ENTRUST PRIVACY STATEMENT

Last Updated: January 9, 2026

CONTENTS

1. INTRODUCTION

At Entrust, we work with businesses, enterprises, and governments around the world to fight fraud and cyber threats using identity-centric security through our products and services ("**Products and Services"**). We also operate several websites to provide our Products and Services, including, amongst others, www.entrust.com (together "**Websites**"). To provide these Products and Services, operate our Websites and to conduct our business operations we process personal data about our website visitors, business contacts, customers and our customers' end users.

We are committed to complying with data protection principles to protect your privacy, which includes being transparent with you about how we process personal data. The purpose of this Privacy Statement ("**Statement**") is to describe our privacy practices in a clear and easy to understand way and to provide you with information about how to exercise your rights with respect to your data.

When we refer to "**Entrust**", "**we**", "**us**", or "**our"** in this Statement, we mean Entrust Corporation and its affiliates and subsidiaries ("**Entrust Group"**).

When we refer to **personal data** in this Statement, we mean information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier. Examples of identifiers include a name, identification number, location data, online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a natural person.

This Statement applies where Entrust processes personal data as a **data controller**, in connection with the operation of our business and management of our relationship with you, including via our Websites. As a data controller, we determine why and how personal data is processed and are ultimately responsible for the correct handling of your data, in accordance with applicable law.

This Statement describes our general privacy practices. Depending on how you interact with us or the specific services you use, additional privacy notices may apply. Additional notices provided at or before the time we collect your personal data, should be read together with this Statement.

We process personal data for most of our Products and Services as a **data processor**. As a data processor, we process personal data about our customers' employees, end users and customers on behalf of our customers to provide the Products and Services based on their instructions. These instructions are set out in our customer agreements, Data Processing Addendum(s) or through a customer's use or configuration of a product. You should contact these organizations directly for information about how they process your personal data as a data controller and to exercise your rights in relation to that data.

Please refer to Section 11 below for details regarding a specific Product or Service, view the relevant Product Privacy Notice.

2. PERSONAL DATA WE PROCESS AND WHY

The personal data we collect about you depends on your relationship with us and the purposes for which we process that personal data. The following list describes the types of personal data that we collected and disclosed for business purposes in the preceding 12 months.

INFORMATION YOU PROVIDE TO US

Business Contact Information – When you use any of our Products and Services, request product information, sign up for a webinar, download a whitepaper or other document from our Websites, ask for a call from our sales team, or participate in industry events, we ask you to provide us with your name, company name, business address, phone number, email address and other contact information. We collect and process this information as it is in our legitimate interest to know who is interested in our Products and Services. We may combine this information with other data we receive or hold about you, such as the data contained within professional profiles that you maintain online.

Customer Account Data – We process personal data to manage our relationship with you and administer you or your company's account. This includes purchase history, names or contact information of individuals authorized to manage the Entrust account on behalf of our customer and to set up, access and manage billing. We collect and process this data as it is in our legitimate interest to ensure that we can provide our Products and Services to you and your company. We also process this data in our legitimate interest to ensure that the information we hold about you and your company's use of our Products and Services is accurate and secure, and to confirm eligibility to use our Products and Services.

Customer Communications – We receive and store the content of communications received from you, information and communications about you from our customers, and other personal data uploaded to the Products and Services, or generated for our customers' use as part of the Products and Services, which we may be authorized by you or our customer to use, where necessary and in accordance with applicable law. We collect this information as it is in our or our customers' legitimate interests to maintain a record of this information for legitimate business purposes.

Marketing and Contact Preferences – We collect and use contact information about you to send you information about our Products and Services. In instances where we inform you about relevant changes or updates to our Products and Services, we do so based on our legitimate interest in keeping you informed about updates we believe may matter to you, or to fulfill our contractual obligations with your company.

We may also contact you to provide us with feedback or complete surveys about our Products, Services and customer service. We do so based on our legitimate interest to invite you to provide this information for us to better understand our customers and how we can improve our business.

We may also contact you with information or messages on behalf of our Customer, including via phone. We do this as it is in our legitimate interest to share such messages to keep you informed of updates from our Customer.

We may also contact you where you have consented to receive marketing or other communications, or where we think that you would be interested in our Products and

Services. We do so based on our legitimate interest to inform you of such information for the purpose of marketing our business. If you opt out of receiving marketing communications from us, we will remove you from marketing lists and prevent you from receiving this information.

You can opt-out of non-essential and marketing communications from us by filling out our marketing opt-out form or by contacting privacy@entrust.com.

Payment Information – In connection with the Products and Services you pay for, we ask you to provide our payment processor with your payment method information like a debit card, credit card or other financial account information, including your billing address. We may also use the information we collect to verify your information and complete online transactions and send related communications and information, including transaction confirmations and invoices.

We use your financial account or credit or debit card information only for the purpose of processing your purchase. Our payment processor, acting on our behalf, may gather this information so we can bill you for use of our Products and Services. Our payment processor will share your billing address with Entrust for this purpose. We collect this information for us to complete our contract with you, where you enter into a contract with us directly. In all other instances, we rely on our legitimate interest in obtaining payment and enforcing the terms of the contract we have in place with your company.

Support and Feedback - When you interact with us on our Websites including through our AI chatbots (e.g. our Help Center Assistant), over the phone or via email, we process the phone number or email address that you use, the content of your interaction and the feedback you provide about our Products and Services. You may also provide us with feedback about our Products and Services in surveys and questionnaires. We collect this information as it is in our legitimate interest to use the context and details provided to enable us to respond to your query, provide you with effective customer service, improve future responses and understand how our Websites, Products and Services are used and can be improved.

We will let you know when a call may be recorded, in accordance with applicable law. Where Entrust communicates with you via SMS to provide customer service or support, we will obtain your consent prior to using this method of communication and that consent will not extend to any third parties.

PERSONAL DATA WE GENERATE OR COLLECT AUTOMATICALLY

Device Information and IP Addresses – When you access our account portal or Websites, we collect your IP address and device information through tracking technologies like cookies, web beacons, pixels, and similar technologies. We also collect IP addresses when you make requests to your APIs and in our server logs. Additionally, we collect information

about your device, such as your computer or mobile device operating system type and version number, manufacturer and model, browser type, screen resolution, unique identifiers, and general location information such as city or town when you use our account portal. **We do not collect precise geolocation information.** We collect this information as it is in our legitimate interest to ensure that your account is secure and to improve our Products and Services. We may use this information to investigate, detect and prevent security incidents and understand how to optimize our Products and Services. Where your consent is required for the use of certain devices (e.g. cookies) we rely on your consent to provide us with this information (please refer to the "Cookies" section below in section 8). We may also use the information we collect about your use of our account portal to analyze your interest in our Products and Services and deliver marketing to you which we think is relevant to you we do this as it is in our legitimate interest to ensure we are advertising effectively.

Website Activity Information – When you visit Entrust Websites, including our web forms, we use tracking technologies such as cookies, web beacons, and pixels to collect the following data: your device and browser, time zone setting, web pages visited, products you view or search for, page response times, download errors, length of visits to certain pages, and page interaction information. We collect some of this data as it is our legitimate interest to understand how you use our Websites, including to optimize and maintain our Websites, debug and troubleshoot errors, and improve the content, functionality and usability of our Websites. We may also use this data to compile statistics about the usage of our Websites and to prevent, detect and investigate security issues associated with our Websites. Some of this information is collected with your consent. Please refer to the "Cookies" section below in section 8.

PERSONAL DATA COLLECTED FROM THIRD-PARTY SOURCES

Professional Data – We collect certain personal data such as employment or professional information from sources other than you. We may combine this data with other personal data that you share with us.

Publicly-Available Sources – We may also use publicly-available information about you that we have gathered through services like LinkedIn, or we may obtain information about you or your company from third party providers, such as your industry, the size of your company, and your company's website URL.

Social Media Data – Social media service providers such as Google, LinkedIn, and Meta may provide us with information about you, in accordance with your privacy settings on those sites.

Single Sign On - Entrust enables Single Sign On (**SSO**) to allow Customer's users to login to multiple Entrust Products and Services with a single email address and password. When you

create an Account with Entrust and your company has opted to use SSO, a profile will be created for you using the SSO that you can utilize to access Entrust websites and products.

Entrust will store the fact that you have set up an account using SSO, as well as information shared with us by the company you work for to enable us to verify and administer your account using SSO. We may also use information provided by you at the point of Account creation, as described in the previous section of this Statement.

Entrust uses Microsoft Entra to enable SSO and specific account details that are stored with Microsoft Entra may be shared with Entrust to enable the provision of SSO accounts across our Products and Services. We may share personal data to enable SSO with Microsoft Entra, as described in section 3 relating to sharing personal data with Third Party Service Providers.

PERSONAL DATA WE INFER

We may combine the information you provide to us and information we collect about you by drawing inferences from such information (including, for example, non-precise geolocation data) to create a profile reflecting your characteristics, interests, and preferences. We do so based on our legitimate interest in using this data as part of Entrust's core business operations and to ensure any processing is in line with legal and regulatory standards and industry codes of practice. Entrust does not use or process special category personal data for the purpose of inferring characteristics about an individual.

3. WHO DO WE SHARE PERSONAL DATA WITH?

We only disclose personal data to third parties in limited circumstances to provide the Products and Services and to otherwise run our business. Below are the different scenarios under which we may disclose your data to third parties:

Third-Party Service Providers

Entrust engages third-party vendors and service providers to carry out certain personal data processing functions on our behalf. These providers are limited to only accessing or using personal data to provide services to us and must provide reasonable assurances they will appropriately safeguard the data. This includes any third-party vendors we use to provide our Products and Services, as well as any third-party we use to enable the function of our business, such as legal and tax advisors, and to facilitate our marketing activities.

Within the Entrust Group

We may disclose your personal data among Entrust Group members. Entrust Group members will only use the information for the purposes described within this Statement. Entrust Group members are all party to appropriate agreements and measures to ensure that personal data is shared in an appropriate and secure manner.

Compliance with Legal Obligations

We may disclose your personal data to a third party if:

- we reasonably believe that disclosure is required by applicable law, regulation, legal process, or a request (including to meet national security, emergency services, or law enforcement requests or requirements);
- to enforce our agreements, policies, and rights;
- to protect the security or integrity of our Products and Services;
- to protect ourselves, our customers, or the public from harm or illegal activities, including security threats, spam and fraud; or
- to respond to an emergency which we believe in good faith requires us to disclose data to assist in preventing a death or serious bodily injury.

If Entrust is required by law to disclose any personal data about you, we will notify you or our customers of the disclosure requirement to the extent we are legally permitted. Further, we will object to information requests we do not believe were issued properly or appropriately.

Business Transfers

In connection with a proposed or active corporate sale, merger, reorganization, dissolution or similar event, personal data about you may be part of the assets transferred or disclosed in connection with the due diligence for any such transaction. If required by law, we will notify you prior to such a transfer and provide you with information about any choices you may have with respect to your personal data.

4. INTERNATIONAL DATA TRANSFERS AND JURISDICTION-SPECIFIC PROVISIONS

As global organization, we may need to transfer your personal data to the Entrust Group, their affiliates, contractors, service providers and/or third parties in various countries and jurisdictions around the world. When we transfer your personal data, we take care to use appropriate safeguards to ensure your personal data remains protected.

Data Transfers to the United States and Other Countries

When you use our Products or Services, your personal data may be transferred to the United States, where our primary processing facilities are located. Where required by applicable data protection law, we ensure that appropriate protections are in place.

Safeguards for Data Transfers and Standard Contractual Clauses

Entrust employs appropriate safeguards for cross-border transfers of personal data, as required by applicable local law. For many jurisdictions, this involves the use of appropriate standard contractual clauses, such as the EU Standard Contractual Clauses and UK Addendum.

For more information about the protections in place which apply to the transfer of your personal data please contact us using the details below in Section 12.

5. HOW WE SECURE PERSONAL DATA

To protect personal data from loss, alteration, destruction or unauthorized use, access or disclosure, Entrust uses reasonable and proportionate security measures designed to protect the security of your personal data both online and offline. Entrust's data security measures are adjusted according to the sensitivity of the personal data we collect, process, and store and are regularly updated to reflect alongside technological advancements. All systems used to support our business are governed by Entrust's Privacy and Information Security Programs, which are built on industry standards and best practices including ISO 27001 and ISO 27701 (Privacy Information Management Systems) certifications.

6. HOW LONG WE RETAIN PERSONAL DATA

We retain personal data only for as long as it is reasonably necessary to fulfill the purposes for which it was originally collected. In line with this principle, we endeavor not to retain personal data in a form which enables the identification of individuals beyond what is necessary for data processing.

Aggregated, anonymized and de-identified data may be derived by Entrust from your personal data but is generally not considered personal data under data protection law as once this data is anonymized and de-identified it can no longer be linked to you and does not directly or indirectly reveal your identity. We may use and retain this information for longer periods of time and may disclose it to third parties. We do not disaggregate or re-identify this data, nor do we provide any information to third parties to enable them to identify this data.

Our data retention practices are governed by Entrust's record retention policies and guidelines, which are reviewed and updated periodically to ensure continued compliance with legal and operational requirements.

If you ask Entrust to delete specific personal data as a website visitor, business contact, customer, or as an end user of our customer, we will honor this request, unless deleting that information prevents us from carrying out necessary business functions, such as billing for our services, complying with legal obligations or conducting required audits.

7. YOUR RIGHTS AND CHOICES ABOUT YOUR DATA

WHERE ENTRUST IS THE DATA CONTROLLER

Depending on where you live and the data protection laws that apply to you, you may be entitled to exercise specific rights regarding the personal data that we process about you as a data controller. The following rights may be available:

- the right to request confirmation of data processing;
- the right to access your personal data, including what we collect, where it comes from, who we share or sell it to, and why we use it;
- the right to a copy of the personal data we collect about you;
- the right to correct or update any inaccurate or incomplete personal data we have about you;
- the right to delete your personal data;
- the right to object or restrict the processing of your personal data, including special category personal data;
- the right to a record of your personal data in a structured, commonly used format;
- the right to request that we directly transmit a record of the information held by us to another controller;
- the right to receive information about automated decision-making, including profiling, and information about the logic involved that produces legal effects or similarly affects your individual rights;
- the right to a free, easy mechanism to object to use of your personal data for direct marketing purposes;
- the right to opt out of personalized advertising, data sharing, and data sales;
- the right to withdraw your consent where consent is relied upon as the legal basis for the processing of your personal data; and
- the right to complain to a competent supervisory authority and/or to commence proceedings in a court of competent jurisdiction.

Entrust will honor your rights subject to limitations in certain situations, such as where Entrust can demonstrate that it has a legal requirement to process your data or can legitimately apply an exemption to the exercise of a right under applicable law.

EXERCISING YOUR RIGHTS

Deleting Your Account

Enterprise Customers

If you are an enterprise customer and choose to end your relationship with Entrust and request deletion of your data, please reach out to your designated Customer Success Manager or visit: https://www.entrust.com/contact-support. Closing your account will permanently end your access to the account and any data stored within it. After your account is closed, certain data may remain in our systems where required by law or for legitimate business purposes until it's no longer needed. Please refer to the **"**How Long We Retain Personal Data**"** section above for additional information.

End Users

If you are an end user using our Products or Services, on behalf of an Entrust customer and would like to request deletion of your data, please refer the Data Subject Request Section of our Privacy Page or contact us at privacy@entrust.com.

Other Requests

To exercise any other rights or to request additional information about how Entrust may be processing your data, please refer to the Data Subject Request Section of our Privacy Page or contact us at privacy@entrust.com.

Contacting our DPO

You also have the right to contact our Data Protection Officer (DPO) at:

Mishcon de Reya LLP
Africa House, 70 Kingsway, London, United Kingdom, WC2B 6AH
dpo@mishcon.com

Identity Verification and Additional Information

In some cases, Entrust may need to verify your identity before honoring your request. Entrust will only request key details proportionate to your request, such as date of birth, date of services, and the name of any affiliated organization connected to your use of our services. In instances where special category data is the subject of the request, Entrust may need to verify additional details before honoring your request. Once your identity is verified, we will process your request and inform you of any decisions we have made about your request.

Authorized Agent

You are entitled to exercise your privacy rights through an authorized agent. If we receive your request from an authorized agent, we may ask for evidence that you have provided such agent with a power of attorney or other written authorization. If you are an authorized agent seeking to make a request, please contact us at privacy@entrust.com.

Non-Discrimination

We will not discriminate against you or alter the pricing of our Products and Services based on your requests. Please note, however, that if you request the deletion of your personal data, this may limit or prevent your ability to access certain features of our Products and Services.

Communication Preferences

You can opt out of receiving marketing communications from Entrust at any time through our marketing preferences form or by clicking the "unsubscribe" link at the bottom of any marketing email you receive from us. You can also contact us directly to communicate your choice to opt out. Please note that it may take some time to remove your contact information from our marketing communications lists. You may continue to receive messages during this time, but no later than 10 days after your request.

To ensure you do not receive future marketing communications, Entrust will maintain the relevant contact information in a database, but will only use your contact information to ensure your opt-out preferences are respected. You will not be able to opt out of essential business, transactional or operating related emails from us, such as password reset emails, service update emails, or notifications of updates to our terms or policies.

IF YOU ARE A U.S. RESIDENT

If you are a U.S. resident interested in the categories of personal data we have disclosed lately for our business purposes, please refer to the list below:

- Identifiers
- Internet or other electronic activity information
- Professional or employment information
- Inferences drawn from the above personal data
- Additional information that is linked to the above personal data

We disclose personal data only as described in our "Who Do Share Data With" and "How We Use Cookies and Other Similar Technologies" sections. We process this personal data to deliver interest-based ads on other websites and apps, which may be considered "sharing" or "targeted advertising" under certain laws. As referenced above, you have the right to opt out and can do so by navigating to the Cookie Preferences tool at the bottom panel of the Entrust website. Your cookie settings and preferences are device and browser specific. If you clear cookies at any point, you may need to reset your preferences.

In instances where you have the right to request the restriction of processing of your special category personal data, the respective special category personal data will be marked accordingly and may only be processed by Entrust for certain limited purposes. Currently, Entrust only uses or discloses special category personal data as necessary to

provide our services, as described in this Statement, or as allowed by law. Special category personal data is sometimes referred to as "sensitive data." These uses are not subject to limitation under California law.

CALIFORNIA PRIVACY RIGHTS

This section contains disclosures required by the California Consumer Privacy Act, as amended by the Consumer Privacy Rights Act ("CCPA").

Personal Data We Collect

In the preceding 12 months, we collected from California consumers the categories of personal data described in Section 2 for the purposes outlined in that section.

Categories of Sources

We collected the above-mentioned personal data from the sources described in Section 2.

Disclosing Personal Data for Business Purposes

We may disclose your personal data to a third party for the purposes set out in Section 3.

Sale and Sharing of Personal Data

We may share your personal data with third parties, including for purposes of cross-context behavioral advertising, which may constitute "selling" or "sharing" under the CCPA. Such sale or sharing does not include information about individuals we know are under the age of 16. In the preceding 12 months, Entrust has sold or shared the categories of personal data listed below with the categories of third parties listed below. For more information or to opt out of this sale or sharing, please see Section 7 or click on the "Do Not Sell or Share My Personal Information" button located in the footer of the Websites.

Categories of Personal Data

- Personal and online identifiers (such as first and last name, email address, IP address, or unique online identifiers)
- Internet or other electronic network activity information (such as browsing history, search history, and information regarding a consumer's interaction with an internet website)
- Professional or employment related information
- Inferences drawn from the above information about your predicted characteristics and preferences
- Additional information about you that is connected to the personal data listed above

Shared With the Following Categories of Third Parties

- Advertising and marketing companies
- Advertising networks
- Marketing analytics providers
- Data analytics providers
- Social networks

We do not collect or use sensitive personal data other than financial account or debit or credit card information when you make a purchase online, which we use solely for the purpose of processing your payment for that purchase.

An Explanation of Your Rights

The CCPA provides consumers, California residents, with specific rights regarding their personal data. Please refer to Section 7 for an explanation of those rights and how you may exercise them.

WHERE ENTRUST IS THE DATA PROCESSOR

In many instances, Entrust processes your personal data as a data processor on behalf of a customer. In these scenarios, if you contact us to enforce your rights, we will direct you to contact our customer, the data controller, to help you to exercise your privacy rights with them.

Additional information about your rights and choices and how to exercise your rights and choices can be found in Entrust's Data Subject Request Procedure.

8. HOW WE USE COOKIES AND OTHER SIMILAR TECHNOLOGIES

Entrust employs widely recognized mechanisms such as cookies, web beacons, pixels and other analytic technologies to seamlessly gather information as you navigate our websites, access your account, or engage with communications that we send to you.

Cookies

Cookies are small text files that are stored in your browser or on your device's hard drive. They are essential for the core functionality of our website and enable Entrust to recognize your device, retain your preferences, and honor your settings to make your interactions with us more seamless and efficient.

Entrust uses both session and persistent cookies. Session cookies are temporary and expire once your browsing session ends, while persistent cookies remain on your device even after it's powered off.

The cookies on our websites fall into four categories: (1) Essential Cookies, (2) Targeted Advertising Cookies, and (3) Personalized Cookies, and (4) Analytic Cookies. To learn more about each category of cookie, and see the different cookies we use, you can navigate to our cookie consent tool by clicking on the "Cookie Preferences" link on the bottom panel of the Entrust website you are visiting.

Manage Your Cookie Preferences

Entrust deploys a cookie consent tool that allows you to manage your cookie preferences. When you first visit our website, a banner will prompt you to set your cookie preferences. You can update your preferences at any time by navigating to the "Cookie Preferences" link on the bottom panel of the Entrust website. Please note that Essential Cookies cannot be disabled as they are essential to the functionality of our website. Opting out of Personalized Cookies may also affect the functionality of our website or your account. Any choice concerning cookies is browser and/or device specific. If you clear cookies from your browser, use a different browser, or switch devices, your choices will need to be reset.

In addition to using our Cookie Consent tool, you can use your browser settings to opt out of Personalized Cookies and Targeted Advertising Cookies. For more information on how to do that, click here.

Web Beacons and Analytics Tools

Entrust uses web beacons and analytics tools to understand how you interact with our websites and communications. Web beacons are clear electronic images embedded in web pages that allow us to identify whether specific content has been viewed and whether you interact with this content. In addition, we employ analytic tools that gather aggregated behavioral data, including where users hover, what they click, and how far they scroll on our website pages. This information enables us to understand usage patterns, improve site functionality, and enhance the overall user experience.

To learn more, visit our Cookie Policy.

Universal Opt-Out Mechanisms

If you would like to opt out of Google Analytics which Google deploy on our websites, please visit the Google site here.

9. CHILDREN'S PRIVACY

Entrust's Websites are not directed to and are not intended for use by children (under the age of 13 in the U.S. and UK, or 16 in the EEA). We do not knowingly collect personal data from children through our websites. We do not knowingly permit children to sign up for an Entrust account. If we become aware that a child has signed up for an account, we will take reasonable steps to deactivate the account and remove their personal data from our records as quickly as possible. If you believe an underage person has signed up for an Entrust account, please contact us at privacy@entrust.com with the subject line "Children".

Certain Entrust Products and Services, such as our Identity Verification Services, may process personal data of children, where our customers choose to use our services for this purpose. For more information about how personal data of children is handled, please refer to our Product Privacy Notices.

10. AUTOMATED DECISION MAKING AND ARTIFICIAL INTELLIGENCE

Automated decision-making refers to when a system is used to make decisions about you based on your personal data, without any human involvement. Automated decision-making may involve advanced artificial intelligence or machine learning models, but it can also be limited to straightforward function or rule-based logic. Entrust uses automated decision-making powered by data from our records, trusted third party vendors, and government sources to identify and prevent fraudulent activity. For additional information on our artificial intelligence and machine learning models, refer to our AI Transparency Notice or email us at AI@entrust.com.

11. RELATED PRIVACY NOTICES AND DOCUMENTATION

For a list of personal data categories processed in connection with a specific Product or Service, please view the relevant Product Privacy Notice.

Digital Card Solution

Identity as a Service (IDaaS)

Identity Essentials

Identity Mobile App

Identity Verification as a Service

Instant Financial Issuance as a Service (IFIaaS)

Instant ID as a Service (IIDaaS)

KeyControl as a Service (KCaaS)

Entrust Identity Verification Services (formerly Onfido Identity Services)

Workflow Signing Service (formerly Signhost)

12. HOW TO CONTACT US

If you have any questions, concerns or complaints about this Statement or our data protection practices, please contact us at privacy@entrust.com or by writing at the following address:

Entrust Corporation
Attention: Director of Privacy
1187 Park Place
Shakopee, MN 55379

Alternatively, you can contact our DPO at:

Mishcon de Reya LLP

DPO@mishcon.com

Mishcon de Reya LLP,

Africa House, 70 Kingsway,

London, WC2B 6AH, UK