Crowdfire Inc.

Privacy Policy

Last modified: March 9, 2022

1. Introduction

In this policy, "**we**", "**us**", " **our**" and "**Crowdfire**" refer to Crowdfire Inc. and its subsidiary Codigami Labs PVT Ltd. For more information about us and how to contact us, see Section 11.

We respect your privacy and are committed to protecting it through our compliance with this Policy.

This privacy policy ("**Policy**") applies when we are acting as a data controller with respect to the personal data of our users. This Policy describes how we collect, use and share personal data of consumer users across our websites, including www.crowdfireapp.com (the "**Website**"), Crowdfire's mobile application (the " **App**") and services offered to users (collectively with the Website and the App, the "**Services**"), and from our partners and other third parties. When using any of our Services you consent to the collection, transfer, storage, disclosure, and use of your personal data as described in this Policy.

Please read this Policy carefully to understand our policies and practices regarding your personal data and how we will treat it. By accessing or using the Services, you agree to this Policy. Our Services also incorporate privacy controls which affect how we will process your personal data. Please refer to Section 5 for a list of rights with regard to your personal data and how to exercise them.

This Policy may change from time to time. Your continued use of the Services after we make changes is deemed to be acceptance of those changes, so please check the Policy periodically for updates.

2. Information We Collect About You and How We Collect It

There are three general categories of information we collect.

2.1. Information You Give to Us.

a. We collect your account data, which may include your name, email address ("**Account Data**"). The Account Data may be processed for the purposes of providing to you our Services and of ensuring their security, maintaining back-ups of our databases and communicating with you. This information is necessary for the adequate performance of the contract between you and us and to allow us to comply with our legal obligations. Without it, we may not be able to provide you with all the requested Services.
b. We process information that you post for publication through our Services ("**Publication Data**"), including the content that you share to your social profiles. The Publication Data is processed for the purposes of enabling such publication and administering our Services. The legal basis for this processing is the performance of a contract between you and us and/or taking steps, at your request, to enter into such a contract. Without it, we may not be able to provide you with all the requested Services.
c. We process financial information such as credit card or PayPal information when you order Services in order to facilitate the processing of payments ("**Payment Information** "). The legal basis for this processing is the performance of a contract between you and us and/or taking steps, at your request, to enter into such a contract and our legitimate interests, namely our interest in the proper administration of our website and business.
d. We may process information contained in or relating to any communication that you send to us (" **Correspondence Data**"). The Correspondence Data may include the communication content and metadata associated with the communication. The correspondence data may be processed for the purposes of communicating with you and record-keeping. The legal basis for this processing is our legitimate interests, namely the proper administration of our website and business and communications with users.
e. We may process information included in your personal profile, which may include your location, time zone and website (" **Profile Data**"). The Profile Data may be processed for the purposes of providing you a better user experience when using the Services. The legal basis for this processing is your consent.

2.2. Information We Automatically Collect from Your Use of the Services.

1. When you use the Services, we may automatically process information about your computer and internet connection (including your IP address, operating system and browser type), your mobile carrier, device information (including device and application IDs), search terms, cookie information, as well as information about the timing, frequency and pattern of your service use ("**Service Data**"). The Service Data is processed for the purpose of providing our Services. The legal basis for this processing is the adequate performance of the contract between you and us, to enable us to comply with legal obligations and our legitimate interest in being able to provide and improve the functionalities of the Services.

2.3. Information We Collect from Third Parties.

a. You may choose to connect the Services to your accounts on third party services such as Twitter, Facebook, Instagram, Tiktok, Linkedin, Pinterest, Shopify, Etsy, Twitch, Wordpress and Youtube (" **Social Networking Service**") for the purpose of managing your social media presence through our Services. Crowdfire uses a third party vendor (Zapier) to facilitate your connection to the Social Networking Services. When you do this, we automatically process personal information about you on such Social Networking Services, including your account and profile data, RSS, lists of followers, social media content and your actions with respect to such content (the " **Social Media Information**"). The Social Media Information is processed for the purposes of optimizing your social media activity on the Social Networking Services and administering our Services. The legal basis for the processing of Social Media Information is the performance of a contract between you and us and/or taking steps, at your request, to enter into such a contract.

3. Disclosure of Personal Data

3.1. We may disclose your personal data to any member of our group of companies (this means our subsidiaries, our ultimate holding company and all its subsidiaries) insofar as reasonably necessary for the purposes, and on the legal bases, set out in this policy.
3.2. Financial transactions relating to the Services are handled by our payment services providers, Paypal, Braintree and Stripe. We will share Payment Information with our payment services providers only to the extent necessary for the purposes of processing your payments, refunding such payments and dealing with complaints and queries relating to such payments and refunds. You can find information about the payment services providers' privacy policies and practices at https://www.paypal.com/in/webapps/mpp/ua/privacy-full , https://www.braintreepayments.com/leg and https://stripe.com/us/privacy/ .
3.3. We may disclose personal data to Social Networking Services insofar as reasonably necessary to allow you to manage your social media presence through our Services.
3.4. We may disclose Service Data to a variety of third party service providers insofar as reasonably necessary to improve the functionalities of the Services. For example, we may disclose Service Data to obtain useful analytics, provide in-app support to mobile app users, determine location data and provide search engine functionality to our users.
3.5. We may share aggregated data (information about our users that we combine together so that it no longer identifies or references an individual user) and other anonymized information for regulatory compliance, industry and market analysis, demographic profiling, marketing and advertising, and other business purposes.
3.6. In addition to the specific disclosures of personal data set out in this Section 3, we may disclose your personal data if we believe that it is reasonably necessary to comply with a law, regulation, legal process, or governmental request; or in order to protect your vital interests or the vital interests of another natural person; to protect the safety or integrity of the Services, or to explain why we have removed content or accounts from the Services; or to address fraud, security, or technical issues; or to protect our rights or property or the rights or property of those who use the Services.
3.7. We offer individuals the opportunity to choose (opt out) whether their personal information is (i) to be disclosed to a third party or (ii) to be used for a purpose that is materially different from the purpose(s) for which it was originally collected or subsequently authorized by the individuals. In order to opt out from disclosure of your personal information, please email us at hello@crowdfireapp.com.

4. International transfers of your personal data

In this Section 4, we provide information about the circumstances in which your personal data may be transferred to countries outside the European Economic Area (EEA). We and our other group companies have offices and facilities in the United States and India. To facilitate our operations we may transfer, store, and process your information within those countries or with service providers based in Europe, India, Asia Pacific and North America. Laws in these countries may differ from the laws applicable to your Country of Residence. For example, information collected within the EEA may be transferred, stored, and processed outside of the EEA for the purposes described in this Privacy Policy. Where we transfer store, and process your personal information outside of the EEA we have ensured that appropriate safeguards are in place to ensure an adequate level of data protection.

4.1. EU-US Privacy Shield Framework

a. In addition, Crowdfire complies with the EU-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of Personally Identifiable Information transferred from the European Union to the United States. Crowdfire has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, please visit https://www.privacyshield.gov/.
b. Individuals may file a complaint concerning Crowdfire's processing of their Personally Identifiable Information. Crowdfire will take steps to remedy issues arising out of its alleged failure to comply with the Privacy Shield Principles. Individuals may contact Crowdfire as specified below about complaints regarding the company's Personally Identifiable Information practices.
c. Where Crowdfire has transferred personal information of EU residents to third parties, Crowdfire shall be liable if those third parties do not process personal information in compliance with the Privacy Shield Principles. This shall not be the case where Crowdfire establishes that it is not responsible for the damage caused by the third party.
d. If an Individuals' complaint cannot be resolved through Crowdfire's internal processes, Crowdfire will cooperate with JAMS pursuant to the JAMS International Mediation Rules, available on the JAMS website at www.jamsadr.com/international-mediation-rules. Individuals may launch a Privacy Shield case by visiting https://www.jamsadr.com/eu-us-privacy-shield. JAMS mediation may be commenced as provided for in the relevant JAMS rules. The mediator may propose any appropriate remedy, such as deletion of the relevant Personally Identifiable Information, publicity for findings of noncompliance, payment of compensation for losses incurred as a result of noncompliance, or cessation of processing of the Personally Identifiable Information of the Individual who brought the complaint. The mediator or the individual also may refer the matter to the U.S. Federal Trade Commission, which has Privacy Shield investigatory and enforcement powers over Crowdfire. Under certain circumstances, Individuals also may be able to invoke binding arbitration to address complaints about Crowdfire's compliance with the Privacy Shield Principles.

4.2. Transfers to our subsidiary in India, to our service providers and other third parties will be protected by appropriate safeguards, namely the use of standard data protection clauses adopted or approved by the European Commission or applicable certification schemes - for example, the EU - U.S. Privacy Shield Framework.

5. Your Rights with Regard to Personal Data

In this Section 5, we have summarized the rights that you have under data protection law. Some of the rights are complex, and not all of the details have been included in our summaries. Accordingly, you should read the relevant laws and guidance from the regulatory authorities for a full explanation of these rights.

5.1 Your principal rights under data protection law are:

a. the right to access;
b. the right to rectification;
c. the right to erasure;
d. the right to restrict processing;
e. the right to object to processing;
f. the right to data portability;
g. the right to complain to a supervisory authority; and
h. the right to withdraw consent.

5.2. You have the right to confirmation as to whether or not we process your personal data and, where we do, access to the personal data, together with certain additional information. That additional information includes details of the purposes of the processing, the categories of personal data concerned and the recipients of the personal data. Providing the rights and freedoms of others are not affected, we will supply to you a copy of your personal data. The first copy will be provided free of charge, but additional copies may be subject to a reasonable fee. You can access your personal data by following the instructions here .
5.3. You have the right to have any inaccurate personal data about you rectified and, taking into account the purposes of the processing, to have any incomplete personal data about you completed. You can request correction or modification of your personal data by following the instructions here.
5.4. In some circumstances you have the right to the erasure of your personal data without undue delay. Those circumstances include: the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; you withdraw consent to consent-based processing; you object to the processing under certain rules of applicable data protection law; the processing is for direct marketing purposes; and the personal data have been unlawfully processed. However, there are exclusions of the right to erasure. The general exclusions include where processing is necessary: for exercising the right of freedom of expression and information; for compliance with a legal obligation; or for the establishment, exercise or defense of legal claims. You can request the deletion of your account by following the instructions here.
5.5. In some circumstances you have the right to restrict the processing of your personal data. Those circumstances are: you contest the accuracy of the personal data; processing is unlawful but you oppose erasure; we no longer need the personal data for the purposes of our processing, but you require personal data for the establishment, exercise or defense of legal claims; and you have objected to processing, pending the verification of that objection. Where processing has been restricted on this basis, we may continue to store your personal data. However, we will only otherwise process it: with your consent; for the establishment, exercise or defence of legal claims; for the protection of the rights of another natural or legal person; or for reasons of important public interest. You can manage your privacy settings and other account features here .
5.6. You have the right to object to our processing of your personal data on grounds relating to your particular situation, but only to the extent that the legal basis for the processing is that the processing is necessary for: the performance of a task carried out in the public interest or in the exercise of any official authority vested in us; or the purposes of the legitimate interests pursued by us or by a third party. If you make such an objection, we will cease to process the personal data unless we can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms, or the processing is for the establishment, exercise or defence of legal claims.
5.7. You have the right to object to our processing of your personal data for direct marketing purposes (including profiling for direct marketing purposes). If you make such an objection, we will cease to process your personal data for this purpose.
5.8. You have the right to object to our processing of your personal data for scientific or historical research purposes or statistical purposes on grounds relating to your particular situation, unless the processing is necessary for the performance of a task carried out for reasons of public interest.
5.9. To the extent that the legal basis for our processing of your personal data is:

a. consent; or
b. that the processing is necessary for the performance of a contract to which you are party or in order to take steps at your request prior to entering into a contract, and such processing is carried out by automated means, you have the right to receive your personal data from us in a structured, commonly used and machine-readable format. However, this right does not apply where it would adversely affect the rights and freedoms of others. You can download your account information, by following the instructions here.

5.10. To the extent that the legal basis for our processing of your personal data is consent, you have the right to withdraw that consent at any time. Withdrawal will not affect the lawfulness of processing before the withdrawal.
5.11. You may exercise any of your rights in relation to your personal data by written notice to us, in addition to the other methods specified in this Section 5.

6. Retaining and deleting personal data

6.1. This Section 6 sets out our data retention policies and procedure, which are designed to help ensure that we comply with our legal obligations in relation to the retention and deletion of personal data.
6.2. Personal data that we process for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6.3. We generally retain your personal information for as long as is necessary for the performance of the contract between you and us and to comply with our legal obligations. If you no longer want us to use your information to provide the Services to you, you can request that we erase your personal information and close your account.
6.4. Notwithstanding the other provisions of this Section 6, we may retain your personal data where such retention is necessary for compliance with a legal obligation to which we are subject, or in order to protect your vital interests or the vital interests of another natural person.

7. Children

Our Services are not intended for children. You must also be old enough to consent to the processing of your personal data in your country without parental consent. No one under age 13 may provide any personal data through the Services. We do not knowingly collect personal data from children under 13. If you are under 13, do not use or provide any information through the Services or on or through any of their features or register an account, make any purchases through the Services, use any of the interactive features of the Services or provide any information about yourself to us, including your name, address, telephone number, e-mail address or any screen name or user name you may use. If we learn we have collected or received personal data from a child under 13, we will delete that information. If you believe we might have any information from or about a child under 13, please contact us at hello@crowdfireapp.com.

8. Cookies

8.1. About cookies

a. A cookie is a file containing an identifier (a string of letters and numbers) that is sent by a web server to a web browser and is stored by the browser. The identifier is then sent back to the server each time the browser requests a page from the server.
b. Cookies may be either "persistent" cookies or "session" cookies: a persistent cookie will be stored by a web browser and will remain valid until its set expiry date, unless deleted by the user before the expiry date; a session cookie, on the other hand, will expire at the end of the user session, when the web browser is closed.
c. Cookies do not typically contain any information that personally identifies a user, but personal information that we store about you may be linked to the information stored in and obtained from cookies.
d. We also use other technologies with similar functionality to cookies, such as web beacons, web storage, and unique advertising identifiers, to collect information about your activity, browser, and device.

8.2. We use these technologies for the following purposes:

a. to identify you and log you into the Services;
b. to store information about your preferences and to personalise the Services for you;
c. as an element of the security measures used to protect user accounts, including preventing fraudulent use of login credentials, and to protect our website and services generally;
d. to help us display content that will be relevant to you;
e. to help us analyse the use and performance of the Services ; and
f. to store your preferences in relation to the use of cookies more generally.

8.3. Cookies used by our service providers

a. We use the following service providers to analyse the use of the Services. Each service provider gathers information about the Services by means of cookies and this information is used to create reports about with usage information. You can find information about the service providers' privacy policies and practices at the URLs set forth below:

Service Provider - Analytics	Privacy Policy
Google Analytics / Fabric / Crashlytics	https://support.google.com/analytics/answer/6004245
Branch	https://branch.io/policies/#privacy
Mixpanel	https://mixpanel.com/legal/privacy-policy/
Clevertap	https://clevertap.com/privacy-policy/
AppsFlyer	https://www.appsflyer.com/privacy-policy/
Freshdesk's Mobihelp SDK	https://www.freshworks.com/privacy/
Foursquare Labs	https://foursquare.com/legal/privacy
Algolia	https://www.algolia.com/policies/privacy
Honeybadger	https://www.honeybadger.io/privacy/
Superfeedr	https://superfeedr.com/privacy/
Cloudniary	https://cloudinary.com/privacy/
Cloudflare	https://www.cloudflare.com/privacypolicy/
AWS	https://aws.amazon.com/privacy/
Headway	https://headwayapp.co/privacy/
Webhose	https://webhose.io/privacy/
Unsplash	https://unsplash.com/privacy/
Pixabay	https://pixabay.com/service/privacy/
Feedly	https://feedly.com/i/legal/privacy/
Firebase	https://firebase.google.com/support/privacy/
Giphy	https://support.giphy.com/hc/en-us/articles/360020028332-GIPHY-Privacy-Policy/

8.4 Managing cookies

a. Most browsers allow you to refuse to accept cookies and to delete cookies. The methods for doing so vary from browser to browser, and from version to version.
b. Your mobile device may allow you to control cookies through its settings function. Refer to your device manufacturer's instructions for more information.
c. If you choose to decline cookies, some parts of the Services may not work as intended or may not work at all.

9. Data Security

9.1. We have implemented measures designed to secure your personal data from accidental loss and from unauthorized access, use, alteration and disclosure. The safety and security of your information also depends on you. Where we have given you (or where you have chosen) a password for access to certain parts of the Services, you are responsible for keeping this password confidential. We ask you not to share your password with anyone.
9.2. Steps taken to ensure data security:

a. All the user information can only be accessed by authorized users;
b. Users need to authenticate themselves with a username-password combination; and
c. All data is hosted on Amazon AWS servers.

9.3. Unfortunately, the transmission of information via public networks such as the internet is not completely secure. Although we do our best to protect your personal data, we cannot guarantee the security of your personal data transmitted through the Services. Any transmission of personal data is at your own risk. We are not responsible for the circumvention of any privacy settings or security measures contained on the Services.

10. Changes to Our Privacy Policy

a. It is our policy to post any changes we make to our Policy on this page. If we make material changes to how we treat our users' personal data, we will notify you by e-mail to the primary e-mail address specified in your account. The date the Policy was last revised is identified at the top of the page. You are responsible for ensuring we have an up-to-date active and deliverable e-mail address for you, and for periodically visiting our Website and this Policy to check for any changes.

11. Contact Information

The data controller responsible for your personal data is Crowdfire Inc. Please contact us by email at hello@crowdfireapp.com or by post at:

Crowdfire Inc.

16192 Coastal Highway

Lewes, DE 19958

United States

12. Privacy Notice For California Residents

This section applies solely to consumers who reside in the State of California.

If you are a California resident, and you wish to access your personal data, request from us that we delete your personal information, or require information about our disclosure practices, you can choose to send us a verifiable consumer request by email at hello@crowdfireapp.com, in addition to using the means set forth above.

In our assessment, we do not "sell" your personal information to third parties for monetary or other valuable consideration.

13. Crowdfire as Data Processor

All transfers of your Personal Data out of the European Union, European Economic Area, and Switzerland are governed by the Standard Contractual Clauses which are incorporated into our standard data processing addendum. Crowdfire will abide by the requirements of European Economic Area and Swiss data protection law regarding the collection, use, transfer, retention, and other processing of Personal Data from the European Economic Area and Switzerland. All transfers of Personal Data to a third country or an international organization will be subject to appropriate safeguards as described in Article 46 of the GDPR and such transfers and safeguards will be documented according to Article 30(2) of the GDPR.

14. Standard Contractual Clauses

The below provisions and the applicable standard contractual clauses referenced below shall be deemed automatically incorporated into the relevant agreement (the "Agreement") that is concluded between Crowdfire Inc., on behalf of itself and its affiliates ("Crowdfire"), and you ("Business Partner") and shall be binding upon the parties to the Agreement (including their affiliates), by virtue of reference to this page in and signature of such Agreement.

For data transfers from the European Economic Area that are subject to the 2021 Standard Contractual Clauses as implemented by the Commission Implementing Decision (EU) 2021/914 of June 4th, 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (the "2021 Standard Contractual Clauses"), the 2021 Standard Contractual Clauses will apply in the following manner:

1. Module One (Transfer controller to controller) will apply to the extent that Crowdfire acts as controller and Business Partner acts as controller.
2. Module Two (Transfer controller to processor) will apply to the extent that Crowdfire acts as controller and Business Partner acts as processor; and
3. Module Three (Transfer processor to processor) will apply to the extent that Crowdfire acts as processor and Business Partner acts as sub-processor.

For each Module, where applicable:

1. in Clause 7, the option docking clause will not apply;
2. in Clause 9, Option 2 will apply, and the time period for prior notice of sub-processor changes will be 10 days;
3. in Clause 11, the optional language will not apply;
4. in Clause 17 (Option 1), the 2021 Standard Contractual Clauses will be governed by Irish law.
5. in Clause 18(b), disputes will be resolved before the courts of Ireland;
6. In Annex I, Part A:
   a. Data Exporter: Crowdfire Inc.
      i. Contact Details: Crowdfire Privacy Team – hello@crowdfireapp.com.
      ii. Data Exporter Role: the Data exporter processes personal data in connection with its business activities such as client services and other business operations.
      iii. Signature & Date: By entering into the Agreement, Data Exporter is deemed to have signed these Standard Contractual Clauses incorporated herein, including their Annexes, as of the Effective Date of the Agreement.
   b. Data Importer: Business Partner and authorized affiliates of Business Partner.
      i. Contact Details: the email address(es) to which Business Partner elects to receive privacy communications in the Agreement.
      ii. Data Importer Role: Data importer provides services to data exporter as required for the latter to accomplish its legitimate business purposes and as described in or instructed by the data exporter pursuant to the relevant services agreement entered into by the Parties.
      iii. Signature & Date: By entering into the Agreement, Data Importer is deemed to have signed these Standard Contractual Clauses, incorporated herein, including their Annexes, as of the Effective Date of the Agreement.

7. In Annex I, Part B:
   a. The categories of Data Subjects to whom the Personal Data relates include the individuals about whom data is provided to Business Partner via the Services (as defined in the Agreement) by (or at the direction of) Data Exporter.
   b. The categories of personal data transferred include data relating to Data Subjects provided to Business Partner via the Services by (or at the direction of) Data Exporter.
   Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.
   c. The frequency of the transfer is a continuous basis for the duration of the Agreement.
   d. The nature of the processing. Detailed in Agreement.
   e. The purpose of the processing of personal data by Data Importer is the performance of the Services pursuant to the Agreement with Data Exporter.
   f. The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period: Crowdfire will process stored Personal Data for the purpose of providing the Services until Data Exporter elects to delete such Personal Data via the Services or in accordance with the Agreement.
   g. For transfers to sub-processors, the subject matter, nature, and duration of the processing: Personal Data may be transferred to sub-processors to process data, on Data Importer's behalf, consistent with Data Exporter's instructions to data importer and data importers published documentation. Data Importer makes available to Data Exporter a current list of sub-processors engaged in connection with the Services with the identities of those sub-processors in its documentation (at). Notice of additions or changes to the list of sub-processors will be provided to Data Exporter from time to time.

8. In Annex I, Part C: The Irish Data Protection Commission will be the competent supervisory authority.
9. Schedule 2 serves as Annex II of the Standard Contractual Clauses.