Vampire: The Masquerade – Bloodhunt

Privacy Policy

Last updated: 7 September 2021

Thank you for using our products and services! We respect your concerns about privacy and appreciate your trust and confidence in us.

Here is a summary of the information contained in this privacy policy ("**Privacy Policy**"). This summary is to help you navigate the Privacy Policy and it is not a substitute for reading everything! You can use the hyperlinks below to jump directly to particular sections.

What information do we need to provide Bloodhunt?

If you register an account to use Bloodhunt, then we will need some information from you such as your email, language, region, user name, password, IP address and OpenID to set this up. We also collect other information, including your region details, IP address and device and log information to personalise the gaming experience and enable Bloodhunt features, or to participate in Bloodhunt.

How will we use your information?

We use your information to provide the many functions in Bloodhunt and to improve Bloodhunt. We do not share your information with any third parties, except where we need to in order to provide Bloodhunt (e.g. to host your data in the cloud, to sign you up to our newsletters (with your consent), for customer support, analytics and advertising purposes), or where we are instructed to by a court, authority or otherwise compelled by law.

Who do we share your information with?

We use some third parties to help us deliver the best possible experience (e.g. to host your data in the cloud, to sign you up to our newsletters (with your consent), for customer support, analytics and advertising purposes). When we use a third party, we only do this to process or store your information for the purposes described in this Privacy Policy. We also have affiliates around the world who help us deliver Bloodhunt, and we may be required by a court or legal obligation to disclose certain information under certain circumstances.

Where do we process your information?

Our servers are located in the United States, Singapore and Sweden. Your information can be accessed from outside of where you live by our support, engineering and other teams around the world, including Singapore, the United States and Sweden. Your data will also be processed by our third-party partners in Bulgaria, Ireland, Singapore, Sweden and the United States.

How long do we keep hold of your information?

Unless otherwise specified in this Privacy Policy, we generally retain your information for the lifetime of your use of Bloodhunt and your Sharkmob account unless you request to delete your Sharkmob account or such data, in which case, the data will be deleted within 30 days of your request. If you do not request account deletion, your data (other than customer service data) will generally be retained for 1 year after Sharkmob is shut down, before it is deleted.

How can I exercise my rights over my information?

You may have certain rights with respect to your information, such as rights of access, to receive a copy of your data, or to delete your data or restrict or object to our processing of your data.

How to get in touch with us

If you have any questions about anything in this Privacy Policy, or want to exercise any of your rights, please contact us at privacy@sharkmob.com.

How will we notify you of changes?

Changes to this Privacy Policy will be posted in our Privacy Policy online. Please check this page frequently to see if there are any updates or changes to this Privacy Policy.

Contact Information

Data Controller: *Sharkmob AB | Email: Privacy@sharkmob.com*

Welcome to the Bloodhunt!

This Privacy Policy explains the *when*, *how* and *why* when it comes to the processing of your personal information in connection with the Vampire: The Masquerade – Bloodhunt (the "**Bloodhunt**") and sets out your choices and rights in relation to that information. Please read it carefully. It is important for you to understand how we collect and use your information, and how you can control it.

If you do not agree to the processing of your personal information in the way this Privacy Policy describes, please do not provide your information when requested and stop using Bloodhunt. By using Bloodhunt you are acknowledging our rules regarding your personal information as described in this Privacy Policy.

Bloodhunt has been developed by Sharkmob AB ("**we**", "**us**", "**our**").

For the purpose of data protection laws, the data controller of your personal information in relation to Bloodhunt is Sharkmob AB. The registered address of Sharkmob AB is Stortorget 11, 211 22 Malmö, Sweden.

Please reach out to us if you have any questions or concerns regarding the processing of your personal information: you can contact us at any time at Privacy@sharkmob.com.

Our representatives for data protection purposes in certain jurisdictions are as follows:

Korean representative, address and contact details:

Kite Bird Yuhan Hoesa

25F, 55, Sejong-daero, Jung-gu, Seoul (Taepyeongro 2-ga)

koreanlocalrep_sharkmob@proximabeta.com

Serbian representative, address and contact details:

Karanovic & Partners o.a.d. Beograd

Resavska 23, Belgrade, 11000, Serbia

local.representative@karanovicpartners.com

Turkish representative, address and contact details:

Özdağıstanli Ekici Avukatlık Ortaklığı.

Varyap Meridian Grand Tower ABlok Al Zambak Sok No: 2 K: 32 D. 270 Ataşehir Istanbul Turkey

localdatarep_sharkmob@iptech-legal.com

1. The Types of Personal Information We Use

This section describes the different types of personal information we collect from you and how we collect it. If you would like to know more about specific types of data and how we use that data, please see the section entitled *"How We Use Your Personal Information"* below.

The following is a high-level summary of the types of personal information we use:

a. Information you provide to us (either directly or through a third party)

- **Bloodhunt account registration, log-in and management:** Email address, verification code, language, region, username, password, IP address, OpenID, user ID, token;
- **Bloodhunt account friends list:** UID, token, user name;
- **Login (via Steam):** When you choose to log into Bloodhunt with your Steam account, we import information from your connected social media account in order to set up your profile. This will include your user ID/token, OpenID, nickname, profile picture (if any) and number of Steam friends relating to you and your Steam friends;
- **Voice chat (if you use voice chat in Bloodhunt):** IP address, session statistics;
- **Newsletter sign-up:** Operating system, browser language, country, IP address, sign-up date, email address, consent to email marketing, vampire type, battle statistics;
- **Email service management:** First login (date), time from first login, last login (date), time from last login, login record (yes/no), registration time, country, language, receiving subscription email address;
- **Customer support information (Zendesk):** First name, last name, email address;
- **Data collection and reporting (APAS):** We will collect your locational details (including region country, province, city), carrier ID and device information (including application version, battery level, Wi-Fi strength, available space, network type, operating system version, platform, device language, screen DPI, device resolution, brand, manufacturer, device model, RAM, ROM and CPU information);
- **Game data (including log information):** OpenID, IP address (only kept in aggregated format for server improvement), device model, details of platform, geographic ranking (manually selected by you), game play statistics (including levels and scores); and
- **Text chat data**: Chat data, anonymous ID, identity information (including user name, platform, comment time, comment content and judgement score).

b. Information about you generated as part of Bloodhunt

We automatically collect certain data from you when you use Bloodhunt, namely:

- **Customer service data:** When you choose to use our Customer Service, we will collect information such as your OpenID and gameplay information (including account ban duration, reasons for account ban, reason for account silence, silence time, item ID, number of items sent to player or deleted from player package, email subject sent to player, email content sent to player, silence start and end times);
- **Game behaviour data**: Identity information (including OpenID, country and role ID), login information (including login time, online time and play-mode) and payment information (including purchase time, purchase value, purchase items information, in-game currency balance collected on an aggregate level) which is not processed by us but by a third-party payment provider;
- **Security**: Security-related information (including a list of hack or cheating software, in-game screen

information), device information (including device operation system settings, device information including brand, model, CPU structure, CPU model, kernel version, resolution, application package of hack software and available memory) and information about your Internet connection including the Wi-Fi name (if applicable) and a list of installed and running apps;

- **Crash information (Sentry)**: IP address, game directory.

2. Cookies

We use cookies and other similar technologies (e.g. web beacons, log files, scripts and eTags) ("**Cookies**") to enhance your experience using Bloodhunt. Cookies are small files which, when placed on your device, enable us to provide certain features and functionalities.

3. Children

Children may not use Bloodhunt for any purpose, except where their parent or guardian has provided consent (to the extent this option is available in your jurisdiction).

By children, we mean users under the age of 18 years old; or in the case of a country where the minimum age for processing personal information differs, such different age. For users located in certain countries we have listed the relevant minimum age below.

Algeria 19

Argentina 18

Australia 18

Bangladesh 18

Brazil 18

Colombia 18

Cambodia 18

Canada 13

Egypt 18

European Economic Area/Switzerland 16

Hong Kong 18

India 18

Indonesia 21

Japan 20

Kingdom of Saudi Arabia 15

Kuwait 21

Macau 18

Malaysia 18

Mexico 18

Morocco 18

Myanmar 18

New Zealand 16

Philippines 18

Qatar 18

Republic of Korea 14

Russia 14

Singapore 18

South Africa 18

Sri Lanka 18

Taiwan 20

Thailand 20

Tunisia 18

Turkey 18

United Arab Emirates 21

United Kingdom 13

United States 13

Vietnam 16

We do not knowingly collect personal information from children under these ages for any purpose. If you believe that we have personal information pertaining to a child under these ages without parental/guardian consent, or if you are the parent or guardian of the user and wish to withdraw consent, please contact us at Privacy@sharkmob.com and we will delete such information.

4. How We Use Your Personal Information

This section provides more detail on the types of personal information we collect from you, and why. For users who live in the United Kingdom, the European Economic Area, Switzerland or Turkey ("**Relevant Jurisdiction**"), it also identifies the legal basis under which we process your data.

Bloodhunt account registration, log-in and management: Email address, verification code, language, region, user name, password, IP address, OpenID, user ID, token. We use this information to allow you to log into your account for Bloodhunt in accordance with your request. This is necessary to perform our contract with you to provide Bloodhunt.

Bloodhunt account friends list: UID, token, user name. We use this information to display which friends are playing in game and to provide the voice chat function. This is necessary to perform our contract with you to provide the voice chat function in Bloodhunt.

Log-in (via Steam): If you choose to log into Bloodhunt with your Steam account, we import information from your connected social media account in order to set up your profile. This will include your user ID/token, OpenID, nickname, profile picture (if any) and number of Steam friends relating to you and your Steam friends. We use this information to allow you to log into your account for Bloodhunt in accordance with your request. This is necessary to perform our contract with you to provide Bloodhunt.

Voice chat (if you use voice chat in Bloodhunt): IP address, session statistics. We use this information to allow you to use VOIP in accordance with your request. This is necessary to perform our contract with you to provide the voice chat function in Bloodhunt

Newsletter sign-up: Operating system, browser language, country, IP address, sign-up date, email address, consent to email marketing, vampire type, battle statistics. We use this information to notify you of the latest news of Bloodhunt. We collect this information after you have consented to the processing of such information.

Email service management: First login (date), time from first login, last login (date), time from last login, login record (yes/no), registration time, country, language, receiving subscription email address. We use this information to maintain our relationship with you and to solve customer support queries via email. This is necessary to perform our contract with you and to assist you with customer support queries regarding Bloodhunt.

Customer support information (Zendesk): First name, last name, email address. We use this information as a customer service support tool to support the customer service functionality provided by Pontica Solutions.

Data collection and reporting (APAS): We will collect your locational details (including region country, province, city), carrier ID and device information (including application version, battery level, Wi-Fi strength, available space, network type, operating system version, platform, device language, screen DPI, device resolution, brand, manufacturer, device model, RAM, ROM and CPU information). We use this information for user acquisition purposes and to monitor the effectiveness of our advertisements via analytics. We have a legitimate interest in processing this information to monitor the effectiveness of our advertisements.

Game data (including log information): OpenID, IP address (only kept in aggregated format for server improvement), device model, details of platform, geographic ranking (manually selected by you), game play statistics (including levels and scores). We use this information to identify you in Bloodhunt logs and to allow you to connect to Bloodhunt. This is necessary to perform our contract with you to provide Bloodhunt.

Text chat data: Chat data, anonymous ID, identity information (including user name, platform, comment time, comment content and judgement score). We use this information to facilitate the posting of your communications with other users. This is necessary to perform our contract with you to provide the text chat function in Bloodhunt.

Customer service data: When you choose to use our Customer Service, we will collect information such as your Open ID and gameplay information (including account ban duration, reasons for account ban, reason for account silence, silence time, item ID, number of items sent to player or deleted from player package, email subject sent to player, email content sent to player, silence start and end times). We use this information to improve Bloodhunt, including the functionality of Bloodhunt; and to provide troubleshooting functions such as addressing and remedying technical issues and bugs. This is necessary to perform our contract with you to provide Bloodhunt and to assist you with customer support queries regarding Bloodhunt.

Game behaviour data: Identity information (including OpenID, country and role ID), login information (including login time, online time and play-mode) and payment information (including purchase time, purchase value, purchase items information, in-game currency balance). We use this information in order to improve the game experience and features so you can enjoy the game. We collect payment information (via Steam) on an aggregate level to adapt the game and our in-game offerings to provide a great game experience, maximize revenue and to allow you to make payments through a third-party payment platform. We have a legitimate interest in processing this information to improve the game experience.

Security data: Security-related information (including a list of hack or cheating software, in-game screen information), device information (including device operation system settings, device information including brand, model, CPU structure, CPU model, kernel version, resolution, application package of hack software and available memory) and information about your internet connection including if applicable the Wi-Fi name and a list of installed and running apps. We use this information in order to secure your use of Bloodhunt. This is necessary to perform our contract with you to provide Bloodhunt.

Crash information (Sentry): IP address, game directory. We use this information in order to improve the game experience and features so you can enjoy the game. We collect this information after you have consented to the processing of such information.

5. How We Store and Share Your Personal Information

Our corporate group operates around the world. Pursuant to our contract with you to provide you with Bloodhunt, your personal information may be processed on servers that are not located where you live. No matter where our servers are located, we take appropriate measures to safeguard your rights in accordance with this Privacy Policy. Our Bloodhunt servers are located in the United States, Singapore and Sweden.

In addition, your information can be accessed from outside of where you live by our support, engineering and other teams around the world, including Bulgaria, Ireland, Singapore, Sweden, and the United States.

By clicking "accept", you consent to the cross-border transfer of your information to any country where we or our partners have databases or affiliates and, in particular, to Bulgaria, Ireland, Singapore, Sweden and the United States.

We will share your personal information with third parties ***only where necessary***. Situations where this occur are:

- **Third parties** that provide services in support of Bloodhunt, including providing cloud server space to process the information identified in this policy on a cloud server, signing you up for our newsletters (with your consent), providing you with crash report services, providing customer support services, processing gameplay statistics for analytics purposes, improving gameplay, and processing payments (such as via Steam). All companies providing services for us are prohibited from retaining, using, or disclosing your personal information for any purpose other than providing us with their services.

- **Companies within our corporate group** who process your personal information in order to operate Bloodhunt and conduct surveys for us. All related group companies may only use your personal information in accordance with this Privacy Policy.

- **Regulators, judicial authorities and law enforcement agencies, and other third parties for safety, security, or compliance with the law.** There are circumstances in which we are legally required to disclose information about you to authorities, such as to comply with a legal obligation or processes, enforce our terms, address issues relating to security or fraud, or protect our users. These disclosures may be made with or without your consent, and with or without notice, in compliance with the terms of valid legal process such as a subpoena, court order or search warrant. We are usually prohibited from notifying you of any such disclosures by the terms of the legal process. We may seek your consent to disclose information in response to a government entity's request when that government entity has not provided the required subpoena, court order or search warrant. We may also disclose your information to:

    - enforce our terms and conditions and other agreements, including investigation of any potential violation thereof;

    - detect, prevent or otherwise address security, fraud or technical issues; or

- protect our rights, property or safety, as well as those of our users, a third party or the public as required or permitted by law (exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction).

- **A third party that acquires all or substantially all of us or our business.** We may also disclose your information to third parties if we either: (a) sell, transfer, merge, consolidate or reorganise any part(s) of our business, or merge with, acquire or form a joint venture with, any other business, in which case we may disclose your data to any prospective buyer, new owner, or other third party involved in such a change to our business; or (b) sell or transfer any of our assets, in which case the information we hold about you may be sold as part of those assets and may be transferred to any prospective buyer, new owner, or other third party involved in such sale or transfer.

6. The Security of Your Personal Information

We are committed to maintaining the privacy and integrity of your personal information no matter where it is stored. We have information security and access policies that limit access to our systems and technology, and we protect data through the use of technological protection measures such as encryption.

Unfortunately, the transmission of information via the Internet is not completely secure. Although we will implement and maintain reasonable measures to protect your personal information, we cannot guarantee the security of the information transmitted via Bloodhunt or otherwise via the Internet; any transmission is at your own risk.

7. Data Retention

We do not keep your data for longer than is necessary unless we are required to do so under law. For further details on how long we keep your data, please refer to the time periods set out below.

Bloodhunt account registration, Bloodhunt account login, Bloodhunt account management, Bloodhunt account friend list and login (via Steam) are stored for the duration of your use of Bloodhunt (unless a deletion request is received, in which case data is deleted within 30 days). If you do not request account deletion, your data will be retained for 1 year after Sharkmob is shut down, before it is deleted.

Voice chat (if you use voice chat in Bloodhunt) is stored for 90 days before automatic deletion (unless a deletion request is received, in which case data is deleted within 30 days).

Newsletter sign-up (via Mailchimp) is stored for 30 days before deletion.

Email service management is stored for the duration of your use of Bloodhunt (unless a deletion request is received, in which case data is deleted within 30 days).

Customer service (Bloodhunt) data is stored for the duration of your use of Bloodhunt (unless a deletion request is received, in which case data is deleted within 30 days). If you do not request account deletion, your data will be retained for 5 years.

Data collection and reporting (APAS) is stored for 7 days before automatic deletion.

Game data (including log information) is stored for the duration of your use of Bloodhunt (unless a deletion request is received, in which case data is deleted within 30 days).

No text chat data is stored.

Customer service (Bloodhunt) data is stored for the duration of your use of Bloodhunt (unless a deletion request is received, in which case data is deleted within 30 days). If you do not request account deletion, your data will be retained for 5 years.

Game behaviour data is stored for the duration of your use of Bloodhunt (unless a deletion request is received, in which case data is deleted within 30 days).

Security data is stored for 90 days (unless a deletion request is received, in which case data is deleted within 30 days) with the exception of the following:

- Malicious files: Stored for 3 years.

- Hardware information, cheat tool monitoring, player identification, game operations data, and troubleshooting logs: stored for 30 days.

- File sample collection and memory sample collection: stored for 7 days and then automatically deleted if the same sample information does not re-appear. If it is identified as a malicious file, however, it is stored for 3 years.

- Malicious game memory samples: Stored for 10 years (together with the associated account ID, date of registration and in-game user behaviour).

- For confirmed non-malicious files: Stored for 60 days

- For users' file MD5 records: Stored for 90 days.

- Actions, status collection, trail collection: Stored for 90 days.

- In-game process information and system information: Stored for 10 years and then manually deleted.

- Security authentication: Stored for 730 days and then automatically deleted.

Crash information (Sentry) is stored for 90 days before automatic deletion.

If we are required to retain your information beyond the retention periods set out above, for example to comply with applicable laws, we will store it separately from other types of personal information.

8. Your Rights

Some jurisdictions' laws grant specific rights to Bloodhunt users, which are set out in this section.

This section entitled "Your Rights" applies to users that are located in the Relevant Jurisdictions. If you are located in a territory outside a Relevant Jurisdiction, please refer to the Supplemental Jurisdiction-Specific Terms for an overview of your rights and how these can be exercised.

The sub-sections entitled "Access", "Correction", and "Erasure" also apply to users that are located in Canada, Argentina, India and Russia.

The sub-section entitled "Advertising" also applies to users that are located in Hong Kong, Macau, Japan, Malaysia, Singapore, Korea, Thailand, United States, Canada, Australia, New Zealand, Argentina, Brazil, Cambodia, Egypt, India, Indonesia, Laos, Maldives, Mexico, Morocco, Myanmar, Philippines, Russia, Sri Lanka, Taiwan, Turkey, UAE, Saudi Arabia and Vietnam.

You have certain rights in relation to the personal information we hold about you, depending on where you are located. Some of these only apply in certain circumstances (as set out in more detail below). We must respond to a request by you to exercise those rights without undue delay and at least within one month (though this may be extended by a further two months in certain circumstances). To exercise any of your rights, please contact us at Privacy@sharkmob.com.

Access

You have the right to access the personal information we hold about you, how we use it and who we share it with. If you want to access the information we are holding about you, please contact us at Privacy@sharkmob.com.

Portability

You have the right to receive a copy of certain personal information we process about you. This comprises any personal information we process on the basis of your consent or pursuant to our contract with you (e.g. game data), as described above in the section *"How we use your personal information"*. You have the right to receive this information in a structured, commonly used and machine-readable format. You also have the right to request that we transfer that personal information to another party, with certain exceptions. We will provide further information to you about this if you make such a request.

If you wish for us to transfer such personal information to a third party, please ensure you provide details of that party in your request. Note that we can only do so where it is technically feasible. Please note that we may not be able to provide you with personal information if providing it would interfere with another's rights (for example, where providing the personal information we hold about you would reveal information about another person or our trade secrets or intellectual property).

Correction

You have the right to correct any of your personal information we hold that is inaccurate. If you believe we hold any personal information about you and that information is inaccurate, please contact us at Privacy@sharkmob.com.

Erasure

You can delete your account, or remove certain personal information, by contacting us at Privacy@sharkmob.com.

We may need to retain personal information if there are valid grounds under data protection laws for us to do so (for example, for the defence of legal claims or freedom of expression) but we will let you know if that is the case. If you have requested that we erase personal information that has been made available publicly on the Service and there are grounds for erasure, we will use reasonable steps to try to tell others that are displaying the personal information or providing links to the personal information to erase it too.

Restriction of Processing to Storage Only

You have a right to require us to stop processing the personal information we hold about you other than for storage purposes in certain circumstances. Please note, however, that if we stop processing the personal information, we may use it again if there are valid grounds under data protection laws for us to do so (for example, for the defence of legal claims or for another's protection). As above, where we agree to stop processing the personal information, we will try to tell any third party to whom we have disclosed the relevant personal information so that they can stop processing it too.

Objection

You have the right to object to our processing of your personal information. We will consider your request in other circumstances as detailed below by contacting us at Privacy@sharkmob.com.

To the extent provided by applicable laws and regulations, you may withdraw any consent you previously provided to us for certain processing activities by contacting us at Privacy@sharkmob.com. Where consent is required to process your personal information, if you do not consent to the processing or if you withdraw your consent, we may not be able to deliver the expected service.

Announcements

From time to time, we may send you announcements when we consider it necessary to do so (for example, when we temporarily suspend access to the Service for maintenance, or security, privacy or administrative-

related communications). You may not opt out of these service-related announcements, which are not promotional in nature.

Advertising

You may choose to stop receiving personalised advertising or marketing promotions from us when using the Service by clicking the unsubscribe button in our newsletter, or you can contact us at Privacy@sharkmob.com.

9. Contact & Complaints

Questions, comments and requests regarding this Privacy Policy are welcomed and should be addressed to Privacy@sharkmob.com.

If you wish to make a complaint about how we process your personal information, please contact us in the first instance at Privacy@sharkmob.com and we will endeavour to deal with your request as soon as possible. This is without prejudice to your right to launch a claim with the data protection authority in the country in which you live or work where you think we have infringed data protection laws.

10. Changes

If we make any material changes to this Privacy Policy, we will post the updated Privacy Policy here. Please check this page frequently to see if there are any updates or changes to this Privacy Policy.

11. Language

Except as otherwise prescribed by law, in the event of any discrepancy or inconsistency between the English version and local language version of this privacy policy, the English version shall prevail.

SUPPLEMENTAL TERMS – JURISDICTION-SPECIFIC

Some jurisdictions' laws contain additional terms for Bloodhunt users, which are set out in this section.

If you are a user located in one of the jurisdictions below, the terms set out below under the name of your jurisdiction apply to you in addition to the terms set out in our Privacy Policy above.

Algeria

By using Bloodhunt, you give us your consent for the collection, storage, treatment and use of your personal information, and transfer of your personal information to a third party (local cloud providers to back up your data or our affiliates around the world to help us deliver Bloodhunt) located in Bulgaria, Ireland, Singapore, Sweden, and the United States (as described in the Privacy Policy) where it is manually and electronically treated.

Argentina

Your rights

If you are dissatisfied with our response to your request for access to, correction, or erasure of your personal information or your privacy complaint in respect of your personal information, you may contact the Agency for Access to Public Information at: Av. Pte. Gral. Julio A. Roca 710, Piso 2°, Ciudad de Buenos Aires (Telephone: +5411 3988-3968 or email: datospersonales@aaip.gob.ar).

Data transfers

While we take reasonable steps to ensure that third-party recipients of your personal information comply with privacy laws that are similar to those of your jurisdiction, by providing us your personal information and by using Bloodhunt, you consent to the transfer of your personal information to a jurisdiction where privacy laws may not offer the same level of protection as the laws that may apply in Argentina.

Australia

Overseas Recipients

We take reasonable steps to ensure that third party recipients of your personal information located outside Australia handle your personal information in a manner that is consistent with Australian privacy laws. However, you acknowledge that we do not control, or accept liability for, the acts and omissions of these third-party recipients.

Access

You have the right to access the personal information we hold about you, how we use it and who we share it with. You can access the personal information you have made available as part of your account by logging into your account. If you believe we hold any other personal information about you, please contact us at Privacy@sharkmob.com.

Correction

You have the right to correct any of your personal information we hold that is inaccurate. You can access the personal information we hold about you by logging into your account. If you believe we hold any other personal information about you and that information is inaccurate, please contact us at Privacy@sharkmob.com.

Children

If you are under the age of 18, you confirm that you have the consent of your parent or legal guardian to register an account on and use Bloodhunt.

Transacting Anonymously

Where practicable, we will give you the option of not identifying yourself or using a pseudonym when registering an account on or using Bloodhunt. You acknowledge that if you do not provide us with your personal information, we may be unable to provide you with access to certain features or sections of Bloodhunt, including social media integration and purchases.

Your Rights

If you are dissatisfied with our response to your request for access to, or correction of, your personal information or your privacy complaint in respect of your personal information, you may contact the Office of the Australian Information Commissioner (Telephone +61 1300 363 992 or email enquiries@oaic.gov.au).

Data Transfers

While we take reasonable steps to ensure that third-party recipients of your personal information comply with privacy laws that are similar to those of your jurisdiction, you acknowledge and agree that we cannot control the actions of third-party recipients and so cannot guarantee that they will comply with those privacy laws.

Bangladesh

Agreement

By accepting this Privacy Policy, you expressly state that you authorise us to collect, use, store and process your personal data, including disclosing to third parties, to the extent provided by this Privacy Policy. By clicking "accept", you consent to the cross-border transfer of your information to any country where we have databases or affiliates and, in particular, to Bulgaria, Ireland, Singapore, Sweden, and the United States.

Age Restriction

In order to use Bloodhunt, you confirm that you are at least 18 years old and, therefore, legally capable of entering into binding contracts.

Brazil

This section applies to users located in Brazil:

Consent Revocation

Whenever we use your personal information based on your consent, you may revoke consent that you have previously given for the collection, use and disclosure of your personal information, subject to contractual or legal limitations. To revoke your consent, you can terminate your account or contact Privacy@sharkmob.com. This may affect our provision of Bloodhunt to you.

Parental and Guardian Consent

If you are under the age of 18, you should not use Bloodhunt for any purpose without first obtaining agreement to this Privacy Policy from your parent/guardian (both for themselves and on your behalf). We do not knowingly collect personal information from any children under the age of 18 without such consent. Please contact our Data Protection Officer if you believe we have any personal information from any children under the age of 18 without such parental/guardian consent – we will promptly investigate (and remove) such personal information.

BY ACCEPTING THIS PRIVACY POLICY, YOU EXPRESSLY STATE THAT YOU AUTHORISE US TO COLLECT, USE, STORE, AND PROCESS YOUR PERSONAL INFORMATION, INCLUDING, DISCLOSING TO THIRD PARTIES, TO THE EXTENT PROVIDED BY THIS PRIVACY POLICY

California

This section applies to California residents covered by the California Consumer Privacy Act of 2018 ("CCPA").

Collection and Disclosure of Personal Information

Over the past 12 months, we have collected and disclosed the following categories of personal information from or about you or your device:

- Identifiers, such as your email address, verification code, language, region, user name, password, IP address and OpenID. This information is collected directly from you.
- Internet or other electronic network activity information, such as your information regarding your use of Bloodhunt, and other device information as described in the main Privacy Policy. This information is collected directly from you and your device.

We collect your personal information for the following purposes:

- To provide you with Bloodhunt, maintain your account, provide customer service, track your payments information (including purchase time, purchase value, purchase items information, in-game currency balance).
- To improve our services, including the functionality of Bloodhunt.
- For security and verification purposes, including to prevent and detect fraudulent activity.
- To address and remedy technical issues and bugs.

For additional information about what each type of personal information is used for, see the chart in the main portion of the Privacy Policy.

- We disclose personal information to the following types of entities:
- Other companies within our corporate group who process your personal information in order to operate Bloodhunt.
- Other companies that provide services on our behalf in support of Bloodhunt and who are prohibited by contract from retaining, using, or disclosing personal information for any purpose other than for providing their services to us.
- Regulators, judicial authorities and law enforcement agencies.
- Entities that acquire all or substantially all of our business.

In the past 12 months, we have not sold the personal information of California residents within the meaning of "sold" in the CCPA.

Rights under the CCPA

If you are a California resident, you have the right to:

- Request we disclose to you free of charge the following information covering the 12 months preceding your request:
    - Categories of personal information about you that we collected;
    - Categories of sources from which the personal information was collected;
    - the purpose for collecting personal information about you;
    - Categories of third parties to whom we disclosed personal information about you and categories of personal information that was disclosed (if applicable) and the purpose for disclosing the personal information about you; and
    - the specific pieces of personal information we collected about you;
- Request we delete personal information we have collected from you, unless CCPA recognizes an exception; and
- Be free from unlawful discrimination for exercising your rights including providing a different level or quality of services or denying goods or services to you when you exercise your rights under the CCPA.

We aim to fulfil all verified requests within 45 days pursuant to the CCPA. If necessary, extensions for an additional 45 days will be accompanied by an explanation for the delay.

How to Exercise Your Rights

First, you may wish to log into your account and manage your data from there. If you are a California resident to

whom the CCPA applies, you may also exercise your rights, if any, regarding other data by contacting us at Privacy@sharkmob.com.

Canada

If you are located in Canada and wish to obtain written information about our policies and practices with respect to our service providers located outside Canada, you may contact us at Privacy@sharkmob.com. Our privacy experts who monitor this email address are also able to answer any questions users may have about the collection, use, disclosure or storage of personal information by our service providers.

Where we use service providers who might have access to your personal information, we require them to have privacy and security standards that are comparable to ours. We use contracts and other measures with our service providers to maintain the confidentiality and security of your personal information and to prevent it from being used for any purpose other than as provided in this Privacy Policy.

Colombia

Language

This Privacy Policy is provided in Spanish for users located in Colombia. In case of dispute, the Spanish version of this Privacy Policy shall prevail.

How We Use Your Personal Information

From the entry into force of this Privacy Policy, at the time of the collection of your personal data, we will request your prior authorisation, by informing you about the specific purposes of the processing of your personal data for which such consent is obtained under the Privacy Policy.

Your authorisation may be expressed (i) by writing, (ii) orally or (iii) through unequivocal conducts that allow us to reasonably conclude that your authorisation was granted, such as the act of accepting the Privacy Policy. We may keep evidence of said authorisations, while respecting the principles of confidentiality and privacy of information.

Your Rights

As a data subject you have certain rights, including (i) to access, update and rectify your personal data; (ii) to request a copy of the consent you have given us; (iii) to be informed about how we have processed your personal data; (iv) to file claims before your country's data protection authority; (v) to revoke the consent you have given us to process your personal data, unless the processing is based on compelling legitimate grounds or is needed for legal reasons; (vi) to ask for the suppression of your personal data (right to erasure); and (vii) to freely access your information.

You can contact us if you want to exercise any of these rights through our contact information in the section 'Contact & Complaints' of this Privacy Policy.

Proceedings For The Exercise Of Your Rights

- **Queries (rights to access)**: You can file queries regarding the processing of your personal data by us. Queries will be attended to within a maximum term of ten (10) business days from the date of receipt. If it is not possible to attend the query within the said term, you will be informed of the reasons for the delay and we will indicate the date on which the consultation will be attended to, which may, in no case, exceed five (5) business days following the expiration of the first term.
- **Claims (right to correction and erasure)**: You have the right to file claims in relation to the processing of your personal data by clearly describing the facts that give rise to your claim. The term to attend to the claim will be fifteen (15) business days from the date of receipt. If it is not possible to attend to the claim within the said term, you will be informed of the reasons for the delay and the date on which the claim will be handled, which may, in no case, exceed eight (8) business days following the expiration of the first term.

Egypt

By clicking “accept” or by proceeding with the sign up process, you acknowledge that you have read, understood, and consented to this Privacy Policy. If you do not consent to this Privacy Policy, you must not participate in Bloodhunt.

You are acknowledging your consent to the processing, storage, and cross-border transfer for your personal data. The cross-border transfer may occur to any country in which we have databases or affiliates, in particular Bulgaria, Ireland, Singapore, Sweden, and the United States.

You also acknowledge your consent to receiving marketing messages from us, whether through emails or pop-ups or other such means.

If you are a new user, you have seven days to inform us of any objection you may have to this Privacy Policy .

As an Egyptian data subject, you have certain rights under the Egyptian Personal Data Protection Law.

France

Your Rights

Instructions for the processing of your personal data after your death

You have the right to provide us with general or specific instructions for the retention, deletion, and communication of your personal data after your death.

The specific instructions are only valid for the processing activities mentioned therein and the processing of these instructions is subject to your specific consent.

You may amend or revoke your instructions at any time.

You may designate a person responsible for the implementation of your instructions. This person will be informed of your instructions, in the event of your death, and be entitled to request their implementation from us. In the absence of designation or, unless otherwise provided for, in the event of the death of the designated person, their heirs will have the right to be informed of your instructions and to request their implementation from us.

If you wish to make such instructions, please contact us at Privacy@sharkmob.com.

Hong Kong

As a Hong Kong data subject you have legal rights in relation to the personal information we hold about you (to the extent permitted under applicable laws and regulations).

You are entitled to make a subject access request to receive a copy of the data we process about you, a data correction request as well as a right to reject to the use of your personal data for direct marketing purposes. A fee may be chargeable by us for complying with a data access request.

India

Age Restrictions

Parental consent is required for children under the age of 18 years to use Bloodhunt.

Sensitive Personal Information

Sensitive Personal Information under local law includes passwords, financial information (such as bank account, credit card, debit card or other payment instrument details), biometric data, physical or mental health, sex life or sexual orientation, and/or medical records or history, but does not include information available in the public

domain, or provided under Indian laws, including the Right to Information Act, 2005.

Sharing of Your Sensitive Personal Information

Where we permit any third parties to collect and use Sensitive Personal Information, we shall use reasonable measures to ensure that the third parties do not further disclose the Sensitive Personal Information to the extent required by applicable laws.

Withdrawal of Consent

To the extent provided by applicable laws and regulations, you may withdraw any consent you previously provided to us for certain processing activities by contacting us at Privacy@sharkmob.com. Where consent is required to process your personal information, if you do not consent to the processing or if you withdraw your consent, we may not be able to deliver the expected service.

Indonesia

Consent

By accepting and consenting to this Privacy Policy, you agree that we may collect, use and share your personal information in accordance with this Privacy Policy, as revised from time to time. If you do not agree to this Privacy Policy, you must not access or use our services and we have the right to not provide you with access to our services.

Parental and Guardian Consent

If you are under the age of 21, you confirm that you have the consent of your parent or legal guardian to register an account on and use Bloodhunt.

Data Subject Rights

You have the right to access your personal information stored in Bloodhunt from time to time in accordance with applicable data privacy laws and regulations in Indonesia.

Data Breach

In the event we fail to maintain the confidentiality of your personal information in Bloodhunt, we will notify you through the contact information provided by you or via Bloodhunt, to the extent required by local laws and regulations.

Data Retention

We will retain your personal information in line with legal requirements.

Notification to Amendment of this Privacy Policy

If you fail to explicitly express your objection to any amended version of this Privacy Policy within fourteen (14) days of the date the relevant amended version of this Privacy Policy is made available, you will be considered as having accepted the changes and agreed to the new Privacy Policy. However, you may stop using or accessing Bloodhunt by unsubscribing or ceasing your use of Bloodhunt at any time, if you cease to agree with the amended Privacy Policy.

Data Accuracy and Third-Party Consent

You are responsible for making sure that any personal details which you provide to us are accurate and current. In order to confirm the accuracy of the information, we may also verify the information provided to us, at any time. You hereby represent that you have secured all necessary consent(s) before providing us with any other person's personal information (for example, for referral promotions), in which case we will always assume that you have already obtained prior consent, and as such, you will be responsible for any claims whatsoever from

any party arising as a result of the absence of such consent(s).

Japan

Minimum Age

You must be at least 20 years of age to use Bloodhunt. Otherwise, parental consent is necessary.

Consent to transfer to third parties

By clicking "accept", you consent to the transfer of your personal information to third parties, which may include the cross-border transfer of your information to any country where we have databases or affiliates and, in particular, to Bulgaria, Ireland, Singapore, Sweden, and the United States.

Consent

By clicking "accept", you consent to the cross-border transfer of your information to any country where we have databases or affiliates and, in particular, to the United States, Singapore and Sweden.

Your Rights

You may request us to notify you about the purposes of use of, to disclose, to make any correction to, to discontinue the use or provision of, and/or to delete any and all of your personal information which is stored by us, to the extent provided by the Act on the Protection of Personal Information of Japan. If you wish to make such requests, please contact us at Privacy@sharkmob.com.

Kingdom of Saudi Arabia

You consent to the collection, use, disclosure, export (to the extent permitted by applicable laws) and storage of your Personal Information as described in this Privacy Policy.

Kuwait

You represent that you are at least 21 years old, or 18 years old and have obtained parental/guardian consent and, therefore, legally capable of contracting under the applicable laws and regulations in Kuwait.

By accepting this Privacy Policy, you expressly state that you authorise us to collect, use, store, and process your personal data and to disclose this data to third parties whether inside or outside of Kuwait, in line with the provisions of this Privacy Policy.

Macau SAR

You have the right not to provide your personal information. However, as a result, we may not be able to provide Bloodhunt to you. As a Macau SAR data subject, you have legal rights in relation to your personal information (to the extent permitted under applicable laws and regulations). You are entitled to make a subject access request to request a copy of the data we process about you, to make a data correction request, and have the right to oppose the use of your personal information for marketing or any other form of commercial prospecting, or on any grounds of personal nature. A fee may be chargeable by us for complying with a data access request.

Malaysia

Language of this Privacy Policy

In the event of any discrepancy or inconsistency between the English version and Bahasa Melayu version of this Privacy Policy, the English version shall prevail.

Parental and Guardian Consent

If you are under the age of 18, please do not use Bloodhunt.

In the event you are agreeing to this Privacy Policy in order for a minor to access and use Bloodhunt, you hereby consent to the provision of personal information of the minor to be processed in accordance with this Privacy Policy and you personally accept and agree to be bound by the terms in this Privacy Policy. Further, you hereby agree to take responsibility for the actions of said minor and that minor's compliance with this Privacy Policy.

Your Rights

Right of access: You have the right to request access to and obtain a copy of your personal information that we have collected and is being processed by or on behalf of us. We reserve the right to impose a fee for providing access to your personal information in the amounts as permitted under law.

When handling a data access request, we are permitted to request certain information to verify the identity of the requester to ensure that he/she is the person legally entitled to make the data access request.

Right of correction: You may request for the correction of your personal information. When handling a data correction request, we are permitted to request for certain information to verify the identity of the requester to ensure that he/she is the person legally entitled to make the data correction request.

Right to limit processing of your personal information: You may request to limit the processing of your personal information by using the contact details provided above. However, this may affect our provision of Bloodhunt to you.

Contact

To protect your personal information and handle complaints relating to your personal information, we have appointed the following department responsible for managing and protecting your personal information.

Our data protection officer, responsible for the management and safety of your personal information

- Email: Privacy@sharkmob.com

Mexico

Language

This Privacy Policy is provided in Spanish for users located in Mexico. In case of dispute, the Spanish version of this Privacy Policy shall prevail.

Age Restrictions

You won't be able to use Bloodhunt unless you are 18 years old or have obtained agreement to this Privacy Policy from your parent/guardian (both for themselves and on your behalf).

Types of Personal Information We Use

For clarification purposes, in section 1 "The types of personal information we use" and section 2 "How we use your personal information" you can find full details about the personal data we use. Therefore, we are providing you with complete information about the personal data we use, in terms of the Federal Law on Protection of Personal Data held by Private Parties and other applicable regulations.

Purposes of Processing

Some of the purposes of processing stated above are for voluntary purposes, including to show you personalised recommendations and advertising. We may also use your personal data for the voluntary purpose of sending information to your email that we may consider relevant to you. You may object the processing of your personal data for voluntary purposes as stated in the section "Your Rights" below.

Please, be informed that we may also use your personal data to comply with legal obligations or requests from competent authorities, assert or defend our rights before the competent authorities/courts, respond to requests you send us in relation to your personal data and to carry out the transfer of personal data detailed in section 3 "How we store and share your personal information".

Data Transfer Consent

In general, we do not require your consent to carry out the transfers detailed in section 3 "How we store and share your personal information". However, we require your consent to transfer your personal data to a third party that acquires all or substantially all of us or our business.

By using Bloodhunt and providing us with your personal data, you agree to the data transfers detailed above that require your consent. You may exercise your rights in connection with your personal data as stated in the section "Your Rights" below.

Your Rights

The sub-sections entitled "Access", "Correction", "Erasure", "Objection", "Restriction of Processing to Storage Only", which includes the limitation to the use and disclosure of your personal data, and "Advertising" included in Section "Your Rights" above also apply to users that are located in Mexico.

You also have the right to revoke the consent that you have provided us to process your personal data.

To exercise any of your rights, contact our Data Protection Officer at Privacy@sharkmob.com.

To know more about your rights, as well as the applicable means, procedures and requirements to exercise any of your rights, please contact our Data Protection Officer at Privacy@sharkmob.com.

Morocco

The protection of your privacy is very important to us. We collect information for purposes strictly necessary for the proper use of Bloodhunt.

By accepting these conditions of use, you explicitly accept that your personal data may be subject to processing by Bloodhunt.

Kindly note:

- the identity of the Data Controller is Sharkmob AB, email: Privacy@sharkmob.com.
- the purposes of the processing for which the data is intended are set out in the table in the section "How we use your personal information".
- recipients or categories of recipients are set out in the second paragraph of the section "How We Store and Share Your Personal Information".
- whether the answer to the questions is compulsory or optional, as well as the possible consequences of a lack of answer: please refer to the section "How we use your personal information" and the section "Your Rights" (sub-paragraph "Objection").

New Zealand

This section applies to users located in New Zealand:

Overseas Recipients

We take reasonable steps to ensure that third-party recipients of your personal information located outside New Zealand handle your personal information in a manner that is consistent with New Zealand privacy laws. However, you acknowledge that we do not control, or accept liability for, the acts and omissions of these third party recipients.

Access

You have the right to access the personal information we hold about you, how we use it and who we share it with. You can access the personal information you have made available as part of your account by logging into your account. If you believe we hold any other personal information about you, please contact us at Privacy@sharkmob.com.

Correction

You have the right to request the correction of any of your personal information we hold that is inaccurate. You can access the personal information we hold about you by logging into your account. If you believe we hold any other personal information about you and that information is inaccurate, please contact us at Privacy@sharkmob.com.

Children

If you are under the age of 16, you confirm that you have the consent of your parent or legal guardian to register an account on and use Bloodhunt.

Your Rights

If you are dissatisfied with our response to your request for access to, or correction of, your personal information or your privacy complaint in respect of your personal information, you may contact the Office of the New Zealand Privacy Commissioner (www.privacy.org.nz).

Data Transfers

While we take reasonable steps to ensure that third-party recipients of your personal information comply with privacy laws that are similar to those of your jurisdiction, you acknowledge and agree that we cannot control the actions of third-party recipients and so cannot guarantee that they will comply with those privacy laws.

Peru

Transfers and delegation of personal information occur as set out in this Privacy Policy and the section "Republic of Korea".

You may exercise rights related to the protection of personal information by requesting access to your personal information or the correction, deletion or suspension of processing of your personal information, etc. pursuant to applicable laws such as the Personal Data Protection Law (the "**Law**").

You may also exercise these rights through your legal guardian or someone who has been authorised by you to exercise the right. However, in this case, you must submit a power of attorney to us in accordance with the Law.

Upon request, we will take necessary measures without delay in accordance with applicable laws such as the Law.

You can also withdraw your consent or demand a suspension of the personal information processing at any time.

If you consider that your request has not been met, you may file a claim with the Peruvian National Authority of Personal Data Protection.

Contact

To protect your personal information and handle complaints relating to your personal information, we have appointed the following department responsible for managing and protecting your personal information.

- Data Protection Team, responsible for the management and safety of your personal information
- Contact: Privacy@sharkmob.com

Philippines

Minimum Age

You must be at least 18 years of age to use Bloodhunt.

Your Rights

You are entitled to the following rights:

- Right to be informed. In certain circumstances, you may have the right to be informed whether personal data pertaining to you is being, or has been processed, including the existence of automated decision-making and profiling.
- Right to object. In certain circumstances, you may have the right to object to the processing of your personal information, including processing for direct marketing, automated processing or profiling.
- Right to access. In certain circumstances, you may have the right to seek reasonable access to, upon request, your personal information.
- Right to rectification. In certain circumstances, you may have the right to dispute an inaccuracy or error in your personal information and have us correct it, unless the request is vexatious or otherwise unreasonable.
- Right to erasure or blocking. In certain circumstances, you may have the right to suspend, withdraw or seek the blocking, removal or destruction of your personal information.

Consent

By consenting to this Privacy Policy, you consent to us:

collecting and processing your personal information as described in the section "How We Use Your Personal Information" above;

sharing your personal information with third parties, companies within our corporate group, and a third party that acquires substantially all or substantially all of us or our business, as described in this Privacy Policy and for the purposes stated herein; and

transferring or storing your personal information in destinations outside the Philippines as described in the section "How We Store and Share Your Personal Information" above.

Qatar

If you are using Bloodhunt in Qatar, you consent (for the purposes of Law No. 13 of 2016 on the Protection of Personal Data as may amended from time to time) to the processing of your information in accordance with this Privacy Policy.

Republic of Korea

How We Store and Share Your Personal Information

Delegation of Processing

For the performance of the services detailed in this Privacy Policy, we delegate the processing of your personal information to the following professional service providers and delegated services:

Mailchimp – Newsletter sign-up for Bloodhunt

Pontica Solutions – Customer support services

Zendesk – Customer support services

Sentry – Crash report services

Google Cloud Platform – Cloud storage (backend)

Microsoft Azure – Cloud storage

Overseas Transfer of Personal Information

We transfer personal information to third parties overseas. Please see the list below for the relevant recipients, country of transfer, date and method of transfer, type of personal information, purpose of use by recipient.

Mailchimp

(https://mailchimp.com/legal/privacy/)

Information is transferred to the United States from time to time. Personal information includes: email address, transactional email delivery history (with timestamp, recipient email address, email body). **This information is used for newsletter sign-up through our Recruitment Website and user recruitment for Bloodhunt. For the data retention period specified under "How We Store and Share Your Personal Information"**

Zendesk

(https://www.zendesk.com/company/agreements-and-terms/privacy-policy)

Information is transferred to Ireland, Singapore and Sweden from time to time. Personal information includes: Customer support-related data. **This information is used for Customer support services. For the data retention period specified under "How We Store and Share Your Personal Information"**

Pontica Solutions

(https://ponticasolutions.com/privacy-policy/)

Information is transferred to Bulgaria from time to time. Personal information includes: Customer support-related data. **This information is used for Customer support services. For the data retention period specified under "How We Store and Share Your Personal Information"**

Sentry

(https://sentry.io/privacy/)

Information is transferred to the United States from time to time. Personal information includes: IP address, game directory. **This information is used for Game analysis and improvement. For the data retention period specified under "How We Store and Share Your Personal Information"**

Google Cloud Platform

(https://cloud.google.com/terms/cloud-privacy-notice)

Information is transferred to the United States from time to time. Personal information includes: All data described in the privacy policy. **The information is stored in Cloud storage (backend) used by Sharkmob AB in the provision of Bloodhunt. For the data retention period specified under "How We Store and Share Your Personal Information"**

Microsoft Azure

(https://privacy.microsoft.com/en-us/privacystatement)

Information is transferred to the United States from time to time. Personal information includes: All data described in the privacy policy. **This information is stored in Cloud storage used by Sharkmob AB in the provision of Bloodhunt. For the data retention period specified under "How We Store and Share Your Personal Information"**

Data Destruction

Personal information is retained in accordance with the data retention periods as detailed in section 4 *"Data Retention".* With the exception of the personal information set out below, personal information, which has fulfilled the purpose for which it was collected or used, and has reached the period of time during which personal information was to be possessed, will be destroyed in an irreversible way. Personal information stored in electronic files will be deleted safely in an irreversible way using technical methods, and printed information will be destroyed by shredding or incinerating such information.

The personal information may be required to be retained beyond the data retention periods as detailed in section 4 *"Data Retention"* pursuant to the following laws:

Act on the Consumer Protection in Electronic Commerce, etc.
Article 6 of the Act on the Consumer Protection in Electronic Commerce
In an electronic commerce or a mail-order sale:
• Records regarding labelling and advertising (6 months)
• Records regarding execution or withdrawal of a contract (5 years)
• Records regarding the payment of a price and the supply of goods and services (5 years)
• Records regarding customer services or dispute resolution (3 years)

Protection of Communications Secrets Act
Article 41 of the Decree of the Act, Article 15-2 of the Protection of Communications Secrets Act
• Log records, IP address (3 months)
• The date of telecommunications by users, the time that the telecommunications start and end, the frequency of use (12 months)

Your Rights

You may exercise rights related to the protection of personal information by requesting access to your personal information or the correction, deletion or suspension of processing of your personal information, etc. pursuant to applicable laws such as the Personal Information Protection Act ("**PIPA**").

You may also exercise these rights through your legal guardian or someone who has been authorised by you to exercise the right. However, in this case, you must submit a power of attorney to us in accordance with the Enforcement Regulations of the PIPA.

Upon your request, we will take necessary measures without delay in accordance with applicable laws such as the PIPA.

You can also withdraw your consent or demand a suspension of the personal information processing at any time.

Additional Use and Provision of Personal Information

In accordance with the PIPA, we may use or provide personal information within the scope of what is reasonab ly related to the initial purpose of the collection, in consideration of whether disadvantages have been caused to data subjects and whether necessary measures have been taken to secure such as encryption, etc. We will determine with due care whether to use or provide personal information in consideration of general circumsta nces including relevant laws and regulations such as the PIPA, the purpose of use or provision of personal infor mation, how personal information will be used or provided, the items of personal information to be used or pr ovided, matters to which data subjects have provided consent or which were notified/disclosed to data subject s, impact on data subjects upon the use or provision, and measures taken to protect subject information. Spec ific considerations are as follows:

- whether the additional use/provision is related to the initial purpose of the collection;
- whether the additional use/provision is foreseeable in light of the circumstances under which personal information was collected and practices regarding processing;
- whether the additional use/provision unfairly infringes on the interests of the data subject; and
- whether the necessary security measures such as pseudonymisation or encryption were taken.

Domestic Privacy Representative

Pursuant to the Article 32-5 of the Network Act and Article 39-11 of the amended PIPA, the information regarding the domestic agent is as follows:

- Name: Kite Bird Yuhan Hoesa
- Address: 25F, 55, Sejong-daero, Jung-gu, Seoul (Taepyeongro 2-ga)
- Telephone number: +82 22185 0902
- Email: koreanlocalrep_sharkmob@proximabeta.com

Contact

To protect your personal information and handle complaints relating to your personal information, we have appointed the following department responsible for managing and protecting your personal information.

- Data Protection Department, responsible for the management and safety of your personal information
- Telephone: +82 22185 0902
- Email: koreanlocalrep_sharkmob@proximabeta.com

Russia

If you are using Bloodhunt in Russia, by using Bloodhunt:

- the processing of your information in accordance with this Privacy Policy, for the purposes of the Russian Federal Law No. 152-FZ dated 27 July 2006 “On Personal Data” (as amended) or any replacement regulations; if legitimate interests, optimisation of Bloodhunt or carrying out of the contract are mentioned herein, you agree that, for the purposes of Russian law, the consent so provided can be considered an additional ground for processing (meaning that the processing is conducted with your consent); this consent also covers the processing of any cookies (to the extent that those qualify as personal data under Russian law);
- the cross-border transfer of your information to any country where we have databases or affiliates, in particular Singapore, Sweden and the United States;

- for the purposes of Article 152.1 of the Russian Civil Code, the processing of your image in accordance with this Privacy Policy; and
- for the purposes of Federal Law "On Marketing/Advertising", that we may share advertising/marketing communications with you, unless you have opted-out from such communications.

The sub-sections "Access", "Correction", "Erasure", "Restriction of Processing to Storage Only", "Objection" and "Advertising" of the section "Your Rights" above apply to users in the Russian Federation.

We will not implement any material changes to the way we process your personal information, as described in the Privacy Policy, unless we have notified you. We will notify you of any such material changes and may request you to acknowledge such changes. Unless we require acknowledgement, you shall be deemed to have agreed to the changes, if you continue using Bloodhunt upon the notification.

As regards the representative for Russia, you can contact us at Privacy@sharkmob.com. Please include the word "Russia" in the subject line of your email.

Serbia

Our designated local representative in Serbia is Karanovic & Partners for the purposes of compliance with the Law on Personal Data Protection, and can be contacted at local.representative@karanovicpartners.com. Please include the word "Serbia" in the subject line of your email.

- Name: Karanovic & Partners o.a.d. Beograd
- Address: Resavska 23, Belgrade, 11000, Serbia
- Telephone Number: +381 11 3094 200
- E-mail: local.representative@karanovicpartners.com

Singapore

By clicking "accept", you consent to the cross-border transfer of your information to any country where we have databases or affiliates or third party service providers and, in particular, Bulgaria, Ireland, Singapore, Sweden, and the United States.

Access

You have the right to access your personal information, how we use it and who we share it with. You can access the personal information you have made available as part of your account by logging into your account. If you believe we hold any other personal information about you, please contact us at Privacy@sharkmob.com.

Correction

You have the right to correct any of your personal information that is inaccurate. You can access the personal information we hold about you by logging into your account. If you believe we hold any other personal information about you and that information is inaccurate, please contact Privacy@sharkmob.com.

Our designated data protection officer for the purposes of compliance with the Personal Data Protection Act 2012 can be contacted at Privacy@sharkmob.com.

South Africa

You have the right to lodge a complaint with the Information Regulator (South Africa) by emailing it on inforeg@justice.gov.za. The Information Regulator (South Africa)'s physical address is 33 Hoofd Street Forum III, 3rd Floor Braampark, Braamfontein, Johannesburg, South Africa.

Sri Lanka

By clicking "accept", you consent to the terms and conditions of the Privacy Policy and permit the collection, use

and disclosure of your personal information. However, if you are under the age of 18, you confirm that you have the consent of your parent or legal guardian to register an account on and use Bloodhunt.

Where you request to withdraw consent or, refrain from further processing of data or, erase or, rectify or, complete your personal information, we will provide you with our response to the request within 21 working days.

Personalised Marketing

By clicking "accept", you hereby consent to being shown personalised advertisements. You may choose to stop receiving personalised advertising from us by following the opt out instructions included in the Settings section of Bloodhunt or by contacting us at Privacy@sharkmob.com.

Taiwan

We do not knowingly collect or solicit personal information from anyone under the age of 7 or knowingly allow such persons to register on Bloodhunt. If you are under 7, please do not attempt to use or register for Bloodhunt or send any personal information about yourself to us. No one under the age of 7 may provide any personal information to us while using Bloodhunt. In the case of users located in Taiwan, persons under the age of 20 are required to obtain the consent of their parent/guardian prior to using Bloodhunt.

Thailand

By clicking "accept", you acknowledge that you have read, understood, and agree to this Privacy Policy. If you do not agree with this Privacy Policy, you must not use Bloodhunt.

You may request us to discontinue, to restrict the use or provision of, and/or to request for data portability of any and all of your personal information which is stored by us, to the extent provided by the Act on the applicable data privacy laws and regulations in Thailand, including the Thai Personal Data Protection Act. If you wish to make such requests, please contact us at Privacy@sharkmob.com.

We will give you notice by email of any material changes to this Privacy Policy, and give you an opportunity to reject such changes, failing which the changes will become effective as stated in the notice.

Turkey

Our Data Controller Representative in Turkey for the purpose of compliance with Turkish Law on Personal Data Protection Law ("DPL") and its secondary regulations, Özdağıstanli Ekici Avukatlık Ortaklığı, can be contacted at localdatarep_sharkmob@iptech-legal.com . Please include the word "Turkey" in the subject line of your email.

You have legal rights, which are set forth in Article 11 of the DPL, in relation to the personal information data we hold about you. As a Turkish data subject, you may have the right to apply to the data controller and (to the extent permitted under applicable laws and regulations):

- learn whether or not your personal data has been processed;
- request information about processing if your personal data has been processed;
- learn the purpose of processing of your personal data;
- know the third parties in the country or abroad to whom personal data has been transferred;
- request rectification in the event personal data is incomplete or inaccurate;
- request deletion or destruction of personal data within the framework of the conditions set forth under Article 7 of the DPL;
- object to certain processing of data, and seek certain remedies in accordance with the DPL.

Ukraine

By accepting this Privacy Policy, you expressly authorise us to collect, use, store, and process your personal data, including disclosing it to third parties and transferring it to countries other than Ukraine, to the extent and for

the purpose provided by this Privacy Policy.

United Arab Emirates

You consent to the collection, use, disclosure, transfer, export (to the extent permitted by applicable laws) and storage of your personal information, as described in the Privacy Policy.

We may voluntarily report a cybersecurity incident where it constitutes a crime under UAE law (e.g. under the UAE Cybercrime Law). The incident can be reported to the relevant authorities for the purpose of investigation. Please note that voluntary reporting of a cybersecurity incident can also be made to the UAE Computer Emergency Response Team ("**CERT**"). CERT is a security awareness organisation that provides a process for logging incidents and advising on known cybersecurity threats in the UAE.

Vietnam

By accepting this Privacy Policy, you expressly agree and authorise us to collect, use, store, and process your personal information, including, lawfully disclosing and transferring it to third parties, as described in this Privacy Policy.

We maintain international standards and security practices for data protection. When your personal information is transferred within or outside your jurisdiction of residence, it will be subject to the same or higher levels of security practices and data protection by the recipient entity as adhered to by us.

Where we permit any third parties to collect and use your personal information, we shall take reasonable measures to ensure that the third parties do not further disclose the personal information.

Your personal information, if required to be disclosed to the law enforcement agencies, public authorities or other judicial bodies and organisations, will be disclosed upon receipt of written request from such organisations.

Your Rights

You have the right to access, correct, and erase the personal information we hold about you. You also have the right to withdraw your earlier provided consent to collect, store, process, use and disclose your personal information and to request us to stop providing your personal information to a third party.