



A PRODUCT OF KHALIFEH CONSULTING GROUP (KCG)

PRIVACY POLICY

How iReveal™ by KCG collects, uses, and protects your information

Effective Date: 2026

Last Updated: 2026

CONFIDENTIAL — PROPRIETARY



Khalifeh Consulting Group (KCG) | Beirut, Lebanon | www.khalifehconsulting.com

Table of Contents

1. Introduction and Acceptance.....	3
2. Definitions and Interpretation	3
3. Information We Collect	4
4. Purposes of Processing.....	4
5. Legal Basis for Processing.....	4
6. Automated Processing and Risk Outputs.....	5
7. Disclosure of Information	5
8. International Transfers of Information	5
9. Data Retention.....	5
10. Information Security	6
11. Your Rights	6
12. Responsibilities of Client Organizations.....	6
13. Cookies and Analytics Technologies	7
14. Children's Privacy.....	7
15. Third-Party Services and Integrations.....	7
16. Amendments to This Policy	7
17. Notices and Contact Information	7
18. Confidentiality and Data Protection Commitment	8
19. General Disclaimer	8

Document Owner	Khalifeh Consulting Group (KCG)
Effective Date	2026
Last Updated	2026
Classification	Confidential

1. INTRODUCTION AND ACCEPTANCE

1.1 This Privacy Policy (this “Policy”) is issued by **Khalifeh Consulting Group**, a consulting group based in Beirut, Lebanon (“**KCG**”, “we,” “our,” or “us”), in its capacity as owner and operator of **iReveal™** (the “**Platform**”), a compliance intelligence and risk assessment platform made available to organizations, notaries, law firms, financial institutions, corporate service providers, other regulated entities, and any other business whose operations may expose it to the risk of financial crime (each, a “**Client**” and, together with its authorized users, “**you**” or “**User**”).

1.2 The Platform is designed to assist Users in conducting sanctions screening, politically exposed person (“**PEP**”) screening, adverse media reviews, beneficial ownership analysis, due diligence reviews, anti-financial crime assessments, risk scoring, and compliance investigations (collectively, the “**Compliance Services**”). The Platform functions solely as a compliance support tool and processes information submitted by Users for legitimate business and compliance purposes, as further described in this Policy.

1.3 By accessing or using the Platform, you acknowledge that you have read and understood this Policy and that your information will be collected, used, stored, processed, transferred, protected, and disclosed as described herein.

2. DEFINITIONS AND INTERPRETATION

2.1 For the purposes of this Policy, the following terms shall have the meanings set out below, unless the context otherwise requires:

“Identification Information” means full legal names, date of birth, nationality, passport numbers, national identification numbers, tax identification numbers, and company registration information;

“Contact Information” means email addresses, telephone numbers, business addresses, and mailing addresses;

“Compliance Information” means beneficial ownership information, corporate structures, source of wealth information, source of funds information, due diligence documentation, and know-your-customer (“KYC”) documentation;

“User Account Information” means usernames, passwords (stored in encrypted form), organization names, user permissions, and subscription information; and

“Personal Information” means collectively, Identification Information, Contact Information, and any other information relating to an identified or identifiable natural person that is processed through the Platform.

2.2 Section headings are inserted for convenience of reference only and shall not affect the interpretation of this Policy. Words importing the singular shall include the plural and vice versa, and references to “including” or “includes” shall mean “including, without limitation.”

3. INFORMATION WE COLLECT

3.1 Information Provided Directly by Users. In the course of accessing or using the Platform, you may provide KCG with Identification Information, Contact Information, Compliance Information, and User Account Information, each as defined in Clause 2.1 above.

3.2 Information Collected Automatically. When you access the Platform, KCG may automatically collect technical and usage information, including IP addresses, browser information, device identifiers, operating system information, access timestamps, login history, activity logs, audit trail information, and security event records.

3.3 Information Obtained from Third Parties. KCG may supplement the information described above with information obtained from sanctions list providers, governmental authorities, public registries, corporate registries, media databases, compliance data providers, open-source intelligence sources, and other publicly available databases.

4. PURPOSES OF PROCESSING

4.1 KCG processes information for legitimate business purposes, including each of the following:

- (a) Compliance Screening, comprising sanctions screening, PEP identification, adverse media reviews, and watchlist screening;
- (b) Due Diligence, comprising customer due diligence, enhanced due diligence, beneficial ownership analysis, and source of wealth assessments;
- (c) Platform Operations, comprising account administration, customer support, system maintenance, and billing and subscription management;
- (d) Security, comprising fraud prevention, cybersecurity monitoring, unauthorized access detection, and audit trail maintenance; and
- (e) Legal Compliance, comprising compliance with applicable legal obligations, regulatory reporting requirements, and responses to lawful requests from competent authorities.

5. LEGAL BASIS FOR PROCESSING

5.1 KCG processes information on the basis of one or more of the following legal grounds, as applicable:

- (a) the necessity of processing for the performance of a contract to which the User is party;
- (b) KCG's legitimate business interests;
- (c) compliance with a legal obligation to which KCG is subject;
- (d) compliance with applicable regulatory requirements; and

-
- (e) the User's consent, where such consent is required by applicable law.

6. AUTOMATED PROCESSING AND RISK OUTPUTS

6.1 The Platform may generate risk classifications, risk scores, screening alerts, matching probabilities, and other compliance indicators (collectively, "Outputs") through automated methodologies.

6.2 You acknowledge and agree that:

- (a) such Outputs are generated using automated methodologies;
- (b) such Outputs are indicative only;
- (c) such Outputs do not constitute final determinations of any kind; and
- (d) human review remains necessary before any compliance decision is made in reliance on an Output.

6.3 For the avoidance of doubt, KCG does not make, and shall not be deemed to make, any regulatory, legal, judicial, or enforcement decision on behalf of any User.

7. DISCLOSURE OF INFORMATION

7.1 KCG does not sell Personal Information. KCG discloses information only to the following categories of recipients, and solely to the extent necessary for the purposes described in this Policy:

- (a) Service Providers, comprising cloud hosting providers, cybersecurity providers, technical support providers, and payment processors;
- (b) Compliance Data Providers, comprising sanctions screening vendors, adverse media providers, and corporate intelligence providers;
- (c) Legal and Regulatory Authorities, where disclosure is required by law, a court order, a regulatory request, or any other lawful governmental demand; and
- (d) Successors in Interest, in connection with a merger, acquisition, corporate restructuring, or sale of business assets.

8. INTERNATIONAL TRANSFERS OF INFORMATION

8.1 Information may be processed or stored in jurisdictions outside your country of residence. Where an international transfer of information occurs, KCG shall implement commercially reasonable safeguards designed to protect the confidentiality and security of the information so transferred.

9. DATA RETENTION

9.1 KCG retains information only for so long as reasonably necessary to:

- (a) provide the Compliance Services;
- (b) maintain audit trails;

- (c) satisfy applicable legal obligations;
- (d) comply with applicable regulatory requirements;
- (e) resolve disputes; and
- (f) enforce KCG's contractual rights.

9.2 Retention periods may vary depending on the applicable legal and regulatory requirements in each relevant jurisdiction. Unless a longer period is required by applicable law, KCG may retain compliance records for up to ten (10) years following the closure of the relevant account.

10. INFORMATION SECURITY

10.1 KCG implements reasonable administrative, technical, and organizational measures designed to protect information against unauthorized access, disclosure, alteration, destruction, loss, or misuse, including encryption, multi-factor authentication, access controls, audit logging, penetration testing, and vulnerability management procedures.

10.2 Notwithstanding the foregoing, no system of information security can guarantee absolute security, and KCG makes no warranty, express or implied, that unauthorized access, disclosure, or loss of information will never occur.

11. YOUR RIGHTS

11.1 Subject to applicable law, you may have the right to:

- (a) access your information;
- (b) correct inaccurate information;
- (c) update your information;
- (d) request the deletion of your information;
- (e) restrict processing;
- (f) object to processing; and
- (g) obtain copies of your information.

11.2 Requests to exercise the rights set out in Clause 11.1 may be submitted to KCG using the contact details set out in Clause 17. KCG reserves the right to verify the identity of the requesting party before acting on any such request.

12. RESPONSIBILITIES OF CLIENT ORGANIZATIONS

12.1 Organizations using the Platform remain solely responsible for:

- (a) obtaining all consents required by applicable law;
- (b) establishing lawful grounds for the processing of information they submit to the Platform;

(c) complying with all applicable privacy and data protection laws; and

(d) ensuring the accuracy and completeness of information submitted to the Platform.

12.2 KCG acts solely as a technology and compliance support provider and does not assume the User's independent legal obligations.

13. COOKIES AND ANALYTICS TECHNOLOGIES

13.1 The Platform may use cookies, session identifiers, authentication tokens, analytics tools, and performance monitoring technologies to improve user experience, maintain security, enhance system performance, and generate operational analytics. Where technically feasible, you may manage your cookie preferences through your browser settings.

14. CHILDREN'S PRIVACY

14.1 The Platform is intended solely for professional and business use and is not directed toward individuals under the age of eighteen (18). KCG does not knowingly collect information from minors.

15. THIRD-PARTY SERVICES AND INTEGRATIONS

15.1 The Platform may contain links to, or integrations with, third-party services. KCG is not responsible for third-party privacy practices, third-party content, or third-party security controls. You should review the privacy policies of those third parties separately.

16. AMENDMENTS TO THIS POLICY

16.1 KCG may amend this Policy from time to time. Material amendments will be communicated through platform notifications, email communications, or website announcements. Your continued use of the Platform following any such amendment constitutes your acceptance of the revised Policy.

17. NOTICES AND CONTACT INFORMATION

Khalifeh Consulting Group (KCG) — Owner and Operator of iReveal™

Email: info@khalifehconsulting.com

Website: www.ireveal.net · www.ireveal.app · www.khalifehconsulting.com

Business Address: PTT Office Street, Jdeideh Tower, 2nd Floor, PO Box 90-667, Zip Code 12022060, Jdeidet El Metn, Beirut, Lebanon

18. CONFIDENTIALITY AND DATA PROTECTION COMMITMENT

18.1 KCG recognizes that information processed through the Platform may include highly sensitive compliance, due diligence, and investigative information. Accordingly, KCG commits to operating the Platform in accordance with internationally recognized principles of confidentiality, integrity, accountability, proportionality, data minimization, legitimate purpose, and information security.

19. GENERAL DISCLAIMER

19.1 The Platform is a compliance support and risk intelligence platform. It is not a governmental authority, financial intelligence unit, law enforcement agency, regulator, court, sanctions authority, or official screening body. Information processed through the Platform is intended solely to support professional compliance decision-making and shall not be interpreted as a definitive legal, regulatory, or criminal finding.