Welcome to Falco's Website. This Website is administered by Falco (further: the "Company"). Please find below our Privacy Policy applicable to Falco website, application and services.

These Privacy Policy constitute a legally binding agreement made between you ("you") and Falco, a company incorporated in Cayman, including its subsidiaries and affiliates ("we", "us", or "our") concerning your access to and use of the https://falco.gg/ website as well as any other media form, media channel, mobile website or application related, linked, or otherwise connected thereto (collectively, the "Website" and the "Application").

In respect for your privacy and personal data this Privacy Policy describes and explains to You how we collect, use, maintain and disclose and process your personal data obtained through our websites, applications, brands, services and products. When using our website and services, we may process personal data owned by You, which is why this Privacy Policy seeks to clarify our practices regarding the collection, use, disclosure and treatment in general of personal data of our users.

The present Privacy Policy does not apply to websites and other services that are owned and operated by unaffiliated third parties.

If you do not agree with the provisions of our Privacy Policy, you should immediately stop accessing or using our websites, applications, brands, services and products.

Our Application cannot be used by people under the age of 18 without parental consent. Therefore, to use our Application you acknowledge that you are above the age of 18 or you have parental consent if you are under the age of 18.

If we become aware that we have unknowingly collected Personal Data of people under the age of 18 without parental consent, such data will be deleted by the Company as soon as possible.

1. Definitions

Capitalized terms within the present Privacy Policy refer to the following:
Personal Data: information related to an identified or identifiable natural person, so that any information that makes it possible to identify a natural person is considered personal data.
Sensitive Personal Data: Personal Data relating to racial or ethnic origin, religious conviction, political opinion, membership of a trade union or religious organization, philosophical or political nature, data relating to health or sex life, genetic or biometric data, when linked to a natural person.

Anonymized Data: data relating to the subject that cannot be identified, considering the use of reasonable technical means available at the time of its treatment.
Database: structured set of Personal Data, established in one or several places, in electronic or physical support.
Data Subject: natural person to whom the Personal Data being processed belongs.
Treatment Agents: the controller and the operator.
Controller: natural person or legal entity, governed by public or private law, responsible for decisions regarding the processing of Personal Data, such as Falco, including its subsidiaries and affiliates.
Operator: natural or legal person, governed by public or private law, who processes Personal Data on behalf of the Controller.
Treatment: any operation carried out with Personal Data, such as those relating to the gathering, production, reception, classification, use, access, reproduction, transmission, distribution, processing, archiving, storage, elimination, evaluation or control of information, modification, communication, transfer, diffusion or extraction.
Anonymization: use of reasonable technical means available at the time of Treatment, through which data loses the possibility of association, directly or indirectly, with an individual, making its identification impossible.
Consent: freely given, specific, informed and unambiguous expression by which the Data Subject agrees to the processing of his/her Personal Data for a specific purpose.
Block: temporary suspension of any Treatment operation, by keeping Personal Data or Database.
Elimination: elimination of data or a set of data stored in a Database, regardless of the procedure used.
Shared Use of Data: communication, dissemination, international transfer, interconnection of Personal Data or shared Treatment of Database by public agencies and entities in the fulfillment of their legal competences, or between these and private entities, reciprocally, with specific authorization, to one or more Treatment modalities allowed by these public entities, or between private entities.

2. Evolution of the privacy policy

Falco reserves its right to amend or supplement the Privacy Policy at any time and without prior notice, except in the case of express legal provision to the contrary. Any change in the present Privacy Policy will be reported by the update of the “last updated” date above associated with the updated terms. The modifications to the Privacy Policy made by Falco will apply immediately. In this sense, it is your responsibility to reread these Privacy Policy in case of any modification, according to the updated data at the top of this document. If you disagree with the updated terms, You have the right to withdraw your Consent.

3. Data subject rights

In compliance with GDPR (General Data Protection Regulation), Data Subject has the right to:

(i) confirm the existence of the processing and treatment of Personal Data;
(ii) access Personal Data;
(iii) correct incomplete, inaccurate or outdated Personal Data;
(iv) request Anonymization, Block, Elimination of unnecessary or excessive Personal Data;
(v) request information about the public or private entities with which your Personal Data has been shared, under the terms of the Privacy Policy;
(vi) request information about the consequences of not providing your Consent;
(vii) withdraw Consent;
(viii) request a copy of: a) the categories and specific Personal Data that are collected, b) the purpose of collecting Personal Data, c) the categories and specific third parties with which Personal Data is shared;
(ix) oppose the Treatment of Personal Data;
(x) request the review of automated decisions, if, eventually, any decision of this nature is taken.

Whenever possible, Personal Data will be deleted after Treatment or will be Anonymized, using techniques available at the time.

It is possible to maintain certain Personal Data in the Company's Database, if such action proves necessary: to comply with applicable legislation or to enable the exercise of the Company's rights in judicial, administrative or arbitration proceedings.

You are aware that the request for the Elimination of Personal Data does not guarantee the complete or comprehensive removal of the content or information relating to Personal Data, in cases where the maintenance of data in our Database is necessary for the strict fulfillment of a legal duty.

4. Reasons of the treatment (personal data)

Personal Data will not be used without adequate justification, provided by the applicable law, for this purpose. In this sense, the Treatment of your Personal Data will only be treated in the following situations, alternatively:

(i) if Consent has been obtained for the Treatment of Personal Data;
(ii) if the Treatment is necessary to perform the services obligations assumed with you;
(iii) to comply with legal or regulatory obligations that require the Treatment of Personal Data;
(iv) if the Treatment of Personal Data is necessary for the purposes of attending the legitimate interests of the Company, provided that, in this case, it does not unduly affect the fundamental rights and freedoms of the Data Subject. Examples of situations that constitute the Company's "legitimate interest" are data Treatment activities carried out for: (a) operations related to the provision of services; (b) responding to

requests; (c) development of the Company's core business, among others;

(v) for the purpose of managing adverse events, carrying out prevention/investigation activities, complying with administrative formalities, records, declarations or audits;

(vi) to enable access to Website and Applications and virtual platforms, manage accounts, perform entry and exit control, among other electronic control platforms;

(vii) to support the Data Subject, provide information about the services and manage other claims;

(viii) identify access credentials, including passwords, password hints, emails, security information and questions, registered identification (ID) and other data;

(ix) crypto wallet address, including related data used to detect cryptocurrency and NFT holdings. The data may be used to track your devices and connect you to alternative datasets, including but not limited to, discord data, social media data, chat programs, your wallet, and game related data.

(x) information deemed necessary to Anti-Money Laundering ("AML"), Counter Financing of Terrorism ("CFT"), and Know Your Customer ("KYC") compliance purposes.

(xi) phone number when some services use two-factor authentication

(xii) in-game activity, quests and games completed, NFT transactions, and avatars created;

(xiii) send news and information about products and services;

(xiv) for the purpose of complying with judicial, administrative or arbitration subpoenas;

(xv) for the purpose of provide the services' functionality, guarantee access to registered account, completing transactions, provide special promotion and benefits and others;

(xvi) if the Consent is given by the Data Subject;

(xvii) for the purpose of enabling the sale of its assets, in order to allow the total or partial acquisition by third parties;

(xviii) identification and registration of the Data Subject in the Company's Databases, making it possible to receive Personal Data from your profile, such as navigation, registration or contact data;

(xix) in order to provide sufficient information to the competent sector for the purpose of NFT transactions;

(xx) respond to any queries made by the Data Subject, including orders, purchases and cancellations, if applicable;

(xxi) carry out analyses, quality control, research on the effectiveness of the activities developed by the Company;

(xxii) respond to requests from public and governmental authorities, national or foreign;

In cases where the Company receives Personal Data from third parties, the Company will assume that prior authorization has been obtained from the Data

Subject, by this third party, or that there is a legal basis capable of supporting such sharing.
If the Data Subject has doubts as to the regularity of the Treatment of their Personal Data, they may contact the Company's DPO directly through the electronic address provided at the beginning of this Privacy Policy.

5. Types of personal data treated by the company

As a rule, and without prejudice of other types of personal data information, we collect email addresses and associate them with Launcher IDs via form when You log in through our website or through a launcher when launching the game. This information is used to user accounts so they can log in from different sources and access their in-game information. Thus, we guide ourselves, where applicable, by gaming industry standards from the International Game Developers Association (IGDA – https://igda.org/resourcelibrary/game-industry-standards/). Falco is not bound by such standards but will apply them where feasible. The below information related with the types of personal data treated by the company shall prevail.

In its legitimate interest and in accordance with the governing legislation, in order to facilitate the provision of services, the Company processes the following categories of Personal Data:

(i) financial or payment information: crypto wallet address, including related data used to detect cryptocurrency and NFT holdings;

(ii) registration information: full name, date of birth, gender, identity documents, username and password, ID and Individual Taxpayer Registration;

(iii) behavioral information: access logs, click data and other data collected including through technologies;

(iv) browsing data: server log information, device IP (internet protocol) address, access to dates and times, operating system, browser type, Internet service provider ("ISP"), location blockchain and other distributed ledger technologies (DLT's) analytics information related to blockchain or other DLT's addresses you provide;

(v) cookie data: cookies, pixel tags and other similar technologies. Falco may utilize cookies, web beacons, links, and other tracking technologies to monitor your usage and engagement with the Services, with the aim of analyzing and enhancing their performance. Through these technologies, Falco may collect information about your online activities, including your interactions with our email communications, third-party services, and client applications, as well as certain online activities that occur after you have exited the Services. Link data is typically examined in an aggregate manner. Disabling cookies may impede the proper functioning of certain Services. The data collected through these technologies may consist of analytics information, details about the websites you visited prior to accessing our Services, information about

your browser and operating system, and tracking data pertaining to your interactions with our content and email communications;

(vi) contact details: registered address, email, phone number;

(vii) Public information: Falco has the ability to gather data about you from sources that are available to the public. Any information that you voluntarily disclose in public or open forums, such as social media platforms, is considered public information under Falco's Privacy Policy and can be obtained and gathered by Falco. It is important to note that any content or information that you provide to third parties in connection with the Services is not considered private or confidential, and Falco cannot be held responsible for any such information or content. If you do not want certain information to be public, it is recommended that you refrain from sharing it;

(viii) Log file information: When using our Services, Falco may obtain log file information, such as your browser type, IP address, domain names, access times, operating system, location, referring web pages, pages visited, search terms, cookie information, as well as device and application IDs. Log file data is acquired whenever you interact with our Services, including visiting our websites, signing into our Services, or engaging with our email notifications. Falco utilizes log file data to provide, comprehend, and enhance our Services, as well as to personalize the content we present to you. Falco may correlate this log file with other information gathered about you through our Services.

6. Data collection method

The data Treated by the Company may be collected by the following methods:

(i) direct provision by the Data Subject;

(ii) receipt of personal data by third parties by sharing data from partners or service providers; and

(iii) automatically collects upon access to our Website or Application, including: characteristics of the device used for access, browser used to access, IP origin (with date and time), information about your interaction on our page, information that will be collected through cookies.

7. Third parties: identification and sharing

The Company guarantees that everyone who has access to the Personal Data under its care undertakes to maintain absolute secrecy regarding them. Falco's staff may access your information as required to provide and maintain the Services in the course of regular business activities. This may involve accessing data relating to your usage and engagement with the Services.

Also, besides following the best practices from our providers (AWS) to store information in the safest way, the Company has split accounts for development and production, so there's separation of duties between internal accounts.
The Company informs that it may share Personal Data with partners, in the development and provision of services or offer of products, always in accordance with the Company's values.
Falco collaborates with various individuals and organizations ("Service Providers") to aid in providing the Services to you, including website and data hosting companies, and entities that provide analytical information like Google Analytics. For the purpose of providing the Services, we may disclose your personal information to our Service Providers. This may encompass data you provide to us, as well as information collected about you, such as Personal Data and details obtained through data collection tools such as cookies, web beacons, log files, Unique Identifiers, and location data, provided we have the legal authority to do so. Falco takes reasonable measures to ensure that our Service Providers are legally obligated to safeguard your information on our behalf, as required by applicable laws. If Falco becomes aware that a Service Provider is improperly utilizing or revealing information, we will take commercially reasonable measures to put an end to or rectify such improper conduct.
The Company has the potential to purchase other companies or their assets, sell off our business assets, or participate in events like mergers, acquisitions, bankruptcies, reorganizations, or asset sales - all of which are known as "Business Transactions". As part of such transactions, it is possible that your information, including Personal Data, may be sold or transferred along with the assets involved.
The Company also emphasizes that it may share the Personal Data under its custody with authorities, governmental entities, national or foreign, or other third parties, for the protection of its interests, in cases where there is any type of conflict, whether of a judicial or administrative.
It is also possible to share Personal Data with third parties when such action proves necessary to comply with legal or regulatory obligations.
In the case of operations involving the Company, it will be possible to share Personal Data with third parties, taking the necessary measures to ensure that privacy rights continue to be protected, in accordance with this Privacy Policy.
The Personal Data held by the Company will also be shared with third parties in the event that such action proves necessary to comply with a court order or at the request of administrative authorities that have legal competence for such request.
It is legitimate to share Personal Data with other companies that may become part of the Company's group.
Personal Data may be shared with marketing partners for the purpose of carrying out marketing actions, provided that there is a legal basis for this and there is no economic exploitation of such data.
Under no circumstances will we sell, share or with economic content, transfer Personal Data with third parties.
In the provision of services and in compliance with the present Privacy Policy, Persona Data could be accessed by: a) our employees (including employees or departments) in the exercise of their functions; b) our service providers who

provide us with products and services; c) our technology systems providers, cloud service providers (“cloud”), base providers and consultants; d) our partners who, together, offer products or services in our line of work; e) any third parties to whom we have transferred our rights and obligations; and f) our external consultants and lawyers.
The aforementioned agents are contractually obliged to protect the confidentiality and security of Personal Data and to comply with the provisions of the General Data Protection Regulation (GDPR).
Personal Data may be processed, accessed or stored in a country other than the Company's headquarters, since such country offers the same level of protection of Personal Data provided for in European legislation.
In the case mentioned above, we ensure that, when sharing Personal Data with companies or third-party located in other jurisdictions, we will ensure the application of the level of protection required by the Personal Data protection/privacy legislation applicable to the Company and we will ensure that we act in accordance with our policies and patterns.

8. Duration of the treatment of Personal Data

As previously informed, all the aforementioned agents have a contractual obligation to protect the security and confidentiality of Personal Data, and must fully comply with all provisions of the General Data Protection Regulation (GDPR).
In this sense, all Personal Data will be retained by the Company for the period necessary to achieve the purposes and objectives described in this Privacy Policy or when there is specific Consent to do so, except in the event that applicable legislation requires or allows a longer retention period.
The Company will Eliminate all Personal Data treated in the event that they become unnecessary for the purposes for which they were collected in the first place.
The Treated Personal Data will also be Eliminated upon the express request of the Data Subject, except in situations whose maintenance is authorized by law, including with regard to the need to comply with a legal obligation, regulatory obligation or when there is a need for exclusive use by the Company, which includes its use for the exercise of the Company's rights in judicial or administrative proceedings.
Personal Dara will be deleted upon express request, provided that such request is accepted, considering the following case scenarios: a) Personal Data collected with Consent; b) Personal Data considered excessive or unnecessary; c) when the Company fails to comply with the rules set forth in the General Data Protection Regulation (GDPR).
Personal Data will not be Eliminated when the maintenance of its treatment proves necessary for: a) compliance with a legal obligation or regulatory obligation; b) transfer to a third party (in compliance with the requirements for data processing in this case); and c) exclusive use by the Company (including for the exercise of rights held by it in judicial or administrative proceedings).

9. Measures taken to protect personal data

The Company adopts technical and administrative measures capable of guaranteeing the protection of Personal Data, observing the necessary levels of security and confidentiality. The Company would audit logs and find the source of any breaches to the best of its abilities. The Company would also employ security auditing and penetration testing consultants to review internal practices.

The protection of Personal Data collected in compliance with this Privacy Policy is carried out in line with the best security practices used by the market, including with regard to the prohibition of unauthorized access.

In addition to the security measures already adopted, we follow standards of conduct that must be observed by our employees to ensure greater effectiveness in the protection of Personal Data, such as:

(i) use of the best physical, technical and administrative measures to reduce the risk of loss, misuse, unauthorized access, disclosure or modification of Personal Data.
(ii) use of encryption.
(iii) access to authorized persons only.
(iv) identified access control.
(v) personal and non-transferable passwords.
(vi) periodic updating of passwords.
(vii) hosting and storing information in secure environments.
(viii) restricted access to the place where Personal Data are stored.
(ix) enforcement of confidentiality for everyone who has access to Personal Data.
(x) prohibition on providing the registration password to third parties.
(xi) immediate change of access credentials in case of unauthorized use or suspected use.
(xii) use of the "https:" model, evidencing that the connection to the website is secure.

All measures aim to preserve the integrity of Personal Data against: a) unauthorized access; b) accidental or unlawful situations of destruction, loss, alteration, communication or dissemination; or c) any other form of illicit treatment.

In addition to the measures listed above, we strongly recommend that you make all the communication with the Company, including the communication related to Personal Data, through official channels and avoid insecure channels.

The Company highlights that, even if the best efforts and the latest technologies are adopted to preserve privacy and Personal Data, no transmission of information is invulnerably secure, being therefore susceptible to the occurrence of technical failures, cyber-attacks through viruses, among others. Despite this, the Company values transparency and will immediately inform the Data Subject if any event of this nature occurs.

10. Additional information regarding international and cross-border transfer of personal data

By using the Services, you agree that your information may be transferred to countries outside of your country of residence, including the United States and the European Union, which may have different data protection laws from your country. Your Personal Information may be stored and processed in any country where we have facilities or where we hire service providers. Certain circumstances may provide those other nations' courts, law enforcement, regulatory, or security authorities access to your personal information.

11. Additional information regarding California residents

We provide the extra information below on the kinds of Personal Information that we collect, use, and disclose about California residents in accordance with the California Consumer Privacy Act of 2018 ("CCPA"). If the Personal Information we gather about a job candidate, an employee, a contractor, an owner, a director, or an officer pertains to their current, past, or prospective involvement with us, this section does not apply to such people.

The categories of Personal Information about California residents that we intend to collect are listed below, along with the categories of Personal Information that we have already gathered and released for our day-to-day business operations during the past 12 months.

Personal Information Categories	For Operational Business Purposes, disclosed to Which Categories of Third Parties
usernames, contact details, IP addresses, and other internet identifiers	Affiliates, service providers (such as IT services, data storage, server providers, hosting), commercial partners, co-promoters of events, sponsors of contests, debt collectors, operators of payment systems, and legal authorities
Personal information as defined California Customer Records statute (examples: name, contact information, digital asset wallet address)	Affiliates, service providers (such as IT services, data storage, server providers, hosting), commercial partners, co-promoters of events, sponsors of contests, debt collectors, operators of payment systems, and legal authorities
Commercial Information (examples: transaction information, purchase history; purchase history for digital assets as well as any further digital goods examined, added to the shopping cart, or otherwise show interest in	Affiliates, service providers (such as IT services, data storage, server providers, hosting), commercial partners, co-promoters of events, sponsors of contests, debt collectors, operators of payment systems, and legal authorities

Internet or network activity information (examples: IP address, browser kind and version, time and date stamps, device type, operational system, error logs, browsing and search history, information about the usage of our services)	Affiliates, service providers (such as IT services, data storage, server providers, hosting), commercial partners, co-promoters of events, sponsors of contests, debt collectors, operators of payment systems, and legal authorities
Geolocation Data	Affiliates, service providers (such as IT services, data storage, server providers, hosting), commercial partners, co-promoters of events, sponsors of contests, debt collectors, operators of payment systems, and legal authorities
Audio and Video Data	Affiliates, service providers (such as IT services, data storage, server providers, hosting), commercial partners, co-promoters of events, sponsors of contests, debt collectors, operators of payment systems, and legal authorities
Product preferences	Affiliates, service providers (such as IT services, data storage, server providers, hosting), commercial partners, co-promoters of events, sponsors of contests, debt collectors, operators of payment systems, and legal authorities

To run, administer, and maintain our business, to deliver our goods and services, and to fulfill our corporate goals and objectives, we utilize certain types of personal information. This includes utilizing personal information to:

(i) Respond to your enquiries and fulfill your demands;
(ii) Create, enhance, fix, deliver, and maintain our goods and services; Customize, promote, and market our goods and services;
(iii) perform analytics, research, data analysis, data aggregation, and data anonymization;
(iv) protect our records and property, and implement quality- and safety-assurance procedures;
(v) Control and monitor risk and security, and identify and stop fraud;
(vi) Perform identification verification, accounting, auditing, and other internal tasks including record-keeping and internal investigations.
(vii) Implement business transactions such as mergers, joint ventures, or acquisitions; abide by internal policies, laws, and legal processes; and assert and defend legal claims.

You may be entitled to the rights listed above with regard to the Personal Information we have gathered about you if you reside in California. We are aware that your jurisdiction may grant you extra rights. To exercise your rights under data protection, you can get in touch with us directly at any time.

(i) provide you with the following details pertaining to the 12 months before your request:
   a. The types of Personal Information we collected about you, the types of sources from which we obtained such Personal Information,
   b. the specific Personal Information we collected about you,
   c. the business or commercial purpose for collection (if applicable),
   d. the types of Personal Information we otherwise shared or disclosed about you, and
   e. the types of third parties with whom we shared or to whom we disclosed Personal Information (if applicable).

(ii) Delete the personal data we have about you.

Your request will be taken into account in line with any relevant legislation. Therefore, these rights are not absolute, though, and in some circumstances, we may reject your request in accordance with the law. In order to exercise your CCPA rights, you are not entitled to any form of unlawful discrimination.

You may contact us via email at support@faloc.gg to exercise your rights. We may ask you for appropriate documentation proving your identity as an authorized agent as part of our verification procedure, which may include:

(i) a copy of your certificate of registration as a business entity with the California Secretary of State;

(ii) a copy of the resident's power of attorney, as required by Probate Code sections 412 through 4130;

(iii) Permission in writing from the resident for you to submit a request on their behalf.

12. Additional information regarding EU/UK residents

Residents of certain other countries, including those in the European Economic Area and the United Kingdom (collectively, the "EEA" for the purposes of this part of the Privacy Policy), are entitled to certain rights and disclosures with regard to their personal data. The legal grounds for gathering and utilizing your personal data are:

(i) the fulfillment of your agreement, the signing of the agreement, and the completion of your requests (examples: completing the registration for your account, offering you our Services and goods, and offering you customer assistance);

(ii) Our proper commercial interests (examples: fraud protection, upkeep of our network and Services' security, direct marketing to you, and upkeep, analysis, and improvement of our goods and services);
(iii) fulfillment of a statutory requirement (examples: keeping administrative documents that must meet strict retention requirements).
(iv) to authenticate your identity when you make requests to exercise your rights and to record those requests.
(v) Where we don't have a different legal basis, we will use the consent you give. The Consent can be withdrawn at any time

If you reside in the EEA and UK, you have some types of rights related to your personal data:

(i) access your private information;
    a. know what personally identifiable information we have about you, how we use it, and with whom we share it.
(ii) rectify incorrect personal information;
(iii) request:
    a. the deletion of your personal data;
    b. that your personal data be processed in a limited manner;
    c. the transfer/portability of your provided personal data;
(iv) protest and object to the use of your personal information.
(v) Withdrawal of consent

We may transmit, store, and process the personal data we obtain from you in locations outside of the European Economic Area (EEA) and the United Kingdom (UK). Additionally, employees of ours or one of our partners' or third-party service providers' that are based outside the EEA and the UK may process your personal information on our behalf.

We may transfer personal data from the EEA to third countries outside of the EEA due to contractual obligations which are referred to as transfers that are required to fulfill our contract obligations to you, in order to provide you with our services, customer support services, and to enhance our services.

We shall take all reasonable measures to guarantee that your personal information is handled securely and in compliance with this Privacy Policy.

According to EEA criteria, the European Commission has recognized certain non-EEA nations as offering an appropriate degree of data protection. The EEA and the designated nations are acknowledged by the UK as offering an appropriate degree of data protection in accordance with UK criteria.

We have put in place suitable safeguards, such as standard contractual provisions established by the relevant authorities, to protect your Personal Information for

transfers from the EEA or the UK to nations not deemed adequate by the European Commission or the UK government.

You may contact us via email at suppor@falco.gg to exercise your rights. We will get back to you as soon as possible.

13. Changes to this privacy policy

Falco reserves its right to modify our privacy policy at any time to take into account modifications to our business procedures, accepted industry standards, or alterations to laws or regulations. If we decide to modify this privacy statement, we will post the updated terms at the same location where you now view this privacy statement, along with the date that it was last updated. Updates to our privacy policy only apply to data gathered after the change's effective date.

Please routinely check the website for notifications of updates to our privacy policy. We shall get in touch with you (in accordance with your chosen choices for communications from us) and all of our registered users with the new information and links to the updated or revised policy if the changes are substantial or if required by applicable law.

If a new use of your personal information is necessary in order to comply with the law, we will request your consent or provide you with the option to opt in or out, as appropriate.

14. Miscellaneous

In the event that one or more provisions of the Privacy Policy is found to be invalid, unenforceable or of no effect, the Privacy Policy will retain its full force and scope and the validity of the remaining provisions shall not be affected thereby. The fact that Falco delays in exercising any of its rights under the Privacy Policy, or fails to exercise such rights shall not be construed as a waiver to exercise the aforementioned rights or obligation.