FanHub Media Privacy Policy

Updated: July 2020

Introduction

Your privacy is important to FanHub, it's Clients and its affiliates who are referred to collectively in this policy as "**FanHub**", "**we**", "**us**" or "**our.**" Our affiliates are:

- Fan Hub Media USA, LLC in the United States.
- Fan Hub Media Trading Pty Ltd, in Australia.
- Fan Hub Media Direct Pty Ltd, in Australia.
- FanHub Media UK Ltd, in the United Kingdom

FanHub provides 'free to play fan engagement games and products' (the "Service") on behalf of it's Clients and their respective Consumers. We fully respect the right to privacy of our Clients and their Consumers as it relates to the interactions with the Service and are committed to being transparent in our dealings with you as to what personal information we will collect and how we will use your personal information. Also, we only collect and use personal information that is necessary for providing Service and where we have a lawful basis to do so.

We have operations in the United States, United Kingdom and Australia. The location of FanHub's main establishment in the European Union is in the United Kingdom and therefore we consider our lead supervisory authority, for purposes of "one stop shop" oversight over our cross-border data processing, to be the EU General Data Protection Regulation ("GDPR").

Our European Union representative for purpose of this Privacy Policy is:

Ali Tavallai
FanHub Media UK Ltd
3rd Floor, The News Building, 3 London Bridge Road, London, SE1 9SG
dpo@fanhubmedia.com

We have created this Privacy Policy to describe our practices and procedures in handling "Personal Information" we collect or receive from you. The term "Personal Information" means any information that identifies, relates to, describes, or is capable of being associated with, or could reasonably be linked, directly or indirectly, to an identified or identifiable living natural person, including but not limited to: (i) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier Internet Protocol address, email address, account name, social security number, driver's license number, government identification card number, passport number, or other similar identifiers; and (ii) information defined as "personal information," "personally identifiable information," "personal data," or similar expressions under applicable privacy laws or data security Laws, which include the European Union's General Data Protection Regulation ("GDPR").

Our Commitment

FanHub and its affiliates are committed to ensuring the security and protection of the personal information that we process, and to provide a compliant and consistent approach to data protection. We have always had a robust and effective data protection program in place which complies with existing law and abides by the data protection principles.

FanHub are dedicated to safeguarding the personal information under our remit and in developing a data protection regime that is effective, fit for purpose and demonstrates an understanding of, and appreciation for difference regulations. Our compliance has been summarised in this policy and include the details of data protection roles, policies, procedures, controls and measures to ensure maximum and ongoing compliance.

When it comes to customer data, is FanHub a "controller" or a "processor"?
Under GDPR, a "controller" determines why and how personal data is processed. A "processor" processes personal data on behalf of the controller. FanHub has limited knowledge of the data that it's clients process via our hosting infrastructure ("Customer Data"). Also, FanHub only processes Customer Data in accordance with our clients instructions. Therefore, FanHub is a "processor" of Customer Data; and our Client's are the "controller".

Our Vendors
We also use the services which confirm they meet compliance with the most relevant Data Regulations including GDPR and CCPA:

Amazon Web Services – hosting infrastructure
Rackspace - hosting
Mailgun - transactional email service
Stripe - payment services
Zendesk - customer support

How we meet compliance for GDPR

FanHub has a consistent level of data protection and security across our organisation which includes:

- ***Information Audit*** - carrying out a company-wide information audit to identify and assess what personal information we hold, where it comes from, how and why it is processed and if and to whom it is disclosed.
- ***Policies & Procedures*** **-** data protection policies and procedures to meet the requirements and standards of the GDPR and any relevant data protection laws, including: -
    - ***Data Protection*** – our main policy and procedure document for data protection is regularly updated to meet the standards and requirements including GDPR. Accountability and governance measures are in place to ensure that we understand and adequately disseminate and evidence our obligations and

responsibilities; with a dedicated focus on privacy by design and the rights of individuals.

- ***Data Retention & Erasure*** – our retention policy and schedule meets the *'data minimisation'* and *'storage limitation'* principles and that personal information is stored, archived and destroyed compliantly and ethically. We have dedicated erasure procedures in place to meet the new *'Right to Erasure'* obligation and are aware of when this and other data subject's rights apply; along with any exemptions, response timeframes and notification responsibilities.
- ***Data Breaches*** – our breach procedures ensure that we have safeguards and measures in place to identify, assess, investigate and report any personal data breach at the earliest possible time. Our procedures are robust and have been disseminated to all employees, making them aware of the reporting lines and steps to follow.
- ***International Data Transfers & Third-Party Disclosures*** – where FanHub stores or transfers personal information outside the EU, we have robust procedures and safeguarding measures in place to secure, encrypt and maintain the integrity of the data. Our procedures include a continual review of the countries with sufficient adequacy decisions, as well as provisions for binding corporate rules; standard data protection clauses or approved codes of conduct for those countries without. We carry out strict due diligence checks with all recipients of personal data to assess and verify that they have appropriate safeguards in place to protect the information, ensure enforceable data subject rights and have effective legal remedies for data subjects where applicable.
- ***Subject Access Request (SAR)*** – our SAR procedures accommodate the 30-day timeframe for providing the requested information and for making this provision free of charge. Our procedures detail how to verify the data subject, what steps to take for processing an access request, what exemptions apply and a suite of response templates to ensure that communications with data subjects are compliant, consistent and adequate.

- ***Legal Basis for Processing*** - we continuously review all processing activities to identify the legal basis for processing and ensuring that each basis is appropriate for the activity it relates to. Where applicable, we also maintain records of our processing activities, ensuring that our obligations under Article 30 of the GDPR and Schedule 1 of the Data Protection Bill are met.
- ***Privacy Notice/Policy*** – we continuously revise our Privacy Notice(s) to comply with Data Regulations such as GDPR and CCPA, ensuring that all individuals whose personal information we process have been informed of why we need it, how it is used, what their rights are, who the information is disclosed to and what safeguarding measures are in place to protect their information.
- ***Obtaining Consent*** - our consent mechanisms for obtaining personal data, ensure that individuals understand what they are providing, why and how we use it and giving clear, defined ways to consent to us processing their information. We have developed stringent processes for recording consent, making sure that we can evidence an

affirmative opt-in, along with time and date records; and an easy to see and access way to withdraw consent at any time.

- ***Direct Marketing*** - the wording and processes for direct marketing, include clear opt-in mechanisms for marketing subscriptions; a clear notice and method for opting out and providing unsubscribe features on all subsequent marketing materials.
- ***Data Protection Impact Assessments (DPIA)*** – where we process personal information that is considered high risk, involves large scale processing or includes special category/criminal conviction data; we have developed stringent procedures and assessment templates for carrying out impact assessments that comply fully with the GDPR's Article 35 requirements. We have implemented documentation processes that record each assessment, allow us to rate the risk posed by the processing activity and implement mitigating measures to reduce the risk posed to the data subject(s).
- ***Processor Agreements*** – where we use any third-party to process personal information on our behalf (*i.e. Payroll, Recruitment, Hosting etc*), we have compliant Processor Agreements and due diligence procedures for ensuring that they (*as well as we*), meet and understand their/our GDPR obligations. These measures include initial and ongoing reviews of the service provided, the necessity of the processing activity, the technical and organisational measures in place and compliance with the GDPR.
- ***Special Categories Data*** **-** where we obtain and process any special category information, we do so in complete compliance with the Article 9 requirements and have high-level encryptions and protections on all such data. Special category data is only processed where necessary and is only processed where we have first identified the appropriate Article 9(2) basis or the Data Protection Bill Schedule 1 condition. Where we rely on consent for processing, this is explicit and is verified by a signature, with the right to modify or remove consent being clearly signposted.

Data Subject Rights

In addition to the policies and procedures mentioned above that ensure individuals can enforce their data protection rights, we provide easy access to "contact us" forms on our websites to request information about, or access to, any personal information that FanHub processes about them including information about:

- What personal data we hold about them
- The purposes of the processing
- The categories of personal data concerned
- The recipients to whom the personal data has/will be disclosed
- How long we intend to store your personal data for
- If we did not collect the data directly from them, information about the source
- The right to have incomplete or inaccurate data about them corrected or completed and the process for requesting this

- The right to request erasure of personal data (*where applicable*) or to restrict processing in accordance with data protection laws, as well as to object to any direct marketing from us and to be informed about any automated decision-making that we use
- The right to lodge a complaint or seek judicial remedy and who to contact in such instances

Information Security & Technical and Organisational Measures

FanHub takes the privacy and security of individuals and their personal information very seriously and takes every reasonable measure and precaution to protect and secure the personal data that we process. We have robust information security policies and procedures in place to protect personal information from unauthorised access, alteration, disclosure or destruction and have several layers of security measures.

Amendments to this Privacy Policy

FanHub may change its Privacy Policy from time to time and at FanHub's sole discretion. The date of the most recent revisions will appear on this page. If material changes are made to the Privacy Policy, we will notify you by placing a prominent notice on our website or by sending you a notification in relation to this. We will not process Account-Related Information in a manner not contemplated by this Privacy Policy without your consent.

Privacy and Data Security Roles and Employees

FanHub have designated **Ali Tavallai** as our Data Protection Officer and have appointed a data privacy team to develop and implement our roadmap for complying with changing data protection Regulation. The team is responsible for promoting awareness of the GDPR and data security policies across the organisation, identifying any gap areas and implementing the new policies, procedures and measures.

FanHub understands that continuous employee awareness and understanding is vital to the continued compliance of the changing landscape of data regulations and have involved our employees in our preparation plans. We have implemented an employee training program which is provided to all employees and forms part of our induction and annual training program.

If you have any questions about our preparation for the GDPR, please contact Ali Tavallai.