark it clearly as “Subject Access Request.” If you agree, we will try to deal with your request informally, for example, by providing you with the specific information you need over the telephone. Unless you agree to a different timeframe, we will complete your subject access request within one (1) month.

11.3. Right to stop marketing messages. You always have the right to stop marketing messages. We will usually include an unsubscribe button in any marketing emails. If you do wish to unsubscribe, please click the “unsubscribe” button and we will promptly action that request. Alternatively, you can update your marketing preferences by contacting us at any-time or when we contact you.

11.4. Right to be forgotten. You may request the deletion of your personal data at any time by emailing privacysupport@vasion.com and we will respond to your request within thirty (30) days, providing confirmation of deletion or reasons for retention, if applicable.

11.5. Right to restrict data. If we hold personal data about you and you believe it is inaccurate, you have the right to request us to restrict the data until it is verified. You also have the right to request that the data is restricted where you have a right to it being deleted but would prefer that it is restricted.

11.6. Transferring your personal data. You can ask us to send your personal information directly to another service provider, and we will do so if this is technically possible. We may not provide you with a copy of your personal information if this concerns other individuals or we have another lawful reason to withhold that information.

11.7. Right to complain. You always have the right to complain to the personal data regulator in your country which can be located at http://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index_en.htm.

12. Changes to this Privacy Policy

We may update this Privacy Policy to reflect changes to our information practices. We encourage you to periodically review this page for the latest information on our privacy practices.