

GLOBAL PRIVACY NOTICE

How Keystone One Data LLC collects personal data through promotional sweepstakes and uses selected data for direct marketing by email, SMS and telephone, and for KYC, identity verification, fraud prevention and identity resolution through specialist third-party partners.

VERSION	1.4
EFFECTIVE / UPDATED	3 March 2026
STATE ENTITY ID	10503601
ADDRESS	8 The Green STE B, Dover, Kent County, DE 19901, United States
WEBSITE	https://keyonedata.com/
PRIVACY CONTACT	privacy@keyonedata.com

PRIVACY AT A GLANCE

HOW DATA IS COLLECTED Through prize draws, sweepstakes and related registration forms, plus website interactions, consent records, correspondence and authorised data sources.	HOW DATA IS USED To administer promotions, validate entries and contact details, send permitted marketing by email, SMS or telephone, and use selected data for KYC, identity verification and identity resolution through specialist partners.
WHEN DATA IS SHARED With technology providers, professional advisers, authorities where required, and selected marketing, KYC, identity, fraud-prevention and verification partners for the purposes disclosed at collection.	YOUR CHOICES Depending on applicable law: choose marketing channels and partners, unsubscribe or object, withdraw consent, and request access, correction, deletion, restriction or portability.

Contents

- 1

About Keystone and this notice
- 3

How the sweepstakes, marketing and KYC/IDR flow works
- 5

Purposes and legal bases
- 7

Disclosures, partners and WINR
- 9

Retention
- 11

Website and communications
- 13

Country legal framework
- 2

EU representative and DPO status
- 4

Personal data and sources
- 6

Marketing, KYC, identity verification and identity resolution
- 8

International transfers
- 10

Security and governance
- 12

Individual rights
- 14

Children, changes and contact

1

About Keystone and this notice

Who we are and the activities covered by this publication

Keystone One Data LLC ("Keystone", "we", "us" or "our") is a Delaware limited liability company with State Entity ID 10503601 and an address at 8 The Green STE B, Dover, Kent County, DE 19901, United States. Keystone operates keyonedata.com and promotional sweepstakes or prize-draw registration experiences through which individuals may provide personal data.

This Global Privacy Notice explains how Keystone collects, receives, records, uses, discloses, stores and otherwise processes personal data in connection with:

- online prize draws, sweepstakes, promotional initiatives and registration forms operated by Keystone or made available through publishers and campaign partners;
- entry administration, eligibility and age checks, duplicate-entry detection, winner contact and prize-related records;

- direct marketing and commercial communications by email, SMS or mobile messaging and telephone, where permitted by the individual's choices and applicable law;
- the disclosure of selected sweepstakes data for KYC, identity verification, fraud prevention and identity-resolution purposes through specialist partners;
- the selection and management of marketing, KYC, identity-verification, identity-resolution and fraud-prevention partners;
- website operation, security, correspondence, supplier and partner management, legal compliance and privacy requests.

SCOPE OF THE NOTICE

This notice is a global baseline. A sweepstakes page, official rules, consent statement, partner list, country supplement or service-specific notice may provide more detailed or additional information. Where there is a direct conflict, the more specific notice applies to that processing.

EU representative and DPO status

Article 27 contact point and current Article 37 assessment

Keystone is established outside the European Union. For processing within the territorial scope of Article 3(2) of the EU General Data Protection Regulation, Keystone has appointed the following representative in the European Union pursuant to Article 27 GDPR:

EU REPRESENTATIVE	GDPRLocal / Instant EU GDPR Representative LTD
CONTACT	Adam Brogden
ADDRESS	Office 2, 12A Lower Main Street, Lucan, Co. Dublin, K78 X5P8, Ireland
EMAIL	contact@gdprlocal.com
TELEPHONE	+44 1772 217800

The EU representative is a local contact point for individuals and supervisory authorities. The appointment does not transfer Keystone's responsibilities or prevent anyone from contacting Keystone directly.

DATA PROTECTION OFFICER

Keystone has not appointed a Data Protection Officer. Based on its current assessment of the nature, scope, context and purposes of processing, Keystone does not presently consider that the mandatory designation criteria in Article 37 GDPR apply. This assessment is kept under review, and a DPO will be appointed if the law or Keystone's activities require one.

3

How the sweepstakes, marketing and KYC/IDR flow works

Collection through promotions, followed by permitted communications and authorised partner disclosures

Keystone's services begin with data supplied by individuals through a sweepstakes, prize-draw or promotional registration flow. The specific form, prize, eligibility conditions and consent choices are shown on the relevant campaign page and in the official rules.

Stage	What happens
1. Registration	An individual enters a sweepstakes or related promotion and submits the requested identity and contact details. Keystone records the entry, source, date, technical information and relevant consent or permission signals.
2. Administration	Keystone uses the data to validate the entry, confirm eligibility, prevent duplicate or abusive participation, respond to requests, contact potential winners and maintain prize and compliance records.
3. Marketing and KYC/IDR choices	The registration form or consent layer explains optional marketing by Keystone and selected partners, the available email, SMS/mobile messaging and telephone channels, and the separate KYC, identity-verification, fraud-prevention or identity-resolution purpose. Where consent is used, it is free and optional.
4. Communications and partner disclosures	According to the choices made, Keystone may send marketing communications itself and may disclose selected identity, contact, preference, source and permission data to the marketing or KYC/IDR partners authorised for the campaign.
5. Independent partner processing	A receiving partner may use the data for its disclosed marketing, KYC, identity-verification, identity-resolution, fraud-prevention or related purpose under its own privacy notice. A partner that determines its own purposes and means acts as an independent controller. This includes WINR and other specifically identified partners.

Stage	What happens
HOW THE MODEL WORKS Keystone collects the sweepstakes data, administers the promotion, records channel and partner choices, may send permitted email, SMS and telephone marketing, and discloses selected data for the stated marketing and KYC/IDR purposes. Specialist recipients carry out their own disclosed processing under their notices.	

Privacy roles

Role	How it applies
Controller / responsible organisation	Keystone generally acts as controller for sweepstakes registration, entry administration, marketing communications, consent and preference records, security, fraud prevention, partner selection and the disclosure of selected data for the marketing and KYC/IDR purposes described in this notice.
Processor / service provider in limited cases	In a separately contracted workflow, Keystone may process campaign or administrative data on documented instructions from a client or campaign operator. The relevant contract and client notice apply in that context.
Independent recipient controllers	Partners that receive data and determine their own direct-marketing, KYC, identity-verification, identity-resolution, fraud-prevention, advertising or other permitted purposes act as independent controllers. Their notices apply to their processing after disclosure.

4

Personal data and sources

The exact fields depend on the campaign, country and permitted purpose

Category	Examples
Identity and eligibility	Name, surname, alias, date of birth, age or age band, gender where requested, nationality or country, eligibility responses and entry identifiers.
Contact and address	Postal address, house number, city, region, postcode, email address, telephone number, language, preferred communication channel and related contact fields selected for the promotion, marketing or partner disclosure.
Sweepstakes and consent records	Campaign, prize, entry date, official-rules acceptance, marketing-channel selections, partner choices, checkbox wording and timestamp, withdrawal or objection records, winner status and prize-administration correspondence.
Technical and security	IP address, device and browser information, timestamps, referring page, campaign parameters, cookies or comparable identifiers, system logs, security events and fraud indicators.
Data disclosed for marketing and KYC/IDR	Identity and contact details, communication preferences, source and permission information, and, where specifically requested and lawful, document type or identifier, address or residency indicators and other fields identified in the relevant consent or partner information.
Source and provenance	Publisher or campaign source, data provider, collection date, permission status, data age, licence restrictions and audit information.
Rights and preferences	Access, correction, deletion, restriction, direct-marketing objections, channel opt-outs, consent withdrawal, suppression and complaint information, plus verification data used to handle a request.
Sensitive or regulated data	Only where specifically authorised, necessary and lawful. Additional restrictions and safeguards apply to special-category data, criminal-offence data, government identifiers and biometric data.

Keystone does not require every category for every sweepstakes or partner disclosure. Forms should request only the fields needed for the promotion and the disclosed marketing or KYC/IDR purpose.

Sources of personal data

- individuals who enter a sweepstakes, complete a form, communicate with Keystone or exercise a privacy right;
- campaign publishers, landing-page operators, clients and promotional partners that collect data for Keystone or make an authorised campaign available;
- campaign and partner information identifying the marketing, KYC, identity-verification, fraud-prevention or identity-resolution recipients selected for a permitted disclosure;
- publicly available or lawfully accessible registers and sources where their use is permitted;
- technology, hosting, analytics, security and communications providers; and
- records generated by Keystone for entry administration, consent, transmission, suppression, security and audit purposes.

5

Purposes and legal bases

Why Keystone processes the data and the grounds generally relied upon

Purpose	What it involves	Typical legal basis
Operate the sweepstakes	Register entries, verify eligibility, administer official rules, respond to requests, contact potential winners and manage prize delivery.	Contract or steps requested by the individual; legal obligation; legitimate interests; consent where required.
Validate entries and prevent misuse	Check contact details, age or eligibility indicators, identify duplicates, detect suspicious or fabricated entries, maintain security and investigate abuse.	Legitimate interests in fair and secure promotions; contract; legal obligation; consent where required.
KYC and identity verification via partners	Disclose selected identity and contact data to specialist partners that carry out KYC, identity verification, AML, fraud-prevention or identity-protection processing.	Consent under Article 6(1)(a) GDPR where the relevant checkbox is used; another lawful ground only where permitted, appropriate and clearly disclosed.
Identity resolution via partners	Disclose selected data to specialist partners that match, link, distinguish or reconcile identity records and generate identity-resolution or data-quality indicators.	Consent where required; another permitted ground only where supported by applicable law and the collection notice.
Manage partner disclosures	Record the partner selection, permission, disclosure date and source, and communicate withdrawals, objections, corrections or suppression instructions where required.	Legal obligation, consent administration and legitimate interests in accountability, compliance and rights handling.
Security and legal compliance	Protect systems, preserve evidence, respond to lawful requests, maintain audit trails and establish, exercise or defend legal claims.	Legal obligation; legitimate interests; legal claims; substantial public interest or another statutory basis where applicable.
Direct marketing and partner marketing	Use contact and preference data to send offers by email, SMS/mobile messaging and telephone, and disclose selected data to identified partners for their own marketing. Telephone may include live-agent calls and, only where separately authorised and lawful, automated or prerecorded calls.	Consent where required; legitimate interests or an existing-customer/soft-opt-in rule only where local law permits; withdrawal and channel-specific opt-out at any time.

CONSENT AND CHOICE

Where the relevant choices are presented, marketing and KYC/IDR disclosures are based on the user's free and optional selections. The registration flow identifies the purposes, communication channels and partners, or provides access to the partner list. Refusing optional marketing or partner consent does not affect the ability to enter the sweepstakes or use the underlying service. Consent may be withdrawn and direct marketing may be opposed at any time for future processing.

Where Keystone relies on legitimate interests, it considers necessity, reasonable expectations, the nature and source of the data, the benefit of the activity, available safeguards and the likely impact on individuals. Consent may be withdrawn for future processing without affecting processing already carried out lawfully.

6

Marketing, KYC, identity verification and identity resolution

How Keystone communicates and how selected third-party partners carry out disclosed processing

Where the individual selects the relevant option, Keystone may use identity, contact and preference data to send commercial offers and promotional communications by email, SMS or mobile messaging and telephone. Keystone may also disclose selected data to identified marketing partners for their own communications. Live-agent telemarketing and automated or prerecorded calls are used only to the extent permitted by local law and the consent or other permission presented at collection.

Keystone also uses selected sweepstakes data for KYC, identity verification and identity resolution by transmitting identity and contact data, together with relevant source and permission information, to specialist partners identified in the registration flow, partner list or this notice.

The receiving partner carries out its disclosed marketing, matching, verification, identity-resolution or fraud-prevention activity using its own systems and sources. It may generate results or manage communications under its own privacy notice. Keystone maintains records of the disclosure and permissions and, where required, communicates withdrawals, objections, corrections, deletion or suppression requests to the relevant partner.

PARTNER PROCESSING

Selected partners may carry out direct marketing, technical matching, verification, identity-resolution and related processing using their own systems, sources and campaign rules. Where a partner determines its own purposes and means, it acts as an independent controller and is responsible for its transparency, legal basis, retention, safeguards, communication practices and any automated-decision obligations.

7

Disclosures, partners and WINR

Who may receive the data and what happens after disclosure

Keystone may disclose personal data only where necessary for the purposes described in this notice, subject to campaign choices, channel permissions, contracts and applicable law. Recipient categories may include:

- campaign operators, publishers and service providers supporting the sweepstakes, entry administration, communications, hosting, security or prize delivery;
- selected marketing partners, agencies, contact centres and campaign recipients authorised for email, SMS/mobile messaging or telephone communications;
- selected KYC, identity-verification, identity-resolution, fraud-prevention and identity-protection partners that carry out the disclosed checks and related processing;
- clients, end clients or designated recipients identified in the campaign or partner information;
- professional advisers, auditors, insurers, banks and corporate-service providers;
- regulators, courts, law-enforcement bodies or other authorities where disclosure is required or permitted; and
- a buyer, investor, lender or successor in connection with a corporate transaction, subject to appropriate safeguards.

A partner that receives data and determines its own purposes and means of processing acts as an independent controller. It is responsible for its direct-marketing, KYC, identity-resolution, fraud-prevention or related processing under its own privacy notice, including its legal basis, communication channels, retention, security, opt-out and rights process. Where Article 14 GDPR or an equivalent rule applies, the partner is responsible for providing the required information to the individual. Keystone remains responsible for the lawfulness and transparency of its own collection, communications and disclosures.

Specific partner statement — WINR Data Pty Ltd

We may share your personal information with WINR Data Pty Ltd and its global partners for the purposes below, relying on our legitimate interests or your consent, where required.

Fraud Prevention and Identity Assurance – helping prevent misuse of your personal information and supporting identity, age and eligibility checks, including fraud, crime and money laundering prevention, debt collection, asset recovery, and reuniting individuals with unclaimed assets.

The WINR Data privacy notice is available at:

<https://www.winrcorp.com/privacy/nexus>

We may share your personal information with WINR Alchemist Pty Ltd and its global partners for the purposes below, relying on our legitimate interests or your consent, where required.

Digital Advertising – supporting the delivery of personalised advertising and content that is relevant to you, including through identity resolution services such as data analysis, matching and linkage.

The WINR Alchemist privacy notice is available at:

<https://www.winrcorp.com/privacy/alchemist>

Once data is disclosed to WINR, WINR processes it for the identity-protection and advertising purposes stated above and in its own privacy policy. Where required, Keystone records the relevant marketing or KYC/IDR permission, provides partner information at collection and communicates withdrawals, objections, corrections or suppression requests to WINR.

8

International transfers

Personal data may be processed outside the country where it was collected

Keystone is established in the United States and works with campaign operators, service providers, data sources and partners in multiple countries. Personal data may therefore be processed in a country with different privacy laws.

Where required, Keystone uses legally recognised transfer mechanisms and safeguards, which may include adequacy decisions, the European Commission Standard Contractual Clauses, transfer impact assessments and supplementary measures, the UK International Data Transfer Agreement or Addendum where relevant, contractual clauses recognised by another jurisdiction, and technical and organisational measures such as encryption, access controls, minimisation, segregation, logging and vendor diligence.

9

Retention

Data is kept only for the period justified by purpose, permission and law

Retention periods depend on the campaign, data category, consent status, partner arrangement, legal duties and the need to protect individuals and Keystone. As a general publication baseline:

Record type	General approach
Sweepstakes entries	Normally retained for the duration of the initiative and for up to 36 months after collection or the end of the campaign, unless a shorter period is stated or a longer period is needed for claims, audit or legal duties.
Winner and prize records	Retained for the period required to verify the winner, deliver the prize, maintain accounting or tax records and establish or defend legal claims.
Marketing and KYC/IDR disclosure records	Keystone retains the relevant channel and partner choices, consent, transmission, audit and rights-handling records for as long as necessary to demonstrate communications and disclosures, manage withdrawals or disputes, and comply with contractual or legal requirements.
Consent and suppression records	Retained as necessary to demonstrate the permission or withdrawal, honour email, SMS and telephone opt-outs, and prevent data from being reintroduced after an objection, deletion or suppression request.
Partner-held data	A receiving independent controller applies the retention period in its own privacy notice for its marketing, KYC/IDR or other disclosed processing, including the WINR statement above.
Security and technical logs	Retained for a limited period proportionate to security, troubleshooting, fraud prevention and legal requirements.

At the end of the relevant period, Keystone deletes, anonymises, returns or securely isolates the data unless continued retention is required or permitted. Backup copies may persist for a limited period until overwritten through the normal backup cycle.

10 Security and governance

Risk-based measures for sweepstakes, identity data and partner disclosures

Keystone applies technical and organisational measures designed to protect personal data against unauthorised access, use, disclosure, alteration, loss and destruction. Depending on the risk and workflow, measures may include:

- role-based access, least privilege, authentication and privileged-access controls;
- encryption in transit and, where appropriate, at rest;
- secure configuration, environment segregation, logging, monitoring and incident response;
- data minimisation, masking, pseudonymisation, tokenisation or suppression where appropriate;
- partner and vendor diligence, contractual privacy and security requirements and access restrictions;
- testing, change control, backups, recovery and business-continuity procedures; and
- staff confidentiality, security awareness and documented privacy processes.

SECURITY IS SHARED

No system can be guaranteed completely secure. Individuals, campaign operators and partners should use accurate information, protect credentials, use secure transfer methods and promptly report suspected misuse or security incidents.

11 Website and communications

Technical logs, cookies, service messages and direct marketing communications

When a person visits keyonedata.com or a campaign page, Keystone or its hosting and security providers may process IP address, date and time, requested pages, browser or device information, referrer, campaign parameters, error information and security signals. This information is used to deliver the page, record the source of an entry, maintain availability, prevent abuse, troubleshoot and understand service performance.

Strictly necessary cookies or comparable technologies may be used for security, session handling, consent records and core operation. Optional analytics or advertising technologies are used only with the notice and consent or opt-out control required by applicable law.

Keystone may send communications necessary to confirm an entry, respond to a request, administer the sweepstakes, contact a potential winner, manage a prize, communicate a security or legal matter, or facilitate a disclosed partner purpose. Where permitted by the choices presented and applicable law, Keystone may also send commercial offers by email, SMS or mobile messaging and telephone. Telephone marketing may include live-agent calls and, only where separately authorised and lawful, automated or prerecorded calls. Recipients can unsubscribe, opt out by channel or contact privacy@keyonedata.com. Necessary service, prize, security and legal messages may continue.

12 Individual rights

Rights depend on location, Keystone's role and the processing activity

Depending on applicable law, an individual may have the right to:

- obtain information about processing and request access to personal data;
- correct inaccurate or incomplete data held or disclosed by Keystone and raise concerns about a partner-generated verification or identity-resolution result through the relevant partner's rights process;
- request deletion, erasure, restriction, blocking or anonymisation;
- object at any time to direct marketing, including related profiling, and opt out separately from email, SMS/mobile messaging or telephone communications;
- withdraw consent for future processing;
- receive portable data in a structured, commonly used format where applicable;
- request information about or human review of a significant automated decision where applicable;
- appeal a refusal where a law provides an appeal right; and
- complain to a competent privacy or data-protection authority.

HOW TO SUBMIT A REQUEST

Email privacy@keyonedata.com or write to Keystone One Data LLC, 8 The Green STE B, Dover, Kent County, DE 19901, United States. Describe the request, the relevant sweepstakes or partner, and the country of residence. For EU GDPR matters, the Article 27 representative in section 2 may also be contacted.

Keystone may take reasonable steps to verify identity and authority. Where data has already been disclosed to an independent controller, that organisation may also need to process the request under its own notice. Keystone will communicate corrections, withdrawals, objections and deletion or suppression requests to recipients where required and reasonably possible.

13 Country legal framework

The primary privacy framework for the intended service countries

This schedule identifies the main general privacy framework and supervisory authority for the requested countries. Applicability depends on territorial scope, thresholds, exemptions, campaign design, marketing channel, Keystone's role and the specific processing. References include amendments, implementing rules and successor provisions; national consumer, sweepstakes, telemarketing and electronic-communications laws may also apply.

EUROPEAN BASELINE

France, Spain, Portugal, Sweden, Belgium, Austria, Denmark, Finland, Ireland, Luxembourg, Germany, Italy, Poland and the Netherlands apply the GDPR together with national supplementary law. Norway applies the GDPR through the EEA framework. Switzerland applies its separate Federal Act on Data Protection.

Jurisdiction	Primary framework	Authority
Australia (AU)	Privacy Act 1988 (Cth), Australian Privacy Principles and Notifiable Data Breaches scheme, where applicable.	OAIC
New Zealand (NZ)	Privacy Act 2020 and the Information Privacy Principles.	Office of the Privacy Commissioner
France (FR)	GDPR and Law No. 78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties, as amended.	CNIL
Spain (ES)	GDPR and Organic Law 3/2018 on Personal Data Protection and Guarantee of Digital Rights.	AEPD
Portugal (PT)	GDPR and Law No. 58/2019 implementing the GDPR.	CNPD
Sweden (SE)	GDPR and Act (2018:218) with supplementary provisions to the EU GDPR.	IMY
Belgium (BE)	GDPR and the Act of 30 July 2018 on the protection of natural persons with regard to personal data processing.	APD/GBA
Switzerland (CH)	Federal Act on Data Protection (FADP) and the related Data Protection Ordinance.	FDPIC
Austria (AT)	GDPR and the Austrian Data Protection Act (Datenschutzgesetz, DSG).	DSB
Denmark (DK)	GDPR and the Danish Data Protection Act, Act No. 502 of 23 May 2018.	Datatilsynet
Norway (NO)	GDPR as incorporated into the EEA framework and the Norwegian Personal Data Act 2018.	Datatilsynet
Finland (FI)	GDPR and the Data Protection Act (1050/2018).	Data Protection Ombudsman
Ireland (IE)	GDPR and the Data Protection Act 2018.	Data Protection Commission
Luxembourg (LU)	GDPR and the Act of 1 August 2018 establishing the national data-protection framework.	CNPD

Jurisdiction	Primary framework	Authority
Germany (DE)	GDPR and the Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG), plus applicable state law.	Federal and state authorities
Italy (IT)	GDPR and Legislative Decree No. 196/2003, as amended, including by Legislative Decree No. 101/2018.	Garante
Poland (PL)	GDPR and the Act of 10 May 2018 on the Protection of Personal Data.	UODO
Netherlands (NL)	GDPR and the GDPR Implementation Act (Uitvoeringswet AVG, UAVG).	Autoriteit Persoonsgegevens

How the regional rules affect this notice

EU / EEA COUNTRIES

Keystone provides GDPR transparency, identifies a lawful basis for collection, communications and disclosure, respects data-subject rights, uses Article 27 representation and applies Chapter V transfer safeguards. Direct marketing by email, SMS and telephone also follows applicable ePrivacy and national electronic-communications rules. Receiving partners apply the controller obligations relevant to their own marketing and KYC/IDR processing.

SWITZERLAND

Where the FADP applies, Keystone addresses transparency, proportionality, accuracy, security, access/correction, automated decisions and cross-border disclosures. A Swiss representative or additional notice will be used if legally required for a particular activity.

AUSTRALIA

Where covered by the Privacy Act, Keystone applies APP-based notice, collection, use/disclosure, data quality, security, access/correction and overseas-disclosure controls, and follows the Notifiable Data Breaches scheme for eligible breaches.

NEW ZEALAND

Where the Privacy Act 2020 applies, Keystone follows the Information Privacy Principles, access and correction rights, overseas-disclosure rules, breach-notification requirements and other applicable local duties.

SWEEPSTAKES AND ELECTRONIC COMMUNICATIONS

The privacy frameworks above operate alongside applicable national consumer, prize-promotion, advertising, telemarketing and electronic-communications rules. The campaign form and consent layer identify the available email, SMS/mobile messaging and telephone channels, relevant partner choices and any separate permission required for automated or prerecorded contact.

SENSITIVE KYC/IDR DATA

Government identifiers, identity-document information, criminal-offence data, biometric data or other specially regulated categories are collected or disclosed only when necessary, expressly authorised and supported by the legal and security controls required in the relevant country and by the receiving partner's processing framework.

LOCAL SUPPLEMENTS

A country, campaign, client or partner-specific supplement may provide additional information, restrictions or rights. That supplement controls to the extent of a direct conflict with this global notice.

14

Children, changes and contact

Age limitation, publication updates and how to reach Keystone

The sweepstakes and services covered by this notice are intended for individuals aged 18 or over. Keystone does not knowingly invite or collect entries directly from persons under 18. If Keystone learns that it collected such data without an appropriate legal basis, it will take reasonable steps to delete or otherwise address it.

Keystone may update this notice to reflect changes in sweepstakes, data uses, partners, technology, law or business operations. The current version will be published on keyonedata.com with the updated effective date. Material changes will be communicated where required. An update does not replace any consent that applicable law requires.

CONTACT KEYSTONE ONE DATA LLC

State Entity ID: 10503601

Address: 8 The Green STE B, Dover, Kent County, DE 19901, United States

Website: <https://keyonedata.com/>

Privacy email: privacy@keyonedata.com

For EU GDPR matters, individuals and supervisory authorities may also contact GDPRLocal / Instant EU GDPR Representative LTD at Office 2, 12A Lower Main Street, Lucan, Co. Dublin, K78 X5P8, Ireland; contact@gdprlocal.com; +44 1772 217800.

Individuals may lodge a complaint with the privacy or data-protection authority competent for their location or the relevant processing activity. Keystone encourages individuals to contact us first so that we can investigate and respond.