

KIK Custom Products Inc.

U.S. State-Specific Privacy Notice

LAST UPDATED: September 23, 2024

We, KIK Custom Products Inc. (“**KIK**”), issue this U.S. State-Specific Privacy Notice to provide information about how we collect, use, disclose and otherwise process the personal information of residents of California, Colorado, Connecticut, Florida, Oregon, Texas, Utah, Virginia and the rights that residents of the aforementioned states may have under the California Consumer Privacy Act of 2018 (“**CCPA**”), Colorado Privacy Act (“**CPA**”), Connecticut Data Privacy Act (“**CDPA**”), Florida Digital Bill of Rights (“**FDBR**”), Oregon Consumer Privacy Act (“**OCPA**”), Texas Data Privacy and Security Act (“**TDPSA**”), Utah Consumer Privacy Act (“**UCPA**”), Virginia Consumer Data Protection Act (“**VCDPA**”), and any other U.S. privacy laws, as each are amended and as and when they become effective, and including any regulations thereunder (each a “**U.S. State Privacy Law**” and collectively, the “**U.S. State Privacy Laws**”). This U.S. State-Specific Privacy Notice applies solely to residents in the states set out above. This U.S. State-Specific Privacy Notice does not reflect our processing of such residents' personal information where an exception under the applicable U.S. State Privacy Law applies.

This U.S. State-Specific Privacy Notice supplements the Privacy Policy found [here](#). In the event of any conflict between any other KIK policy, statement, or notice and this U.S. State-Specific Privacy Notice, this U.S. State-Specific Privacy Notice will prevail as to the consumers to whom U.S. State Privacy Laws apply.

The notices at collection of any third parties that control the collection of personal information via our services should be requested of the third party collecting the information at the point of collection.

1. Our Personal Information Handling Practices over the Preceding 12 Months

We collect, retain, process, and disclose your personal data generally for business and commercial purposes, as described elsewhere in the Privacy Policy. The table below sets out the categories of non-sensitive and sensitive personal information (as defined by the U.S. State Privacy Laws) that we collected over the preceding 12 months, their source, and to whom and for what purpose we may have disclosed (which may be considered a Sale or Share under certain U.S. Privacy Laws) the information. This U.S. State-Specific Privacy Notice also applies to our current data practices such that it is also meant to provide you with “notice of collection,” which is notice of personal data (also referred to in some of the U.S. State Privacy Laws as “personal information”) we collect online and offline, and the purposes for which we process personal data as required by the U.S. State Privacy Laws. For any new or substantially different processing activities that are not described in this U.S. State-Specific Privacy Notice, we will notify you as required by the U.S. State Privacy Laws, including by either notifying you at the time of collecting personal data, or by updating this U.S. State-Specific Privacy Notice earlier than required. We reserve the right to amend this U.S. State Privacy Policy at our discretion and at any time.

The table is followed by a description of the purposes for which we collected personal information from: (1) individual representatives of our prospective, current or past suppliers and customers (collectively, “**B2B contacts**”); and (2) our prospective, current and past employees and other personnel (collectively, “**employees**”). We do not sell or share for cross-context behavioral advertising any of the categories of personal information that we collect about California residents.

Category of personal information	Did we collect? If so, from what source?	Did we disclose? If so, to whom and for what purpose?	Retention Period
<i>Non-Sensitive Personal Information</i>			
Identifiers and contact information, such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, or other similar identifiers.	Yes, from employees, consumers, and B2B contacts.	Yes, to certain service providers who provide services to us.	After no longer needed for processing purpose(s) or after a maximum of 8 years of non-activity, whichever is longer, unless required by law or contract to retain.
Personal records that identify, relate to, describe, or are capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, or government-issued records.	Yes, from employees, consumers, and B2B contacts.	Same as above.	After no longer needed for processing purpose(s) or after a maximum of 8 years of non-activity, whichever is longer, unless required by law or contract to retain.
Characteristics of protected classifications.	Yes, from employees.	Same as above.	After no longer needed for processing purpose(s) or after a maximum of 8 years of non-activity, whichever is longer, unless required by law or contract to retain.
Commercial information, including but not limited to records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.	Yes, from consumers and B2B contacts.	Same as above.	After no longer needed for processing purpose(s) or after a maximum of 8 years of non-activity, whichever is longer, unless required by law or contract to retain.
Biometric information	Yes, from employees.	N/A	After no longer needed for processing purpose(s), unless required to retain for legal or compliance/regulatory purposes.

Category of personal information	Did we collect? If so, from what source?	Did we disclose? If so, to whom and for what purpose?	Retention Period
Internet or other electronic network activity information.	Yes, from employees, consumers, and B2B contacts.	Yes, to our service providers who provide services to us in accordance with service provider contracts.	After no longer needed for processing purpose(s) or after a maximum of 8 years of non-activity, whichever is longer, unless required by law or contract to retain.
Geolocation data.	Yes, from employees, consumers and B2B contacts.	Same as above.	After no longer needed for processing purpose(s) or after a maximum of 8 years of non-activity, whichever is longer, unless required by law or contract to retain.
Audio, electronic, visual, thermal, olfactory, or similar information.	Yes, from employees and B2B contacts.	Same as above.	After no longer needed for processing purpose(s) or after a maximum of 8 years of non-activity, whichever is longer, unless required by law or contract to retain.
Professional or employment-related information.	Yes, from employees and B2B contacts.	Same as above.	After no longer needed for processing purpose(s) or after a maximum of 8 years of non-activity, whichever is longer, unless required by law or contract to retain.
Education information.	Yes, from employees.	Same as above.	After no longer needed for processing purpose(s) or after a maximum of 8 years of non-activity, whichever is longer, unless required by law or contract to retain.
Inferences drawn from any personal information to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends,	Yes, from employees and consumers.	Same as above.	After no longer needed for processing purpose(s) or after a maximum of 8 years of non-activity, whichever is longer,

Category of personal information	Did we collect? If so, from what source?	Did we disclose? If so, to whom and for what purpose?	Retention Period
predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.			unless required by law or contract to retain.
<i>Sensitive Personal Information</i>			
A consumer's social security, driver's license, state identification card, or passport number.	Yes, from employees.	Yes, to our service providers who provide services to us in accordance with service provider contracts.	After no longer needed for processing purpose(s) or after a maximum of 8 years of non-activity, whichever is longer, unless required by law or contract to retain.
A consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account.	Yes, from employees.	Same as above.	After no longer needed for processing purpose(s) or after a maximum of 8 years of non-activity, whichever is longer, unless required by law or contract to retain.
A consumer's precise geolocation.	Yes, from employees.	Same as above.	After no longer needed for processing purpose(s) or after a maximum of 8 years of non-activity, whichever is longer, unless required by law or contract to retain.
A consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership.	Yes, from employees.	Same as above.	After no longer needed for processing purpose(s) or after a maximum of 8 years of non-activity, whichever is longer, unless required by law or contract to retain.
The contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication.	Yes, from employees.	Same as above.	After no longer needed for processing purpose(s) or after a maximum of 8 years of non-activity, whichever is longer,

Category of personal information	Did we collect? If so, from what source?	Did we disclose? If so, to whom and for what purpose?	Retention Period
			unless required by law or contract to retain.
A consumer's genetic data.	No.	N/A	NA
The processing of biometric information for the purpose of uniquely identifying a consumer.	No.	N/A	N/A
Personal information collected and analyzed concerning a consumer's health.	Yes, from employees.	Yes, to our service providers who provide services to us in accordance with service provider contracts.	After no longer needed for processing purpose(s) or after a maximum of 8 years of non-activity, whichever is longer, unless required by law or contract to retain.
Personal information collected and analyzed concerning a consumer's sex life or sexual orientation.	No.	N/A	N/A

We use the personal information that we collect from **B2B contacts and consumers** for the following purposes:

- To better understand how visitors use our website.
- To improve our website to better meet B2B contacts' and consumer needs.
- To enhance website functionality.
- To respond to inquiries.
- To supply requested products or services.
- To send informational or promotional communications.
- To monitor and maintain the security of our website.
- To execute transactions.
- To carry out other purposes that are disclosed to B2B contacts and consumers and to which they consent.
- To carry out any other purpose permitted or required by law.

We use the personal information that we collect from **employees** for the following purposes:

- To perform the services or provide the goods reasonably expected by our employees in their role as our employees, including those services and goods that are reasonably necessary for us to administer the employment relationship and for our employees to perform their duties;
- To detect security incidents that compromise the availability, authenticity, integrity, and confidentiality of stored or transmitted personal information, including in or via our premises, computers, software, networks, communications devices, and other similar system;
- To resist malicious, deceptive, fraudulent or illegal actions directed at us and to pursue those responsible for those actions;
- To ensure the physical safety of natural persons;
- To verify or maintain the quality or safety of our services and products;
- To perform functions that are required under laws that apply to us; and
- To fulfil the other purposes set forth in our privacy notices at collection to employees;

We do not have actual knowledge that we sell or share the personal information of individuals under 16 years of age. We do not use sensitive personal information for purposes other than those permitted under applicable U.S. State Privacy Laws, and do not sell personal information in the sense of exchanging personal information for money.

2. Your Rights under U.S. State Privacy Laws

Certain U.S. State Privacy Laws provide you with some or all of the following rights:

- The **right to know** what personal information we have collected about you, including the categories of personal information, the categories of sources from which the personal information is collected, the business or commercial purpose for collecting, selling, or sharing personal information, the categories of third parties to whom we disclose personal information, and the specific pieces of personal information we have collected about you. You may only exercise your right to know twice within a 12-month period.
- The **right to delete** personal information that we have collected from you, subject to certain exceptions.
- The **right to correct** inaccurate personal information that we maintain about you.
- The **right to opt-out of the sale or sharing** of your personal information by us. We do not sell or share for cross-context behavioral advertising any of the categories of personal information that we collect.
- The **right to limit** our use of sensitive personal information to purposes specified in various U.S. State Privacy Laws. Some U.S. State Privacy Laws require consent for the processing of Sensitive Personal Information which can be revoked, subject to certain exceptions. Depending on your state of residence, you may have the right to revoke such consent or limit our use and disclosure of Sensitive Personal Data.
- The **right not to receive discriminatory treatment** by the business for the exercise of privacy rights.
- The **right to obtain** your personal information upon request in a readily usable format that allows you to transmit the information.

3. How to Exercise Your CCPA Rights

- **Methods of Submission and Instructions:** To submit a request to exercise your **rights to know, delete or correct**, please email privacyofficer@kikcorp.com or call 1-800-276-8260 (toll free).
- **Verification:** Only you, or someone legally authorized to act on your behalf, may make a request related to your personal information. You may designate an authorized agent by taking the steps outlined under "Authorized Agent" further below. In your request or in response to us seeking additional information, you, or your authorized agent, must provide sufficient information to allow us to reasonably verify that you are, in fact, the person whose personal information was collected which will depend on your prior interactions with us and the sensitivity of the personal information being requested. We may ask you for information to verify your identity and, if you do not provide enough information for us to reasonably verify your identity, we will not be able to fulfil your request. We will only use the personal information you provide to us in a request for the purposes of verifying your identity and to fulfill your request.
- **Authorized Agents:** You can designate an authorized agent to make a request on your behalf if the authorized agent is a natural person or a business entity registered with the Secretary of State, we receive a written authorization stating that you have authorized the authorized agent to submit a request on your behalf which has been signed by you and the authorized agent, and we have verified the identity of you and the authorized agent.

4. **Appeal Rights**

You may appeal a denial of your request by emailing privacyofficer@kikcorp.com.

5. **Contact Us**

If you have questions or concerns about our privacy policies or practices, please contact us directly at privacyofficer@kikcorp.com or call 1-800-276-8260 (toll free).