Reyes Holdings Global Privacy Notice

Reyes Holdings, L.L.C, and its affiliates (collectively "Reyes Holdings", "we", or "our") take data privacy very seriously, and this privacy notice is designed to help you understand how we use your personal information.

We encourage you to read the whole notice. Alternatively, if you wish to read about specific privacy practices that interest you, please click on the relevant links below.

Table of Contents

1. The purpose of this privacy notice

1.1 Identity

This privacy notice applies to each of the organizations that form part of the Reyes Holdings group of companies. Click here to find an up-to-date list of the organizations that make up the Reyes Holdings group of companies.

1.2 Our use of personal information

In common with most global organizations, we collect, use, and share information, including personal information, in connection with providing our services and solutions and running our business.

1.3 This privacy notice

This is our main general privacy notice that applies across our business, although we may publish additional privacy statements that apply to:

- Our operations in specific jurisdictions to help ensure our compliance with local data protection requirements; and/or
- Specific services and solutions that we offer to our customers from time to time.

If an additional privacy statement is relevant to you because of the way in which you engage with us and there is a conflict between the information set out in this notice and the additional privacy statement, then the additional privacy statement will take precedence over the information set out in this notice.

1.4 Local differences

Whilst this privacy notice describes the data protection practices adopted by us generally across the world, local data protection laws may vary and our operations in some jurisdictions may mean that we are subject to different, or additional, local data protection requirements.

This section of our privacy notice lists those countries/states where our data protection practices differ from those set out in the rest of this notice. By clicking on the link to the relevant country/state you can find how our data protection practices differ in that country/state as well as any additional information that we are obliged to provide to you to comply with local data protection laws in that country/state.

If any of the country/state specific privacy practices and additional statements are relevant to you because of the way in which you engage with us and there is a conflict between those practices or statements and the information set out elsewhere in this notice, then the country/state specific practices and statements will take precedence.

Australia

Brazil

Canada

Costa Rica

France

Ireland

New Zealand

Panama

Puerto Rico

Singapore

South Korea

United Kingdom

United States

We have a separate privacy notice that sets out how we process the personal information of our staff, which prospective, current, and former members of staff should refer to.

1.5 Updating this privacy notice

This notice may be updated from time to time. When we do so, we will post the revised Privacy Policy on this page with a new "Last Updated" date. This version is dated May 2026. If we make a material change that affects Personal Information that we collected prior to the change, depending on the nature of the change, we might notify you of the change and we might request your consent to the change.

1.6 What is personal information?

Personal information is information that relates to you or allows us to identify you. This includes obvious things like your name, address, and telephone number but can also include less obvious things like analysis of your use of our websites. There are different types of personal information. The most important types for you to know about are:

- Special categories of personal information – these categories of personal information often have additional protection under data protection laws around the world. These categories include information about your health, racial or ethnic origin, political opinions, religious or philosophical beliefs and trade union membership, your genetic data and biometric data, and information concerning your sex life or sexual orientation. Local data protection laws may limit the way in which we can use this information when compared to, for example, your name and address.

- Criminal convictions information – this is information relating to your criminal convictions and offences. Local data protection laws may restrict the way in which we can use this information when compared to, for example, your name and address.

Please note that under data protection laws around the world, certain other types of personal information may also be deemed to be particularly sensitive and given additional protection, including tax identification numbers issued by government taxing authorities, financial account numbers and insurance information.

Many countries also provide additional protection for children's/minors' personal information, but, ordinarily, we do not need, nor do we look, to process children's/minors' personal information.

Unless we request it, we ask that you not send us, and you not disclose, any special categories of personal information, criminal convictions information or other types of information such as those listed above which may be deemed to be particularly sensitive.

We describe the various types of personal information we collect in the "Your personal information" section below.

1.7 Our responsibility to you

We process your personal information in our capacity as a *controller*. This means that we are responsible for ensuring that we comply with relevant data protection laws when processing your personal information.

1.8 Data Protection Officer

We have a Global Data Protection Officer whose job is to oversee our data protection compliance. You can contact our Data Protection Officer by sending an email to: privacy@reyesholdings.com.

2. Your personal information

2.1 Why are we collecting personal information about you?

We collect personal information about you in connection with providing our services and running our business. We will hold information about you if:

- you are a prospective, actual, or former customer, or you represent, work for, or own a prospective, actual, or former customer;
- you are a consumer of goods and services that we distribute;
- you provide services to us (or you represent, work for, or own an organization which provides services to us);
- you represent or work for a regulator, certification body or government body which has dealings with us; or
- you visit our online properties or enter our contests or sweepstakes;
- you attend our events, receive our updates, participate in a promotion that we operate or visit our offices or websites.

2.2 What personal information do we collect about you?

The types of information we process about you may include:

Types of personal information	Details
Individual details	Name, address (including the state or country within which you are based), other contact details (e.g., email and telephone numbers), gender, date and place of birth, nationality, employer, job title.
Identification details	Identification numbers issued by government bodies or agencies, such as your national insurance number, passport number, tax identification number and driving license number.

Financial information	Bank account or payment card details, income, or other financial information.
Credit, anti-fraud, and sanctions data	Credit history, credit score and information received from various anti-fraud and sanctions databases relating to you.
Special categories of personal information	Information about your health, racial or ethnic origin, political opinions, religious or philosophical beliefs and trade union membership.
Criminal convictions information	Information relating to your criminal convictions and offences.
IP address	Information about your usage of our websites that can be traced back to you, such as an IP address.

2.3 Where do we collect your personal information from?

We collect your personal information from various sources, including:

- you;
- your employer or the organization that you represent, work for or own;
- our affiliates;
- the companies that we distribute products for;
- our service providers;
- data analytics providers;
- data brokers;
- joint marketing partners;
- credit reference agencies;
- anti-fraud databases, sanctions list, court judgements and other databases;
- government agencies and publicly accessible registers or sources of information;

- social media outlets, including in the context of promotions that we operate; and/or

- by actively obtaining your personal information ourselves, for example using website tracking devices or the information we collect through your use of our websites, services, and solutions.

Which of the sources apply to you will depend on why we are collecting your personal information. Where we obtain your information from a third party, in particular your employer or the organization that you represent, we may ask them to provide you with a copy of this privacy notice (or a shortened version of it) to ensure you know we are processing your information and the reasons why.

3. Our use of your personal information

3.1 How do we use your personal information?

We may process your personal information in many different ways – including collecting, recording, organizing, storing, analyzing, modifying, extracting, sharing, deleting or destroying it.

In this section we set out in more detail:

- the main purposes for which we process your personal information; and

- the legal bases upon which we are processing your personal information.

Purpose	Legal bases
Operate, maintain and manage our business <u>Managing contractual relationships</u> If you are our (prospective) customer or supplier, or a representative of our customer or supplier, we collect your personal information to manage our (contractual) relationship with you. This includes negotiating, entering into, tracking, and performing agreements.	**To manage our contractual relationship with you**
Know your customer, supplier and counterparty and other legal obligations We obtain information about our	For all information – **compliance with a legal obligation**. For special category and criminal

(prospective) customers, suppliers and counterparties and their representatives and beneficial owners and others to help us comply with legislation on money laundering, terrorist financing, and sanctions and for fraud prevention and security monitoring purposes. We also collect and disclose personal information under applicable legislation and under orders from courts and regulators. Our disclosures will be to those bodies and persons who are entitled to receive the required information. In some cases, this information will include special categories of personal data and criminal convictions data.	convictions data – **assessing the risk of, preventing or detecting unlawful acts**, and **suspicion of terrorist financing or money laundering**.
Enquiries about and use of our services and solutions, conducting research <u>Responding to enquiries and providing information about our products, services, and solutions</u> We may collect personal information such as your name and contact details to respond to enquiries from you and to provide you with information about our products, services, and solutions. We do not generally look to collect special categories of personal data and criminal convictions data for this purpose. <u>Access to our services and solutions</u>: When you use our services, we may collect certain personal information to complete certain transactions, to facilitate your use of the services and solutions on a day-to-day basis, including your name, email address	<u>Responding to enquiries and providing information about our services and solutions</u>: **Legitimate interests** We have a legitimate interest in using your information where this is necessary or appropriate to respond to your enquiries or provide you with information on our services and solutions. <u>Access to our services and solutions</u>: **Compliance with a legal obligation**. **To manage our contractual relationship with you**. **Legitimate interests**

and login credentials (for example, your username), or as part of the initial customer on-boarding process. We do not generally look to collect special categories of personal data and criminal convictions data for this purpose. <u>Conducting research about your opinions and developing, improving, repairing, and maintaining our services and solutions:</u> We may use your personal information when carrying out research about your opinion of our current services and solutions and new services and solutions that may be offered and in developing, improving, repairing, and maintaining our services and solutions. We do not generally look to collect special categories of personal data and criminal convictions data for this purpose.	We have a legitimate interest in contacting and dealing with individuals engaged by our customers that are involved in our provision of services to those customers. We also have a legitimate interest in understanding when and how our services and solutions are used and by whom. <u>Conducting research about your opinions and developing, improving, repairing, and maintaining our services and solutions:</u> **Legitimate interests** We have a legitimate interest in conducting research about your opinions on our services and solutions/new services and solutions that may be offered, and in developing, improving, repairing, and maintaining our services and solutions.
Service providers We collect information about you in connection with your provision of services to us or your position as a representative or worker of a provider of services to us. We do not generally look to collect special categories of personal data and criminal convictions data for this purpose, other than where we are required to do so to meet our legal obligations (see 'Know Your Customer and other legal obligations above).	**Legitimate interests** We have a legitimate interest in contacting and dealing with individuals involved in providing services to us.
Events and updates, contests, sweepstakes, and marketing-related emails If you wish to attend one of our events, schedule a catch- up with us at a third-party	For communications with you – **legitimate interests, or with your consent**. We have a legitimate interest in keeping you informed about events and

event that we are attending or receive our updates, we ask you to provide us with a limited amount of information (normally your work contact details, your employer's name, your job title, and the topics, services, or solutions of interest). We use this information to communicate with you about our events, third party events we are attending, and our updates to ensure that you are an appropriate audience for them, and to conduct analysis for marketing purposes. We do not generally look to collect special categories of personal data and criminal convictions data for this purpose. (Please also see 'Marketing' below.)	developments in our business and the topics, services and solutions that may be of interest to you. When we send you marketing communications, there are separate laws regarding marketing communications that we adhere to, in addition to data protection laws. You may opt out of receiving marketing communications from us. For all other purposes – **legitimate interests**. Our events, the third-party events we attend, and our updates are intended primarily for customers and potential customers. We have a legitimate interest in confirming that our events and updates are being made available to their intended audience. We also have a legitimate interest in understanding your use of our events and updates, and whether this presents any opportunity for us to improve the services and solutions we offer to you.
Marketing We use relationship management software to understand the strength of our relationship with our customers and potential customers, which includes individual representatives of those customers – for example records of frequency of contact with those individuals. Where we have a sales opportunity, we may obtain information about relevant decision makers to improve the prospects of our sales pitch or proposal being successful. This information may come from a variety of public databases and information sources. We do not generally look to collect special categories of personal data and criminal	**Legitimate interests** We have a legitimate interest in understanding our relationship with our customers and potential customers. Using the frequency of your contact with our organization and analyzing how you interact with our marketing activities is a reasonable means of doing so. We also have a legitimate interest in understanding relevant information about you where you are likely to be involved in deciding whether you or the person you represent will buy our services and solutions.

convictions data for this purpose.	
Visitors to our websites Our websites may invite you to provide us with your personal information. Where you provide us with your information, we will only use it for the purpose for which it has been provided by you. Most of our websites use cookies to help them work more efficiently and to provide us with information on how the website is being used. For those of our websites where we are legally obliged to provide you with further information about the cookies we use, we have prepared separate cookie notices which you can find on the relevant websites and which provide you with the information you need to know. We do not generally look to collect special categories of personal data and criminal convictions data on our websites.	**Legitimate interests** We have a legitimate interest in providing to you the facilities on our websites that you have requested and in understanding how our websites are used and the relative popularity of the content on our websites.
Visitors to our offices We have security measures in place at our offices, which include building access controls and may include CCTV. Images captured by CCTV are securely stored and only accessed on a need-to-know basis – for example, to investigate an incident. CCTV recordings are typically automatically overwritten after a short period of time unless an issue is identified that requires investigation (such as a theft). We require visitors to our offices to sign in at reception, and we keep a record of visitors for a short period of time. Our visitor records are securely stored and only accessible on a need-to-know basis – for example, to investigate an incident.	**Legitimate interests** We have a legitimate interest in making sure our offices, and the people that visit and work at our offices, are safe and secure.

We do not generally look to collect special categories of personal data and criminal convictions data for this purpose.	
Establishing our legal position and complying with law We may use your personal information, including sharing it with our legal advisers, when looking to establish our legal position, including exercising and defending against legal claims. We may also use your personal information if this is necessary to comply with a legal obligation (e.g., such as to maintain records), legal processes, or internal policies. In some cases, this information will include special categories of personal data and criminal convictions data.	For all information – l**egitimate interests.** We have a legitimate interest in understanding and establishing our legal rights and obligations. For special category and criminal convictions data – **the establishment, exercise, or defense of legal claims or prospective legal claims**.
Accomplishing our business purposes We may use your personal information for data analysis (for example, to improve the efficiency of our products, services, and websites), for developing new products and services, for enhancing, improving, repairing, maintaining, or modifying our current products and services, and for operating and expanding our business activities. Our business purposes also included operating and maintaining our facilities and infrastructure; undertaking quality and safety assurance measures; conducting risk and security control and monitoring; detecting and preventing fraud; performing identity verification; performing accounting, audit, and other internal functions, such as internal investigations; facilitating and implement any reorganization, financing transaction,	**To manage our contractual relationship with you**. **Compliance with a legal obligation**. **Legitimate interests** We have a legitimate interest in carrying out our business purposes and activities.

merger, sale, joint venture, partnership, assignment, transfer, or other disposition of all or any portion of our business, assets or stock (including in connection with any bankruptcy or similar proceedings). We do not generally look to collect special categories of personal data and criminal convictions data for this purpose.	

We may aggregate and/or anonymize personal information so that it will no longer be considered personal information. We do so to generate other data for our use, which we may use and disclose for any purpose, as it no longer identifies you or any other individual.

3.2 Failure to provide your personal information to us

We cannot force you to provide your personal information to us and you can choose not to provide us with your personal information. Where we need to collect your personal information by law or in order to process your instructions, provide you with our services or perform a contract we have with you and you decide not to provide that information when requested, we may not be able to carry out your instructions, provide our services or perform the contract we have or are trying to enter into with you. In other circumstances where you choose not to provide us with your personal information we request, your decision not to provide us with your personal information may affect our ability to provide certain of our products and services.

3.3 Consent

We do not generally process your personal information based on your consent (as we can usually rely on another legal basis). Where we do process your personal information based on your consent, you have the right to withdraw your consent at any time. To withdraw your consent, please email us at privacy@reyesholdings.com or, to stop receiving our marketing emails or updates, please click on the unsubscribe link in the relevant email you receive from us. Once we have received notification that you have withdrawn your consent, we will no longer process your personal information for the purpose(s) to which you originally consented unless there is another legal ground for the processing. Please note that where we rely on your consent to process your personal information and you choose to withdraw your consent, your decision may affect our ability to provide certain of our products and services.

3.4 Do we share your information with anyone else?

We do not sell your information. But we do disclose your information in the following circumstances:

- our organization is made up of several different entities around the world. Where it is necessary or appropriate for the purposes for which we hold your information, we share your relevant information across our affiliated companies. All our affiliated companies covered by this notice manage your personal information in the manner and to the standards set out in this notice, subject to any local jurisdictional compliance requirements. Details of the affiliated companies to which this notice applies are set out in Section 1.1 above;

- if you are a customer or work for or are a representative or owner of a customer, then we might provide your relevant information to search companies so they can verify your identity;

- we use the services of various external organizations to help us run our business efficiently. We may share your personal information with our trusted third-party service providers, to facilitate services they provide to us, such as internet services, call centers, website hosting, data analytics, payment processing, order fulfilment, information technology and related infrastructure provision, customer service, email delivery, marketing, auditing, background checks, event organization and hosting, and other services. In each case where we share your information with one of our service providers, the service provider is required to keep it safe and secure. They are also not permitted to use your information for their own purposes;

- where we use external companies to organize or host events for us, we may need to provide these service providers with your relevant information;

- in connection with a sale or business transaction. If we sell our business or undergo another business transaction (such as a reorganization, merger, joint venture, assignment, transfer, or other disposition of any or all portion of our business, assets, or stock, including in connection with any bankruptcy or similar proceedings), then your information may be transferred to a third party;

- to protect the rights, property and safety of Reyes Holdings and others. Such information will be disclosed in accordance with applicable laws and regulations. This includes where we share information with other parties in the context of litigation discovery and in response to subpoenas and court orders;

- we share your personal information with other third parties, such as relevant public and government authorities, including regulators and law enforcement, where we are required or requested to do so to comply with legal or regulatory requirements;

- to comply with applicable law and regulations, which may include laws outside your country of residence;

- to enforce our policies;

- to prevent, investigate and identify persons or organizations potentially involved in activity that appears to us to be illegal, or we believe may expose us to legal liability; and

- in situations that we believe to be emergencies involving potential threats to the physical safety of any person or property if we believe that the information in any way relates to that threat.

4. Other important things you should know

4.1 Keeping your personal information safe

We take security issues seriously. We implement appropriate steps to help maintain the security of our information systems and processes and prevent the accidental destruction, loss, or unauthorized disclosure of the personal information we process. Some of the safeguards we use are firewalls and data encryption, physical access controls to data centers, and information access authorization controls. Unfortunately, no data transmission or storage system is guaranteed to be 100% secure.

4.2 Profiling and automated decision making

We do not use profiling (where an electronic system uses personal information to try and predict something about you) or automated decision making (where an electronic system uses personal information to decide about you without human intervention).

4.3 How long do we keep your personal information?

We keep your personal information in accordance with our data retention policy that categories all the personal information held by us and specifies the appropriate retention period for each category of personal information. Those periods are based on the requirements of relevant data protection laws and the purpose for which the information is collected and used, considering legal and regulatory requirements to retain the information for a minimum period, limitation periods for taking legal action, good practice, and our business purposes.

4.4 Third party services

This privacy notice does not address, and we are not responsible for, the privacy, information, or other practices of any third parties, including any third party operating any website or service to which our websites link.

In addition, we are not responsible for the information collection, use, disclosure, or

security policies or practices of other organizations, such as Facebook, Apple, Google, Microsoft, or any other social media platform provider, operating system provider, wireless service provider, or device manufacturer, including with respect to any personal information you disclose to other organizations through or in connection with our social media pages.

4.5 Cross border transfers of your personal information

We are a global business that operates and provides services and solutions to customers located in many different countries around the world.

The global nature of our business means that your personal information may well be transferred across national boundaries, including, potentially, to countries that do not require organizations by law to look after your personal information in the way in which you have come to expect in your own country.

Where we transfer your personal information across national boundaries, we will protect your personal information by ensuring that those transfers are made in compliance with all relevant data protection laws. For example, where we transfer personal information from a country located within the European Union to a country outside of the European Union that is not recognized by the European Commission as providing an adequate level of data protection, we normally do so subject to safeguards that assure the protection of your personal information, such as European Commission approved standard contractual clauses.

If you would like further details of how your personal information is protected when transferred from one country to another then please email us at privacy@reyesholdings.com.

5. Your rights

5.1 Contacting us and your rights

If you have any questions or complaints in relation to our use of your personal information, please email us at privacy@reyesholdings.com.

Alternatively, you may call us using the number below where the local language is spoken.

- US, Canada and Puerto Rico: (888) 295-6392
- Brazil: 0800-891-2871
- Panama: 001-888-597-1408
- United Kingdom: 0808-234-9917
- Malaysia: 800-81-6398
- Qatar: 704-552-8066
- Dubai: 877-635-2795

- Ireland: 1-800-559-036
- New Zealand: 1-877-635-2795
- Australia: 1-800-68-7913
- Bahrain: 8000-4322
- Costa Rica: 0-800-011-1250
- France: 0800-91-5911
- Korea: 00308-13-2759
- Oman: 001-704-552-8066
- Singapore: 800-110-2086

Under certain conditions, you may have the right to require us to:

- provide you with further details on the use we make of your personal information
- provide you with access to the personal information we hold about you
- update any inaccuracies in the personal information we hold about you
- delete any of your personal information that we no longer have a lawful ground to use
- where processing is based on consent, stop that processing by withdrawing your consent
- object to any processing based on our legitimate interests unless our reasons for undertaking that processing outweigh any prejudice to your data protection rights
- restrict how we use your personal information whilst a complaint is being investigated
- transfer your personal information to a third party in a standardized machine-readable format

In certain circumstances, we may need to restrict your rights to safeguard the public interest (e.g., the prevention or detection of crime) and our interests (e.g., the maintenance of legal privilege).

We are obliged to keep your personal information accurate and up to date. Please help us to do this by advising us of any changes to your personal information.

5.2 Your right to complain

If you are not satisfied with our use of your personal information or our response to any request by you to exercise your rights, or if you think that we have breached any relevant data protection laws, then you have the right to complain to the authority that supervises

our processing of your personal information or, where you are based in the UK or the EU, the data protection authority in your country.

If you are unsure of the authority that supervises our processing of your personal information, then please email us at privacy@reyesholdings.com.

Australia

Our main general privacy notice together with the information set out on this page constitutes our privacy notice for the purposes of our compliance with the data protection laws in Australia.

This page sets out the additional information, over and above the information set out in our main general privacy notice, that we are obliged to provide to you to comply with local data protection laws in Australia. It also sets out how our data protection practices differ in Australia compared to the practices described in our main general privacy notice.

The name and address of our Australian business can be found here.

Differences/Additional Information

- Any reference to identification details in clause 1.10 of the main general privacy notice does not include your Tax File Number (**TFN**) unless we are specifically authorized by law to process TFNs for the relevant purpose and, if so, we will inform you of that on collection.

- By providing us with any special categories of personal information or criminal convictions information (**sensitive information**) or continuing with our services you consent to us processing your sensitive information in accordance with our privacy notice.

- Under Australian data protection laws, your rights described in clause 4.1 of the main general privacy notice are restricted to only a right of access to, and a right to correct inaccuracies in, the personal information we hold about you. If we refuse to provide access to or correct your personal information, we will give you a written notice within 30 days and outline the reasons for our refusal and avenues available for you to complain about our refusal.

- If you make a complaint directly to us in relation to our use of your personal information, we will investigate your complaint and inform you of any steps we will take to resolve the complaint. We will notify you in writing if we require any additional information and also of the outcome of the investigation. If you are not happy with the outcome of our investigation, you may complain to the Office of the Australian Information Commissioner (**OAIC**) whose contact details can be obtained at www.oaic.au.

Brazil

Our main general privacy notice together with the information set out on this page constitutes our privacy notice for the purposes of our compliance with the data protection laws in Brazil.

This page sets out the additional information, over and above the information set out in our main general privacy notice, that we are obliged to provide to you to comply with local data protection laws in Brazil. It also sets out how our data protection practices differ in Brazil compared to the practices described in our main general privacy notice.

The name and address of our Brazilian business can be found here.

Differences/Additional Information

Legal Bases

- In addition to the legal bases provided in the topic 3.1. of this Notice:
    - For the purposes of marketing and visitors to our website, consent may also be the applicable legal basis; and
    - For the purpose of establishing our legal position and complying with law, the legal basis may be legal obligation or exercise of rights.
    - For Know Your Customer (KYC) purposes, the legal basis may be compliance with a legal or regulatory obligation, where applicable to regulated activities; otherwise, and where applicable, legitimate interest, fraud prevention or exercise of rights may apply.

Your Rights:

- Brazil's General Data Protection Law (Law No. 13,709/2018, or "LGPD"), along with regulations issued by the National Data Protection Agency ("ANPD"), grants you specific rights concerning your personal data. These rights include, among others:
    - confirmation of the existence of the processing;
    - access to the personal information;
    - correction of incomplete, inaccurate or outdated personal information;

- anonymization, blocking or erasure of unnecessary or excessive data or data processed in noncompliance with the LGPD;
- portability of personal information to another service provider or product provider, upon express request and the regulation to be issued by the ANPD;
- erasure of the personal information processed with the consent of the data subject;
- information on government and private entities with which the controller has shared personal information;
- information on the possibility of denying consent and the consequences of such denial;
- revocation of consent,
- review of automated decisions that may affect your interests;
- petitioning regarding your personal information before the ANPD; and
- requesting the availability of the full text of the clauses used for international data transfer, subject to commercial and industrial secrecy.

- You can exercise these rights by contacting us through Data Subject Request Form. We will use reasonable efforts to respond promptly, within the time limits set by the LGPD, and we will keep you informed about the progress of your request.
- If you wish to withdraw your consent for any processing activities based on consent, you may do so through the Privacy Tools Portal or by contacting our Data Protection Officer using the details provided in the Contact Information Section below. To withdraw consent via the Portal, you will need to provide the email address you used when you originally provided consent. You will then receive an authentication code to verify your identity before completing the request.
- For your security and to ensure the proper processing of personal information, we may need to verify your identity before taking any action. If you do not provide enough information to confirm that you are the data subject, we may be unable to carry out your request.

International Transfer of Personal Data:

- We may transfer your personal data to other Reyes Holdings entities worldwide, consistent with our international operations, as well as to third party service providers based in other countries. These service providers include software and application providers (e.g., e-mail) and cloud storage providers. As a result, your personal data may be transferred to and processed in any locations where Reyes Holdings entities operate, including Australia, Brazil, Canada, Costa Rica, France, Ireland, New Zealand, Panama, Puerto Rico, Singapore, South Korea, the United Kingdom, and the United States. In practice, however, transfers typically occur only to the United States. Such transfers are performed via secure virtual access and will continue for as long as necessary to fulfill the purposes described in this Notice.

Contact Information:

You can find more information about the Brazilian privacy notice or talk to the Data Protection Officer, Thiago Logygensky Russo, by writing an email to protecaodedados@martinbrower.com.br.

Canada

Our main general privacy notice together with the information set out on this page constitutes our privacy notice for the purposes of our compliance with the data protection laws in Canada.

This page sets out the additional information, over and above the information set out in our main general privacy notice, that we are obliged to provide to you to comply with local data protection laws in Canada. It also sets out how our data protection practices differ in Canada compared to the practices described in our main general privacy notice.

The name and address of our Canada business:

1 City Centre Drive – 16th floor
Mississauga, Ontario, L5B 1M2

Contact:
Data Privacy Office
Email: Privacyofficer@mbcan.com

Differences/Additional Information

- Consent and Additional Purpose: The only legal bases we rely on when processing your personal information for the purposes of local data protection laws in Canada are: consent; or where the privacy laws in Canada set out circumstances under which we may collect, use or disclose your personal information without your consent (such as emergency circumstances or the investigation of a breach of an agreement or law). Other than in the limited circumstances expressly specified, we will not collect, use or disclose your personal information for the purposes set out in this privacy notice except with your consent.

- Cross-Border Collection and Transfer of Personal Information: We may use third parties, including service providers and affiliated companies, located outside Canada to collect, use, disclose or store some of your personal information for the purposes set out in section 3.1 of the main general privacy notice. These third parties may be located in the following countries: United States, United Kingdom and France

- Disclosure in the Context of a Business Transaction: Personal information may be disclosed or transferred to another party (including to another member of the Reyes Holdings group of companies) in the event that MB sells its business or undergoes another business transaction (such as leasing of company assets, direct financing operations, legal structure modification, reorganization, merger, joint venture, assignment, transfer, or other

disposition of any or all portion of MB business, assets or stock, including in connection with any bankruptcy or similar proceeding).

- Collection of Personal Information through Technological Means: We collect information through technological means, including:

    - CCTV Camera: MB collects surveillance footage for the purpose of building access controls.

    - Social Media Outlets: MB collects LinkedIn information for the purpose of service promotions.

    - Website Tracking Devices: MB collects technical and usage information for the purpose of tracking the use of our website, services and solutions.

  We collect this information from various vendors. We implement appropriate steps to help maintain the security of our information systems and processes and prevent accidental destruction, loss, or unauthorized disclosure of the personal information we process. Some of the safeguards we use are firewalls and data encryption, physical access controls to data centers, and information access authorization controls. CCTV recordings are typically automatically overwritten after a short period of time unless an issue is identified that requires investigation (such as a theft).

- Sensitive Personal Information: Subject to your consent if required by applicable law, we may use sensitive personal information for purposes of performing services for our business or providing goods or services as requested by you, ensuring security and integrity, short term transient use such as displaying first party, non- personalized advertising, payment/customer service, verifying customer information, and activities relating to quality and safety control or product improvement. We do not use sensitive personal information beyond these purposes.

  Canadian privacy laws define sensitive information as information which, due to its medical, biometric, or otherwise intimate nature or the context of its use or disclosure, entails a high level of reasonable expectation of privacy. We understand that MB does not generally collect sensitive information - but to the extent that they do, we wanted to ensure that same would be compliant with privacy laws.

Processing Requests: Access to personal data (or correction of personal data) will be provided, upon request of the data subject, within a period of 30 days of the data subject's request. If we refuse to provide access to or correct your personal information, we will give you a written notice within 30 days and outline the reasons for our refusal and avenues available for you to complain about our refusal.

Costa Rica

Our main general privacy notice together with the information set out on this page constitutes our privacy notice for the purposes of our compliance with the data protection laws in Costa Rica.

This page sets out the additional information, over and above the information set out in our main general privacy notice, that we are obliged to provide to you to comply with local data protection laws in Costa Rica. It also sets out how our data protection practices differ in Costa Rica compared to the practices described in our main general privacy notice.

The name and address of our Costa Rican business can be found here.

You can find more information about the Costa Rica privacy notice or talk to the Data Protection Officer, Thiago Logygensky Russo, by writing an email to protecciondedatoslatam@martinbrower.com.

Differences/Additional Information

- Your personal information will be stored and processed in a database that is our property.

- For Costa Rica: your ***informed, express, and prior consent*** is the primary legal basis. You are informed that providing data is voluntary, though refusal may prevent the provision of services. The only legal bases we rely on when processing your personal information for the purposes of local data protection laws in Costa Rica is ***informed, express, and prior*** *consent*. For other data processing: a substantiated order issued by a competent judicial authority or an agreement adopted by a special investigative commission of the Legislative Branch in the exercise of its duties; public personal information; or where the information must be delivered by constitutional or legal provision.

- When collecting your personal information, we will inform you whether it is mandatory or optional for you to provide the information requested. If you refuse to provide the personal information that is mandatory, penalties/consequences may apply. There are no consequences if you refuse to provide optional personal data, save that our ability to fully provide some of our services may be compromised.

- The supervisory authority in Costa Rica regarding data protection is PROHAB, where you may file a claim in the event that your rights have not been properly addressed by MARTIN BROWER Costa Rica.

France

Our main general privacy notice together with the information set out on this page constitutes our privacy notice for the purposes of our compliance with the data protection laws in France.

This page sets out the additional information, over and above the information set out in our main general privacy notice, that we are obliged to provide to you to comply with local data protection laws in France. It also sets out how our data protection practices differ in France compared to the practices described in our main general privacy notice.

The name and address of our French business can be found here.

Differences/Additional Information

- You may have the right to define guidelines related to the management of your data after your death (or alternatively postmortem guidelines). Such guidelines can be delivered directly to us or to a confidential third party that you have appointed.

- In addition to our general contact details for data protection queries set out in clause 4.1 of the main general privacy notice, if you have any specific questions relating to our use of your personal information and its protection under the data protection laws in France, please contact us at rgpd@martinbrower.com.

- If you are not satisfied with our response, please let us know so that we can work to address any concerns. Alternatively, a complaint can be submitted through the website of the Commission Nationale de l'Informatique et des Libertés (CNIL) (https://www.cnil.fr/en) in France. Additional details and information on submitting a complaint can be found on their website.

Ireland

Our main general privacy notice together with the information set out on this page constitutes our privacy notice for the purposes of our compliance with the data protection laws in Ireland.

This page sets out the additional information, over and above the information set out in our main general privacy notice, that we are obliged to provide to you to comply with local data protection laws in Ireland. It also sets out how our data protection practices differ in Ireland compared to the practices described in our main general privacy notice.

The name and address of our Irish business can be found here.

Differences/Additional Information

- In addition to our general contact details for data protection queries set out in clause 4.1 of the main general privacy notice, if you have any specific questions relating to our use of your personal information and its protection under the data protection laws in Ireland, please contact us at MB-IE-DPC@martinbrower.com.

- If you are not satisfied with our response, please let us know so that we can work to address any concerns. Alternatively, a complaint can be submitted through the Data Protection Commission website (www.dataprotection.ie) in Ireland. Additional details and information on submitting a complaint can be found on their website.

New Zealand

Our main general privacy notice together with the information set out on this page constitutes our privacy notice for the purposes of our compliance with the data protection laws in New Zealand.

This page sets out the additional information, over and above the information set out in our main general privacy notice, that we are obliged to provide to you to comply with local data protection laws in New Zealand. It also sets out how our data protection practices differ in New Zealand compared to the practices described in our main general privacy notice.

The name and address of our New Zealand business can be found here.

Differences/Additional Information

- Where, as described in clause 2.3 of the main general privacy notice, we share your personal information with a third party that is located overseas, please note that the recipient may not be subject to the New Zealand Information Privacy Principles.

- Under New Zealand data protection laws, your rights described in clause 4.1 of the main general privacy notice are restricted to only a right of access to, and a right to correct inaccuracies in, the personal information we hold about you.

Panama

Our main general privacy notice together with the information set out on this page constitutes our privacy notice for the purposes of our compliance with the data protection laws in Panama.

This page sets out the additional information, over and above the information set out in our main general privacy notice, that we are obliged to provide to you to comply with local data protection laws in Panama. It also sets out how our data protection practices differ in Panama compared to the practices described in our main general privacy notice.

The name and address of our Panamanian business can be found here.

You can find more information about the Panamá privacy notice or talk to the Data Protection Officer, Thiago Logygensky Russo, by writing an email to protecciondedatoslatam@martinbrower.com.

Differences/Additional Information

- The *only* legal bases we rely on when processing your personal information for the purposes of local data protection laws in Panama are consent; to comply with a legal obligation; or to fulfil our contractual relationship.

Law No. 81 on Personal Data Protection entered into effect, on 29 March 2021, following its enactment in 2019. Furthermore, the law provides for, among other things:

- consent procedures for the processing of personal data;
- obligations for the cross-border processing of personal data originating in Panama; and
- a Personal Data Protection Council with advising power and functions.

Puerto Rico

Puerto Rico was within the scope of the United States review related to data breach notification statutes.

When reviewing materials related to comprehensive consumer privacy laws (e.g., in the "Data For Which Consumers Have Heightened Notice Rights and Opt-in or Opt-out Rights With Respect to Some Kinds of Data Processing Under U.S. State Laws" table of the Sensitive Personal Information appendix), Puerto Rico was not referenced, as it has not yet passed a law of this kind.

Our main general privacy notice together with the information set out on this page constitutes our privacy notice for the purposes of our compliance with the data protection laws in Puerto Rico.

This page sets out the additional information, over and above the information set out in our main general privacy notice, that we are obliged to provide you to comply with local data protection laws in Puerto Rico. It also sets out how our data protection practices differ in Panama compared to the practices described in our main general privacy notice.

The name and address of our Puerto Rican business can be found here.

You can find more information about the Puerto Rico privacy notice or talk to the Data Protection Officer, Thiago Logygensky Russo, by writing an email to protecciondedatoslatam@martinbrower.com.

Singapore

Our main general privacy notice together with the information set out on this page constitutes our privacy notice for the purposes of our compliance with the data protection laws in Singapore.

This page sets out the additional information, over and above the information set out in our main general privacy notice, that we are obliged to provide to you to comply with local data protection laws in Singapore. It also sets out how our data protection practices differ in Singapore compared to the practices described in our main general privacy notice.

The name and address of our Singapore business can be found here.

Differences/Additional Information

- Our general contact details for data protection queries set out in clause 4.1 of the main general privacy notice, if you have any specific questions relating to our use of your personal data and its protection under the data protection laws in Singapore, please contact the Data Protection Officer by writing an email to dposea@martinbrower.com.

South Korea

Our main general privacy notice together with the information set out on this page constitutes our privacy notice for the purposes of our compliance with the data protection laws in South Korea.

This page sets out the additional information, over and above the information set out in our main general privacy notice, that we are obliged to provide to you to comply with local data protection laws in South Korea. It also sets out how our data protection practices differ in South Korea compared to the practices described in our main general privacy notice.

The name and address of our South Korean business can be found here.

Differences/Additional Information

- **Personal Information Processed and Legal Basis**
    - Personal information processed without consent

Purpose	Items of personal information	Legal bases
Operate, maintain and manage our business	Name, email address, IP address, accessed device's information	Personal Information Protection Act ("PIPA") Article 15(1)(iv) (conclusion and performance of contracts)
Accomplishing our business purposes	System menu usage history, IP address, connection time, device OS information.	PIPA Article 15(1)(iv) (conclusion and performance of contracts) PIPA Article 15(1)(vi) (legitimate interests)

- **Outsourcing of Personal Information**

Outsourced	Outsourced Tasks
LG Uplus	Sending SMS notifications related to orders
Smile EDI	CMS Payment

Billingone Plus	CMS Payment
Hyosung CMS	CMS Payment

- **Third-party Provision of Personal Information**
    - We do not provide personal information to any third-party provision.
- **Cross-Border Collection and Transfer of Personal Information**
    - We do not collect personal data from outside of Korea, nor do we transfer personal data outside of Korea.
- Our procedures and methods for the destruction of personal information are as follows:
    - **Destruction Procedure:** We identify personal information that meets the criteria for destruction and, upon approval from our Chief Privacy Officer, proceed to destroy the information.
    - **Destruction Method:** Personal information recorded or stored in electronic file format is destroyed in a manner that prevents reconstruction. Personal information recorded or stored on paper documents is destroyed by shredding or incineration.
- When our company collects unique identification information (excluding Resident Registration Numbers) and sensitive information under the PIPA, we will lawfully obtain consent or process the information based on legal grounds in accordance with the PIPA.
- Where we collect your personal information from a third party as described in clause 1.11 of the main general privacy notice, you can require us, on request, to: provide you with the source we collected this personal information from; provide you with the purpose for which we collected this information; and suspend the processing of this personal information.
- In respect of how long we keep your personal information that is subject to the data protection laws in South Korea, we intend to process and retain your personal information for no longer it is required to comply with the privacy legislations or legal obligations in the country.
- The processing and retention period of personal information in accordance with applicable laws and regulations are as follows.

- Records of transactions such as indications, advertisements, contract details and performance in accordance with the 「Act on Consumer Protection in Electronic Commerce, Etc.」

  - Records on display and advertisement: 6 months
  - Record of contract or subscription withdrawal, payment, supply of goods, etc.: 5 years
  - Records on consumer complaints or dispute resolution: 3 years

- Storage of communication confirmation data pursuant to Article 41 of the 「Enforcement Decree of Communication Secret Protection Act」

  - Computer communication, internet log record data, access point tracking data: 3 months

- We use "cookies" to store and retrieve usage information from time to time in order to provide users with personalized services and enhanced convenience. A cookie is a small piece of data sent from the server (HTTP) operating the website to the user's browser and stored on the user's computer or mobile device. When the user accesses the website, the information is automatically transmitted from the browser to the server. Users may configure their browser settings to allow or block cookies.

< How to Allow or Block Cookies >

▶ On Web Browsers

- Chrome: Click the "⋮" icon at the top right of the browser > Select New Incognito Window (Shortcut: Ctrl + Shift + N)
- Edge: Click the "…" icon at the top right of the browser > Select New InPrivate Window (Shortcut: Ctrl + Shift + N)

▶ On Mobile Browsers

- Chrome: Tap the "⋮" icon at the top right of the mobile browser > Select New Incognito Tab
- Safari: Go to Settings > Safari > Advanced > Block All Cookies
- Samsung Internet: Tap the Tabs icon at the bottom of the browser > Turn on Secret Mode > Start

- Under South Korean data protection laws, your rights described in clause 4.1 of the main general privacy notice are restricted to only a: right to have confirmed if your personal

information is being processed by us; right of access to the personal information we hold about you; right to update any inaccuracies in your personal information; right to require us to suspend the processing of your personal information; and right to require us to erase and destroy the personal information we hold about you.

- In addition to our general contact details for data protection queries set out in clause 4.1 of the main general privacy notice, if you have any specific questions relating to our use of your personal information and its protection under the data protection laws in South Korea, please contact the Chief Privacy Officer (Steve Chung, Managing Director) by writing an email to cposouthkorea@martinbrower.com.

United Kingdom

Our main general privacy notice together with the information set out on this page constitutes our privacy notice for the purposes of our compliance with the data protection laws in the United Kingdom.

This page sets out the additional information, over and above the information set out in our main general privacy notice, that we are obliged to provide to you to comply with local data protection laws in the United Kingdom. It also sets out how our data protection practices differ in the United Kingdom compared to the practices described in our main general privacy notice.

The name and address of our business in the United Kingdom can be found here.

Differences/Additional Information

- In addition to our general contact details for data protection queries set out in clause 4.1 of the main general privacy notice, if you have any specific questions relating to our use of your personal information and its protection under the data protection laws in the United Kingdom, please contact us at MB-UK-DPC@martinbrower.com.

- If you are not satisfied with our response, please let us know so that we can work to address any concerns. Alternatively, a complaint can be submitted through the Information Commissioner's Office's website (www.ico.org.uk) in the UK. Additional details and information on submitting a complaint can be found on their website.

United States

Our main general privacy notice together with this Notice at Collection set out on this page constitutes our privacy notice for the purposes of our compliance with the data protection laws in the United States.

Reyes Holdings, L.L.C. and its U.S. affiliates (collectively, "Reyes," "we" or "our") provide the following details regarding the categories of Personal Information that we collect, use, and disclose about California, Colorado, Connecticut, Delaware, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Rhode Island, Tennessee, Texas, Utah, Virginia residents, and residents of other states to the extent they have privacy laws applicable to us that grant their residents the right described below (collectively, the "State Privacy Laws"), who are consumers of our goods and services, visitors to our websites and online services or representatives of businesses that we interact with. This includes the following U.S. affiliates for Utah residents to the extent they are deemed a "controller": The Martin-Brower Company, L.L.C. and Reyes Fleet Management, L.L.C. We have a separate privacy notice that sets out how we process the personal information of our staff, which prospective, current, and former members of staff should refer to. This also includes the residents of Oregon, with any assumed business name that Reyes uses in Oregon, in addition to the business name Reyes used to register with the Oregon Secretary of State.

For purposes of this section, the term "Personal Information" means information that relates to an identified or identifiable natural person, or that is reasonably capable of being used to identify, contact, or precisely locate a natural person, household, or a particular computing system or device.

Collection and Disclosure of Personal Information

The following chart details which categories of Personal Information we collect and process, as well as which categories of Personal Information we disclose to third parties for our operational business purposes, including within the 12 months preceding the date this Privacy Policy was last updated.

We disclose Personal Information to the following categories of third parties:

1. "Service Providers." We disclose Personal Information to our trusted third-party service providers, to facilitate services they provide to us, such as internet services, call centers, website hosting, data analytics, payment processing, order fulfillment, information technology and related infrastructure provision, customer service, email delivery, marketing, auditing, background checks, and other services. They use Personal Information to provide their service to us consistent with our instructions. In some cases, they de-identify Personal Information and use the de-identified information for their own purposes such as to improve their products and services.

2. "Legal Authorities." We disclose Personal Information to public and government authorities, including regulators and law enforcement, to respond to requests, as well as to protect and defend legal rights. They use Personal Information, for example, to investigate unlawful activities, enforce laws, and adjudicate disputes.

3. "Other Parties in Litigation" We disclose Personal Information in the context of litigation discovery and in response to subpoenas and court orders. They use Personal Information to assert and defend their legal rights.

4. "Our Affiliates" We disclose Personal Information to our parent company, subsidiaries and other corporate affiliates. They use Personal Information to conduct their business in accordance with this Privacy Policy.

Categories of Personal Information	**Disclosed to Which Categories of Third Parties for Operational Business Purposes**
Identifiers, such as name, contact information, unique personal identifiers, IP addresses that can reasonably be linked or associated with a particular consumer or household, online identifiers, and government-issued identifiers	Service Providers, Legal Authorities Parties in Litigation, Our Affiliates[2]
Personal information as defined in the California customer records law, such as name, contact information, signature; financial account information; medical, insurance, financial information	Service Providers, Legal Authorities Parties in Litigation, Our Affiliates
Commercial Information, such as transaction information	Service Providers, Legal Authorities Parties in Litigation, Our Affiliates
Geolocation Data, such as device location and location derived from IP address	Service Providers, Legal Authorities Parties in Litigation, Our Affiliates
Audio/Video Data. Audio, electronic, visual and similar information, such as call and video recordings created in connection with our business activities	Service Providers, Legal Authorities Parties in Litigation, Our Affiliates
Education Information subject to the federal Family Educational Rights and Privacy Act such as student transcripts,	Service Providers, Legal Authorities Parties in Litigation, Our Affiliates

grade point average, grades, and disciplinary records	
Employment Information. Professional or employment-related information, such as work history and prior employer	Service Providers, Legal Authorities Parties in Litigation, Our Affiliates
Sensitive Personal Information. • Personal Information that reveals an individual's social security, driver's license, state identification card, or passport number; 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; contents of a communication to which you were not a party; precise geolocation; racial, national, or ethnic origin, religious or • Also includes sensitive personal information such as: philosophical beliefs, citizenship, immigration status, or union membership; the contents of mail, email, and text messages unless Reyes is the intended recipient of the communication; genetic, biometric, neural or biological data; • Personal Information collected and analyzed concerning an individual's health, mental or physical condition or diagnosis or disability condition or diagnosis, history, treatment or other health data; pregnancy; sex life, sexuality or sexual orientation; status as transgender or non-binary; status as a victim of crime.	Service Providers, Legal Authorities Parties in Litigation, Our Affiliates

We may also disclose your Personal Information to a third party in the context of any reorganization, financing transaction, merger, sale, joint venture, partnership, assignment, transfer, or other disposition of all or any portion of our business, assets, or stock (including in connection with any bankruptcy or similar proceedings).

Under the State Privacy Laws, if a business sells or shares Personal Information for purposes of cross-context behavioral advertising or processes Personal Information for purposes of targeted advertising, it must allow residents protected by those laws to opt out of such activities pursuant to applicable law. However, we do not sell or share or otherwise process Personal Information, including Sensitive Personal Information, for purposes of cross-context behavioral or targeted advertising, as defined under applicable law. We have not engaged in such activities in the 12 months preceding the date this Privacy Policy was last updated.

We do not sell or knowingly use for cross-context behavioral advertising or targeted advertising the personal Information of minors under 18 years of age.

Under the CCPA, if a business uses or discloses Sensitive Personal Information beyond certain purposes, it must allow California residents to opt out of such uses or disclosures. However, we do not use or disclose Sensitive Personal Information beyond such purposes, nor have we used or disclosed Sensitive Personal Information beyond such purposes in the last 12 months. You can opt-out of our processing your Sensitive Personal Information by electing not to provide it to us.

Purposes of Collection, Use and Disclosure of Personal Information

We may collect, use and disclose each category of Personal Information to operate, manage, and maintain our business; provide, develop, improve, repair, and maintain our products and services; enter into, track and perform agreements with customers and suppliers; personalize, advertise, and market our products and services; provide customer support and respond to requests for information; manage customer and supplier relationships; conduct research, analytics, and data analysis; operate, maintain and improve our website and other online services or applications; operate and maintain our facilities and infrastructure; undertake quality and safety assurance measures; conduct risk and security control and monitoring; detect and prevent fraud; perform identity verification; perform accounting, audit, and other internal functions, such as internal investigations; facilitate and implement any reorganization, financing transaction, merger, sale, joint venture, partnership, assignment, transfer, or other disposition of all or any portion of our business, assets or stock (including in connection with any bankruptcy or similar proceedings); comply with law (including anti-money laundering laws), legal process, and internal policies; maintain records; and exercise and defend legal claims. We disclose Personal Information to our service providers and processors so that they can use it on our behalf to provide services to us.

Use of Sensitive Personal Information

Subject to your consent if required by applicable law, we may use Sensitive Personal Information for purposes of performing services for our business or providing goods or services as requested by you, ensuring security and integrity, short term transient use such as displaying first party, non-personalized advertising, payment/customer service, verifying customer information, and activities relating to quality and safety control or product improvement. We do not use Sensitive Personal Information beyond these purposes, or to infer characteristics about individuals.

Retention Period

We retain each category of Personal Information for as long as needed or permitted considering the purpose(s) for which it was collected. The criteria used to determine our retention periods include:

- The length of time we have an ongoing relationship with you and provide services to you (for example, for as long as you have a relationship with us or keep using our services) and the length of time thereafter during which we may have a legitimate need to reference your Personal Information to address issues that may arise;

- Whether there is a legal obligation to which we are subject (for example, certain laws require us to keep records of your transactions for a certain period of time before we can delete them); or

- Whether retention is advisable in light of our legal position (such as in regard to applicable statutes of limitations, litigation or regulatory investigations).

Sources of Personal Information

We collect this Personal Information from you, your employer or the organization that you represent, work for or own, and from the companies that we distribute products for, our affiliates, service providers, data analytics providers, data brokers, credit reference agencies, government agencies and publicly available databases or sources of information (e.g., anti-fraud databases, sanctions lists, court judgements and other databases), joint marketing partners, social media outlets, including in the context of promotions that we operate and by using website tracking devices or collecting information through your use of our websites, services, and solutions.

De-identified data

Where we maintain or use de-identified data, we will continue to maintain and use the de-identified data only in a de-identified fashion and will not attempt to re-identify the data.

Individual Rights and Requests

You may request to exercise the rights listed below. We will respond to your request in accordance with applicable law. We may decline to honor your request where an exception applies.

1. The right to know whether we process or have processed your Personal Information, and the right to access such Personal Information.

2. You may request that we disclose to you the following information covering the 12 months preceding your request and how we will continue to do so:

    i. The categories of Personal Information we collected about you and the categories of sources from which we collected such Personal Information;

    ii. The business or commercial purpose for collecting Personal Information about you;

    iii. The categories of Personal Information about you that we disclose for business purposes, and the categories of third parties to whom we disclosed such Personal Information; and

    iv. The specific third parties to whom we have disclosed Personal Information.

3. The right to correct inaccuracies in your Personal Information;

4. The right to delete Personal Information we have collected from or about you or information derived from Personal Information;

5. The right to receive a copy or representative summary of your Personal Information (or, just your Personal Information that you provided to us directly), including specific pieces of Personal Information, including, where applicable, the right to obtain a copy of such Personal Information in a portable, readily usable format;

6. You can opt-out of our processing your Sensitive Personal Information by electing not to provide it to us or by notifying us of your opt-out;

7. The right to revoke consents that you previously provided such as any consent that you have provided for us to process your sensitive personal information;

8. The right to exercise any of the rights described above free from discrimination as prohibited by applicable state privacy laws;

9. The right to appeal our denial of any request validly submitted.

To make a request to know, access, correct, delete, or receive a copy of your Personal Information, please contact us at privacy@reyesholdings.com or 888-295-6392. We will verify and respond to your request consistently with applicable law, taking into account the type and sensitivity of the Personal Information subject to the request. In some instances, we may decline to honor your request where the law or your right does not apply or where an exception applies. We may need to verify your identity in order to action your request we will do this by using existing consumer identity data for example, by requesting you to provide a driver's license or a current utility bill in

order to verify your identity and protect against fraudulent requests. If you make a request to delete, we may ask you to confirm your request before we delete your Personal Information.

Appeal Process

If we refuse to take action on your request, you may appeal this refusal within a reasonable period after you have received notice of the refusal. You may file an appeal by contacting us via privacy@reyesholdings.com or 888-295- 6392.

Authorized Agents

If you want to make a request as an authorized agent of a consumer as permitted under applicable law, you may use the submission methods noted above. Under the law, not all kinds of requests can be made by authorized agents in all states. As part of our verification process, we may request that you provide, as applicable, proof concerning your status as an authorized agent. If you are making a request on behalf of a California resident, this may include:

1. A power of attorney from the California resident pursuant to California Probate Code sections 4121-4130; or

2. If you have not provided #1:

    a. We may require an authorized agent to provide proof that the resident has provided signed permission authorizing you to make a request on the resident's behalf. "Signed" means that the permission has either been physically signed or provided electronically in accordance with the Uniform Electronic Transactions Act, Civil Code 1633.7 et seq.

    b. We may require the resident to:

        i. Verify the resident's own identity directly with us

        ii. Directly confirm with us that the resident provided you permission to submit the request.

Additional Information

Consumers under 18. We do not have actual knowledge that we have collected, sold, or shared the personal information of residents who are under 18 years of age.

Additional information for California residents. California's "Shine the Light" law, Civil Code section 1798.83, requires certain businesses to respond to requests from California customers asking about the businesses' practices related to disclosing personal information to third parties for the third parties' direct marketing purposes. Alternately, such businesses may have in place a policy not to disclose personal information of customers to third parties for the third parties' direct

marketing purposes if the customer has exercised an option to opt-out of such information sharing. If you wish to opt-out of our sharing of your information with third parties for the third parties' direct marketing purposes, contact us at privacy@reyesholdings.com (please include your name, mailing address and email address).

Additional information for Connecticut residents. We may disclose any personal data that we collect, use, or sell for the purpose of training large language models ("LLMs").

Additional information for Nevada residents. If you are a Nevada "consumer" as the term is defined under Nevada's Revised Statute Chapter 603A ("Nevada Privacy Law"): Reyes has established privacy@reyesholdings.com as the designated request address for the submission of verified requests not to "sell" covered information, for purposes of the Nevada Privacy Law. Reyes does not "sell" and does not anticipate that it will "sell", the covered information of Nevada consumers as defined under the Nevada Privacy Law. Should Reyes ever begin to "sell" your covered information, you may submit a verified request not to sell to privacy@reyesholdings.com.

Contact Us

If you have any questions regarding this Privacy Policy, please contact us privacy@reyesholdings.com.