Battlefinity Privacy Policy

Last Updated: (August 12, 2025)

Thank you for using Battlefinity! This Privacy Policy explains what information we collect when you use the Battlefinity mobile app and related services (collectively, the “**Service**” or “**App**”), how we use and share that information, and your rights in relation to that information. We are committed to protecting your privacy and handling your personal data in an open and transparent manner.

By using Battlefinity, you agree to the collection and use of information in accordance with this Privacy Policy. If you do not agree with our practices, please do not use the App. We may update this Privacy Policy from time to time (see **Changes to This Privacy Policy** below), and we will notify you of any significant changes.

Who We Are

Battlefinity is developed and operated by **Loadout Sàrl** (“**Company**”, “**we**”, “**us**” or “**our**”), a company based in Geneva, Switzerland. For the purposes of data protection laws, Loadout Sàrl is the “data controller” of your personal information when you use our App (this means we are responsible for deciding how to collect, use, and protect your data). Our contact information is provided at the end of this policy (see **Contact Us**).

Our App is distributed globally via the Apple App Store and Google Play Store. As such, we strive to comply with privacy laws applicable to our users, including but not limited to the **General Data Protection Regulation (GDPR)** in the European Union, the **California Consumer Privacy Act (CCPA)** in the United States, and other applicable data protection laws. We also adhere to platform-specific privacy requirements from Apple and Google, and Firebase’s policies for user data.

No Age Restriction (Use by Minors): Battlefinity does not enforce a strict age restriction for its users; however, it is not directed at children under 13, and we do not knowingly collect personal data from children under 13 without verifiable parental consent. If you are under 13 (or under the minimum age required by the laws of your jurisdiction), you should use the App only with parental or guardian supervision and consent. Parents or guardians who believe their child under 13 may have provided personal data to us should contact us immediately so we can delete such information (see **Children’s Privacy** below for more details).

Information We Collect

We aim to **minimize** the personal data we collect and **only collect what is necessary** to provide and improve the Service. In fact, Battlefinity is designed so that you can use it without providing sensitive personal information like your full name, address, or phone number. We do **not** ask you for such PII (Personally Identifiable Information) and we do not store what is traditionally considered sensitive PII. That said, certain information is collected in order for the App to function (for example, an account identifier) and for us to understand how the App is used (analytics). Below, we describe the categories of information we collect:

1. Information You Provide Directly:

- **Account Information:** When you create an account on Battlefinity, you provide certain information. This may include:

    - **Email Address:** If you sign up with email and password, we collect your email address for account verification, login, and communication purposes. *(Note: If you sign up using a third-party authentication like "Sign in with Apple" or Google, we may receive either your email or an anonymous identifier from those services. If using Apple's "Hide My Email" feature, we get a proxy email that forwards to your real email without us seeing it.)*

    - **Authentication Credentials:** If using email sign-up, we collect your password (stored in a secure hashed form – we cannot read your actual password). For third-party logins, we don't collect your password to those services, but we get a token/ID to authenticate you via Firebase.

    - **Username/Profile Name:** You may set a public username or handle for your Battlefinity profile. This can be a nickname or alias and does not have to be your real name. This name will be visible to others, so please do not use personal information you don't want to share.

    - **Profile Details:** The App may allow you to add optional information to your profile (such as a profile picture/avatar, a short bio, links to your gaming accounts or social media). All such information is optional and, if provided, will be visible to other users. We do not require any profile field that would be considered sensitive (like age, gender, real name, etc.), and you should not include such details if you want to keep them private.

- **User-Generated Content:** This includes any content you post or upload on Battlefinity, such as:

    - **Loadouts and Descriptions:** The core of Battlefinity is user-posted game loadouts (weapon/equipment setups) with descriptions. If you post a loadout, we store the information you provide (e.g., the configuration of the loadout, your textual description, any title or tags). The description text you write is stored on our servers (via Firebase) and associated with your account. Please note this content is public to other users of the App. **Do not include private or sensitive info** about yourself or others in these descriptions.

  - **Likes and Follows:** When you "like" a loadout or follow another user, we record that interaction (so that we can display like counts and your feed of followed creators). This is part of your usage data but tied to your account identity (so we know which posts you liked or who you follow). Other users may see that you liked their loadout (we might show a username who liked a post), and users can see followers/following lists for profiles. If you prefer to use the App more privately, you may choose not to engage in liking/following, but those features are inherently social.

  - **Comments or Messages (if applicable):** Currently, Battlefinity does not have a feature for commenting on posts or direct messaging. If we introduce any communication features, any messages or comments you submit would be collected and stored. We will update this policy if such features are added.

  - **User Support Inquiries:** If you contact us for support or feedback (for example, via email or an in-app support form), we collect the information you choose to give us (such as your email address, description of the issue, screenshots, etc.) and any additional info needed to help resolve your query. Support communications may be stored for reference.

We **do not collect** any financial information from you directly. All subscription purchases are handled by Apple or Google, so we never see your credit card number or banking details. We do receive transaction confirmations from the app stores (via RevenueCat) to know that you purchased a subscription, but that data is limited to things like an anonymous transaction ID, subscription tier, and expiry date. We also do not collect any government-issued IDs, social security numbers, or any similarly sensitive personal identifiers.

2. Information We Collect Automatically:

When you use Battlefinity, certain information gets collected automatically from your device and about how you use the App. This includes:

- **Device Information:** We may collect information about the device you use to access the App. This includes data like: device model (e.g., iPhone 12, Samsung Galaxy S21), operating system and version (e.g., iOS 16 or Android 13), unique device identifiers or advertising ID (if allowed – note, we do **not** use IDFA for advertising, since we have no ads; if our analytics or RevenueCat SDK uses an ID for their legitimate functions, we ensure it's not used for ad tracking), language setting, region or locale setting (e.g., "en-US" for English, United States), and the app version installed. We might also collect network information such as IP address and network provider (this is usually ephemeral and used for communication routing and security). IP address may also give a coarse indication of your location (city or country level), which we use for things like language or regional analytics. We do not collect or derive precise GPS location.

- **Usage Data & Analytics:** We use **Firebase Analytics** and **Google Analytics for Firebase** (these services are part of Google) to collect data about how the App is used. This usage data includes events like: screens or features you access, buttons or links you tap, time spent in the app, crash logs, and other interaction information. For example, we might log that "User X opened the app and viewed 5 loadouts, liked 2 loadouts, then visited the subscription screen." These analytics events help us understand feature popularity and identify issues. The data collected typically includes timestamps and event types, along with device information (as described above). Google Analytics may also collect certain identifiers such as your Firebase Installation ID (a random ID assigned to your app install) or Advertising ID (which, as mentioned, we do not use for ads, but may still be counted as an "Identifier" in App Privacy disclosures). We have configured Analytics in line with platform guidelines to ensure it's used for **App functionality and analytics purposes**, not for ad tracking. For instance, Apple's App Store privacy disclosures require us to state that we collect **"Usage Data"** and **"Diagnostics"** for analytics, and possibly **"Device or Other Identifiers"**, but all such data is used internally to improve the app and is **not linked to your identity** where feasible (we rely on random IDs rather than names).

- **Crash and Performance Data:** We may use tools like **Firebase Crashlytics** (not explicitly mentioned in the user's question, but commonly used with Firebase) or other logging to collect crash reports and performance metrics. These help us debug issues. Crash reports typically include technical info like device model, OS, stack trace of the error, and potentially user IDs. We treat crash data as diagnostic and don't use it for marketing.

- **RevenueCat Data:** We integrate **RevenueCat** SDK for managing subscriptions across iOS and Android. RevenueCat by default uses an **anonymous user identifier** unless we choose to associate it with our own user ID. We currently link the RevenueCat customer record to your Firebase user ID (which is a random UID, or possibly hashed email). RevenueCat collects data necessary for subscription management, such as purchase receipts, the status of your subscription (active, canceled, expiration date), and purchase history (like which products you've bought). This data helps us unlock premium features for you across devices and maintain your subscription status. RevenueCat does **not** collect your payment info (credit card, etc.) and does not collect personal info like your name or email unless we provide it (we generally do not, aside from an internal user ID). It does collect **purchase history** and might use device identifiers to ensure a purchase is tied to the correct user/device. All communication with RevenueCat is encrypted. We ensure that RevenueCat is configured in a privacy-friendly way (e.g., using their **anonymous ID** feature where possible).

- **Log Information:** Like most online services, our servers (or the Firebase backend) automatically record certain log information when you use the app. These logs may include information such as your IP address, device type, app version, the pages or features you accessed, the time and date of each request, how you interacted with the Service, and other diagnostic data. We use log data primarily to troubleshoot issues and monitor the health of the service (for example, to detect and fix errors or to prevent abuse).

We want to emphasize that we **do not collect any of the following**: your address, phone number, financial information, health information, biometric data, or any sensitive personal fields like ethnicity, political opinions, or religious beliefs. We also do not collect any **precise location** data (no GPS). Any location-related data is limited to coarse info like country or region derived from your IP or locale settings, used for analytics and to localize content.

3. Information from Third-Party Sign-Ins or Services: If you choose to link or sign up via a third-party account (such as Google or Apple sign-in), we receive information from those services to authenticate you. For example:

- **Sign in with Apple:** We get a unique Apple-generated user ID and (if you choose to share) your name and email. If you use “Hide My Email”, we get a random Apple relay email that forwards to your real email (Apple doesn’t share your real email unless you permit). We use the email for account creation and may use it for password resets or important communication. If Apple only provides us an anonymous relay email, we treat that as your contact email. We do not collect any other data from Apple.

- **Google Sign-In:** We would get your Google account basic info (name, email) and a unique ID token. We primarily use the email to create/identify your account and for communication. We do not request access to your Google Drive or contacts or anything beyond basic profile info needed for login.

If in the future we integrate other social or gaming accounts (e.g., linking your game account to import stats), we will update this policy. Currently, Battlefinity does not pull data from game publisher APIs; loadouts are user-entered, not fetched from your game account.

4. Cookies and Tracking Technologies: Because Battlefinity is a mobile app, it does not use “cookies” in the same way a website does. However, the SDKs and services we use (Firebase, Google Analytics, RevenueCat) may use unique identifiers or similar technologies within the app’s context to remember your device or track usage. For example, Google Analytics might assign a **Instance ID** or use the device’s Advertising ID (though we have disabled any Ad features). These function akin to cookies by identifying an app instance. We do not use webview trackers or embed content that sets cookies, except if you follow a link (like to YouTube or an external site) – in which case that external site might set cookies in your device’s web browser. Those are outside our control and governed by the third-party’s cookie policies.

In summary, Battlefinity's **data collection is very limited**. Most personal data is what you choose to provide (email, username, content) and basic technical info for functionality. Even though we strive to not collect PII, certain data we collect (like an email or an IP address) could be considered personal data under privacy laws, so we handle it with care and transparency. And as mentioned, **we do not collect sensitive personal data** such as your real name (unless you volunteer it), physical address, contacts, photos, or other private files from your device.

How We Use Your Information

We use the information we collect for the following purposes, and we rely on various legal bases under data protection law (such as your consent, the necessity to perform a contract with you, and our legitimate interests) to do so:

- **To Provide and Maintain the Service:** We use your information to operate Battlefinity and provide its core functionalities. For example:
  - We use your login credentials (email/ID and password or token) to authenticate you and let you access your account.
  - We use your posted content (loadouts, etc.) to display it to you and other users as part of the App's content feed.
  - If you like or follow, we use that info to update counters, and to populate your personalized content (like showing posts from creators you follow).
  - We keep your account data so that each time you return, your profile and content are intact.
  - If you're a subscriber, we use your subscription status to grant access to premium features. We verify subscription receipts with RevenueCat to ensure you're entitled to what you paid for.
  - We may use device information and operating system info to ensure compatibility and troubleshoot (for instance, if a feature only fails on a certain OS version, we need that info to fix it).
- In these cases, processing your data is necessary **to fulfill our contract with you** (i.e., to provide the services you requested) and our legitimate interest in running an effective service.
- **To Improve, Personalize, and Develop the Service:** We analyze usage data and feedback to understand how our App is used and how we can make it better. This includes:

  - Using analytics data to identify popular features or areas where users drop off, so we can improve the user experience. For example, if analytics show most users skip a certain tutorial or struggle with a feature, we might redesign it.

  - Personalizing some aspects of the experience for you. For instance, we might highlight new loadouts from games you seem interested in (based on which loadouts you view or like). Or we could rank content in a feed in a way that is more relevant (though currently content is mostly chronological or by popularity). Any personalization uses in-app activity and is aimed at improving content relevance.

  - Monitoring and fixing technical issues. Crash logs and error reports help us find and fix bugs to improve app stability.

  - Conducting data analysis and testing. We might run A/B tests using analytics to try out new features on a subset of users and see how they perform.

- We typically rely on **legitimate interests** to process data for improvement and personalization – we have an interest in understanding how our service is used and making it better, and this processing does not outweigh your privacy rights (especially since much of it uses aggregated or pseudonymized data). In some contexts, we might ask for consent – for example, if in the future we introduce push notification preferences or if any analytics would require user consent in certain regions (like Europe, where we might offer an opt-out of certain analytics per GDPR). As of now, our use of Google Analytics for Firebase is configured to respect privacy (no ad-sharing, honoring any “limit ad tracking” flags on devices, etc.).

- **Subscriptions and Transactions:** We use purchase information to **manage your subscriptions and in-app purchases**. This includes verifying that a purchase was successful, unlocking premium content for the duration of your subscription, reminding you of upcoming renewals if applicable, and handling any issues with transactions (like resolving a double-charge or an upgrade/downgrade scenario). We may also send you transactional communications about your subscription: for example, a confirmation email or receipt when you purchase, or a notice if your subscription is set to expire or if there was an issue with billing. Processing this data is necessary to perform our contract with you (delivering the paid features) and for our legitimate interest in ensuring users get what they paid for (and handling billing appropriately).

- **Communication:** We may use your contact information (like your email) to send you **important updates or notices** about the Service. For instance:

  - **Account-related communication:** We might send a welcome email to verify your address, password reset emails upon request, or notifications of significant changes to our terms or privacy policy. If you contact us, we’ll use your info to respond.

  - **Transaction emails:** As mentioned, receipts or subscription notices.

  - **Service alerts:** If there's a major outage, security issue, or something that affects your use, we might email users to inform them.

  - **Feedback requests:** Occasionally, we might send an email asking for feedback or rating (though this is more likely done via in-app prompts than email).

  - We will **not** spam you with newsletters or promotions unrelated to the App without your consent. Since we currently have no advertising and our model is subscription, we have little need to send marketing emails. If that ever changes and we want to send, say, a newsletter, we will provide an opt-in mechanism.

- We rely on our legitimate interests and/or contractual necessity to send most of these communications (they're either necessary for service or expected as part of using the app). For any marketing-type communications, we would seek consent if required by law (e.g., GDPR or CAN-SPAM rules for promotional emails).

- **Moderation and Safety:** We use the data (especially content and usage patterns) to **keep our community safe and enforce our Terms**. Specifically:

  - We may review user-generated content or messages if flagged by users or algorithms to ensure it complies with our Terms (no hate speech, etc.). This might involve an automated system or human moderators looking at the content in question.

  - If we detect suspicious activity (like a user creating multiple accounts to spam likes, or using automated means to scrape data), we may analyze logs and device info to investigate and take action (e.g., blocking an IP or banning an account).

  - We keep logs and records as needed to **detect, prevent, or address fraud, security breaches, and activities that are illegal or violate our policies**. For example, IP addresses and device identifiers can help identify and block malicious actors.

  - If necessary, we may use information to contact you as part of an investigation (for example, reaching out to verify account ownership or warn about policy violations).

- This processing is based on legitimate interests in maintaining a safe environment, our legal obligations (if any, e.g., responding to lawful requests or preventing illegal activity), and the necessity to enforce our contractual terms.

- **Compliance with Legal Obligations:** We may process and disclose data as required by law or legal process. This includes:
  - Responding to lawful requests from public authorities (e.g., to comply with national security or law enforcement requirements, court orders, or subpoenas).
  - Using data to comply with applicable laws and regulations (data retention obligations, accounting requirements for purchases, etc.). For example, financial transaction records might be kept for tax and accounting purposes.
  - We may also use or preserve data to establish or exercise our legal rights, or defend against legal claims (for instance, keeping evidence of communications if there's a dispute).
- This is based on legal obligation or legitimate interest in protecting our legal rights.
- **Business Transfers:** If we ever (knock on wood) undergo a business transaction, like a merger, acquisition, reorganization, or sale of assets, user information might be transferred as part of that deal. In such a case, we would use data to facilitate that transition and ensure continuity of service. If the new entity's use of your data would differ materially, we'd notify you.
- **Aggregate and De-Identified Data:** We may aggregate or anonymize the data we collect so that it can no longer identify any individual user, and use that data for purposes such as statistical analysis, research, and improving our service. For example, we might compile statistics like "most popular loadout categories" or "percentage of users per country" without any personal details. Such information is not personal data and may be shared publicly or with partners (e.g., showing usage trends) in a manner that **does not identify individuals**.

Importantly, **we do not sell your personal data** to third parties. We also do not use the data we collect to profile you for advertising or share with advertisers (since our app does not have ads). Any use of data is primarily internal and for providing the service to you.

Where we rely on **consent** (for example, if required for analytics cookies on a future web integration, or sending marketing communications), you have the right to withdraw that consent at any time, which will not affect the lawfulness of processing before withdrawal.

How We Share or Disclose Information

We understand that your information is important, and we only share personal data in a few specific circumstances, outlined below. We do **not** share, sell, rent, or trade your personal information to third parties for their own promotional or marketing purposes. The instances in which we share information are:

1. Service Providers (Sub-Processors): We use trusted third-party companies and services to help us operate and improve Battlefinity. These providers perform services on our behalf and under our instructions, and they are bound by contractual obligations to keep your information confidential and use it only for the purposes we dictate. Key service providers include:

- **Firebase by Google:** Our app heavily relies on Google Firebase as a backend. Firebase provides us with user authentication, real-time database and cloud storage for content, analytics (Google Analytics for Firebase), and possibly Crashlytics for crash reporting. **Firebase Analytics** and related services collect usage data and device identifiers for analytics purposes. Google, as our processor, may have access to certain data for providing these services. We have configured data sharing settings with Firebase to limit data use; for example, we have disabled any integration that would use analytics data for ad personalization. Google processes Firebase data in accordance with their privacy policy and the Firebase Data Processing and Security Terms. (Refer to Google's Privacy Policy and Firebase's privacy information for more details.) We ensure no prohibited categories of personal data are sent to Firebase (Firebase forbids sending sensitive info like passwords, payment info, or biometric data in analytics events).

- **RevenueCat:** This is a service specifically for managing in-app subscriptions across platforms. We share with RevenueCat the minimum necessary information to manage subscriptions: e.g., a user identifier (like your Firebase UID or an anonymous ID), and receipts from Apple/Google for purchases. RevenueCat's servers then validate receipts and notify our app of subscription status. RevenueCat is **privacy-focused** and by default uses anonymous identifiers for users. They do not get personal info like your name or actual payment details. They do store purchase history and subscription status, which we access to know if a user is premium. According to RevenueCat, they don't sell user data and they encrypt data in transit. We have a data processing agreement with them through their terms.

- **Hosting and Infrastructure:** Firebase covers most hosting (since it's cloud-based). If we have any other servers (like a backend for our website or any proxy server), those would also have access to data. For instance, our **website codmunity.gg** and warzoneloadout.games domain might host our terms/privacy pages and possibly user account site. If you visit those, our web hosting provider might log your IP and interactions (common for websites). But as far as the **App data**, it's mainly in Firebase/Google Cloud.

- **Email/Communication Tools:** If we send emails (like verification or support responses), we may use an email service provider or SMTP relay. For example, we might use SendGrid, Mailgun, or Firebase's email services to send transactional emails. Those providers would have the email address and content of the email. They're obligated to secure it and not use it for other purposes.

- **Analytics Tools:** Beyond Firebase Analytics, we currently do not use separate analytics or tracking SDKs. If we did add something like Mixpanel or Amplitude (we have not, but hypothetically), those would get usage data too. We'd list them here and ensure they are governed by privacy commitments. But right now, all analytics is under the Firebase/Google umbrella (which we've covered).

In all cases, we share data with these providers only to the extent needed for them to perform their functions. For example, Google processes analytics to provide us insights, but cannot use that data for their own advertising because we've disabled such options. We have data protection agreements in place as required (Google's Firebase operates under the standard data processing terms compliant with GDPR).

2. Within our Corporate Group: If Loadout Sàrl has affiliates or subsidiaries (currently, Loadout Sàrl itself is the entity; if in future we form related companies), we may share info within our corporate structure as necessary to operate the service. Any such entities would follow this Privacy Policy.

3. Other Users: By the nature of the app, some information is **shared with other users**. Specifically:

- **Public Profile:** Your username, any profile picture, bio, and the list of loadouts you have posted will be visible to others. Similarly, your followers and who you follow might be visible on the platform. We design these features such that you have control: if you choose to put identifying info in your profile or content, that's a choice you make to share publicly. But inherently, *user-generated content is visible to the community by design*. If you "like" a loadout, the creator may see your username among the likers. If you follow someone, they may be notified or see you as a follower. We do not consider this "third-party sharing" in a traditional sense (like selling data), but rather part of the service's functionality which **you control by choosing what to share**. If you want to remain more anonymous, you can use a pseudonymous username and avoid posting personal details.

- **Social Sharing:** If you decide to share content from Battlefinity externally (for example, using a "share" feature to post a loadout to Twitter or Discord), then obviously you are voluntarily sharing that content outside the app. The app might facilitate that by generating an image or link, but the actual sharing is user-initiated. That content will then be subject to the third-party platform's policies.

4. Legal Compliance and Protection: We may disclose your information to third parties (such as attorneys, courts, or law enforcement authorities) if we determine that such disclosure is reasonably necessary to:

- **Comply with the law or legal process:** If we receive a valid subpoena, court order, or other legal demand, we may have to disclose certain data (for example, account information or usage records). We will evaluate each request carefully and push back when appropriate (e.g., overly broad or unlawful requests). When allowed, we may notify affected users of such requests.

- **Protect rights and safety:** We might share data when we believe it's necessary to prevent fraud, abuse, or to protect the rights, property, and safety of the Company, our users, or the public. For instance, if someone is attempting to hack others' accounts, we might provide relevant info to law enforcement with a report. Or if someone's posts threaten violence, we could assist authorities.

- **Enforce our Terms and policies:** Information might be shared with legal counsel or others to enforce our agreements or policies. If we need to pursue a user for malicious activities (like legal action for hacking or for content that caused legal liability), data would be evidence.

We will only disclose the minimum information necessary in such cases and will follow applicable legal procedures.

5. Business Transfers: If we are involved in a merger, acquisition, financing due diligence, reorganization, bankruptcy, receivership, sale of company assets, or transition of service to another provider, your information may be disclosed to our successor or potential acquirers (and their agents and advisors) as part of that transaction. We would ensure any such party is bound by confidentiality until it's completed and that they understand they must honor the commitments we've made in this Privacy Policy with respect to your data (or provide notice if they plan to change them). If a transaction does occur that affects the processing of your personal data, we will notify you (for example, via email and/or a prominent notice in the App) about the change of ownership and any choices you may have regarding your personal data.

6. Aggregate or De-Identified Data: We may share aggregated information that does not identify you personally with third parties – such as press, partners, or in reports. For example, "Battlefinity has X thousand users and Y million loadouts posted" or "80% of our users play Game Z". This info will not include personal data and is shared for legitimate purposes (showcasing usage, industry analytics, etc.).

We do **not** share personal data with advertisers or ad networks, since our App does not have advertising. In the future, if we ever introduce ads, we would update this section and likely give you opt-in controls as required. But as of now, no ad-related sharing exists.

Third-Party Content and Links: Although not “sharing” per se, note that if you click a link to a third-party site (like YouTube), you will leave our app and go to that service, which may collect data from you (like cookies, account info if you’re logged in, etc.) under their own privacy policy. We are not responsible for those external privacy practices. We encourage you to review the privacy policies of any third-party websites or services that you access through Battlefinity.

International Data Transfers

Battlefinity is a global service, and your information will likely be transferred to and processed in **countries other than your own**. In particular, our servers and service providers are located in multiple countries. For example:

- Our primary data storage (Firebase/Google Cloud) might be in the **United States** or in the **European Union** depending on server settings. We have users worldwide, but given our company is based in Switzerland, we may choose EU servers. However, Firebase Analytics data and some processing might occur in the U.S. or other locations. Google’s infrastructure is global, and they have committed to compliance with EU data protection for transfers.
- RevenueCat is a U.S.-based service (likely processing data in the USA).
- If you’re using our app from outside of where the servers are, data obviously travels across borders (e.g., a user in Europe accessing data stored in U.S., or vice versa).

When we transfer personal data outside of the country it was collected in, we take steps to ensure **appropriate safeguards** are in place to protect it. For users in the European Economic Area (EEA), UK, or Switzerland: whenever we transfer your personal data to countries which are not deemed by your local authorities to have adequate data protection, we rely on legal transfer mechanisms such as the **European Commission’s Standard Contractual Clauses (SCCs)** or other equivalent safeguards. For example, our contracts with Google (Firebase) include SCCs as part of Google’s Data Processing Terms, which means Google has committed to protect EEA data to EU standards even when transferred to the US or elsewhere. Similarly, if we engage other providers, we ensure they are certified under frameworks (like EU-U.S. Data Privacy Framework if applicable) or sign SCCs.

If you are located in a jurisdiction (like some Asia-Pacific countries) that imposes certain requirements on cross-border data transfers, we will ensure compliance by using similar contractual and technical protections.

Your Acknowledgment: By using Battlefinity, you understand that your data may be transferred to and processed in countries outside of your own. Different countries have different data protection laws, which might not be as protective as those in your jurisdiction. However, we will always treat your personal information in accordance with this Privacy Policy and take appropriate measures to protect it.

If you have questions about our transfer mechanisms or want more information about cross-border handling of your data, please contact us at the email provided.

Data Retention

We retain your personal information **only for as long as necessary** to fulfill the purposes for which it was collected, as described in this Privacy Policy, and for as long as your account is active. Specifically:

- **Account Data:** We keep your account information (email, username, profile, etc.) and content for as long as you maintain an account with us. If you decide to delete your account, we will initiate deletion of your personal data from our active databases. In most cases, account deletion will result in your profile and all posts, likes, follows being removed or anonymized in the app. (For example, your loadouts might be removed entirely or dissociated from any user identity.) We aim to complete such deletions promptly, generally within 30 days of confirmation of the request, unless legal requirements mandate otherwise. Some data may persist for a short time in backups, but we have processes to eventually purge those as well, unless backups need to be retained longer for legal reasons.

- **User-Generated Content:** Content you post is stored until you delete it or delete your account. You can manually delete a loadout or other content, and it will no longer be visible to others (though it may remain in our system backups or logs temporarily). If another user has interacted with your content (e.g., quoted it or if it's been shared), there may be residual references; but since we don't have content resharing features inside the app (aside from likes), deletion should effectively remove general access. We may retain server logs of the deletion action (like an audit trail), but not the content itself in active use.

- **Subscription and Transaction Data:** We retain records of your purchases and subscriptions for as long as needed for financial reporting, audits, and compliance with tax and accounting regulations. For instance, we might need to keep purchase receipts for X number of years under local law. This data includes info like transaction IDs, subscription status, and associated user ID, but not your credit card info (which we never had). If you delete your account, we will disconnect your personal identity from subscription records, but we might still keep anonymized transactional records for legitimate business/legal purposes.

- **Analytics Data:** Firebase Analytics allows configuration of data retention. By default, Google retains user-level and event-level data for a certain period (e.g., 14 months). We have set our retention to the shortest duration that meets our needs (often 14 months for user-level data, which is the default minimum, and possibly longer for aggregated reports). Analytics logs and reports might be kept indefinitely in aggregate form (e.g., monthly usage counts, which are not tied to individuals). If you clear the app data or reset your advertising ID, Analytics will treat you as a new user. If you request deletion of your data, where feasible, we will also remove analytics identifiers associated with you from our data sets. Crashlytics and diagnostics data retention may vary, but generally is used for the most recent app versions and problems.

- **Logs and Security Data:** Our server logs (which include IP addresses and device info) are generally rotated and deleted periodically, typically within a few weeks to months, unless retained for security analyses. If any logs are kept longer (for instance, to investigate a specific security incident or to comply with legal obligations), access to them is restricted and they are deleted once the purpose is fulfilled.

- **Legal Hold:** If we are under a legal obligation to keep data (for example, in response to a legal dispute or law enforcement request), we will retain the specific data required for as long as the obligation lasts. Also, if deletion requests come when an account is under investigation for abuse, we may retain data until that process is resolved, after which we'll proceed with deletion.

After the retention period expires or the purpose for collecting the data is fulfilled, we will either delete your data or anonymize it so that it can no longer be associated with you. For example, we might aggregate usage data for statistical purposes which does not identify you.

Backup and Archival: Please note that due to the way our systems are designed with backups, residual copies of your personal data might not be immediately removed from backup systems after deletion. However, these backups are retained only for disaster recovery and are inaccessible for normal use. We have retention limits for backups as well, after which they are overwritten or deleted.

Inactive Accounts: If you stop using Battlefinity and your account remains inactive for an extended period (we might define this as 1-2 years of inactivity), we may remove or anonymize your data as part of routine housekeeping. We might send a warning email before doing so. This is to limit retaining data longer than necessary. Of course, if you log back in before that, your account will be considered active.

In summary, we retain your data as needed to provide you service and as required by law or legitimate business needs, and we strive not to keep it longer than necessary. You have the right to request deletion of your data – see **Your Rights** below for how to exercise that.

Protecting Your Information (Data Security)

We take the security of your personal information seriously. We have implemented a variety of **technical and organizational measures** to protect your data from unauthorized access, alteration, disclosure, or destruction. These include:

- **Encryption:** All network communications between the Battlefinity app and our servers (including Firebase and RevenueCat) are encrypted in transit using HTTPS (TLS). This means that data like your login credentials, content, and analytics events are transmitted securely and cannot be easily intercepted. Where possible, we also enable encryption at rest. For instance, Firebase automatically encrypts data at rest on their servers, and RevenueCat also states that data is encrypted in transit and at rest. Any sensitive fields (like passwords) are stored in hashed form using secure algorithms via Firebase Auth – we never see your raw password.

- **Access Controls:** We restrict access to personal data to authorized personnel who need it to operate, develop, or improve our App. Within our small team, only personnel with a legitimate need (for example, a support staff responding to a user query, or an engineer debugging an account issue) can access user data, and even then, access is limited to what is necessary. We utilize Firebase's security rules to ensure that, for example, users can only read their own data (and public data) but not others' private data. Administrator access to databases is protected by strong authentication (e.g., multi-factor authentication on our Google Cloud accounts and other tools).

- **Secure Development Practices:** We follow secure coding practices and conduct code reviews to catch security issues early. We keep our systems and dependencies up-to-date with security patches. We also use Firebase's built-in security features (like Firestore security rules, Auth rules) to enforce data read/write protections on the backend.

- **Testing and Monitoring:** We regularly monitor our services for potential vulnerabilities and attacks. Firebase provides some monitoring, and we use logging to detect anomalies. We may also run penetration tests or use third-party security tools to evaluate our app's security posture. Any vulnerabilities found are addressed with high priority.

- **Anonymization & Least Privilege:** Where feasible, we anonymize or pseudonymize data. For instance, analytics are tied to random IDs rather than directly to your name or email. Internally, if we analyze usage, we often do so on an aggregated level. We apply the principle of least privilege: our service providers and components get only the data they need. (Example: RevenueCat gets subscription receipts but not your other app data; our email provider gets your email and message but not other info.)

- **Physical Security:** We rely on reputable cloud providers (Google Cloud, etc.) that have strong physical security at their data centers. This includes safeguards like controlled facility access, surveillance, etc.

- **Backups and Recovery:** We maintain backups to ensure data isn’t lost accidentally. Those backups are protected and encrypted. In case of any data incidents (loss or corruption), we have the ability to restore from backups, and those processes are also secured.

Despite all these efforts, it’s important to note that **no method of transmission over the Internet or electronic storage is 100% secure**. We strive to protect your data, but we cannot guarantee absolute security. Users also play a role in security: you must keep your account credentials confidential and use a strong, unique password. If you use third-party login, protect that account too. If you suspect any unauthorized access to your account, please contact us immediately.

In the event of a data breach that affects your personal data, we will act promptly to contain and investigate it, and we will notify you and relevant authorities as required by law. We have an incident response plan in place for such situations.

Your Rights and Choices

Depending on where you live and the applicable data protection laws, you may have certain rights regarding your personal information. We are committed to honoring these rights. Below is a general outline of those rights and how you can exercise them:

- **Access Your Information:** You have the right to request access to the personal data we hold about you. This means you can ask us to confirm if we’re processing your personal data, and you can request a copy of that data (commonly known as a data subject access request). For example, you can ask for a copy of your profile info, posts, and any other personal data we have on you. We will provide this in a structured, commonly used electronic format. In many cases, you can view much of your data directly in the app (e.g., your profile details, your content), but for a comprehensive export, you can contact us.

- **Rectification (Correction):** If any of your personal information is inaccurate or incomplete, you have the right to request that we correct or update it. You can usually do this by editing your profile in the app (e.g., change your email if allowed, or update your username or bio). For things you cannot self-update (like if your email is wrong and you can’t change it through settings), contact us and we’ll help correct it.

- **Deletion (Right to be Forgotten):** You have the right to request deletion of your personal data. As noted, you can achieve much of this by deleting your account in the app settings (if this feature exists) or by contacting us to request account deletion. Once we verify your identity and that you want to delete, we will remove your personal data (while retaining only what we're permitted or required to keep by law). Deletion is irreversible – it means you'll lose access to the account and data (posts, etc.) afterwards. If you simply want to remove certain content (like a specific loadout you posted), you can delete that content without deleting your whole account. If other users' data is intertwined (for example, they sent you something or you had a joint content), we will handle deletion requests in a way that doesn't infringe others' rights while honoring yours to the extent possible.

- **Objection to Processing:** You have the right, in certain situations, to object to our processing of your data. For instance, if we process your data on the basis of "legitimate interests," you can object to that if you believe it impacts your rights. If you object, we will evaluate whether our legitimate grounds for processing override your interests or rights. If they do not, we will stop or adjust the processing. For example, you can object to receiving certain notifications or being included in non-essential analytics. (Note: You always can turn off push notifications at the device level too.)

- **Restriction of Processing:** You can request that we limit the processing of your data in certain circumstances. This is typically applicable if you contest the accuracy of data (until we verify it), or if you need data preserved for a legal claim but don't want us to otherwise process it, or during the period of an objection resolution. While processing is restricted, we can still store your data but not use it further except for legal reasons.

- **Portability:** For data you provided to us and that we process by automated means based on consent or contract, you have the right to request a copy in a machine-readable format to transfer to another provider. Practically, this overlaps with the access right – we'd give you data in a structured format like JSON or CSV, which you could then import elsewhere. (Keep in mind, other apps might not have a place to import our specific data, but the right is there.)

- **Withdraw Consent:** In cases where we rely on your consent to process data, you have the right to withdraw your consent at any time. For example, if you consented to receive promotional emails, you can opt-out. Or if you gave us permission to collect certain data, you can revoke that permission (like disabling location if we ever used it, or turning off analytics if we offered an opt-in/out switch). Withdrawing consent does not affect the lawfulness of processing based on consent before its withdrawal.

- **Opt-Out of Marketing:** Even though we currently do not send marketing communications, if we ever did, you would have a right to opt-out or unsubscribe. We would include an "unsubscribe" link in any such email. Also, as mentioned, no third-party marketing use of data occurs.

- **Opt-Out of Sale or Sharing (CCPA):** Under the CCPA (for California residents), you have the right to opt-out of the "sale" of personal information. We do not sell personal info, and we don't share it for cross-context behavioral advertising. If that ever changes, we would implement a “Do Not Sell or Share My Personal Information” link. As of now, this is not applicable because we don’t do those activities.

- **Non-Discrimination:** If you exercise any of your privacy rights, we will not discriminate against you for doing so. For example, deleting your data will obviously mean you can’t use the service (since we need data to run an account), but we won’t deny you features or charge you differently just because you made a privacy request.

To exercise any of these rights, you can reach out to us at **alex@codmunity.gg** with your request. Please specify which right you seek to exercise and the scope of the request. We may need to verify your identity (to ensure, for example, that someone else isn’t trying to delete or access your account data). Verification might involve checking your email ownership or asking some information only you would know related to the account.

We will respond to your request within a reasonable timeframe. For EU/EEA residents, that’s typically within 1 month, with a possible extension to 3 months for complex requests (we’ll inform you if an extension is needed). For California residents, we aim for 45 days (with up to 90 if needed). There is generally no fee for making a request, unless it is manifestly unfounded or excessive, in which case we may charge a reasonable fee or decline.

If you are in the EEA/UK/Switzerland and have concerns about our data practices, you also have the right to lodge a complaint with your country’s **Data Protection Authority** (DPA). For example, in France it’s CNIL, in the UK it’s the Information Commissioner’s Office (ICO), etc. We encourage you to reach out to us first so we can try to address your concerns directly, but it is your right to contact your DPA at any time.

Similarly, California users have the right to contact the California Attorney General’s office if they believe we have not addressed a concern properly.

Managing Your Information in the App: In addition to formal rights, we provide you with controls directly in Battlefinity wherever possible:

- You can edit profile details (except perhaps email, if it’s tied to login in some cases – but you can contact support to change email if needed).

- You can delete content you’ve posted (loadouts, etc.).

- You can unsubscribe from communications (via link in emails or app settings for push notifications).

- You can cancel subscriptions via the app stores if you no longer want them.

Note: If you request deletion or object to processing that is essential for us to provide the service (like the processing of your account data), it might result in account closure because we cannot practically provide the app without processing certain data.

We are committed to respecting your rights and will not refuse to fulfill them without a valid reason. If we ever cannot comply fully with a request (like deletion when we have a legal duty to keep certain data), we will explain the situation to you.

Children's Privacy

Battlefinity's community and content are generally intended for a general audience of gamers and are **not specifically directed at children under the age of 13**. We do not knowingly collect or solicit personal information from children under 13. If you are under 13, please do not attempt to register an account or send any personal information about yourself to us. If we learn that we have inadvertently collected personal data from a child under 13 without verifiable parental consent, we will take steps to delete that information as soon as possible.

No Age Gate: As the user noted, there is "no age restriction" within the app in terms of usage — meaning we are not currently gating or blocking younger users from accessing it. However, we rely on the truthfulness of users about their age. Our policy is that **individuals under 13 (or under the applicable minimum age in their jurisdiction, which may be 16 in some regions for certain data laws) should only use the App with parental permission**. We advise parents or guardians who allow their children to use Battlefinity to teach them about online safety and to supervise their activity when possible.

Parental Involvement: If you are a parent or guardian and you believe that your child under 13 has created an account on Battlefinity or otherwise provided personal information to us without your consent, please contact us immediately at **alex@codmunity.gg**. We will promptly remove the data and terminate the child's account if we find that we have unknowingly collected such information. We may ask for proof of your relationship to the child (to ensure we are talking to the actual parent/guardian) before taking action.

Users 13-18: For minors who are 13 or older but under the age of majority (typically 18), we recommend using the App with parental guidance. Such users should review this Privacy Policy and our Terms with a parent or guardian to ensure they understand them. While our content is user-generated and typically about games, we cannot guarantee all content is appropriate for younger teens (though our community guidelines prohibit extreme inappropriate content). If any user under 18 has questions about their privacy on the app, they or their parent can contact us.

COPPA Compliance: We comply with the **Children's Online Privacy Protection Act (COPPA)** in the U.S. That means if in the future we intentionally offer features aimed at children under 13, we would implement COPPA's requirements (like parental consent mechanisms). As of now, we avoid collecting data from that age group altogether by policy. We also avoid certain types of data collection that could be sensitive for minors (like precise location or profiling).

No Targeted Ads to Children: Since we have no advertising at all, there’s no concern of serving behavioral ads to children. If we ever did have ads, we would ensure that data from any user identified as under 16 is not used for targeted advertising, in line with laws like GDPR and upcoming changes in US state laws.

International Age Requirements: We also take into account other age-related regulations:

- In the EU, per GDPR, if a child is under 16 (though member states can set this as low as 13), processing of personal data in relation to online services is only lawful with parental consent. We do not knowingly engage users under that age threshold without consent.

- If we identify a user from an EU country who is under the required age, we will similarly remove their data unless consent is provided by a parent.

- In regions like California, the CCPA has provisions about minors under 16 (opt-in for sale of data; but we don’t sell data anyway). If we ever considered “selling” data, we’d exclude minors by default or get proper consent.

In summary, we treat the privacy of children with care:

- We **minimize** data collection to start with, which reduces risk to all users including minors.

- We do not knowingly let under-13s on the platform.

- If a minor (13-17) is using the app, the nature of data we collect (username, email, usage data) is fairly limited and not highly sensitive, but we still protect it.

- We encourage families to use parental controls (both Apple and Google offer parental control features that can restrict app usage by age rating, etc. – though our app likely has a 12+ or similar rating on stores due to user content).

- If content appropriate issues arise, we moderate them as per our guidelines, which also protects minors from seeing harmful content.

Third-Party Services and SDKs

Battlefinity integrates third-party services and software development kits (SDKs) to function. We have mentioned many of these above (Firebase, Google Analytics, RevenueCat, etc.). Here we provide a consolidated overview of key third-party services we use, what data they collect or share, and how you can find more information about their privacy practices:

- **Firebase and Google Services:** Battlefinity uses multiple Firebase modules (by Google) such as:

  - *Firebase Authentication:* To handle user login (email/password and third-party OAuth). It stores user identifiers and hashed passwords. Google, as the provider, technically processes that data to authenticate you.

  - *Cloud Firestore / Realtime Database:* To store app data like loadouts, profiles, likes, etc. Your content and profile info are stored on Google's cloud servers. Data in Firestore is typically stored in the US (or EU if configured) and is encrypted. Google's staff doesn't access it unless necessary for support, under strict controls.

  - *Firebase Cloud Storage:* If we stored any media (we currently don't allow images or video uploads, only text and external links), it would go here. But since "no image or video except YouTube link", we might not use Storage much. If we do in future (say for profile avatars), those files are stored on Google's storage.

  - *Google Analytics for Firebase:* As discussed, collects usage stats and events (see earlier sections). You can find Google's Analytics privacy info here: **Google Analytics Privacy** (https://support.google.com/analytics/answer/6004245) and specifically for Firebase: **Firebase Data and Privacy** (https://firebase.google.com/support/privacy). Google Analytics may use device identifiers and cookies-like tech (on mobile, Google's Advertising ID or Instance IDs). If you have enabled "Limit Ad Tracking" or "Opt out of Ads Personalization" on your device, Firebase Analytics respects that by not using the advertising ID. We have ensured analytics is set to only use data for analytics and not to share with other Google products unless we explicitly allow (we have not).

  - *Firebase Crashlytics:* If included, collects crash reports (stack traces, device state). This might incidentally include a user identifier (like the Firebase Installation ID or your user ID if we attach it for context). Crash reports help us fix bugs.

  - *Firebase Remote Config / A/B Testing:* We might use these to deliver feature flags or test variations. These would use non-identifiable segmentation (like random splits or based on analytics audience).

  - *Firebase Cloud Messaging (FCM):* If we send push notifications, FCM is used to deliver them. It uses a push token to send to your device. That token is not something that identifies *you* personally, but it's tied to the app instance.
    All Firebase services adhere to Google's privacy and security commitments. Google does not use data from Firebase for any advertising or profiling outside of our use of it (unless we chose to link to other Google services, which we have not

    for ad purposes). As a user, if you want to limit Firebase Analytics, you could disable ad tracking on your device or in iOS specifically choose to not allow apps to track (though Firebase Analytics under Apple's definitions, when configured for "App Functionality" and "Analytics", is not considered tracking for advertising).

- **RevenueCat SDK:** RevenueCat is integrated to manage purchases. The SDK will collect purchase receipts and may assign an **app user ID**. By default, RevenueCat creates an anonymous user ID for each installation. When you log in to our app, we likely tell RevenueCat to use a stable identifier (like your Firebase UID) so your subscription works across devices. RevenueCat collects data on subscription status and sends it to us. As per RevenueCat's site, they do not collect personal info beyond what's necessary (no payment info, no contact lists, etc.). They do note that if an app uses advertising ID for integrations, you must disclose it. We do not use any advertising integration with RevenueCat. Our usage is limited to "Purchases" and optionally "User ID" categories. According to RevenueCat's own privacy policy, data is used to provide the subscription service and they may aggregate data to understand general trends. For more details, see the **RevenueCat Privacy Policy** (https://www.revenuecat.com/privacy). If you wish to opt-out of RevenueCat's tracking of your app usage, there isn't a user-facing opt-out because it's an internal service; however, since they mostly track purchases, the concept of opt-out isn't directly applicable. They do allow apps to configure whether to collect the advertising ID; we have not integrated any such ad ID usage.

- **Apple App Store / Google Play Services:** When you install via Apple or Google, those platforms gather certain info (like device type, OS, etc.). Apple also provides privacy details on the App Store listing which are based on our disclosures. The **App Store** and **Play Store** themselves collect data like your device model, app version, and usage time for their own analytics and might share some aggregated data with us (e.g., number of downloads, crash counts). If you enable in-app purchases, Apple/Google handle the financial transaction; they may keep your billing info and purchase history per their own privacy policies. We do not get your credit card, but Apple/Google will know that you subscribed to our service. Check Apple's Privacy Policy and Google's Privacy Policy for information on what they collect.

    - Apple also has something called **App Privacy Report** on your device which can show what domains the app contacts and what permissions it uses. We primarily contact domains like our Firebase endpoints and RevenueCat endpoints; those should be visible if you inspect that on iOS 15+. This can give insight into third-party communications.

    - We have also provided to Apple's App Store a summary of data linked to you (which includes identifiers, usage data, user content, etc., as required). These are based on the categories Apple defines.

- **YouTube Links:** If you view a YouTube video via a link in a loadout, note that it likely opens in the YouTube app or a browser. If it opens inside a webview, YouTube might load cookies or trackers. YouTube (Google) will track views, and if you're logged in to YouTube, it associates it with your account as usual. That interaction is governed by YouTube's own privacy policy. We are not sending any data to YouTube except the referral that a user clicked a link. We don't embed YouTube videos directly in our app currently (if we did via YouTube API, we'd abide by YouTube API Services Terms and show their consent dialogs if needed). For now, it's just a link. Users should be mindful that playing a YouTube video will subject them to YouTube's data practices (like possibly recording the watch in their history).

- **Other External Links:** Similarly, any link to external content (like a game wiki or news site, if someone posted one) will take you outside our app and into that domain's jurisdiction. We do not automatically open unknown links inside the app for safety; typically it should open in your external browser. Those sites might collect data like your IP, set cookies, etc. Always review those sites' privacy notices if concerned.

We strive to **minimize** the number of third-party SDKs and ensure those we use are **reputable and necessary**. We have listed the main ones. If in the future we integrate additional SDKs (say a social media sharing SDK, or an advertising network if that business model changes), we will update this Privacy Policy accordingly and disclose relevant info on our App Store privacy section and in-app.

For transparency, here is a quick list of any other minor third-party libraries that might collect data:

- Possibly the app uses an open-source UI or utility library that does not transmit data anywhere (like a date-picker library, etc.). Those don't count as "third-party services" in terms of data transfer, as they run locally.

- If we integrate something like **Sentry** for error tracking (we haven't, Crashlytics covers it), that would send error data to Sentry's servers. We currently rely on Crashlytics (Google).

- If we use **Amplitude** or **Mixpanel** (not currently, as said), that would send usage data to their servers. Not used at the moment.

- If we at some point add a **social login** for another service (like sign in with Discord or similar), then data flows to/from that provider. Presently, just Apple and Google as discussed.

We ensure that each third-party service we use is compliant with relevant privacy regulations (GDPR, etc.) and that there is a contract in place for data processing. If any of these services experience a data breach affecting our users' data, we will follow appropriate steps to inform users and remediate (just as we would for our own system issues).

Your interactions with these third-party services are somewhat within our control (as we set what data to send), but also governed by their terms:

- For example, by using our app, you also agree to Google's privacy terms to the extent that Google processes data as described.

- For Apple, usage of any Apple frameworks (like sign-in) implicates Apple's terms.

If you have questions about a specific third-party component, feel free to contact us.

Changes to This Privacy Policy

We may update or modify this Privacy Policy from time to time to reflect changes in our practices, technologies, legal requirements, or for other operational reasons. When we make changes, we will let you know by updating the "Last Updated" date at the top of this policy. In the case of significant or material changes, we will provide a more prominent notice of the update, such as via an in-app notification or by emailing you (if we have your email on file).

Examples of material changes might include: adding new personal data processing activities, changing how or why we use data, implementing new third-party integrations that affect privacy, or changing how users can exercise rights. Minor changes might include clarifications or administrative updates that do not substantially affect your rights or obligations.

We encourage you to review this Privacy Policy periodically to stay informed about how we are protecting the personal information we collect. If you continue to use Battlefinity after a revised Privacy Policy has become effective, you are indicating that you have read and understood the latest version of the policy.

If you do not agree with any updates to the Privacy Policy, you should stop using the App and may delete your account. We will always indicate the effective date of the most recent changes so you know if something has changed since your last read.

For users in certain jurisdictions, if required by law, we will seek your explicit consent to any material changes in how we collect, use, or share your personal data. For example, if a change would require new consent under GDPR or similar regimes, we will provide a way for you to consent (or opt-out, as appropriate) before applying those changes to your data.

Contact Us

If you have any questions, concerns, or requests regarding this Privacy Policy or our data practices, you can contact us at:

- **Loadout Sàrl** (Battlefinity App Support)
- **Email:** alex@codmunity.gg
- **Attn:** Data Protection Officer / Privacy Inquiry (We do not formally require a DPO under GDPR, but we will treat your inquiry with similar care.)

We will do our best to respond promptly to your inquiries. If you contact us by email regarding your rights or a privacy concern, please include as much detail as possible about your request and the context (so we can locate your data, etc.), and we may ask you to verify identity to protect your privacy.

In addition, if you reside in the European Economic Area (EEA) or UK, you may contact our **EU Representative** or **UK Representative** (if we designate one for GDPR/UK-GDPR compliance) at alex@codmunity.gg – *Note: if our user base in EU grows, we might appoint a representative or DPO; currently, as a Swiss company handling global data, we comply with Swiss FADP and GDPR as needed.*

For California residents: you can use the above contact to exercise your California privacy rights as well (just specify you are a California resident making a CCPA request).

We value your privacy and will address your questions to the best of our ability.

By using Battlefinity, you acknowledge that you have read and understood this Privacy Policy. If there's anything you do not understand or if you need further clarification, please reach out to us. Your trust is important to us, and we are happy to explain our practices or accommodate your requests where possible.

Thank you for being a part of the Battlefinity community and for reviewing our Terms and Privacy Policy. We hope you enjoy using the App safely and securely!