

Privacy Notice for Managers and Team Members

Last updated [May.03.2026]

INTRODUCTION

Thank you for choosing to be part of our community at Kampfire, operated by Obrecsys LLC. ("Kampfire", "We", "Us", or "Our"). We are committed to protecting your Personal Information and your right to privacy.

When this privacy notice uses the term "Managers" We refer to event managers or campaign managers using the Services, as defined below, to create events or marketing campaigns for their audience ("Audience") or for Managers' service providers, such as hosts, co-hosts, co-managers ("Team Members"), or for any other reason. Managers and third parties using Our Services are all referred to in these Terms collectively as "you" or "your".

WE PROCESS AUDIENCE INFORMATION ON YOUR BEHALF AND UNDER YOUR INSTRUCTIONS, IN ACCORDANCE WITH OUR DATA PROCESSING AGREEMENT.

"Audience Information" means personal information that we collect, process, and manage on your behalf, or directly from Audience, as part of rendering Our Services through Our Platforms.

This privacy notice applies to all information collected through Our platforms, and/or any related services, sales, marketing or campaigns (We refer to them collectively in this privacy notice as the "Platforms" or "Services").

We take your privacy very seriously, in this privacy notice, We seek to explain to you in the clearest way possible what information We collect, how We use it and what rights you have in relation to it.

Please read this privacy notice carefully as it will help you make informed decisions about sharing your Personal Information and your Audience Information with Us.

If there are any terms in this privacy notice that you do not agree with, please discontinue use of Our Platforms and Our Services.

WHAT INFORMATION DO WE COLLECT?

When We talk about "Personal Information" in this privacy notice, We mean all of the information collected by Us as detailed below, as long as this information is by itself or with other data or information, We possess identify you or any other individual.

Specifically, We collect the following information by the following means:

***Personal Information you disclose to Us: ***

The Short Story: We collect Personal Information that you provide to Us such as name, email address, your Audience Information, location data, contact information, including country of residence, payment information, and login credentials provided by Google or Apple when you use them to login to our Platforms.

We collect Personal Information that you voluntarily provide to Us:

- When you are registering at the Platforms as "Managers" or "Team Members";

- When you interact with Our customer support;
- When you fill out or upload texts, images, videos, logos, ads, CTAs, forms in our templates;
- When you upload photos to the Platforms;
- When you share photos through the Platforms with Us, your Audience or other users;
- When you share with Us text, files and documents;
- When you submit a request to exercise a right identified in this policy, in order to fulfill your request, We may collect your email address, contact information, photo, or an image of your government-issued ID.

Personal Information you disclose to Us includes the following:

Credentials and Account Data. When you create an account or interact with Our Platforms, We may collect your first and last name, title, email address, postal address, phone number, company name, and other similar contact data, passwords, password hints, and similar security information used for authentication and account access and general accesses to Our Services and Platforms.

Payment Data. We collect data necessary to process your payment if you make any purchases through Our Platforms, such as the last 4 digits of your payment instrument number (such as a credit card number), and billing address. Other than that, all other payment data is collected, processed and stored by Our payment processor Stripe, and is governed by their privacy policies found here: <https://stripe.com/privacy>

Audience Information that We collect on your behalf, includes the following:

Photos, Text, Files and Documents you share with Us to be processed for the provisions of Our Services. Some of this information is collected for Our own purposes to improve Our Platforms and to deliver a better and more personalized experience, as further detailed below.

Please note that when your Audience interacts directly with our Platforms we will collect Personal Information directly from them such as selfies, name, and email address – such processing is governed by our Audience Privacy Policy.

Biometric data and other metadata information derived from photos: As part of Our normal business operations, We process photos of Audience members through Our Services. Such photos are uploaded to Our Platform by Managers, Team Members, or on their behalf. From these photos, We may derive limited biometric data consisting of a digital representation of facial features solely for the purpose of matching Audience members to photos in which they appear, as initiated by the Audience or the event organizer.

We do not perform biometric identification of individuals against external databases, nor do We conduct behavioral analysis, profiling, or automated decision-making based on such data.

Biometric templates are processed solely within Kampfire's controlled environment and are not used to infer personal characteristics, emotions, intent, or behavior.

All Personal Information that you provide to Us must be true, complete and accurate, and you must notify Us of any changes to such Personal Information.

You also represent and warrant to Us that you have the full right and authority and received all necessary consents and approvals (in such cases where such consent and approvals are required) from your Audience to share with Us Audience Information or any other Personal Information.

You undertake to include in the RSVP and entry to the event a disclaimer informing the Audience that they are being photographed and that the Audience's Personal Information, including their photos may be used for the purposes outlined in this Privacy Policy.

For your convenience, see below proposed disclaimers.

For EU event managers:

"Please note that photography and video recording may take place at this event.

Participation in this experience is voluntary. If you choose to participate, your photo may be processed using automated facial-feature matching technology solely to match you with event photos and videos in which you appear.

This processing does not involve biometric identification against external databases, behavioral analysis, profiling, or automated decision-making.

You may choose not to participate or withdraw your consent at any time, without affecting your ability to attend the event. Additional information is available in the event's privacy notice."

For U.S event managers:

"Photography and video recording may occur at this event.

This event may offer an optional photo-matching service that allows attendees to receive photos in which they appear.

If you choose to participate, your image may be processed using automated facial-feature matching technology solely to group photos of you from the event. This technology is not used for identity verification, behavioral analysis, or profiling.

Participation is voluntary and subject to the event's privacy notice. You may decline participation without impacting your ability to attend the event."

Important note for Illinois: For IL events, you should add a separate written consent checkbox or flow — a disclaimer alone is not enough.

You are fully responsible for ensuring that each member of your Audience has given his consent to the use and processing of his/her Personal Information by Us.

We do not control the registration and onboarding process of your Audience, nor the Personal Information that you or your Team Members collect.

In addition, other third parties that are involved on your behalf with regard to an event or marketing campaign or any other activity may receive Audience Information as well. In that case, We may provide Audience Information to such third parties as per your specific instructions and on your behalf.

All processing of such Audience Personal Information shall be done according to your instructions and a signed data processing agreement, and evidently, We are not responsible for any actions of you, your Team Members (or other downstream recipients of Audience Information), with respect to the Audience Information.

Information automatically collected:

The Short Story: Some information – such as IP address and/or browser and device characteristics – are collected automatically when you log into Our Platforms and use Our Services. This information is primarily needed to maintain the security and operation of Our Platforms, the provisions of Our Services and for Our internal analytics and reporting purposes.

Personal Information We automatically collect does not reveal your specific identity (like your name or contact information) but may include the following:

- Device and usage activity, such as your IP address, browser and device characteristics, mobile network information (including, internet browsing speed), and login history;
- Country, location, information about how and when you use Our Platforms and other technical information.
- The Platforms also may access metadata and other information associated with other files stored on your device. This may include, for example, photographs, and video clips.

Information collected from other Sources:

The Short Story: We may collect limited data from public databases, marketing partners, social media platforms, and other outside sources.

We may obtain information about you from other sources, such as public databases, joint marketing partners, social media platforms (such as Facebook, Instagram, Google, Twitter and LinkedIn), as well as from other third parties.

Examples of the information We receive from other sources include:

Your name, gender, birthday, email, current city, state and country, user identification numbers for your contacts, profile picture URL and any other information that you choose to make public.

HOW DO WE USE YOUR INFORMATION AND INFORMATION WE COLLECT ON YOUR BEHALF?

We use information that We collect about you or that you provide to Us or We collect on behalf of you (for example, Audience Information), including any Personal Information such as your first and last name, your images and photos, your Audience images and photos, email address, postal address, phone number, company name, and other similar contact data, to:

- Provide you with the access to the Platforms, its content and Our Services, and any other information, products or services that you request from Us.
- Pair Audience Information with the biometric data and other metadata information derived from photos, as part of Our core Services.
- Identify your Audience in photos taken on events or for marketing campaigns and which are uploaded to Our Services, using facial recognition software, which is provided by AWS, in order to create grouped personalized albums.

Facial recognition is used by Us to analyze photos uploaded to the Platforms and to identify if a user appears in any of such uploaded photos. The Managers, then have the option to group such photos and send to Audience the specific photos in which they appear.

The facial recognition is governed by AWS's privacy policy.

- Fulfill any other purpose for which you provided it.
- If you create an account, register to Our newsletter or otherwise approve communications with us, to give you notices about your account, including expiration and renewal notices.
- Carry out Our obligations and enforce Our rights arising from any contracts entered into between you and us, including for billing and collection.
- Notify you when Our Platforms are available, and of changes to any products or services We offer or provide through it.
- Request feedback and to contact you about your use of Our Platforms and Services.
- Keep Our Platforms, you and the Audience safe and secure (for example, for fraud monitoring and prevention).

The usage information We collect helps Us to improve Our Platforms and to deliver a better and more personalized experience by enabling Us to:

- Estimate Our users' size and usage patterns.
- Store information about your preferences, allowing Us to customize Our Platforms according to your individual interests.
- Speed up your searches.
- Recognize you and the Audience when using the Platforms.

****LEGAL BASIS FOR PROCESSING PERSONAL INFORMATION (FOR RESIDENTS OF THE EEA OR UK ONLY) ****

The basis for collecting and utilizing your Personal Information will depend on the specific information and the context in which we obtain it. Generally, we will collect your Personal Information only if you consent to it, if it is necessary to fulfill a contractual obligation with you, or if the processing aligns with our legitimate interests without infringing on your data protection rights and fundamental freedoms. In some instances, We may also have a legal obligation to collect certain Personal Information from you.

If We request you to provide Personal Information to comply with a legal requirement or to perform a contract with you, we will clearly communicate this at the appropriate time and inform you whether providing the information is mandatory or optional (and the potential consequences of not providing it). Similarly, if we collect and use your Personal Information based on our legitimate interests (or those of any third party), we will transparently explain those legitimate interests to you at the relevant time.

HOW WE SHARE YOUR INFORMATION?

The short story: *We only share information with your consent, to comply with laws, to protect your rights, or to fulfill Our contract and legal obligation to you or other business obligations.*

We only share and disclose your information in the following situations:

- **With your Consent.** We may disclose your Personal Information for any other purpose with your consent.
- **Compliance with Laws.** We may disclose your information where We are legally required to do so in order to comply with applicable law, governmental requests, a judicial proceeding, court order, or legal process, such as in response to a court order or a subpoena (including in response to public authorities to meet national security or law enforcement requirements).
- **Vital Interests and Legal Rights.** We may disclose your information where We believe it is necessary to investigate, prevent, or take action regarding potential violations of Our policies, suspected fraud, situations involving potential threats to the safety of any person and illegal activities, or as evidence in litigation in which We are involved.
- **Affiliates.** We may share your information with Our affiliates, in which case We will require those affiliates to honor this privacy notice. Affiliates include Our parent company and any subsidiaries, joint venture partners or other companies that We control or that are under common control with us.
- **Business Partners, Vendors, Consultants and Other Third-Party Service Providers.** We may share your data with third party vendors, service providers, contractors or agents who perform services for Us or on Our behalf and require access to such information to do that work. Examples include: payment processing, data analysis, email delivery, hosting services, customer service and marketing efforts. We may allow selected third parties to use tracking technology on the Platforms, which will enable them to collect data about how you interact with the Platforms over time. These service providers may have access to your Personal Information, depending on each of their specific roles and purposes, and may only use it for such limited purposes as determined in Our agreements with them.
For a copy of Our current list of affiliates, business partners, vendors, consultants and Other Third-Party service providers, please contact Us at contact@kampfire.events.
- **Business Transfers.** We may share or transfer your information in connection with, or during negotiations of, any merger, sale of company assets, financing, or acquisition of all or a portion of Our business to another company.
- Kampfire's use and transfer of information received from Google APIs to any other app will adhere to [Google API Services user Data Policy](#), including the Limited Use requirements.

INTERNATIONAL TRANSFERS

Our servers and cloud provider AWS, located in the USA. Please be aware that your information may be transferred to, stored, and processed by us in Our facilities and by those third parties with whom we may share your Personal Information in the USA.

If you are a resident of the European Economic Area, please be advised that all transfers to the USA are based on the European Commission's Standard Contractual Clauses.

European Commission's Standard Contractual Clauses - The European Commission has determined that the Standard Contractual Clauses provide sufficient safeguards to protect the personal data transferred outside the EU or EEA.

For more information, please visit at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

All such transfers based on Standard Contractual Clauses require all such recipients to protect the Personal Information that they process from the EEA in accordance with European data protection laws.

If you are a resident of the United Kingdom, we rely on the UK Addendum to the Standard Contractual Clauses (approved by the UK authorities).

For all such transfers based on Standard Contractual Clauses or the UK Addendum to the Standard Contractual Clauses, We also whenever necessary, have implemented similar appropriate safeguards with Our third-party service providers and partners. These safeguards may include commercially accepted, industry-standard secure encryption methods to protect customer data both at rest and during transmission, web application firewall protection, and other suitable contractual and organizational measures.

AD NETWORKS AND DO NOT TRACK

Due to lack of standardization, currently, Our systems do not recognize browser “do-not-track” requests.

THIRD-PARTY WEBSITES AND CONTENT

The Short Story: We are not responsible for the safety of any information that you share with third-party providers who advertise, but are not affiliated with, Our Platforms.

The Platforms may contain advertisements from third parties that are not affiliated with Us and which may link to other websites, online services or mobile applications. We cannot guarantee the safety and privacy of data you provide to any third parties. Any data collected by third parties is not covered by this privacy notice. We are not responsible for the content or privacy and security practices and policies of any third parties, including other websites, services or applications that may be linked to or from the Platforms. You should review the policies of such third parties and contact them directly to respond to your questions.

HOW LONG DO WE KEEP YOUR INFORMATION?

The Short Story: We keep your information for as long as necessary to fulfill the purposes outlined in this privacy notice unless otherwise required by law.

We will only keep your Personal Information for as long as it is necessary for the purposes set out in this *privacy notice*, unless a longer retention period is required or permitted by law (such as tax, accounting or other legal requirements).

Specific retention periods for photos and biometric data. Photos, selfies, derived metadata and biometric templates associated with an event are retained for the period You configure for that event, subject to a maximum of three (3) years from the date the event was created in Our Platforms. You may set a shorter retention period at any time. Following deletion (whether by automatic expiration, your action, or an Audience erasure request), residual copies may persist in encrypted backups for up to thirty-five (35) days before being permanently destroyed.

Affiliate and coupon records. Where You participated in Our affiliate or coupon programs, We may retain encrypted, pseudonymized records of those transactions for up to seven (7) years following deletion of Your account, solely for tax, accounting, audit, fraud-prevention and other legal-compliance purposes.

When We have no ongoing legitimate business need to process your Personal Information, We will either delete or anonymize it, or, if this is not possible (for example, because your Personal Information has been stored in backup archives), then We will securely store your Personal Information and isolate it from any further processing until deletion is possible.

KEEPING YOUR INFORMATION SAFE

The Short Story: *We aim to protect your Personal Information through a system of organizational and technical security measures.*

We have implemented measures designed to secure your Personal Information from accidental loss and from unauthorized access, use, alteration, and disclosure. All information you provide to Us is stored on Our secure servers according to industry standards.

Unfortunately, the transmission of information via the Internet is not completely secure. Although We do Our best to protect your Personal Information, We cannot guarantee the security of your Personal Information transmitted to Our Platforms. Any transmission of Personal Information is at your own risk. We are not responsible for the circumvention of any privacy settings or security measures contained on the Platforms.

YOUR PRIVACY RIGHTS AND HOW TO EXERCISE THEM?

The Short Story: *In some regions, you have rights that allow you greater access to and control over Your Personal Information. You may review, change, or terminate your account at any time.*

Subscription and Account Information

You may at any time review, unsubscribe from Our mailing list, change the information in your account or terminate your account by:

- Logging into your account settings and updating your account.

- Adjusting your device or Platforms permissions.
- Contacting Us using the contact information provided below.

Upon your request to unsubscribe or terminate your account, We will deactivate or delete your account and information from Our active databases. However, some information may be retained in our files to prevent fraud, troubleshoot problems, assist with any investigations, enforce Our Terms And Conditions and/or comply with legal requirements.

Manager controls over Audience data. From within Our Platforms You may, at any time and on Your own initiative, (i) set or change the deletion date for any event You manage, up to the three (3) year maximum, (ii) erase the Personal Information of an individual Audience member ("forget guest"), or (iii) erase the Personal Information of all Audience members of an event ("forget all guests"). Once actioned, the affected data is removed from active systems immediately; residual copies in encrypted backups are permanently destroyed within thirty-five (35) days. Limited anonymous engagement statistics, with all identifiers removed, may be retained for Your analytical use.

Opting Out - If you do not want Us to collect your information do not use the Platforms or delete it from your device and do not use Our Services. In addition, you may opt-out at any time by contacting Us at contact@kampfire.events.

Children Under the Age of 16

The Services are not intended for children under 16 years of age, and We do not knowingly collect Personal Information from children under 16. If We learn We have collected or received Personal Information from a child under 16 without verification of parental consent, We will delete that information. If you believe We might have any information from or about a child under 16, please contact Us at contact@kampfire.events. California residents under 16 years of age may have additional rights regarding the collection and sale of their Personal Information. Please see Your California Privacy Rights below for more information.

Use of Artificial Intelligence Systems — Notice Under Regulation (EU) 2024/1689 ("EU AI Act")

This section applies where the AI systems described below operate on natural persons located in the European Union, including where Audience members of Your events are located in the European Union. It supplements the rest of this Privacy Notice and is provided in fulfilment of Our transparency obligations, and to support Yours, under Article 50 of the EU AI Act.

1. AI system in operation. When You enable photo-matching for an event, an AI system performs automated facial-feature matching, comparing the digital template derived from each participating Audience member's selfie with face crops detected in the event photos and videos uploaded to Our Platforms. This system is a "biometric categorisation system" within the meaning of Article 3 of the EU AI Act, deployed for the sole purpose of grouping with each participating Audience member the photos and videos in which they appear.

2. Provider of the AI system. The underlying facial-feature matching is performed using **Amazon Rekognition**, provided by Amazon Web Services, Inc. ("AWS"), acting as Kampfire's service provider under contractual confidentiality and processing-restriction obligations. Kampfire configures and deploys this system within Our Platforms.

3. Scope and limits. The system performs comparison of biometric templates **only within the photo set of the specific event(s) for which photo-matching has been enabled**. It does not identify Audience members against external databases, does not assign categories based on protected characteristics (such categorisation would be prohibited under Article 5(1)(g) of the EU AI Act), and does not perform behavioural analysis, profiling, automated decision-making within the meaning of Article 22 GDPR, or emotion recognition. Kampfire does not engage in any of the practices prohibited by Article 5 of the EU AI Act, including untargeted scraping of facial images.

4. Your role and joint responsibility. Where You enable photo-matching for an event with Audience members located in the European Union, You participate in deploying an AI system within the meaning of the EU AI Act. You acknowledge and agree that:

- You shall not represent to Audience members that the system performs functions other than those described in paragraph 3;
- You shall ensure that **explicit consent** under Article 9(2)(a) of the GDPR is obtained from each participating Audience member before biometric processing begins, including via Our consent flows where provided;
- You shall not configure events in any way that would cause Kampfire's AI system to engage in practices prohibited by Article 5 of the EU AI Act;
- You shall promptly action Audience erasure or consent-withdrawal requests through the in-product "forget guest" / "forget all guests" tooling;
- You shall flow down the substance of paragraphs 1–3 of this notice (including by referring Audience members to the corresponding Audience-facing notice at https://docs.kampfire.events/Pr_No_Au.pdf) at the latest at the time of an Audience member's first interaction or exposure to the AI system.

5. Audience-facing transparency. The substantive notice required by Article 50(3) for natural persons exposed to the system is provided to Audience members in the Privacy Notice for Audience and other participants at https://docs.kampfire.events/Pr_No_Au.pdf.

6. Contact. For questions regarding the use of AI systems within Our Services, contact contact@kampfire.events.

Rights of The European Economic Area Residents

If you are a resident of the European Economic Area, according to the General Data Protection Regulation (**GDPR**) provides you have the following rights:

- The right to access – access and receive confirmation of the existence of your Personal Information, access its content and obtain a copy.
- The right to rectification – to update, rectify and/or correct your Personal Information.
- The right to erasure and the right to be forgotten - to request the erasure of your data. where We have made your Personal Information public, you have also the right to request the erasure of your Personal Information and to take reasonable steps, including technical measures, to inform other data controllers

which are processing the Personal Information that you have requested the erasure by such controllers of any links to, or copy or replication of, those Personal Information.

- The right to restriction – to request to restrict your data that has been processed in violation of the law, including whose storage is not necessary for the purposes for which the data was collected or otherwise processed.
- Right to data portability - to receive a copy of your Personal Information you provided to Us for a contract or with your consent in a structured, commonly used and machine-readable format, and to ask Us to transfer that Personal Information to another data controller.
- Right to Object – you have the right to object to the processing of your Personal Information. To make such a request, please use the contact details provided below. We will consider and act upon any request in accordance with applicable data protection laws.
- Right to withdraw your consent - If We are relying on your consent to process your Personal Information, you have the right to withdraw your consent at any time. Please note however that this will not affect the lawfulness of the processing before its withdrawal.

If you believe we are unlawfully processing your Personal Information, or you believe that your data protection rights have been violated, you also have the right to complain to your local data protection supervisory authority. You can find their contact details here:

http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm

Data Controller/Processor and Data Processing Agreements

The short story: *We are the controller of some of your Personal Information; we are the processor of any Personal Information processed on your behalf.*

In some incidents We may be the “Data Controller” of Personal Information not specifically excluded above. In such instances, Our service providers processing such data will assume the role of “Data Processor”.

If you upload or submit information / data or other content to our Platforms or through Our Services and products which include Personal Information, such data will only be processed by Us on behalf of you. In such instances, you shall be deemed the “Data Controller” of such data or information, and We will process such information on your behalf, as your “Data Processor”, in accordance with your reasonable instructions, Our data processing agreement with such customer (to the extent applicable) and other commercial agreements. Our service providers shall act as designated Sub-Processors in these instances.

You will be responsible for meeting any legal requirements applicable to Data Controllers (such as establishing a legal basis for processing and responding to Data Subject Rights requests concerning the data they control).

For more information see https://docs.kampfire.events/Dp_Ma.pdf.

Rights of California Residents

If you are a California resident, California law may provide you with additional rights regarding Our use of your Personal Information. To learn more about your California privacy rights, please visit at https://docs.kampfire.events/ccpa_cpma_Ma.pdf^{**}.

Rights of Nevada Residents

As a Nevada resident you have the right to request to opt-out of the sale of your Personal Information, by contacting Us please contact Us using the contact information provided below and include the email address associated with your account and a statement that you reside in Nevada.

Rights of Illinois Residents — Notice Under the Biometric Information Privacy Act ("BIPA")

If you are a resident of Illinois, the Illinois Biometric Information Privacy Act, 740 ILCS 14 ("**BIPA**"), applies to certain information processed about you through Our Platforms. This section is Kampfire's publicly-available written policy under BIPA Section 15(a) and supplements the rest of this Privacy Notice.

1. Information covered. This section covers "biometric identifiers" and "biometric information" as defined in BIPA — namely, the digital templates derived from selfies, photos and videos uploaded to Our Platforms and used to identify the photos and videos in which an individual appears.

2. Specific purpose and length of term (BIPA §15(b)(1)–(2)). Such biometric data is collected, stored and used for one purpose only: to match Audience members with the photos and videos taken at events they attended, and to deliver to them a personalized photo collection. The data is retained only for as long as that purpose is being served, subject to the destruction schedule in paragraph 4 below.

3. Written release / opt-in (BIPA §15(b)(3)). Kampfire does not collect, capture, purchase, receive through trade, or otherwise obtain biometric identifiers or biometric information from Illinois residents without the written notice in paragraphs 1 and 2 above and the individual's affirmative written release. As a Manager or Team Member, You shall not enable photo-matching for any Audience member who is an Illinois resident and has not provided such a release through Our Platforms.

4. Retention schedule and destruction guidelines (BIPA §15(a)). Biometric identifiers and biometric information are permanently destroyed at the **earliest** of the following events:

- (a) When the initial purpose for which they were collected has been satisfied — namely, when the relevant event has concluded and the Audience member has received (or has ceased to access) the personalized photo collection;
- (b) Three (3) years after the individual's last interaction with Kampfire's Platforms; or
- (c) Promptly following the individual's erasure request submitted via the in-product "Forget Me" tooling, or the Manager's request submitted via the "forget guest" / "forget all guests" tooling, or by writing to contact@kampfire.events.

Destruction is effected immediately in Our active systems. Residual copies in encrypted backups are permanently destroyed within thirty-five (35) days. Kampfire does not retain Illinois biometric identifiers or biometric information beyond the foregoing schedule absent a valid warrant or subpoena issued by a court of competent jurisdiction.

5. No sale or profit (BIPA §15(c)). Kampfire does not sell, lease, trade, or otherwise profit from biometric identifiers or biometric information, and You shall not direct or permit Kampfire to do so.

6. Disclosure restrictions (BIPA §15(d)). Kampfire does not disclose, redisclose, or otherwise disseminate biometric identifiers or biometric information unless: (i) the individual consents to the disclosure; (ii) the disclosure completes a financial transaction the individual requested or authorized; (iii) the disclosure is required by federal, state, or municipal law; or (iv) the disclosure is required pursuant to a valid warrant or subpoena. Facial-feature matching is performed using AWS Rekognition acting solely as Kampfire's service provider, under contractual confidentiality and processing-restriction obligations.

7. Standard of care (BIPA §15(e)). Kampfire stores, transmits and protects biometric identifiers and biometric information using a reasonable standard of care within Our industry, and in a manner that is the same as or more protective than the manner in which Kampfire stores, transmits and protects other confidential and sensitive information.

8. Your responsibilities as a Manager regarding Illinois Audience. You acknowledge and agree that, in addition to Your obligations under the Terms and Conditions for Managers and applicable Data Processing Agreement, You shall: (i) not represent to Illinois Audience members that biometric data will be retained beyond the schedule in paragraph 4; (ii) promptly action erasure requests received from Illinois Audience members through the in-product "forget guest" tooling or otherwise; and (iii) refrain from any conduct prohibited by BIPA §§15(c), 15(d) or 25.

9. Exercising BIPA rights. Illinois individuals may at any time request information about the categories of biometric data held about them, request its destruction, or revoke their release, by emailing contact@kampfire.events or by using the in-product "Forget Me" tooling within the guest panel. Complaints may also be directed to the Illinois Attorney General.

Rights of Virginia, Colorado and Connecticut Residents

As a resident of Virginia, Colorado or Connecticut you have the following rights:

- The right to request information about Personal Information that We have collected about you in the 12 months preceding the yours request (including the categories of information collected, the source of that information, the business purpose of that collection, the categories of third parties with whom that information is shared, and the specific pieces of Personal Information collected about that particular customer);
- The right to receive requested information in a readily-usable format if provided electronically;
- The right to request that We delete any Personal Information about you that We have collected (although We may be entitled to retain some information for certain purposes);

- The right to opt-out of "sales" of Personal Information to third parties, the sharing of Personal Information with third parties for targeted advertising purposes, and/or the processing of Personal Information for targeted advertising purposes;
- The right to update or correct any Personal Information which is out of date or incorrect; and
- The right to be free from discrimination based on your exercise of your privacy rights.

To exercise your rights as a resident of Virginia, Colorado or Connecticut, please email Us at contact@kampfire.events

Rights of South African Residents — Notice Under the Protection of Personal Information Act, 4 of 2013 ("POPIA")

If you are a resident of the Republic of South Africa, the Protection of Personal Information Act, 4 of 2013 ("POPIA") applies to Our processing of your Personal Information. This section supplements the rest of this Privacy Notice and, in respect of South African data subjects, controls in case of conflict.

1. Responsible Party. The "Responsible Party" within the meaning of POPIA is Obrecsys LLC. (operating as "Kampfire"), at the postal address set out at the end of this Notice.

2. Information Officer. Our Information Officer can be contacted at contact@kampfire.events.

3. Special Personal Information (POPIA §26 and §27). "Biometric information" is "special personal information" within the meaning of POPIA §26. Where Audience biometric information is processed through Our Platforms, processing is carried out only on the basis of the **explicit consent** of the data subject under POPIA §27(1)(a), given freely, specifically and on an informed basis when the Audience member chooses to participate in Our optional photo-matching experience. As a Manager, You are jointly responsible for ensuring that such consent is obtained before You enable photo-matching for any South African Audience member.

4. Purpose specification and minimality (POPIA §10 and §13). We collect and process the minimum Personal Information necessary to deliver to Audience members a personalized photo collection from events they attended, and We do not further process Personal Information in a manner incompatible with that purpose.

5. Retention and destruction (POPIA §14). We do not retain records of Personal Information longer than is necessary to achieve the purpose for which it was collected, except where (i) retention is required or authorised by law, (ii) retention is required by Our contract with the relevant party, or (iii) the data subject has consented to longer retention. Photos, videos, derived metadata and biometric templates are subject to the maximum 3-year per-event retention cap and 35-day backup-purge window described in the section "How Long Do We Keep Your Information?" above. Once We are no longer authorised to retain a record, We destroy or de-identify it in a manner that prevents its reconstruction in an intelligible form.

6. Data subject rights (POPIA §23–25). South African data subjects have the right to:

- Confirm, free of charge, whether We hold Personal Information about them, and to access a copy;
- Request that We correct, destroy or delete Personal Information that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or unlawfully obtained;
- Object, on reasonable grounds, to the processing of their Personal Information;
- Object to processing for direct marketing purposes (We will not process Personal Information for direct marketing without consent);
- Withdraw consent at any time, where We rely on consent.

These rights may be exercised via the in-product "Forget Me" tooling for erasure, or by emailing contact@kampfire.events. The Form 1 / Form 2 procedures under the POPIA Regulations apply to formal requests.

7. Children (POPIA §35). For South African data subjects, "children" means persons under the age of 18 years. Neither Kampfire nor any Manager may knowingly process the Personal Information of South African children without the prior consent of a competent person (parent or legal guardian).

8. Cross-border transfer (POPIA §72). Our Platforms and certain sub-processors are located in the United States and Israel. When Personal Information of South African data subjects is transferred outside South Africa, the transfer is made on the basis that one or more of the conditions in POPIA §72 is met, including (i) the data subject has consented, (ii) the transfer is necessary for the performance of a contract, or (iii) the recipient is bound by contractual obligations (such as the Standard Contractual Clauses available at https://docs.kampfire.events/SCC_TOMS_Ma.pdf) that uphold principles for reasonable processing of the information substantially similar to the conditions in POPIA.

9. Security compromise notification (POPIA §22). If there are reasonable grounds to believe that Personal Information has been accessed or acquired by an unauthorised person, We will notify the Information Regulator (South Africa) and, where required, the affected data subjects, as soon as reasonably possible. As a Manager, You shall promptly notify Us of any actual or suspected security compromise affecting Personal Information processed in respect of Your events.

10. Complaints. Data subjects have the right to lodge a complaint with the Information Regulator (South Africa) at JD House, 27 Stiemens Street, Braamfontein, Johannesburg, 2001; PO Box 31533, Braamfontein, Johannesburg, 2017; complaints email POPIAComplaints@inforegulator.org.za; website <https://inforegulator.org.za>.

UPDATES TO THIS NOTICE

We may update this privacy notice from time to time. The updated version will be indicated by an updated "Revised" date and the updated version will be effective as soon as it is accessible. If We make material changes to this privacy notice, We may notify you either by prominently posting a notice of such changes or by directly sending you a notification. We encourage you to review this privacy notice frequently to be informed of how We are protecting your information.

HOW CAN YOU CONTACT US ABOUT THIS NOTICE?

If you have questions or comments about this notice, email Us at contact@kampfire.events or by post to:

Obreccsys LLC.

Attn: Legal Department

3349 Hwy138

Wall, NJ 07119

US