Vampire: The Masquerade – Bloodhunt

Datenschutzrichtlinie

Zuletzt aktualisiert am: 7. September 2021

Vielen Dank, dass Sie unsere Produkte und Dienste nutzen! Wir respektieren Ihre Bedenken bezüglich der Privatsphäre und schätzen Ihr Vertrauen in uns.

Hier ist eine Zusammenfassung der in dieser Datenschutzrichtlinie enthaltenen Informationen („**Datenschutzrichtlinie**"). Diese Zusammenfassung soll Ihnen beim Navigieren der Datenschutzrichtlinie helfen und ist kein Ersatz dafür, alles zu lesen! Sie können die folgenden Hyperlinks nutzen, um direkt zu bestimmten Abschnitten zu springen.

Welche Daten benötigen wir, um Bloodhunt zur Verfügung zu stellen?

Wenn Sie ein Konto anmelden, um Bloodhunt zu nutzen, benötigen wir einige Daten von Ihnen wie Ihre E-Mail-Adresse, Sprache, Region, Benutzername, Passwort, IP-Adresse und OpenID, um dies einzurichten. Wir erfassen auch andere Daten, einschließlich Ihrer Regionsdetails, IP-Adresse und Geräte- und Protokolldaten, um das Spielerlebnis zu personalisieren und Bloodhunt-Funktionen zu aktivieren oder Ihre Teilnahme an Bloodhunt zu ermöglichen.

Wie verwenden wir Ihre Daten?

Wir verwenden Ihre Daten, um die vielen Funktionen von Bloodhunt bereitzustellen und Bloodhunt zu verbessern. Wir geben Ihre Daten nicht an Dritte weiter, es sei denn, dies ist erforderlich, um Bloodhunt bereitzustellen (z. B. um Ihre Daten in der Cloud zu hosten, um Sie – mit Ihrer Zustimmung – für unseren Newsletter anzumelden, für den Kundendienst und zu Analyse- und Werbezwecken), oder wenn wir von einem Gericht, einer Behörde oder im gesetzlichen Rahmen dazu angehalten werden.

Mit wem teilen wir Ihre Daten?

Wir nutzen einige Drittanbieter, die uns helfen, das bestmögliche Erlebnis zu bieten (z. B. um Ihre Daten in der Cloud zu hosten, um Sie – mit Ihrer Zustimmung – für unseren Newsletter anzumelden, für den Kundendienst und zu Analyse- und Werbezwecken). Nutzen wir Drittanbieter, verarbeiten oder speichern wir Ihre Daten nur zu den in dieser Datenschutzrichtlinie beschriebenen Zwecken. Wir haben außerdem Partnerunternehmen überall auf der Welt, die uns bei der Bereitstellung von Bloodhunt unterstützen, und wir können unter bestimmten Umständen von einem Gericht oder durch eine gesetzliche Verpflichtung zur Offenlegung bestimmter Daten angehalten werden.

Wo verarbeiten wir Ihre Daten?

Unsere Server befinden sich in den USA, Singapur und Schweden. Auf Ihre Daten kann von außerhalb Ihres Wohnortes durch unsere Kundendienst-, Techniker- und andere Teams auf der ganzen Welt, einschließlich Singapur, Schweden und Vereinigte Staaten, zugegriffen werden. Ihre Daten werden auch von unseren Drittanbietern in Bulgarien, Irland, Singapur, Schweden und den USA verarbeitet.

Wie lange speichern wir Ihre Daten?

Sofern in dieser Datenschutzrichtlinie nicht anders angegeben, speichern wir Ihre Daten im Allgemeinen für die gesamte Dauer Ihrer Nutzung von Bloodhunt und Ihres Sharkmob-Kontos, es sei denn, Sie beantragen die Löschung Ihres Sharkmob-Kontos oder solcher Daten. In diesem Fall werden die Daten auf Anfrage innerhalb von

30 Tagen gelöscht. Wenn Sie keine Kontolöschung beantragen, werden Ihre Daten (außer Kundendienstdaten) im Allgemeinen 1 Jahr nach der Schließung von Sharkmob aufbewahrt, bevor sie gelöscht werden.

Wie kann ich meine Rechte an meinen Daten ausüben?

Sie haben möglicherweise bestimmte Rechte in Bezug auf Ihre Daten, wie z. B. Zugriffsrechte, das Recht auf Erhalt einer Kopie Ihrer Daten oder die Löschung Ihrer Daten, oder unsere Verarbeitung Ihrer Daten einzuschränken oder ihr zu widersprechen.

So erreichen Sie uns

Wenn Sie Fragen zu dieser Datenschutzrichtlinie haben oder Ihre Rechte ausüben möchten, kontaktieren Sie uns bitte unter privacy@sharkmob.com.

Wie informieren wir Sie über Änderungen?

Änderungen an dieser Datenschutzrichtlinie werden online in unserer Datenschutzrichtlinie gepostet. Bitte besuchen Sie diese Seite regelmäßig, um zu sehen, ob es Aktualisierungen oder Änderungen an dieser Datenschutzrichtlinie gibt.

Kontaktinformationen

Datenverantwortlicher: Sharkmob AB | E-Mail: Privacy@sharkmob.com

Willkommen bei Bloodhunt!

Diese Datenschutzrichtlinie erläutert, *wann, wie* und *warum* Ihre personenbezogenen Daten in Bezug auf Vampire: The Masquerade - Bloodhunt („**Bloodhunt**“) verarbeitet werden und legt Ihre Auswahlmöglichkeiten und Rechte in Bezug auf diese Daten dar. Bitte lesen Sie sie sorgfältig durch – es ist wichtig für Sie, dass Sie verstehen, wie wir Ihre Daten erfassen und verwenden und wie Sie dies steuern können.

Wenn Sie mit der Verarbeitung Ihrer personenbezogenen Daten gemäß dieser Datenschutzrichtlinie nicht einverstanden sind, übermitteln Sie Ihre Daten bitte nicht, wenn Sie darum gebeten werden, und nutzen Sie Bloodhunt nicht weiter. Durch die Nutzung von Bloodhunt erkennen Sie unsere Regeln bezüglich Ihrer personenbezogenen Daten an, wie in dieser Datenschutzrichtlinie beschrieben.

Bloodhunt wurde von Sharkmob AB (**„wir“, „uns“, „unser“**) entwickelt.

Im Sinne der Datenschutzgesetze ist Sharkmob AB der Datenverantwortliche für Ihre personenbezogenen Daten in Bezug auf Bloodhunt. Die eingetragene Adresse von Sharkmob AB lautet Stortorget 11, 211 22 Malmö, Schweden.

Bitte kontaktieren Sie uns, wenn Sie Fragen oder Bedenken bezüglich der Verarbeitung Ihrer personenbezogenen Daten haben: Sie können uns jederzeit unter Privacy@sharkmob.com kontaktieren.

Unsere Vertreter in Datenschutzangelegenheiten in bestimmten Gerichtsbarkeiten sind im Folgenden:

Koreanischer Vertreter, Adresse und Kontaktinformationen:

Kite Bird Yuhan Hoesa

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

koreanlocalrep_sharkmob@proximabeta.com

Serbischer Vertreter, Adresse und Kontaktinformationen:

Karanovic & Partners o.a.d. Beograd

Resavska 23, Belgrad, 11000, Serbien

local.representative@karanovicpartners.com

Türkischer Vertreter, Adresse und Kontaktinformationen:

Özdağıstanli Ekici Avukatlık Ortaklığı.

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

localdatarep_sharkmob@iptech-legal.com

1. Die Arten der von uns verwendeten personenbezogenen Daten

Dieser Abschnitt beschreibt die verschiedenen Arten von personenbezogenen Daten, die wir erfassen, und wie wir sie erfassen. Wenn Sie mehr über bestimmte Arten von Daten erfahren möchten und wie wir diese Daten verwenden, lesen Sie bitte den Abschnitt „*Verwendung Ihrer personenbezogenen Daten*“ unten.

Im Folgenden finden Sie eine allgemeine Zusammenfassung der Arten von personenbezogenen Daten, die wir verwenden:

a. Daten, die Sie uns zur Verfügung stellen (entweder direkt oder über einen Dritten)

- **Bloodhunt-Kontoanmeldung, Anmeldung und Verwaltung des Kontos:** E-Mail-Adresse, Verifizierungscode, Sprache, Region, Benutzername, Passwort, IP-Adresse, OpenID, Benutzer-ID, Token.

- **Bloodhunt-Konto-Freundesliste:** Benutzer-ID, Token, Benutzername.

- **Anmeldung (über Steam):** Wenn Sie sich mit Ihrem Steam-Account bei Bloodhunt anmelden, importieren wir Daten aus Ihrem verbundenen Social-Media-Konto, um Ihr Profil einzurichten. Dazu gehören Ihre Benutzer-ID/Token, OpenID, Spitzname, Profilbild (sofern vorhanden) und die Anzahl der Steam-Freunde in Bezug auf Sie und Ihre Steam-Freunde.

- **Sprachchat (wenn Sie Sprachchat in Bloodhunt verwenden):** IP-Adresse, Sitzungsstatistiken.

- **Anmeldung zum Newsletter:** Betriebssystem, Browsersprache, Land, IP-Adresse, Anmeldedatum, E-Mail-Adresse, Zustimmung zum E-Mail-Marketing, Vampirtyp, Kampfstatistiken.

- **Verwaltung von E-Mail-Diensten:** Erste Anmeldung (Datum), Zeit seit der ersten Anmeldung, letzte Anmeldung (Datum), Zeit seit der letzten Anmeldung, Anmeldedatensatz (ja/nein), Anmeldungszeit, Land, Sprache, E-Mail-Adresse des Abonnements.

- **Kundendienst-Daten (Zendesk):** Vorname, Nachname, E-Mail-Adresse.

- **Datenerfassung und Berichterstattung (APAS):** Wir erfassen Ihre Standortdaten (einschließlich Region, Land, Provinz, Stadt), Mobilfunkanbieter-ID und Gerätedaten (einschließlich Anwendungsversion, Akkustand, WLAN-Stärke, verfügbarer Speicherplatz, Netzwerktyp, Betriebssystemversion, Plattform, Gerätesprache, Bildschirm-DPI, Geräteauflösung, Marke, Hersteller, Gerätemodell, RAM, ROM und CPU-Daten).

- **Spieldaten (einschließlich Anmeldedaten):** OpenID, IP-Adresse (nur in Sammelformat zur Serververbesserung gespeichert), Gerätemodell, Details zur Plattform, geografisches Ranking (manuell von Ihnen ausgewählt), Spielstatistiken (einschließlich Level und Punktzahlen).

- **Textchat-Daten:** Chatdaten, anonyme ID, Identitätsdaten (einschließlich Benutzername, Plattform, Kommentarzeit, Kommentarinhalte und Beurteilungspunktzahl).

b. Im Rahmen von Bloodhunt generierte Daten über Sie

Wir erfassen automatisch bestimmte Daten über Sie, wenn Sie Bloodhunt nutzen, und zwar:

- **Kundendienst-Daten:** Wenn Sie sich für die Nutzung unseres Kundendiensts entscheiden, erfassen wir Daten wie Ihre OpenID und Spieldaten (einschließlich Dauer der Kontosperrung, Gründe für die Kontosperrung, Grund für das Ruhen des Kontos, Ruhezeit, Gegenstands-ID, Anzahl der an den Spieler gesendeten oder aus dem Spieler-Paket gelöschten Gegenstände, an Spieler gesendeten E-Mail-Betreff, an Spieler gesendete E-Mail-Inhalte, Start- und Endzeiten der Ruhephase).

- **Daten zum Spielverhalten:** Identitätsdaten (einschließlich OpenID, Länder- und Rollen-ID),

Anmeldedaten (einschließlich Anmeldezeit, Onlinezeit und Spielmodus) und Zahlungsdaten (einschließlich Kaufzeit, Kaufwert, Daten zu gekauften Artikeln, Spielwährungsguthaben, gesammelt auf Aggregatebene), die nicht von uns, sondern von Zahlungsdienstleistern verarbeitet werden.

- **Sicherheit:** Sicherheitsbezogene Daten (einschließlich einer Liste von Hack- oder Cheating-Software, Bildschirmdaten im Spiel), Gerätedaten (einschließlich Einstellungen des Betriebssystems des Geräts, Gerätedaten einschließlich Marke, Modell, CPU-Struktur, CPU-Modell, Kernelversion, Auflösung, App-Paket mit Hack-Software und verfügbarem Speicher) und Daten zu Ihrer Internetverbindung, einschließlich WLAN-Namen und einer Liste der installierten und laufenden Apps.

- **Absturzdaten (Sentry):** IP-Adresse, Spielverzeichnis.

2. Cookies

Wir verwenden Cookies und weitere ähnliche Technologien (z. B. Zählpixel, Logdateien, Skripte und ETags) („**Cookies**“), um Ihr Bloodhunt-Spielerlebnis zu verbessern. Cookies sind kleine Dateien, die auf Ihrem Gerät abgelegt werden und uns erlauben, bestimmte Features und Funktionalitäten anzubieten.

3. Kinder

Kinder dürfen Bloodhunt zu keinem Zweck nutzen, es sei denn, ihre Eltern oder Erziehungsberechtigten haben ihre Zustimmung erteilt (soweit diese Option in Ihrer Gerichtsbarkeit verfügbar ist).

Mit Kindern meinen wir Nutzer unter 18 Jahren, oder im Falle eines Landes, in dem das Mindestalter für die Verarbeitung personenbezogener Daten abweicht, dieses abweichende Alter. Für Nutzer in bestimmten Ländern haben wir das entsprechende Mindestalter unten aufgeführt.

Algerien 19

Argentinien 18

Australien 18

Bangladesch 18

Brasilien 18

Kolumbien 18

Kambodscha 18

Kanada 13

Ägypten 18

Europäischer Wirtschaftsraum/Schweiz 16

Hongkong 18

Indien 18

Indonesien 21

Japan 20

Königreich Saudi-Arabien 15

Kuwait 21

Macau 18

Malaysia 18

Mexiko 18

Marokko 18

Myanmar 18

Neuseeland 16

Philippinen 18

Katar 18

Republik Korea 14

Russland 14

Singapur 18

Südafrika 18

Sri Lanka 18

Taiwan 20

Thailand 20

Tunesien 18

Türkei 18

Vereinigte Arabische Emirate 21

Vereinigtes Königreich 13

Vereinigte Staaten 13

Vietnam 16

Wir erfassen wissentlich zu keinem Zweck personenbezogene Daten von Kindern unter diesem Alter. Wenn Sie der Meinung sind, dass wir ohne Zustimmung der Eltern/Erziehungsberechtigten personenbezogene Daten eines Kindes unter diesem Alter erfasst haben, oder wenn Sie der Elternteil oder Vormund des Nutzers sind und die Zustimmung widerrufen möchten, kontaktieren Sie uns bitte unter Privacy@sharkmob.com und wir löschen diese Daten.

4. Verwendung Ihrer personenbezogenen Daten

In diesem Abschnitt finden Sie weitere Informationen zu den Arten von personenbezogenen Daten, die wir erfassen, und die Gründe dafür. Für Nutzer, die im Vereinigten Königreich, im Europäischen Wirtschaftsraum, in der Schweiz oder in der Türkei leben (**„Zuständige Gerichtsbarkeit“**), wird auch die Rechtsgrundlage angegeben, auf der wir ihre Daten verarbeiten.

Bloodhunt-Kontoanmeldung, Anmeldung und Verwaltung des Kontos: E-Mail-Adresse, Verifizierungscode, Sprache, Region, Benutzername, Passwort, IP-Adresse, OpenID, Benutzer-ID, Token. Wir verwenden diese

Daten, damit Sie sich gemäß Ihrer Anfrage bei Ihrem Konto für Bloodhunt anmelden können. Dies ist notwendig, um unseren Vertrag mit Ihnen zur Bereitstellung von Bloodhunt zu erfüllen.

Bloodhunt-Konto-Freundesliste: Benutzer-ID, Token, Benutzername. Wir verwenden diese Daten, um anzuzeigen, was Freunde im Spiel spielen, und um die Sprachchat-Funktion bereitzustellen. Dies ist notwendig, um unseren Vertrag mit Ihnen zur Bereitstellung der Sprachchat-Funktion in Bloodhunt zu erfüllen.

Anmeldung (über Steam): Wenn Sie sich mit Ihrem Steam-Account bei Bloodhunt anmelden, importieren wir Daten aus Ihrem verbundenen Social-Media-Konto, um Ihr Profil einzurichten. Dazu gehören Ihre Benutzer-ID/Token, OpenID, Spitzname, Profilbild (sofern vorhanden) und die Anzahl der Steam-Freunde in Bezug auf Sie und Ihre Steam-Freunde. Wir verwenden diese Daten, damit Sie sich gemäß Ihrer Anfrage bei Ihrem Konto für Bloodhunt anmelden können. Dies ist notwendig, um unseren Vertrag mit Ihnen zur Bereitstellung von Bloodhunt zu erfüllen.

Sprachchat (wenn Sie Sprachchat in Bloodhunt verwenden): IP-Adresse, Sitzungsstatistiken. Wir verwenden diese Daten, um Ihnen die Nutzung von VOIP gemäß Ihrer Anfrage zu ermöglichen. Dies ist notwendig, um unseren Vertrag mit Ihnen zur Bereitstellung der Sprachchat-Funktion in Bloodhunt zu erfüllen.

Anmeldung zum Newsletter: Betriebssystem, Browsersprache, Land, IP-Adresse, Anmeldedatum, E-Mail-Adresse, Zustimmung zum E-Mail-Marketing, Vampirtyp, Kampfstatistiken. Wir verwenden diese Daten, um Sie über aktuelle Neuigkeiten zu Bloodhunt zu informieren. Wir erfassen diese Daten, nachdem Sie einer solchen Datenverarbeitung zugestimmt haben.

Verwaltung von E-Mail-Diensten: Erste Anmeldung (Datum), Zeit seit der ersten Anmeldung, letzte Anmeldung (Datum), Zeit seit der letzten Anmeldung, Anmeldedatensatz (ja/nein), Anmeldungszeit, Land, Sprache, E-Mail-Adresse des Abonnements. Wir verwenden diese Daten, um unsere Beziehung zu Ihnen aufrechtzuerhalten und um Kundendienst-Anfragen per E-Mail zu lösen. Dies ist notwendig, um unseren Vertrag mit Ihnen zu erfüllen und Sie bei Kundendienst-Anfragen zu Bloodhunt zu unterstützen.

Kundendienst-Daten (Zendesk): Vorname, Nachname, E-Mail-Adresse. Wir verwenden diese Daten als Hilfsmittel, um die Funktionalität des von Pontica Solutions bereitgestellten Kundendiensts zu unterstützen.

Datenerfassung und Berichterstattung (APAS): Wir erfassen Ihre Standortdaten (einschließlich Region, Land, Provinz, Stadt), Mobilfunkanbieter-ID und Gerätedaten (einschließlich Anwendungsversion, Akkustand, WLAN-Stärke, verfügbarer Speicherplatz, Netzwerktyp, Betriebssystemversion, Plattform, Gerätesprache, Bildschirm-DPI, Geräteauflösung, Marke, Hersteller, Gerätemodell, RAM, ROM und CPU-Daten). Wir verwenden diese Daten zum Zwecke der Benutzerakquise und zur Überprüfung der Wirksamkeit unserer Werbung durch Analysen. Wir haben berechtigtes Interesse an der Verarbeitung dieser Daten, um die Wirksamkeit unserer Werbung zu überprüfen.

Spieldaten (einschließlich Anmeldedaten): OpenID, IP-Adresse (nur in Sammelformat zur Serververbesserung gespeichert), Gerätemodell, Details zur Plattform, geografisches Ranking (manuell von Ihnen ausgewählt), Spielstatistiken (einschließlich Level und Punktzahlen). Wir verwenden diese Daten, um Sie in Bloodhunt-Protokollen zu identifizieren und Ihnen zu ermöglichen, sich mit Bloodhunt zu verbinden. Dies ist notwendig, um unseren Vertrag mit Ihnen zur Bereitstellung von Bloodhunt zu erfüllen.

Textchat-Daten: Chatdaten, anonyme ID, Identitätsdaten (einschließlich Benutzername, Plattform, Kommentarzeit, Kommentarinhalte und Beurteilungspunktzahl). Wir verwenden diese Daten, um Ihre Kommunikation mit anderen Nutzern über Textbeiträge zu erleichtern. Dies ist notwendig, um unseren Vertrag mit Ihnen zur Bereitstellung der Textchat-Funktion in Bloodhunt zu erfüllen.

Kundendienst-Daten: Wenn Sie sich für die Nutzung unseres Kundendiensts entscheiden, erfassen wir Daten wie Ihre OpenID und Spieldaten (einschließlich Dauer der Kontosperrung, Gründe für die Kontosperrung, Grund für das Ruhen des Kontos, Ruhezeit, Gegenstands-ID, Anzahl der an den Spieler gesendeten oder aus dem

Spieler-Paket gelöschte Gegenstände, an Spieler gesendeten E-Mail-Betreff, an Spieler gesendete E-Mail-Inhalte, Start- und Endzeiten der Ruhephase). Wir verwenden diese Daten, um Bloodhunt zu verbessern, einschließlich der Funktionalität von Bloodhunt, und zur Fehlerbehebung, wie z. B. dem Beheben von technischen Problemen und Fehlern. Dies ist notwendig, um unseren Vertrag mit Ihnen zu erfüllen, um Bloodhunt bereitzustellen und Sie bei Kundendienst-Anfragen zu Bloodhunt zu unterstützen.

Daten zum Spielverhalten: Identitätsdaten (einschließlich OpenID, Länder- und Rollen-ID), Anmeldedaten (einschließlich Anmeldezeit, Onlinezeit und Spielmodus) und Zahlungsdaten (einschließlich Kaufzeit, Kaufwert, Daten zu gekauften Artikeln, Spielwährungsguthaben). Wir verwenden diese Daten, um das Spielerlebnis und die Funktionen zu verbessern, damit Sie das Spiel genießen können. Wir sammeln Zahlungsdaten (via Steam) auf Aggregatebene zur Anpassung des Spiels und unserer Angebote im Spiel, um ein großartiges Spielererlebnis zu bieten, den Ertrag zu maximieren und Ihnen Zahlungen über eine Drittanbieter-Zahlungsplattform zu ermöglichen. Wir haben berechtigtes Interesse an der Verarbeitung dieser Daten, um das Spielerlebnis verbessern zu können.

Sicherheitsdaten: Sicherheitsbezogene Daten (einschließlich einer Liste von Hack- oder Cheating-Software, Bildschirmdaten im Spiel), Gerätedaten (einschließlich Einstellungen des Betriebssystems des Geräts, Gerätedaten einschließlich Marke, Modell, CPU-Struktur, CPU-Modell, Kernelversion, Auflösung, App-Paket mit Hack-Software und verfügbarem Speicher) und Daten zu Ihrer Internetverbindung, einschließlich WLAN-Namen und einer Liste der installierten und laufenden Apps. Wir verwenden diese Daten, um Ihre Nutzung von Bloodhunt zu sichern. Dies ist notwendig, um unseren Vertrag mit Ihnen zur Bereitstellung von Bloodhunt zu erfüllen.

Absturzdaten (Sentry): IP-Adresse, Spielverzeichnis. Wir verwenden diese Daten, um das Spielerlebnis und die Funktionen zu verbessern, damit Sie das Spiel genießen können. Wir erfassen diese Daten, nachdem Sie einer solchen Datenverarbeitung zugestimmt haben.

5. Wie wir Ihre personenbezogenen Daten speichern und weitergeben

Unsere Unternehmensgruppe ist weltweit tätig. Gemäß unserer Vereinbarung mit Ihnen, Ihnen Bloodhunt bereitzustellen, werden Ihre personenbezogenen Daten auf Servern verarbeitet, die sich möglicherweise nicht dort befinden, wo Sie wohnen. Unabhängig davon, wo sich unsere Server befinden, ergreifen wir geeignete Maßnahmen, um Ihre Rechte gemäß dieser Datenschutzrichtlinie zu schützen. Unsere Server für Bloodhunt befinden sich in den USA, Singapur und Schweden.

Außerdem kann von außerhalb Ihres Wohnortes durch unsere Kundendienst-, Techniker- und andere Teams auf der ganzen Welt, einschließlich Bulgarien, Irland, Singapur, Schweden und den USA, auf Ihre Daten zugegriffen werden.

Wenn Sie auf „Annehmen“ klicken, stimmen Sie zu, dass Ihre Daten an Datenbanken oder Partner im Ausland weitergegeben werden dürfen, insbesondere nach Bulgarien, Irland, Singapur, Schweden und in die USA.

Nur bei Bedarf geben wir Ihre personenbezogenen Daten an Dritte weiter. Mögliche Fälle können sein:

- **Drittanbieter**, die Dienstleistungen zur Unterstützung von Bloodhunt bereitstellen, einschließlich der Bereitstellung von Cloud-Server-Speicherplatz, um die in dieser Richtlinie identifizierten Daten auf einem Cloud-Server zu verarbeiten, Ihrer Anmeldung für unseren Newsletter (mit Ihrer Zustimmung), der Bereitstellung von Absturzberichtsdiensten für Sie, der Bereitstellung von Kundendiensten, der Verarbeitung von Spielstatistiken zu Analysezwecken, der Verbesserung des Spiels und der Abwicklung von Zahlungen (beispielsweise über Steam). Allen Unternehmen, die Dienstleistungen für uns erbringen, ist es untersagt, Ihre personenbezogenen Daten für andere Zwecke als die Bereitstellung ihrer Dienstleistungen für uns zu speichern, zu verwenden oder offenzulegen.

- **Unternehmen innerhalb unserer Unternehmensgruppe**, die Ihre personenbezogenen Daten verarbeiten, um Bloodhunt bereitzustellen und Umfragen für uns durchzuführen. Alle zugehörigen

Unternehmen dürfen Ihre personenbezogenen Daten nur in Übereinstimmung mit dieser Datenschutzrichtlinie verwenden.

- **Aufsichtsbehörden, Justizbehörden und Strafverfolgungsbehörden und andere Dritte im Rahmen von Sicherheit, Schutz oder Einhaltung des Gesetzes.** Es gibt Umstände, unter denen wir gesetzlich verpflichtet sind, Ihre Daten an Behörden weiterzugeben, z. B. um einer rechtlichen Verpflichtung oder einem Verfahren nachzukommen, unsere Bedingungen durchzusetzen, Probleme in Bezug auf Sicherheit oder Betrug zu lösen oder unsere Nutzer zu schützen. Diese Offenlegungen können mit oder ohne Ihre Zustimmung und mit oder ohne Vorankündigung in Übereinstimmung mit den geltenden rechtlichen Verfahren wie einer Vorladung, einem Gerichtsbeschluss oder einem Durchsuchungsbefehl erfolgen. In der Regel ist es uns gemäß den Bedingungen des rechtlichen Verfahrens untersagt, Sie über solche Offenlegungen zu informieren. Wir können Ihre Zustimmung zur Offenlegung von Daten als Reaktion auf die Anfrage einer staatlichen Stelle einholen, wenn diese staatliche Stelle nicht die erforderliche Vorladung, gerichtliche Verfügung oder einen Durchsuchungsbefehl vorgelegt hat. Wir können Ihre Daten auch offenlegen, um

    - unsere Geschäftsbedingungen und andere Vereinbarungen durchzusetzen, einschließlich der Untersuchung möglicher Verstöße dagegen,

    - Sicherheits-, Betrugs- oder technische Probleme aufzudecken, zu verhindern oder anderweitig anzugehen, oder

    - die Rechte, das Eigentum oder die Sicherheit von uns, unseren Nutzern, Dritten oder der Öffentlichkeit zu schützen, wie es gesetzlich vorgeschrieben oder zulässig ist (Datenaustausch mit anderen Unternehmen und Organisationen zum Zwecke des Betrugsschutzes und der Kreditrisikominderung).

- **Dritte, die uns komplett oder im Wesentlichen oder unser Unternehmen erwerben.** Wir können Ihre Daten auch an Dritte weitergeben, wenn wir entweder: (a) Teile unseres Unternehmens verkaufen, übertragen, fusionieren, konsolidieren oder neu organisieren oder mit anderen fusionieren, sie erwerben oder ein Gemeinschaftsunternehmen bilden, und in diesem Fall können wir Ihre Daten an potenzielle Käufer, neue Eigentümer oder andere Dritte weitergeben, die an einer solchen Änderung unseres Unternehmens beteiligt sind; oder (b) unsere Vermögenswerte verkaufen oder übertragen, wobei in diesem Fall die Daten, die wir von Ihnen besitzen, als Teil dieser Vermögenswerte verkauft und an potenzielle Käufer, neue Eigentümer oder andere an einem solchen Verkauf oder Transfer beteiligte Dritte übertragen werden können.

6. Die Sicherheit Ihrer personenbezogenen Daten

Wir verpflichten uns, Ihre Privatsphäre und die Integrität Ihrer personenbezogenen Daten zu wahren, unabhängig davon, wo sie gespeichert sind. Wir haben Datenschutz- und Zugriffsrichtlinien, die den Zugriff auf unsere Systeme und Technologien einschränken, und wir schützen Daten durch den Einsatz technischer Schutzmaßnahmen wie Verschlüsselung.

Leider ist die Datenübertragung über das Internet nicht vollständig sicher. Obwohl wir angemessene Maßnahmen zum Schutz Ihrer personenbezogenen Daten ergreifen und beibehalten, können wir die Sicherheit der über Bloodhunt oder anderweitig über das Internet übermittelten Daten nicht garantieren; jede Übertragung erfolgt auf eigene Gefahr.

7. Datenspeicherung

Wir speichern Ihre Daten nicht länger als notwendig, es sei denn, wir sind gesetzlich dazu verpflichtet. Weitere Einzelheiten zur Speicherdauer Ihrer Daten entnehmen Sie bitte den unten aufgeführten Zeiträumen.

Bloodhunt-Kontoregistrierung, Bloodhunt-Kontoanmeldung, Bloodhunt-Kontoverwaltung, Bloodhunt-Konto-Freundesliste und Anmeldung (über Steam) werden für die Dauer Ihrer Nutzung von Bloodhunt gespeichert. (Es sei denn, ein Löschantrag geht ein. In diesem Fall werden die Daten innerhalb von 30 Tagen gelöscht.) Wenn Sie

keine Kontolöschung beantragen, werden Ihre Daten 1 Jahr nach der Schließung von Sharkmob aufbewahrt, bevor sie gelöscht werden.

Der Sprachchat (wenn Sie Sprachchat in Bloodhunt verwenden) wird vor der automatischen Löschung 90 Tage lang gespeichert. (Es sei denn, ein Löschantrag geht ein. In diesem Fall werden die Daten innerhalb von 30 Tagen gelöscht.)

Die Anmeldung zum Newsletter (über Mailchimp) wird 30 Tage gespeichert, bevor sie automatisch gelöscht wird.

Die Verwaltung von E-Mail-Diensten wird für die Dauer Ihrer Nutzung von Bloodhunt gespeichert. (Es sei denn, ein Löschantrag geht ein. In diesem Fall werden die Daten innerhalb von 30 Tagen gelöscht.)

Kundendienstdaten (Bloodhunt) werden für die Dauer Ihrer Nutzung von Bloodhunt gespeichert. (Es sei denn, ein Löschantrag geht ein. In diesem Fall werden die Daten innerhalb von 30 Tagen gelöscht.) Wenn Sie keine Kontolöschung beantragen, werden Ihre Daten 5 Jahre gespeichert.

Datenerfassung und Berichterstattung (APAS) wird für 7 Tage gespeichert, bevor sie automatisch gelöscht wird.

Spieldaten (einschließlich Anmeldedaten) werden für die Dauer Ihrer Nutzung von Bloodhunt gespeichert. (Es sei denn, ein Löschantrag geht ein. In diesem Fall werden die Daten innerhalb von 30 Tagen gelöscht.)

Textchat-Daten werden nicht gespeichert.

Kundendienstdaten (Bloodhunt) werden für die Dauer Ihrer Nutzung von Bloodhunt gespeichert. (Es sei denn, ein Löschantrag geht ein. In diesem Fall werden die Daten innerhalb von 30 Tagen gelöscht.) Wenn Sie keine Kontolöschung beantragen, werden Ihre Daten 5 Jahre gespeichert.

Daten zum Spielverhalten werden für die Dauer Ihrer Nutzung von Bloodhunt gespeichert. (Es sei denn, ein Löschantrag geht ein. In diesem Fall werden die Daten innerhalb von 30 Tagen gelöscht.)

Sicherheitsdaten werden 90 Tage lang gespeichert (es sei denn, ein Löschantrag geht ein, in diesem Fall werden die Daten innerhalb von 30 Tagen gelöscht) mit Ausnahme der folgenden:

- Bösartige Dateien werden 3 Jahre gespeichert.

- Hardwaredaten, Cheat-Tool-Überwachung, Spieleridentifikation, Spielbetriebsdaten und Fehlerbehebungsprotokolle werden 30 Tage gespeichert.

- Erfassung von Datei- und Speicherproben wird 7 Tage gespeichert und dann automatisch gelöscht, wenn die gleichen Probendaten nicht erneut auftauchen. Werden sie jedoch als bösartige Datei identifiziert, so werden sie 3 Jahre gespeichert.

- Bösartige Spielspeicherproben werden 10 Jahre gespeichert (zusammen mit zugehöriger Konto-ID, Registrierungsdatum und Nutzerverhalten im Spiel).

- Bei bestätigten nicht-bösartigen Dateien beträgt die Speicherdauer 60 Tage.

- Bei MD5-Datensätzen der Benutzerdatei beträgt die Speicherdauer 90 Tage.

- Aktionen, Statuserfassung, Trailerfassung werden 90 Tage gespeichert.

- Verarbeitungsdaten und Systemdaten im Spiel werden 10 Jahre gespeichert und dann manuell gelöscht.

- Sicherheitsauthentifizierung wird 730 Tage gespeichert und dann automatisch gelöscht.

Absturzdaten (Sentry) werden 90 Tage gespeichert, bevor sie automatisch gelöscht werden.

Wenn wir Ihre Daten über die oben genannten Aufbewahrungsfristen hinaus speichern müssen, beispielsweise um geltende Gesetze einzuhalten, speichern wir sie getrennt von anderen Arten personenbezogener Daten.

8. Ihre Rechte

Die Gesetze einiger Gerichtsbarkeiten räumen Bloodhunt-Nutzern besondere Rechte ein, die in diesem Abschnitt aufgeführt sind.

Dieser Abschnitt mit dem Titel „Ihre Rechte" gilt für Nutzer, die sich in den zuständigen Gerichtsbarkeiten befinden. Wenn Sie sich in einem Gebiet außerhalb einer zuständigen Gerichtsbarkeit befinden, finden Sie in den ergänzenden spezifischen Gerichtsbarkeit-Bedingungen einen Überblick über Ihre Rechte und wie diese ausgeübt werden können.

Die Unterabschnitte „Zugriff", „Korrektur" und „Löschen" gelten auch für Nutzer, die sich in Kanada, Argentinien, Indien und Russland befinden.

Der Unterabschnitt „Werbung" gilt auch für Nutzer, die sich in Hongkong, Macau, Japan, Malaysia, Singapur, Korea, Thailand, den USA, Kanada, Australien, Neuseeland, Argentinien, Brasilien, Kambodscha, Ägypten, Indien, Indonesien, Laos, den Malediven, Mexiko, Marokko, Myanmar, den Philippinen, Russland, Sri Lanka, Taiwan, der Türkei, den Vereinigten Arabischen Emiraten, Saudi-Arabien und Vietnam befinden.

Sie haben bestimmte Rechte in Bezug auf die personenbezogenen Daten, die wir über Sie gespeichert haben, je nachdem, wo Sie sich befinden. Manche finden nur unter bestimmten Bedingungen Anwendung (wie sie unten detaillierter erklärt werden). Wir müssen Ihrer Aufforderung zur Ausübung dieser Rechte unverzüglich und spätestens innerhalb eines Monats nachkommen (dies kann jedoch unter bestimmten Umständen um weitere zwei Monate verlängert werden). Um eines Ihrer Rechte auszuüben, kontaktieren Sie uns bitte unter Privacy@sharkmob.com.

Zugriff

Sie haben das Recht, auf Ihre von uns gespeicherten personenbezogenen Daten zuzugreifen sowie auf Informationen darüber, wie wir sie verwenden und mit wem wir sie teilen. Wenn Sie Zugriff auf die Daten haben möchten, die wir über Sie gespeichert haben, kontaktieren Sie uns bitte unter Privacy@sharkmob.com.

Übertragbarkeit

Sie haben das Recht, eine Kopie bestimmter personenbezogener Daten zu erhalten, die wir über Sie verarbeiten. Dies umfasst alle personenbezogenen Daten, die wir aufgrund Ihrer Einwilligung oder gemäß unserem Vertrag mit Ihnen (z. B. Spieldaten) verarbeiten, wie oben im Abschnitt *„Verwendung Ihrer personenbezogenen Daten* beschrieben. Sie haben das Recht, diese Daten in einem strukturierten, gängigen und computerlesbaren Format zu erhalten. Sie haben auch das Recht zu verlangen, dass wir diese personenbezogenen Daten mit bestimmten Ausnahmen an eine andere Partei weitergeben. Auf Anfrage liefern wir Ihnen hierzu weitere Informationen.

Wenn Sie möchten, dass wir solche personenbezogenen Daten an Dritte weitergeben, stellen Sie bitte sicher, dass Sie diese Partei in Ihrer Anfrage angeben. Bitte beachten Sie, dass wir dies nur tun können, wenn es technisch machbar ist. Bitte beachten Sie, dass wir Ihnen möglicherweise keine personenbezogenen Daten zur Verfügung stellen können, wenn deren Bereitstellung die Rechte anderer beeinträchtigen würde (z. B. wenn die Bereitstellung der von uns über Sie gespeicherten personenbezogenen Daten Informationen über eine andere Person oder unsere Geschäftsgeheimnisse oder unser geistiges Eigentum preisgeben würde).

Korrektur

Sie haben das Recht auf Korrektur fehlerhafter von uns gespeicherter personenbezogener Daten über Sie. Wenn Sie der Meinung sind, dass wir personenbezogene Daten über Sie gespeichert haben und diese Daten fehlerhaft sind, kontaktieren Sie uns bitte unter Privacy@sharkmob.com.

Löschung

Sie können Ihr Konto löschen oder bestimmte personenbezogene Daten entfernen, indem Sie uns unter Privacy@sharkmob.com kontaktieren.

Möglicherweise müssen wir personenbezogene Daten speichern, wenn es dafür datenschutzrechtliche Gründe gibt (z. B. zur Verteidigung von Rechtsansprüchen oder zur Meinungsfreiheit), aber wir werden Sie in diesem Fall informieren. Haben Sie angefragt, dass wir personenbezogene Daten löschen, die öffentlich im Dienst zur Verfügung gestellt wurden, und gibt es Gründe für die Löschung, werden wir angemessene Schritte unternehmen, damit andere, die die personenbezogenen Daten anzeigen oder Links zu den personenbezogenen Daten bereitstellen, sie ebenfalls löschen.

Beschränkung der Verarbeitung auf die ausschließliche Speicherung

Sie haben das Recht, von uns zu verlangen, dass wir unter bestimmten Umständen die Verarbeitung der von uns über Sie gespeicherten personenbezogenen Daten zu anderen als zu Speicherzwecken einstellen. Bitte beachten Sie jedoch, dass wir, wenn wir die Verarbeitung der personenbezogenen Daten einstellen, diese wieder verwenden können, wenn hierfür datenschutzrechtliche Gründe vorliegen (z. B. zur Verteidigung rechtlicher Ansprüche oder zum Schutz Dritter). Wenn wir wie oben aufgeführt zustimmen, die Verarbeitung der personenbezogenen Daten einzustellen, versuchen wir, jedem Drittanbieter, dem wir die relevanten personenbezogenen Daten offengelegt haben, mitzuteilen, dass dieser ebenfalls die Verarbeitung einstellen kann.

Einspruch

Sie haben das Recht, unserer Verarbeitung Ihrer personenbezogenen Daten zu widersprechen. Wir werden Ihre Anfrage unter anderen Umständen wie unten beschrieben berücksichtigen, wenn Sie uns unter Privacy@sharkmob.com kontaktieren.

Soweit dies durch geltende Gesetze und Vorschriften vorgesehen ist, können Sie jegliche Einwilligung widerrufen, die Sie uns zuvor für bestimmte Verarbeitungsaktivitäten erteilt haben, indem Sie uns unter Privacy@sharkmob.com kontaktieren. Wenn für die Verarbeitung Ihrer personenbezogenen Daten eine Einwilligung erforderlich ist, Sie der Verarbeitung nicht zustimmen oder Ihre Einwilligung widerrufen, können wir den erwarteten Dienst möglicherweise nicht bereitstellen.

Ankündigungen

Wir können Ihnen von Zeit zu Zeit Ankündigungen senden, falls erforderlich (z. B. wenn wir den Zugriff auf den Dienst für Wartungsarbeiten vorübergehend aussetzen oder für Sicherheits-, Datenschutz- oder verwaltungstechnische Mitteilungen). Sie können diese dienstbezogenen Ankündigungen, die keinen Werbecharakter haben, nicht abbestellen.

Werbung

Sie können bei der Nutzung des Dienstes personalisierte Werbung oder Marketingaktionen durch uns abbestellen, indem Sie in unserem Newsletter auf die Schaltfläche „Abmelden“ klicken oder uns unter Privacy@sharkmob.com kontaktieren.

9. Kontakt & Beschwerden

Fragen, Anmerkungen und Anfragen zu dieser Datenschutzrichtlinie sind immer willkommen und sollten an Privacy@sharkmob.com gerichtet werden.

Falls Sie sich über unsere Verarbeitung Ihrer personenbezogenen Daten beschweren möchten, kontaktieren Sie uns bitte zunächst unter Privacy@sharkmob.com und wir werden uns bemühen, Ihre Anfrage so schnell wie möglich zu bearbeiten. Dies gilt unbeschadet Ihres Rechts, eine Klage bei der Datenschutzbehörde des Landes einzureichen, in dem Sie leben oder arbeiten, und in dem wir Ihrer Meinung nach gegen Datenschutzgesetze verstoßen haben.

10. Änderungen

Wenn wir wesentliche Änderungen an dieser Datenschutzrichtlinie vornehmen, werden wir die aktualisierte Datenschutzrichtlinie hier posten. Bitte besuchen Sie diese Seite regelmäßig, um zu sehen, ob es Aktualisierungen oder Änderungen an dieser Datenschutzrichtlinie gibt.

11. Sprache

Sofern gesetzlich nicht anders festgehalten, gilt im Falle von Abweichungen oder Widersprüchen zwischen der englischen Version und der lokalen Sprachversion dieser Datenschutzrichtlinie die englische Version.

ERGÄNZENDE BEDINGUNGEN – SPEZIFISCHE GERICHTSBARKEIT

Die Gesetze einiger Gerichtsbarkeiten beinhalten zusätzliche Bedingungen für Bloodhunt-Nutzer, die in diesem Abschnitt aufgeführt sind.

Wenn Sie Nutzer mit Sitz in einer der unten aufgeführten Gerichtsbarkeiten sind, gelten für Sie zusätzlich zu den Bedingungen in unserer Datenschutzrichtlinie oben die Bedingungen, die unter dem Namen Ihrer Gerichtsbarkeit aufgeführt sind.

Algerien

Indem Sie Bloodhunt nutzen, erteilen Sie uns Ihre Zustimmung zur Erhebung, Speicherung, Verarbeitung und Nutzung Ihrer personenbezogenen Daten sowie zur Übermittlung an Drittanbieter (lokale Cloud-Anbieter, die Ihre Daten sichern, oder unsere Partnerunternehmen weltweit, die uns bei der Bereitstellung von Bloodhunt helfen) in Bulgarien, Irland, Singapur, Schweden und den USA (wie in der Datenschutzrichtlinie beschrieben), wo sie manuell und elektronisch verarbeitet werden.

Argentinien

Ihre Rechte

Sollten Sie mit unserer Reaktion auf Ihre Anfrage nach dem Zugriff, der Korrektur oder der Löschung Ihrer personenbezogenen Daten oder mit Ihrer Datenschutzbeschwerde bezüglich Ihrer personenbezogenen Daten unzufrieden sein, können Sie sich an die Behörde für den Zugang zu öffentlichen Informationen unter folgender Adresse wenden: Av. Pte. Gral. Julio A. Roca 710, Piso 2°, Ciudad de Buenos Aires (Telephone: +5411 3988-3968 oder E-Mail: datospersonales@aaip.gob.ar).

Datenweitergabe

Wir unternehmen zwar angemessene Maßnahmen, um sicherzustellen, dass Drittanbieter mit Ihren personenbezogenen Daten entsprechend der für Sie geltenden Datenschutzgesetze umgehen, durch die Bereitstellung Ihrer personenbezogenen Daten und die Nutzung von Bloodhunt stimmen Sie aber der Weitergabe Ihrer personenbezogenen Daten an eine Gerichtsbarkeit zu, deren Datenschutzgesetze womöglich nicht das gleiche Maß an Schutz bieten wie die in Argentinien geltenden Gesetze.

Australien

Ausländische Empfänger

Wir ergreifen angemessene Maßnahmen, um sicherzustellen, dass der Umgang von nicht in Australien ansässigen Drittanbietern mit Ihren personenbezogenen Daten den australischen Datenschutzgesetzen entspricht. Allerdings räumen Sie ein, dass wir die Handlungen oder Unterlassungen dieser Drittanbieter nicht kontrollieren und keine Haftung für sie übernehmen.

Zugriff

Sie haben das Recht, auf Ihre von uns gespeicherten personenbezogenen Daten zuzugreifen sowie auf Informationen darüber, wie wir sie verwenden und mit wem wir sie teilen. Der Zugriff auf die von Ihnen über Ihr Konto bereitgestellten personenbezogenen Daten ist per Anmeldung bei Ihrem Konto möglich. Wenn Sie der Meinung sind, dass wir noch andere personenbezogene Daten über Sie gespeichert haben, kontaktieren Sie uns unter Privacy@sharkmob.com.

Korrektur

Sie haben das Recht auf Korrektur fehlerhafter von uns gespeicherter personenbezogener Daten über Sie. Der Zugriff auf Ihre von uns gespeicherten personenbezogenen Daten ist per Anmeldung bei Ihrem Konto möglich. Wenn Sie der Meinung sind, dass wir noch andere personenbezogene Daten über Sie gespeichert haben und diese Daten fehlerhaft sind, kontaktieren Sie uns unter Privacy@sharkmob.com.

Kinder

Solltest du unter 18 Jahre alt sein, verbürgst du, dass du das Einverständnis eines Erziehungsberechtigten zur Registrierung eines Kontos und zur Nutzung von Bloodhunt eingeholt hast.

Anonym agieren

Wo es durchführbar ist, geben wir Ihnen die Möglichkeit, sich bei der Registrierung eines Kontos für Bloodhunt oder bei dessen Nutzung nicht selbst zu identifizieren oder ein Pseudonym zu verwenden. Sie räumen ein, dass wir Ihnen, wenn Sie uns keine personenbezogenen Daten anvertrauen, womöglich bestimmte Funktionen oder Bereiche von Bloodhunt nicht zur Verfügung stellen können, einschließlich der Integration von Social Media und Einkaufsmöglichkeiten.

Ihre Rechte

Sollten Sie mit unserer Reaktion auf Ihre Anfrage nach dem Zugriff oder der Korrektur Ihrer personenbezogenen Daten oder Ihrer Datenschutzbeschwerde bezüglich Ihrer personenbezogenen Daten unzufrieden sein, können Sie sich an das Büro des australischen Datenschutzbeauftragten wenden (Telefon +61 1300 363 992 oder E-Mail enquiries@oaic.gov.au).

Datenweitergabe

Wir unternehmen zwar angemessene Maßnahmen, um sicherzustellen, dass Drittanbieter mit Ihren personenbezogenen Daten entsprechend der für Sie geltenden Datenschutzgesetze umgehen, aber Sie akzeptieren und stimmen zu, dass wir die Handlungen Dritter nicht steuern und nicht für deren Einhaltung der Datenschutzgesetze garantieren können.

Bangladesch

Vereinbarung

Durch Annahme dieser Datenschutzrichtlinie bestätigen Sie ausdrücklich, dass Sie uns dazu ermächtigen, personenbezogene Informationen von Ihnen in dem von dieser Datenschutzrichtlinie vorgesehenen Maße zu sammeln, zu verwenden, zu speichern, zu verarbeiten und an Dritte weiterzugeben. Wenn Sie auf „Annehmen“ klicken, stimmen Sie zu, dass Ihre Daten an Datenbanken oder Partner im Ausland weitergegeben werden dürfen, insbesondere nach Bulgarien, Irland, Singapur, Schweden und in die USA.

Altersbeschränkungen

Zur Nutzung von Bloodhunt versichern Sie, dass Sie mindestens 18 Jahre alt und damit rechtlich dazu befähigt sind, verbindliche Verträge einzugehen.

Brasilien

Dieser Abschnitt gilt für in Brasilien ansässige Nutzer:

Widerruf der Einwilligung

Wann immer wir ihre personenbezogenen Daten auf Basis ihrer Einwilligung nutzen, können Sie die zuvor gegebene Einwilligung zur Sammlung, Nutzung und Weitergabe Ihrer personenbezogenen Daten vorbehaltlich vertraglicher oder gesetzlicher Beschränkungen widerrufen. Um Ihre Einwilligung zu widerrufen, können Sie Ihr Konto entfernen oder Sie kontaktieren Privacy@sharkmob.com. Allerdings kann dies Auswirkungen auf Ihre Nutzung von Bloodhunt haben.

Zustimmung der Erziehungsberechtigten

Solltest du unter 18 Jahre alt sein, sieh bitte von jeglicher Nutzung von Bloodhunt ab, bevor nicht ein Erziehungsberechtigter dieser Datenschutzrichtlinie zugestimmt hat (sowohl für sich als auch in deinem Namen).

Wir erfassen wissentlich zu keinem Zweck personenbezogene Daten von Kindern unter 18 Jahren ohne eine solche Zustimmung. Bitte kontaktieren Sie unseren Datenschutzbeauftragten, wenn Sie glauben, dass wir personenbezogene Daten von Kindern unter 18 Jahren ohne die Zustimmung eines Erziehungsberechtigten erfasst haben – wir untersuchen (und entfernen) derlei personenbezogene Daten unverzüglich.

DURCH ANNAHME DIESER DATENSCHUTZRICHTLINIE BESTÄTIGEN SIE AUSDRÜCKLICH, DASS SIE UNS DAZU ERMÄCHTIGEN, PERSONENBEZOGENE INFORMATIONEN VON IHNEN IN DEM VON DIESER DATENSCHUTZRICHTLINIE VORGESEHENEN MASSE ZU SAMMELN, ZU VERWENDEN, ZU SPEICHERN UND ZU VERARBEITEN, EINSCHLIESSLICH DER WEITERGABE AN DRITTE.

Kalifornien

Dieser Abschnitt gilt für Einwohner Kaliforniens, die unter den California Consumer Privacy Act („CCPA“) von 2018 fallen.

Sammlung und Weitergabe personenbezogener Daten

Im Lauf der letzten 12 Monate haben wir folgende Kategorien personenbezogener Daten von oder über Sie oder über Ihr Gerät gesammelt und weitergegeben:

- Identifikatoren wie Ihre E-Mail-Adresse, Verifizierungscode, Sprache, Region, Benutzername, Passwort, IP-Adresse und OpenID. Diese Information wurde direkt von Ihnen eingeholt.
- Daten zur Internet- oder anderen elektronischen Netzwerk-Aktivitäten, z. B. Ihre Daten bezüglich der Verwendung von Bloodhunt, und andere Gerätedaten wie in der Datenschutzrichtlinie beschrieben. Diese Information wurde direkt von Ihnen eingeholt und von Ihrem Gerät gesammelt.

Wir sammeln Ihre personenbezogenen Daten für die folgenden Zwecke:

- Um Ihnen Bloodhunt zur Verfügung zu stellen, Ihr Konto zu warten, Kundendienste bereitzustellen, Ihre Zahlungsdaten (einschließlich Kaufzeit, Kaufwert, Daten zu gekauften Artikeln, Spielwährungsguthaben) nachzuvollziehen.
- Um unsere Dienste zu verbessern, einschließlich der Funktionalität von Bloodhunt.
- Zu Sicherheits- und Verifizierungszwecken, einschließlich der Verhinderung und Erkennung betrügerischer Aktivitäten.
- Um uns mit technischen Problemen und Fehlern zu beschäftigen und sie zu beseitigen.

Zusätzliche Informationen darüber, für was jeweils welche Art personenbezogener Daten genutzt wird, finden Sie in dieser Tabelle im Hauptteil der Datenschutzrichtlinie.

- Wir geben personenbezogene Daten an folgende Stellen weiter:
- Andere Unternehmen innerhalb unserer Unternehmensgruppe, die Ihre personenbezogenen Daten verarbeiten, um Bloodhunt zu betreiben.
- Andere Unternehmen, die in unserem Auftrag Dienste zur Unterstützung von Bloodhunt bereitstellen und denen es vertraglich untersagt ist, personenbezogene Daten für einen anderen Zweck als die Bereitstellung ihrer Dienste für uns aufzubewahren, zu verwenden oder weiterzugeben.
- Aufsichtsbehörden, Justizbehörden und Strafverfolgungsbehörden.
- Dritte, die unser Unternehmen komplett oder im Wesentlichen erwerben.

In den letzten 12 Monaten haben wir keine personenbezogenen Daten von Einwohnern Kaliforniens im Sinne des CCPA verkauft.

Rechte im Rahmen des CCPA

Wenn Sie ein Einwohner Kaliforniens sind, dann haben Sie folgende Rechte:

- Sie können verlangen, dass wir ihnen kostenlos folgende Informationen bezüglich der letzten zwölf

Monate vor ihrem Ersuchen zur Verfügung stellen:
    - Kategorien der personenbezogenen Daten, die wir über sie gesammelt haben.
    - Kategorien der Quellen, aus denen wir die personenbezogenen Daten gesammelt haben.
    - Der Zweck der Sammlung personenbezogener Daten über Sie.
    - Kategorien von Dritten, an die wir personenbezogene Daten über Sie weitergegeben haben, und Kategorien der personenbezogenen Daten, die weitergegeben wurden (wenn zutreffend), und den Zweck der Weitergabe personenbezogener Daten über Sie.
    - Die spezifischen Teile personenbezogener Daten, die wir über sie gesammelt haben.
- Sie können verlangen, dass wir personenbezogene Daten löschen, die wir von Ihnen gesammelt haben, außer der CCPA erkennt eine Ausnahme an.
- Sie sind frei von unrechtmäßiger Diskriminierung bei der Ausübung Ihrer Rechte einschließlich der Bereitstellung eines anderen Niveaus oder einer anderen Qualität von Diensten oder der Verweigerung von Waren und Dienstleistungen, wenn Sie Ihre Rechte im Rahmen des CCPA ausüben.

Unser Ziel ist, allen überprüften Anfragen gemäß CCPA innerhalb von 45 Tagen nachzukommen. Falls nötig wird eine Verlängerung des Zeitraums um weitere 45 Tage von einer Begründung für die Verzögerung begleitet.

Wie Sie Ihre Rechte wahrnehmen

Zunächst sollten Sie sich an ihrem Konto anmelden und Ihre Daten dort verwalten. Wenn sie ein Einwohner Kaliforniens sind, für den der CCPA gilt, können Sie Ihre Rechte, die Sie gegebenenfalls bezüglich anderer Daten besitzen, wahrnehmen, indem Sie uns über Privacy@sharkmob.com kontaktieren.

Kanada

Wenn Sie sich in Kanada befinden und schriftliche Auskünfte über unsere Richtlinien und Praktiken in Bezug auf unsere Dienstanbieter außerhalb Kanadas erhalten wollen, dann kontaktieren Sie uns unter Privacy@sharkmob.com. Unsere Datenschutzexperten, die unter dieser E-Mail-Adresse erreichbar sind, können auch jegliche Fragen beantworten, die Nutzer bezüglich der Sammlung, Verwendung, Weitergabe und Speicherung personenbezogener Daten durch unsere Dienstanbieter haben.

In den Fällen, in denen wir Dienstanbieter einsetzen, die mitunter Zugriff auf Ihre personenbezogenen Daten haben, verlangen wir von diesen Datenschutz- und Sicherheitsstandards, die mit den unsrigen vergleichbar sind. Über Verträge und andere Maßnahmen im Hinblick auf unsere Dienstanbieter sorgen wir für die Vertraulichkeit und Sicherheit Ihrer personenbezogenen Daten und verhindern, dass diese für einen anderen Zweck als den in dieser Datenschutzrichtlinie vorgesehenen verwendet werden.

Kolumbien

Sprache

Für in Kolumbien ansässige Nutzer ist diese Datenschutzrichtlinie in spanischer Sprache verfügbar. Im Zweifelsfall hat die spanische Version dieser Datenschutzrichtlinie Vorrang.

Verwendung Ihrer personenbezogenen Daten

Ab dem Inkrafttreten dieser Datenschutzrichtlinie werden wir Sie bei der Erfassung Ihrer personenbezogenen Daten um Ihre vorherige Zustimmung bitten, indem wir Sie über die spezifischen Zwecke der Verarbeitung Ihrer personenbezogenen Daten informieren, für die eine solche Zustimmung gemäß der Datenschutzrichtlinie eingeholt wird.

Ihre Zustimmung kann (i) schriftlich, (ii) mündlich oder (iii) durch unmissverständliche Handlungen gegeben werden, die uns vernünftigerweise zu folgern erlauben, dass Ihre Zustimmung gegeben wurde, beispielsweise durch die Annahme der Datenschutzrichtlinie. Wir halten mitunter Nachweise besagter Zustimmungen vor, wobei wir die Prinzipien von Vertraulichkeit und Schutz Ihrer Daten achten.

Ihre Rechte

Als betroffene Person haben Sie bestimmte Rechte, einschließlich (i) Zugriff, Aktualisierung und Korrektur Ihrer

personenbezogenen Daten, (ii) Anfordern einer Kopie der Zustimmung, die Sie uns gegeben haben, (iii) darüber informiert zu werden, wie wir Ihre personenbezogenen Daten verarbeitet haben, (iv) Klagen bei der Datenschutzbehörde Ihres Landes einzureichen, (v) die Zustimmung zu widerrufen, die Sie uns für die Verarbeitung Ihrer personenbezogenen Daten gegeben haben, es sei denn, die Verarbeitung stützt sich auf zwingende rechtmäßige Gründe oder ist aus rechtlichen Gründen erforderlich, (vi) die Unterdrückung Ihrer personenbezogenen Daten zu fordern (Recht auf Löschung) und (vii) freier Zugriff auf Ihre Daten.

Wenn Sie eines dieser Rechte ausüben wollen, dann können Sie uns über die Kontaktinformationen im Abschnitt „Kontakt & Beschwerden“ dieser Datenschutzrichtlinie kontaktieren.

Verfahren der Rechtewahrnehmung

- **Anfragen (Recht auf Zugriff):** Sie können Anfragen bezüglich der Verarbeitung Ihrer personenbezogenen Daten an uns stellen. Anfragen werden innerhalb eines maximalen Zeitraums von zehn (10) Arbeitstagen ab Eingang bearbeitet. Wenn es nicht möglich ist, eine Anfrage innerhalb dieses Zeitraums zu bearbeiten, wird Ihnen der Grund für die Verzögerung mitgeteilt und wir werden Ihnen ein Datum nennen, an dem eine Rücksprache stattfindet, was in keinem Fall mehr als fünf (5) Arbeitstage nach Ablauf des ersten Zeitraums liegen wird.
- **Anträge (Recht auf Korrektur und Löschung)** Sie haben das Recht, Anträge in Verbindung mit der Verarbeitung Ihrer personenbezogenen Daten zu stellen, in denen Sie klar die Fakten beschreiben, die Ihren Anspruch begründen. Anträge werden innerhalb eines maximalen Zeitraums von fünfzehn (15) Arbeitstagen ab Eingang bearbeitet. Wenn es nicht möglich ist, einen Antrag innerhalb dieses Zeitraums zu bearbeiten, wird Ihnen der Grund für die Verzögerung mitgeteilt und wir werden Ihnen ein Datum nennen, an dem der Antrag bearbeitet wird, was in keinem Fall mehr als acht (8) Arbeitstage nach Ablauf des ersten Zeitraums liegen wird.

Ägypten

Wenn Sie auf „Annehmen“ klicken oder mit dem Anmeldeprozess fortfahren, erklären Sie, dass Sie diese Datenschutzrichtlinie gelesen und verstanden haben und ihr zustimmen. Wenn Sie dieser Datenschutzrichtlinie nicht zustimmen, dürfen Sie Bloodhunt nicht nutzen.

Sie bestätigen Ihre Zustimmung zur Verarbeitung, Speicherung und grenzüberschreitenden Übertragung Ihrer personenbezogenen Daten. Die grenzüberschreitende Übertragung kann in alle Länder stattfinden, in denen wir Datenbanken oder Partner haben, insbesondere nach Bulgarien, Irland, Singapur, Schweden und in die USA.

Sie bestätigen zudem Ihre Zustimmung, Marketingnachrichten von uns zu erhalten, ob durch E-Mails, Pop-ups oder ähnliche Verfahren.

Als neuer Nutzer haben Sie sieben Tage Zeit, um uns von möglichen Einsprüchen gegenüber dieser Datenschutzrichtlinie zu informieren.

Als ägyptische betroffene Person haben Sie bestimmte Rechte nach dem ägyptischen Gesetz zum Schutz persönlicher Daten.

Frankreich

Ihre Rechte

Anweisungen zur Verarbeitung Ihrer personenbezogenen Daten nach dem Tode

Sie haben das Recht, uns allgemeine oder spezifische Anweisungen für die Aufbewahrung, Löschung und Vermittlung Ihrer personenbezogenen Daten nach Ihrem Tod zu geben.

Diese spezifischen Anweisungen gelten nur für die Aktivitäten der Verarbeitung, die hier genannt sind, und die Verarbeitung dieser Anweisungen unterliegt Ihrer ausdrücklichen Zustimmung.

Sie können Ihre Anweisungen jederzeit abändern oder widerrufen.

Sie können eine Person bestimmten, die verantwortlich für die Umsetzung dieser Anweisungen ist. Diese Person wird im Fall Ihres Todes über Ihre Anweisungen informiert und dazu berechtigt, deren Umsetzung von uns zu fordern. Mangels Benennung oder – sofern nichts anderes festgelegt wurde – im Todesfall der benannten Person, haben deren Erben das Recht, über Ihre Anweisungen informiert zu werden und deren Umsetzung von uns zu verlangen.

Wenn Sie solche Anweisungen machen möchten, kontaktieren Sie uns bitte unter Privacy@sharkmob.com.

Hongkong

Als betroffene Person in Hongkong haben Sie gesetzliche Rechte in Bezug auf die von uns über Sie gespeicherten personenbezogenen Daten (entsprechend der geltenden Gesetze und Bestimmungen).

Sie können eine Kopie der von uns über sie erhobenen Daten oder eine Korrektur der Daten beantragen und haben das Recht, der Verwendung ihrer personenbezogenen Daten zu direkten Marketingzwecken zu widersprechen. Für den Datenzugriff kann unsererseits eine Gebühr erhoben werden.

Indien

Altersbeschränkungen

Für Kinder unter 18 Jahren ist die Zustimmung der Eltern erforderlich, um Bloodhunt zu nutzen.

Vertrauliche personenbezogene Daten

Zu den vertraulichen personenbezogenen Daten nach lokalem Recht gehören Passwörter, Finanzinformationen (wie Bankkonto, Kreditkarte, Kundenkarte oder andere Zahlungsmitteldetails), biometrische Daten, körperliche oder geistige Gesundheit, Sexualleben oder sexuelle Orientierung und/oder Krankenakten oder Krankengeschichte. Sie beinhalten jedoch keine Daten, die öffentlich zugänglich sind oder nach indischem Recht bereitgestellt werden, einschließlich des Gesetzes zum Auskunftsrecht von 2005.

Teilen Ihrer vertraulichen personenbezogenen Daten

Wenn wir Dritten die Erfassung und Nutzung Ihrer vertraulichen personenbezogenen Daten gestatten, ergreifen wir angemessene Maßnahmen, um sicherzustellen, dass diese Dritten die vertraulichen personenbezogenen Daten nicht weiter offenlegen, soweit dies nach geltendem Recht erforderlich ist.

Widerruf der Einwilligung

Soweit dies durch geltende Gesetze und Vorschriften vorgesehen ist, können Sie jegliche Einwilligung widerrufen, die Sie uns zuvor für bestimmte Verarbeitungsaktivitäten erteilt haben, indem Sie uns unter Privacy@sharkmob.com kontaktieren. Wenn für die Verarbeitung Ihrer personenbezogenen Daten eine Einwilligung erforderlich ist, Sie der Verarbeitung nicht zustimmen oder Ihre Einwilligung widerrufen, können wir den erwarteten Dienst möglicherweise nicht bereitstellen.

Indonesien

Einwilligung

Indem Sie diese Datenschutzrichtlinie akzeptieren und ihr zustimmen, stimmen Sie zu, dass wir Ihre personenbezogenen Daten in Übereinstimmung mit dieser Datenschutzrichtlinie in ihrer von Zeit zu Zeit überarbeiteten Fassung erheben, verwenden und weitergeben dürfen. Wenn Sie dieser Datenschutzrichtlinie nicht zustimmen, dürfen Sie nicht auf unsere Dienste zugreifen oder diese nutzen und wir haben das Recht, Ihnen keinen Zugriff auf unsere Dienste zu gewähren.

Zustimmung der Erziehungsberechtigten

Solltest du unter 21 Jahre alt sein, verbürgst du, dass du das Einverständnis eines Erziehungsberechtigten zur

Registrierung eines Kontos und zur Nutzung von Bloodhunt eingeholt hast.

Rechte des Betroffenen

Sie haben das Recht, von Zeit zu Zeit gemäß den geltenden Datenschutzgesetzen und -vorschriften in Indonesien auf Ihre bei Bloodhunt gespeicherten personenbezogenen Daten zuzugreifen.

Datenschutzverletzung

Falls wir die Vertraulichkeit Ihrer personenbezogenen Daten bei Bloodhunt nicht wahren können, benachrichtigen wir Sie über die von Ihnen bereitgestellten Kontaktinformationen oder über Bloodhunt, soweit dies gemäß den lokalen Gesetzen und Vorschriften erforderlich ist.

Datenspeicherung

Wir bewahren Ihre personenbezogenen Daten gemäß den gesetzlichen Bestimmungen auf.

Benachrichtigung zur Änderung dieser Datenschutzrichtlinie

Wenn Sie Ihren Widerspruch gegen eine geänderte Version dieser Datenschutzrichtlinie nicht innerhalb von vierzehn (14) Tagen nach dem Datum der Veröffentlichung der entsprechenden geänderten Version dieser Datenschutzrichtlinie deutlich zum Ausdruck bringen, gelten die Änderungen als akzeptiert und Sie haben der neuen Datenschutzrichtlinie zugestimmt. Sie können jedoch die Nutzung oder den Zugriff auf Bloodhunt beenden, indem Sie sich jederzeit abmelden oder Ihre Nutzung von Bloodhunt einstellen, wenn Sie der geänderten Datenschutzrichtlinie nicht mehr zustimmen.

Richtigkeit der Daten und Einwilligung Dritter

Sie sind dafür verantwortlich, sicherzustellen, dass alle personenbezogenen Daten, die Sie uns zur Verfügung stellen, korrekt und aktuell sind. Um die Richtigkeit der Angaben zu bestätigen, können wir die uns zur Verfügung gestellten Daten auch jederzeit überprüfen. Sie erklären hiermit, dass Sie alle erforderlichen Einwilligungen eingeholt haben, bevor Sie uns die personenbezogenen Daten eines Dritten zur Verfügung stellen (z. B. für Weiterempfehlungs-Aktionen). In diesem Fall gehen wir immer davon aus, dass Sie zuvor eine Einwilligung eingeholt haben. Sie sind für alle Ansprüche jeglicher Art verantwortlich, die sich aus dem Fehlen solcher Einwilligungen ergeben.

Japan

Mindestalter

Sie müssen mindestens 20 Jahre alt sein, um Bloodhunt nutzen zu dürfen. Andernfalls ist die Zustimmung der Eltern erforderlich.

Einwilligung zur Weitergabe an Dritte

Wenn Sie auf „Annehmen“ klicken, stimmen Sie zu, dass Ihre Daten an Dritte weitergegeben werden dürfen, darunter Datenbanken oder Partner im Ausland, insbesondere nach Bulgarien, Irland, Singapur, Schweden und in die USA.

Einwilligung

Wenn Sie auf „Annehmen“ klicken, stimmen Sie zu, dass Ihre Daten an Datenbanken oder Partner im Ausland weitergegeben werden dürfen, insbesondere in die Vereinigten Staaten, nach Singapur und Schweden.

Ihre Rechte

Sie können uns darum bitten, Sie über die Verwendungszwecke zu informieren, sie offenzulegen, sie zu korrigieren, die Nutzung oder Bereitstellung einzustellen und/oder alle Ihre personenbezogenen Daten zu löschen, die bei uns gespeichert sind, entsprechend dem japanischen Gesetz zum Schutz personenbezogener

Daten. Wenn Sie einen solchen Antrag stellen möchten, kontaktieren Sie uns bitte unter Privacy@sharkmob.com.

Königreich Saudi-Arabien

Sie stimmen der Erfassung, Nutzung, Offenlegung, dem Export (entsprechend der geltenden Gesetze) sowie der Speicherung Ihrer personenbezogenen Daten entsprechend dieser Datenschutzrichtlinie zu.

Kuwait

Sie erklären, dass Sie mindestens 21 oder 18 Jahre alt sind und die Zustimmung der Eltern/Erziehungsberechtigten eingeholt haben und daher gemäß den geltenden Gesetzen und Vorschriften in Kuwait geschäftsfähig sind.

Durch Annahme dieser Datenschutzrichtlinie bestätigen Sie ausdrücklich, dass Sie uns dazu ermächtigen, personenbezogene Daten von Ihnen in dem von dieser Datenschutzrichtlinie vorgesehenen Maße zu sammeln, zu verwenden, zu speichern und zu verarbeiten, einschließlich der Weitergabe an Dritte in oder außerhalb Kuwaits.

SAR Macau

Sie haben das Recht, Ihre personenbezogenen Daten nicht anzugeben. Infolgedessen können wir Ihnen Bloodhunt jedoch möglicherweise nicht zur Verfügung stellen. Als betroffene Person in SAR Macau haben Sie gesetzliche Rechte in Bezug auf Ihre personenbezogenen Daten (entsprechend der geltenden Gesetze und Bestimmungen). Sie können eine Kopie der von uns über sie erhobenen Daten oder eine Korrektur der Daten beantragen und haben das Recht, der Verwendung ihrer personenbezogenen Daten zu Marketing- oder anderen gewerblichen Zwecken aus beliebigen persönlichen Gründen zu widersprechen. Für den Datenzugriff kann unsererseits eine Gebühr erhoben werden.

Malaysia

Sprache der Datenschutzrichtlinie

Im Falle von Unterschieden zwischen der englischen und der Bahasa-Melayu-Fassung dieser Datenschutzrichtlinie gilt die englische Fassung.

Zustimmung der Erziehungsberechtigten

Solltest du unter 18 Jahre alt sein, sieh bitte von der Nutzung von Bloodhunt ab.

Sollten Sie dieser Datenschutzrichtlinie zustimmen, um einem Minderjährigen Zugang zu Bloodhunt zu gewähren, stimmen Sie hiermit der Verarbeitung personenbezogener Daten dieses Minderjährigen entsprechend dieser Datenschutzrichtlinie sowie den in dieser Datenschutzrichtlinie enthaltenen Bedingungen zu. Des Weiteren übernehmen Sie hiermit die Haftung für jegliche Handlungen des Minderjährigen sowie die Verantwortung dafür, dass dieser sich an diese Datenschutzrichtlinie hält.

Ihre Rechte

Zugriffsrecht: Sie haben das Recht, Zugriff auf ihre personenbezogenen Daten zu beantragen und eine Kopie der von uns oder in unserem Namen erhobenen und verarbeiteten Daten zu erhalten. Wir behalten uns das Recht vor, eine im gesetzlichen Rahmen befindliche Gebühr für den Zugriff auf Ihre personenbezogenen Daten zu erheben.

Zur Bearbeitung von Datenzugriffsanträgen dürfen wir bestimmte Informationen zur Identitätsbestimmung des Antragstellers einfordern, um sicherzustellen, dass dieser gesetzlichen Anspruch auf die Stellung dieses Antrags besitzt.

Recht auf Korrektur: Sie können die Korrektur Ihrer personenbezogenen Daten beantragen. Zur Bearbeitung von

Datenkorrekturanträgen dürfen wir bestimmte Informationen zur Identitätsbestimmung des Antragstellers einfordern, um sicherzustellen, dass dieser gesetzlichen Anspruch auf die Stellung dieses Antrags besitzt.

Recht auf Einschränkung der Verarbeitung Ihrer personenbezogenen Daten: Sie können die Einschränkung der Verarbeitung Ihrer personenbezogenen Daten beantragen, indem Sie sich an obige Adresse wenden. Allerdings kann dies Auswirkungen auf Ihre Nutzung von Bloodhunt haben.

Kontakt

Zum Schutz Ihrer personenbezogenen Daten und der Bearbeitung von Beschwerden bezüglich dieser haben wir folgende Abteilung mit der Verwaltung und dem Schutz Ihrer personenbezogenen Daten betraut.

Unser Datenschutzbeauftragter, der für die Verwaltung und Sicherheit Ihrer personenbezogenen Daten verantwortlich ist.

- E-Mail: Privacy@sharkmob.com

Mexiko

Sprache

Für in Mexiko ansässige Nutzer ist diese Datenschutzrichtlinie in spanischer Sprache verfügbar. Im Zweifelsfall hat die spanische Version dieser Datenschutzrichtlinie Vorrang.

Altersbeschränkungen

Bloodhunt kann nur von Ihnen genutzt werden, wenn Sie entweder mindestens 18 Jahre alt sind oder ein Erziehungsberechtigter dieser Datenschutzrichtlinie zugestimmt hat (sowohl für sich als auch in Ihrem Namen).

Arten der von uns verwendeten personenbezogenen Daten

Zur Klarstellung: In Abschnitt 1 „Arten der von uns verwendeten personenbezogenen Daten“ und Abschnitt 2 „Verwendung Ihrer personenbezogenen Daten“ finden Sie sämtliche Einzelheiten zu den von uns verwendeten personenbezogenen Daten. Folglich führen wir sämtliche Informationen zu den von uns verwendeten personenbezogenen Daten entsprechend des Bundesgesetzes über den Schutz personenbezogener Daten für Privatpersonen sowie anderer geltender Bestimmungen auf.

Verarbeitungszweck

Einige der oben aufgeführten Verarbeitungszwecke dienen freiwilligen Zwecken wie der Versorgung mit personalisierten Empfehlungen und Werbung. Des Weiteren können wir Ihre personenbezogenen Daten zum freiwilligen Zweck der Übermittlung von Informationen, die wir als für Sie relevant betrachten, per E-Mail verwenden. Sie können der Verarbeitung Ihrer personenbezogenen Daten zu freiwilligen Zwecken entsprechend des weiter unten stehenden Abschnitts „Ihre Rechte“ widersprechen.

Bitte nehmen Sie zur Kenntnis, dass wir Ihre personenbezogenen Daten auch zur Einhaltung gesetzlicher Verpflichtungen oder zur Bearbeitung von Anfragen zuständiger Behörden, der Wahrung oder dem Schutz unserer Rechte bezüglich zuständiger Behörden/Gerichte, zur Beantwortung von Anfragen, die von Ihnen bezüglich Ihrer personenbezogenen Daten an uns gerichtet werden, und zur Ausführung der in Abschnitt 3 „Wie wir Ihre personenbezogenen Daten speichern und weitergeben“ beschriebenen Datenweitergabe verwenden.

Zustimmung zur Datenweitergabe

Im Allgemeinen benötigen wir Ihre Zustimmung zur in Abschnitt 3 „Wie wir Ihre personenbezogenen Daten speichern und weitergeben“ beschriebenen Datenweitergabe nicht. Allerdings benötigen wir Ihre Zustimmung, um Ihre personenbezogenen Daten an Dritte, die uns komplett oder im Wesentlichen oder unser Unternehmen erwerben, weiterzugeben.

Durch die Nutzung von Bloodhunt und die Bereitstellung Ihrer personenbezogenen Daten stimmen Sie der oben beschriebenen Datenweitergabe zu. Sie können Ihre Rechte bezüglich Ihrer personenbezogenen Daten ausüben, wie im Abschnitt „Ihre Rechte“ aufgeführt.

Ihre Rechte

Die Untersektionen „Zugriff“, „Korrektur“, „Löschung“, „Widerspruch“, „Beschränkung der Verarbeitung auf Speicherung“, die die Beschränkung der Nutzung und Offenlegung Ihrer personenbezogenen Daten umfassen, sowie die Untersektion „Werbung“ im obigen Abschnitt „Ihre Rechte“ gelten auch für nicht in Mexiko ansässige Nutzer.

Sie haben außerdem das Recht, Ihre Zustimmung zur Verarbeitung Ihrer personenbezogenen Daten zu widerrufen.

Um eines Ihrer Rechte auszuüben, kontaktieren Sie bitte unseren Datenschutzbeauftragten unter Privacy@sharkmob.com.

Um mehr über Ihre Rechte sowie geltende Maßnahmen, Abläufe und Erfordernisse zur Ausübung Ihrer Rechte zu erfahren, kontaktieren Sie bitte unseren Datenschutzbeauftragten unter Privacy@sharkmob.com.

Marokko

Der Schutz Ihrer Privatsphäre ist für uns von großer Bedeutung. Wir erfassen ausschließlich Daten, die für die ordnungsgemäße Nutzung von Bloodhunt unbedingt erforderlich sind.

Durch Ihre Zustimmung zu diesen Verwendungszwecken stimmen sie ausdrücklich der Verarbeitung Ihrer personenbezogenen Daten durch Bloodhunt zu.

Bitte beachten Sie:

- Die Identität des Datenverantwortlichen ist Sharkmob AB, E-Mail: Privacy@sharkmob.com.
- Die Verarbeitungszwecke der Daten sind in der Tabelle im Abschnitt „Verwendung Ihrer personenbezogenen Daten“ aufgeführt.
- Empfänger oder Empfängerkategorien sind im zweiten Absatz des Abschnitts „Wie wir Ihre personenbezogenen Daten speichern und weitergeben“ dargelegt.
- Ob die Beantwortung Ihrer Fragen verpflichtend oder optional ist sowie die möglichen Konsequenzen der Nichtbeantwortung finden sie im Abschnitt „Verwendung Ihrer personenbezogenen Daten“ und im Abschnitt „Ihre Rechte“ (Unterabsatz „Widerspruch“).

Neuseeland

Dieser Abschnitt gilt für in Neuseeland ansässige Nutzer:

Ausländische Empfänger

Wir ergreifen angemessene Maßnahmen, um sicherzustellen, dass der Umgang von nicht in Neuseeland ansässigen Dritten mit Ihren personenbezogenen Daten den neuseeländischen Datenschutzgesetzen entspricht. Allerdings räumen Sie ein, dass wir die Handlungen oder Unterlassungen dieser Drittanbieter nicht kontrollieren und keine Haftung für sie übernehmen.

Zugriff

Sie haben das Recht, auf Ihre von uns gespeicherten personenbezogenen Daten zuzugreifen sowie auf Informationen darüber, wie wir sie verwenden und mit wem wir sie teilen. Der Zugriff auf die von Ihnen über Ihr Konto bereitgestellten personenbezogenen Daten ist per Anmeldung bei Ihrem Konto möglich. Wenn Sie der Meinung sind, dass wir noch andere personenbezogene Daten über Sie gespeichert haben, kontaktieren Sie uns unter Privacy@sharkmob.com.

Korrektur

Sie haben das Recht, die Korrektur fehlerhafter von uns gespeicherter personenbezogener Daten über Sie zu verlangen. Der Zugriff auf Ihre von uns gespeicherten personenbezogenen Daten ist per Anmeldung bei Ihrem Konto möglich. Wenn Sie der Meinung sind, dass wir noch andere personenbezogene Daten über Sie gespeichert haben und diese Daten fehlerhaft sind, kontaktieren Sie uns unter Privacy@sharkmob.com.

Kinder

Solltest du unter 16 Jahre alt sein, verbürgst du, dass du das Einverständnis eines Erziehungsberechtigten zur Registrierung eines Kontos und zur Nutzung von Bloodhunt eingeholt hast.

Ihre Rechte

Sollten Sie mit unserer Reaktion auf Ihre Anfrage nach dem Zugriff oder der Korrektur Ihrer personenbezogenen Daten oder Ihrer Datenschutzbeschwerde bezüglich Ihrer personenbezogenen Daten unzufrieden sein, können Sie sich an das Büro des neuseeländischen Datenschutzbeauftragten wenden (www.privacy.org.nz).

Datenweitergabe

Wir unternehmen zwar angemessene Maßnahmen, um sicherzustellen, dass Drittanbieter mit Ihren personenbezogenen Daten entsprechend der für Sie geltenden Datenschutzgesetze umgehen, aber Sie akzeptieren und stimmen zu, dass wir die Handlungen Dritter nicht steuern und nicht für deren Einhaltung der Datenschutzgesetze garantieren können.

Peru

Die Weitergabe und Verteilung personenbezogener Daten erfolgt entsprechend dieser Datenschutzrichtlinie und des Abschnitts „Republik Korea“.

Sie können Rechte zum Schutz personenbezogener Daten ausüben, indem Sie den Zugriff auf oder die Korrektur Ihrer personenbezogenen Daten, die Löschung oder Aussetzung der Verarbeitung ihrer personenbezogenen Daten usw. entsprechend der geltenden Gesetze wie dem Gesetz zum Schutz personenbezogener Daten (das „**Gesetz**“) verlangen.

Außerdem können Sie diese Rechte durch Ihren gesetzlichen Vertreter oder eine von Ihnen bevollmächtigte Person ausüben lassen. Allerdings müssen Sie in diesem Falle eine dem Gesetz entsprechende Handlungsvollmacht vorlegen.

Auf Ihre Anfrage hin werden wir unverzüglich sämtliche erforderlichen Maßnahmen entsprechend der geltenden Vorschriften wie dem Gesetz ergreifen.

Sie können Ihre Zustimmung zur Verarbeitung der personenbezogen Daten oder Ihren Antrag auf Aussetzung dieser jederzeit widerrufen.

Sollten Sie der Meinung sein, dass Ihr Antrag nicht erfüllt wurde, können Sie Klage bei der peruanischen Datenschutzbehörde einreichen.

Kontakt

Zum Schutz Ihrer personenbezogenen Daten und der Bearbeitung von Beschwerden bezüglich dieser haben wir folgende Abteilung mit der Verwaltung und dem Schutz Ihrer personenbezogenen Daten betraut.

- Unser Datenschutzteam, das für die Verwaltung und Sicherheit Ihrer personenbezogenen Daten verantwortlich ist.
- Kontakt: Privacy@sharkmob.com

Philippinen

Mindestalter

Sie müssen mindestens 18 Jahre alt sein, um Bloodhunt nutzen zu dürfen.

Ihre Rechte

Sie besitzen folgende Rechte:

- Das Recht auf Information. Unter bestimmten Umständen haben Sie das Recht, darüber informiert zu werden, ob personenbezogene Daten über Sie verarbeitet werden oder wurden. Dies umfasst auch die Information über die Existenz von automatisierten Entscheidungen und Profilerstellung.
- Widerspruchsrecht. Unter bestimmten Umständen haben Sie das Recht, gegen die Verarbeitung Ihrer personenbezogenen Daten für unter anderem Direktmarketing und automatisierte Verarbeitung oder Profilerstellung Widerspruch einzulegen.
- Zugriffsrecht. Unter bestimmten Umständen haben Sie das Recht, auf Antrag angemessenen Zugriff auf Ihre personenbezogenen Daten zu erhalten.
- Recht auf Korrektur. Unter bestimmten Umständen haben Sie das Recht, Ungenauigkeiten oder Fehler in Ihren personenbezogenen Daten anzufechten und diese durch uns korrigieren zu lassen, es sei denn, Ihr Antrag erfüllt den Tatbestand der Schikane oder ist anderweitig unangemessen.
- Recht auf Löschung oder Sperrung. Unter bestimmten Umständen haben Sie das Recht, die Aussetzung der Sperrung sowie die Löschung oder Vernichtung Ihrer personenbezogenen Daten aufzuheben oder zu verlangen.

Zustimmung

Durch die Zustimmung zu dieser Datenschutzrichtlinie erteilen Sie uns Ihr Einverständnis für:

Die Erfassung und Verarbeitung Ihrer personenbezogenen Daten entsprechend des obigen Abschnitts „Verwendung Ihrer personenbezogenen Daten“.

Die Weitergabe Ihrer personenbezogenen Daten an Dritte innerhalb unserer Unternehmensgruppe und eines Dritten, der uns komplett oder im Wesentlichen oder unser Unternehmen erwirbt, entsprechend dieser Datenschutzrichtlinie und zu dem darin beschriebenen Zwecke.

Die Weitergabe und Speicherung Ihrer personenbezogenen Daten an Orten außerhalb der Philippinen entsprechend des obigen Abschnitts „Wie wir Ihre personenbezogenen Daten speichern und weitergeben“.

Katar

Durch die Nutzung von Bloodhunt in Katar stimmen Sie (im Rahmen des Gesetzes Nr. 13 von 2016 zum Schutz personenbezogener Daten sowie dessen Änderungen) der Verarbeitung Ihrer Daten entsprechend dieser Datenschutzrichtlinie zu.

Republik Korea

Wie wir Ihre personenbezogenen Daten speichern und weitergeben

Verarbeitungsübertragung

Zur Durchführung der in dieser Datenschutzrichtlinie beschriebenen Dienste übertragen wir die Verarbeitung Ihrer personenbezogenen Daten an folgende professionelle Anbieter und ausgewählte Dienste:

Mailchimp – Anmeldung zum Newsletter für Bloodhunt

Pontica Solutions – Kundendienst

Zendesk – Kundendienst

Sentry – Absturzbericht-Dienst

Google Cloud Platform – Cloud-Speicher (Backend)

Microsoft Azure – Cloud-Speicher

Weitergabe personenbezogener Daten ins Ausland

Wir geben personenbezogene Daten an Dritte im Ausland weiter. Die jeweiligen Empfänger, das Land der Weitergabe, Weitergabedatum und -methode, die Art der personenbezogenen Daten und den Verwendungszweck durch den Empfänger entnehmen Sie bitte der nachfolgenden Liste.

Mailchimp

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

Gelegentliche Übermittlung von Daten in die USA. Personenbezogene Daten beinhalten: E-Mail-Adresse, Transaktionsverlauf der E-Mail-Zustellung (mit Zeitstempel, E-Mail-Adresse des Empfängers, E-Mail-Text). **Diese Daten werden zur Anmeldung zum Newsletter über die Recruiting-Website und Nutzerrekrutierung für Bloodhunt verwendet. Datenspeicherungsfrist entsprechend dem Abschnitt „Wie wir Ihre personenbezogenen Daten speichern und weitergeben“.**

Zendesk

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

Gelegentliche Übermittlung von Daten nach Irland, Singapur und Schweden. Personenbezogene Daten beinhalten: Kundendienst-Daten. **Diese Daten werden für Kundendienste verwendet. Datenspeicherungsfrist entsprechend dem Abschnitt „Wie wir Ihre personenbezogenen Daten speichern und weitergeben“.**

Pontica Solutions

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

Gelegentliche Übermittlung von Daten nach Bulgarien. Personenbezogene Daten beinhalten: Kundendienst-Daten. **Diese Daten werden für Kundendienste verwendet. Datenspeicherungsfrist entsprechend dem Abschnitt „Wie wir Ihre personenbezogenen Daten speichern und weitergeben“.**

Sentry

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

Gelegentliche Übermittlung von Daten in die USA. Personenbezogene Daten beinhalten: IP-Adresse, Spielverzeichnis. **Diese Daten werden für Spielanalyse und -verbesserungen verwendet. Datenspeicherungsfrist entsprechend dem Abschnitt „Wie wir Ihre personenbezogenen Daten speichern und weitergeben“.**

Google Cloud Platform

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

Gelegentliche Übermittlung von Daten in die USA. Personenbezogene Daten beinhalten: Alle in der Datenschutzrichtlinie aufgeführten Daten. **Die Daten werden im Cloud-Speicher (Backend) gespeichert, der von Sharkmob AB bei der Bereitstellung von Bloodhunt verwendet wird. Datenspeicherungsfrist entsprechend dem Abschnitt „Wie wir Ihre personenbezogenen Daten speichern und weitergeben".**

Microsoft Azure

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

Gelegentliche Übermittlung von Daten in die USA. Personenbezogene Daten beinhalten: Alle in der Datenschutzrichtlinie aufgeführten Daten. **Die Daten werden im Cloud-Speicher gespeichert, der von Sharkmob AB bei der Bereitstellung von Bloodhunt verwendet wird. Datenspeicherungsfrist entsprechend dem Abschnitt „Wie wir Ihre personenbezogenen Daten speichern und weitergeben".**

Datenvernichtung

Personenbezogene Daten werden entsprechend der in Abschnitt 4 „*Datenspeicherung*" angegebenen Fristen gespeichert. Mit der Ausnahme der im Folgenden angegebenen personenbezogenen Daten werden personenbezogene Daten, die den Zweck ihrer Erfassung oder Verwendung erfüllt und die erlaubte Speicherungsdauer erreicht haben, unwiederbringlich vernichtet. Elektronisch gespeicherte personenbezogene Daten werden mittels technischer Methoden auf sichere Art und Weise unwiederbringlich gelöscht und gedruckte Daten werden geschreddert oder verbrannt.

Die in Abschnitt 4 „*Datenspeicherung*" angegebenen personenbezogen Daten, die über die Speicherungsfrist hinaus gespeichert werden müssen, werden entsprechend folgender Gesetze gespeichert:

Konsumentenschutzgesetz für elektronischen Geschäftsverkehr usw.
Artikel 6 des Konsumentenschutzgesetzes für elektronischen Geschäftsverkehr
Im elektronischen Handel oder Versandhandel:
•Daten zu Etikettierung und Werbung (6 Monate)
•Daten zu Abwicklung oder Widerruf eines Vertrages (5 Jahre)
•Daten zu Bezahlung und der Lieferung von Waren und Dienstleistungen (5 Jahre)
•Daten zu Kundendienst oder Streitlösung (3 Jahre)

Gesetz zum Schutz von Kommunikationsgeheimnissen
Artikel 41 des Gesetzesdekrets, Artikel 15-2 des Gesetzes zum Schutz von Kommunikationsgeheimnissen
•Verlaufsprotokolle, IP-Adresse (3 Monate)
•Das Datum der Telekommunikation von Nutzern, Start- und Endzeit der Telekommunikation, Nutzungsfrequenz (12 Monate)

Ihre Rechte

Sie können Rechte zum Schutz personenbezogener Daten ausüben, indem Sie den Zugriff auf Ihre oder die Korrektur Ihrer personenbezogenen Daten, die Löschung oder Aussetzung der Verarbeitung ihrer

personenbezogenen Daten usw. entsprechend der geltenden Gesetze wie dem Gesetz zum Schutz personenbezogener Daten („**GSPD**“) verlangen.

Außerdem können Sie diese Rechte durch Ihren gesetzlichen Vertreter oder eine von Ihnen bevollmächtigte Person ausüben lassen. Allerdings müssen Sie in diesem Falle eine entsprechende Handlungsvollmacht entsprechend der Vollzugsbestimmungen des GSPD vorlegen.

Auf Ihre Anfrage hin werden wir unverzüglich sämtliche erforderlichen Maßnahmen entsprechend der geltenden Gesetze wie dem GSPD ergreifen.

Sie können Ihre Zustimmung zur Verarbeitung der personenbezogen Daten oder Ihren Antrag auf Aussetzung dieser jederzeit widerrufen.

Weitere Nutzung und Erfassung personenbezogener Daten

Entsprechend des GSPD können wir personenbezogene Daten in angemessenem Rahmen bezogen auf den urs prünglichen Erfassungszweck unter Beachtung der Nachteile für Betroffene sowie ausreichendem Schutz der D aten, z. B. mittels Verschlüsselung usw., nutzen oder bereitstellen. Wir entscheiden sorgfältig über die Nutzun g oder Bereitstellung personenbezogener Daten unter Beachtung der allgemeinen Umstände wie geltenden Ge setzen und Bestimmungen wie dem GSPD, des Nutzungs- oder Bereitstellungszweckes, der Nutzungs- oder Ber eitstellungsart, der einzelnen Nutzungs- oder Bereitstellungsdaten, der Zustimmung oder Benachrichtigung/Inf ormation Betroffener, der Nutzungs- oder Bereitstellungsfolgen für Betroffene sowie der für diese Daten ergrif fenen Schutzmaßnahmen. Spezifisch wird auf Folgendes geachtet:

- Ob die zusätzliche Nutzung/Bereitstellung mit dem ursprünglichen Erfassungszweck zusammenhängt,
- ob die zusätzliche Nutzung/Bereitstellung eingedenk der Umstände der Datenerfassung und der Verarbeitungspraxis vorhersehbar ist,
- ob die zusätzliche Nutzung/Bereitstellung die Interessen des Betroffenen verletzt, und
- ob die erforderlichen Sicherheitsmaßnahmen wie Pseudonymisierung oder Verschlüsselung ergriffen wurden.

Inländischer Datenschutzvertreter

Entsprechend Artikel 32-5 des Netzwerkgesetzes sowie Artikel 39-11 des abgeänderten GSPD lauten die Kontaktdaten des inländischen Vertreters wie folgt:

- Name: Kite Bird Yuhan Hoesa
- Adresse: 25F, 55, Sejong-daero, Jung-gu, Seoul (Taepyeongro 2-ga)
- Telefonnummer: +82 22185 0902
- E-Mail: koreanlocalrep_sharkmob@proximabeta.com

Kontakt

Zum Schutz Ihrer personenbezogenen Daten und der Bearbeitung von Beschwerden bezüglich dieser haben wir folgende Abteilung mit der Verwaltung und dem Schutz Ihrer personenbezogenen Daten betraut.

- Datenschutzabteilung, die für die Verwaltung und Sicherheit Ihrer personenbezogenen Daten verantwortlich ist.
- Telefonnummer: +82 22185 0902
- E-Mail: koreanlocalrep_sharkmob@proximabeta.com

Russland

Wenn Sie Bloodhunt in Russland nutzen,

- stimmen Sie entsprechend des russischen Bundesgesetzes zu personenbezogenen Daten Nr. 152-FZ vom 27. Juli 2006 (wie abgeändert) oder jeglichen ersetzenden Bestimmungen der Verarbeitung Ihrer Daten entsprechend dieser Datenschutzrichtlinie zu. Sollten hier rechtmäßige Interessen, eine Optimierung von Bloodhunt oder die Umsetzung des Vertrages erwähnt sein, erklären Sie sich damit einverstanden, dass entsprechend des russischen Gesetzes dieses Einverständnis ein weiterer Grund für die Verarbeitung (sofern diese auf Grundlage Ihres Einverständnisses erfolgt) darstellen kann. Dieses Einverständnis beinhaltet auch die Verarbeitung jeglicher Cookies (sofern diese laut russischem Gesetz als personenbezogene Daten betrachtet werden).
- stimmen Sie zu, dass Ihre Daten an Datenbanken oder Partner im Ausland weitergegeben werden dürfen, insbesondere nach Singapur, Schweden und in die Vereinigten Staaten.
- stimmen Sie zu, dass entsprechend Artikel 152.1 des russischen bürgerlichen Gesetzbuches die Verarbeitung Ihres Bildes entsprechend dieser Datenschutzrichtlinie durchgeführt werden darf.
- stimmen Sie zu, dass wir entsprechend des Bundesgesetzes zu Marketing/Werbung Werbe-/Marketingmaterial an Sie senden dürfen, es sei denn, Sie haben derlei Kommunikation abgelehnt.

Die Unterabschnitte „Zugriff“, „Korrektur“, „Löschung“, „Beschränkung der Verarbeitung auf Speicherung“, „Widerspruch“ und „Werbung“ des obigen Abschnitts „Ihre Rechte“ gelten für Nutzer, die sich in der Russischen Föderation befinden.

Wir nehmen entsprechend der Datenschutzrichtlinie keine wesentlichen Veränderungen an der Verarbeitungsart Ihrer personenbezogenen Daten vor, ohne Sie vorher darüber zu informieren. Im Falle von wesentlichen Veränderungen benachrichtigen wir Sie mit der Bitte, diesen Änderungen zuzustimmen. Sollte keine Einverständniserklärung vonnöten sein, gehen wir von Ihrer Zustimmung zu diesen Änderungen aus, sofern Sie Bloodhunt nach der Benachrichtigung weiter nutzen.

Der Vertreter Russlands ist erreichbar unter Privacy@sharkmob.com. Bitte geben Sie in der Betreffzeile Ihrer E-Mail das Wort „Russland“ an.

Serbien

Unsere lokalen Vertreter zur Einhaltung des Gesetzes zum Schutz personenbezogener Daten in Serbien sind Karanovic & Partners, die unter local.representative@karanovicpartners.com erreichbar sind. Bitte geben Sie in der Betreffzeile Ihrer E-Mail das Wort „Serbien“ an.

- Name: Karanovic & Partners o.a.d. Beograd
- Adresse: Resavska 23, Belgrad, 11000, Serbien
- Telefonnummer: +381 11 3094 200
- E-Mail: local.representative@karanovicpartners.com

Singapur

Wenn Sie auf „Annehmen“ klicken, stimmen Sie zu, dass Ihre Daten an Datenbanken oder Partner oder Drittanbieter im Ausland weitergegeben werden dürfen, insbesondere nach Bulgarien, Irland, Singapur, Schweden und in die USA.

Zugriff

Sie haben das Recht, auf Ihre personenbezogenen Daten zuzugreifen sowie auf Informationen darüber, wie wir sie verwenden und mit wem wir sie teilen. Der Zugriff auf die von Ihnen über Ihr Konto bereitgestellten personenbezogenen Daten ist per Anmeldung bei Ihrem Konto möglich. Wenn Sie der Meinung sind, dass wir noch andere personenbezogene Daten über Sie gespeichert haben, kontaktieren Sie uns unter Privacy@sharkmob.com.

Korrektur

Sie haben das Recht auf Korrektur fehlerhafter personenbezogener Daten über Sie. Der Zugriff auf Ihre von uns

gespeicherten personenbezogenen Daten ist per Anmeldung bei Ihrem Konto möglich. Wenn Sie der Meinung sind, dass wir noch andere personenbezogene Daten über Sie gespeichert haben und diese Daten fehlerhaft sind, kontaktieren Sie uns unter Privacy@sharkmob.com.

Unser Datenschutzbeauftragter zur Einhaltung des Gesetzes zum Schutz personenbezogener Daten von 2012 ist erreichbar unter Privacy@sharkmob.com.

Südafrika

Sie können beim Datenschutzbeauftragen (Südafrika) per E-Mail an inforeg@justice.gov.za Beschwerde einreichen. Die physische Adresse des Datenschutzbeauftragten (Südafrika) ist 33 Hoofd Street Forum III, 3rd Floor Braampark, Braamfontein, Johannesburg, Südafrika.

Sri Lanka

Wenn Sie auf „Annehmen" klicken, stimmen Sie den Geschäftsbedingungen der Datenschutzrichtlinie zu und gestatten die Erfassung, Nutzung und Offenlegung Ihrer personenbezogenen Daten. Solltest du allerdings unter 18 Jahre alt sein, verbürgst du, dass du das Einverständnis eines Erziehungsberechtigten zur Registrierung eines Kontos und zur Nutzung von Bloodhunt eingeholt hast.

Sollten Sie Ihre Zustimmung widerrufen oder der weiteren Verarbeitung Ihrer Daten widersprechen oder Ihre personenbezogenen Daten löschen, korrigieren oder vervollständigen wollen, beantworten wir Ihre Anfrage innerhalb von 21 Werktagen.

Personalisiertes Marketing

Wenn Sie auf „Annehmen" klicken, erklären Sie sich damit einverstanden, personalisierte Werbung angezeigt zu bekommen. Sie können den Erhalt personalisierter Werbung von uns unterbinden, indem Sie die im Bereich „Einstellungen" von Bloodhunt aufgeführten Anweisungen befolgen oder uns unter Privacy@sharkmob.com kontaktieren.

Taiwan

Wir erfassen oder erbitten wissentlich keine personenbezogenen Daten von Personen unter 7 Jahren oder gestatten diesen Personen wissentlich die Registrierung für Bloodhunt. Wenn du unter 7 Jahre alt bist, versuche bitte nicht, Bloodhunt zu nutzen oder dich dort zu registrieren und schicke uns auch keine personenbezogenen Daten über dich. Keine Person unter 7 Jahren darf uns während der Nutzung von Bloodhunt personenbezogene Daten zukommen lassen. Für Nutzer in Taiwan gilt, dass Personen unter 20 Jahren vor der Nutzung von Bloodhunt das Einverständnis eines Erziehungsberechtigten einholen müssen.

Thailand

Wenn Sie auf „Annehmen" klicken, erklären Sie, dass Sie diese Datenschutzrichtlinie gelesen und verstanden haben und ihr zustimmen. Wenn Sie dieser Datenschutzrichtlinie nicht zustimmen, dürfen Sie Bloodhunt nicht nutzen.

Sie können uns darum bitten, die Nutzung oder Bereitstellung von Teilen oder Ihrer gesamten personenbezogenen Daten auszusetzen oder zu beschränken und/oder die Datenübertragbarkeit der von uns gespeicherten Daten entsprechend der geltenden Datenschutzgesetze und -bestimmungen in Thailand, wie dem thailändischen Gesetz zum Schutz personenbezogener Daten, beantragen. Wenn Sie einen solchen Antrag stellen möchten, kontaktieren Sie uns bitte unter Privacy@sharkmob.com.

Wir benachrichtigen Sie per E-Mail über jegliche wesentliche Veränderungen an dieser Datenschutzrichtlinie und geben Ihnen die Gelegenheit, diese Änderungen abzulehnen, andernfalls werden die Änderungen wie in der Mitteilung angegeben wirksam.

Türkei

Unser Datenverantwortlicher in der Türkei zur Einhaltung des türkischen Gesetzes zum Schutz personenbezogener Daten („TGSPD“) und dessen Nebenbestimmungen ist Özdağıstanli Ekici Avukatlık Ortaklığı, der unter localdatarep_sharkmob@iptech-legal.com erreichbar ist. Bitte geben Sie in der Betreffzeile Ihrer E-Mail das Wort „Türkei“ an.

Sie sind im Besitz des in Artikel 11 des TGSPD ausgeführten gesetzlich festgelegten Rechts bezüglich der von uns gespeicherten personenbezogenen Daten über Sie. Als türkische betroffene Person können Sie das Recht haben, sich an den Datenverantwortlichen zu wenden und (entsprechend der geltenden Gesetze und Bestimmungen)

- zu erfahren, ob Ihre personenbezogenen Daten verarbeitet wurden.
- Informationen über deren Verarbeitung anzufordern.
- den Verarbeitungszweck Ihrer personenbezogenen Daten zu erfahren.
- über die in- oder ausländischen Drittanbieter informiert zu werden, an die personenbezogene Daten weitergegeben wurden.
- im Falle fehlerhafter oder unvollständiger personenbezogener Daten deren Korrektur zu beantragen.
- im Rahmen der in Artikel 7 des TGSPD beschriebenen Bedingungen die Löschung oder Vernichtung personenbezogener Daten zu beantragen.
- Widerspruch gegen bestimmte Datenverarbeitungsarten und entsprechend des TGSPD bestimmte Rechtsmittel einzulegen.

Ukraine

Durch Annahme dieser Datenschutzrichtlinie bestätigen Sie ausdrücklich, dass Sie uns dazu ermächtigen, personenbezogene Informationen von Ihnen in dem von dieser Datenschutzrichtlinie dargelegten Maße zu sammeln, zu verwenden, zu speichern und zu verarbeiten, einschließlich der Weitergabe an Dritte außerhalb der Ukraine.

Vereinigte Arabische Emirate

Sie stimmen der Erfassung, Nutzung, Offenlegung, Weitergabe, dem Export (entsprechend der geltenden Gesetze) sowie der Speicherung Ihrer personenbezogenen Daten entsprechend dieser Datenschutzrichtlinie zu.

Wir können freiwillig einen Cybersicherheitsvorfall melden, sofern er entsprechend der Gesetze der VAE eine Straftat darstellt (d. h. entsprechend des Gesetzes zur Cyberkriminalität der VAE). Der Vorfall kann den zuständigen Behörden zur Strafermittlung gemeldet werden. Bitte beachten Sie, dass die freiwillige Meldung von Cybersicherheitsvorfällen auch an das Computernotfallteam der VAE („**CNT**“) gemeldet werden kann. Das CNT ist eine Sicherheitsorganisation, die Vorfälle nachverfolgt und über bekannte Cybersicherheitsbedrohungen in den VAE informiert.

Vietnam

Durch Annahme dieser Datenschutzrichtlinie bestätigen Sie ausdrücklich, dass Sie uns dazu ermächtigen, personenbezogene Informationen von Ihnen in dem von dieser Datenschutzrichtlinie vorgesehenen Maße zu sammeln, zu verwenden, zu speichern und zu verarbeiten, einschließlich der Weitergabe an Dritte entsprechend dieser Datenschutzrichtlinie.

Wir halten internationale Standards und Sicherheitsmaßnahmen zum Datenschutz ein. Wenn Ihre personenbezogenen Daten innerhalb oder außerhalb der Gerichtsbarkeit ihres Wohnorts weitergegeben werden, gelten beim Empfänger die gleichen oder sogar höhere Sicherheitsstandards für Sie.

Wenn wir Dritten die Erfassung und Nutzung Ihrer personenbezogenen Daten gestatten, ergreifen wir angemessene Maßnahmen, um sicherzustellen, dass diese Dritten die personenbezogenen Daten nicht weiter offenlegen.

Sollten Ihre personenbezogenen Daten den Strafermittlungsbehörden, staatlichen Behörden oder anderen juristischen Körperschaften und Organisationen offengelegt werden müssen, erfolgt dies nur auf schriftlichen Antrag solcher Organisationen.

Ihre Rechte

Sie haben das Recht, auf Ihre von uns gespeicherten personenbezogenen Daten zuzugreifen, sie zu korrigieren und sie zu löschen. Des Weiteren haben Sie das Recht, Ihre zuvor erteilte Zustimmung zur Erfassung, Speicherung, Nutzung und Offenlegung Ihrer personenbezogenen Daten zu widerrufen und die Unterbindung der Weitergabe Ihrer personenbezogenen Daten an Dritte zu beantragen.